ANEXO I

TERMO DE REFERÊNCIA

1. **OBJETO: Contratação de empresa especializada na prestação de Serviços Gerenciados de Tecnologia da Informação incluindo Serviços Gerenciados de Segurança da Informação, Serviços Gerenciados de Backup, Suporte Técnico Avançado e Monitoramento devidamente descritos e caracterizados nas especificações técnicas de cada item presente no Termo de Referência.**

2. **LOCAL DE EXECUÇÃO DOS SERVIÇOS E DA CLASSIFICAÇÃO DOS SERVIÇOS:**

2.1. Os serviços serão executados na Câmara Municipal de Osasco, sito a Av. dos Autonomistas, 2607 – Centro, Osasco – SP, CEP: 06090-905

2.2. A natureza do objeto a ser contratado é comum nos termos do parágrafo único, do art. 1°, da Lei 10.520, de 2002.

3. **JUSTIFICATIVA:**

3.1. O Departamento de Tecnologia da Informação da CMO está estudando a contratação de serviços e mão-de-obra especializada para garantir o planejamento, implementação, verificação e melhoria dos processos relacionados à Tecnologia da Informação e Segurança da Informação em função da legislação e normas vigentes com especial atenção a:

- LEI Nº 12.965, DE 23 DE ABRIL DE 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);
- LEI Nº 13.853, DE 8 DE JULHO DE 2019: Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.
- ABNT NBR ISO/IEC 27002:2013: Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
- ABNT NBR ISO/IEC 20000: especifica requisitos para o provedor de serviço planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gerenciamento de Serviços (SGS)

4. **ESPECIFICAÇÃO TÉCNICA**

4.1. No quadro a seguir temos os itens do lote de produtos e serviços que devem ser atendidos pelo edital:

SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

ITEM	DESCRIÇÃO	QTD
1	Serviços Gerenciados de Segurança da Informação	1
2	Serviços Gerenciados de Backup	1
3	Serviços de Suporte Técnico e Monitoramento	1

5. DESCRIÇÃO DA PRESTAÇÃO DE SERVIÇOS DOS ITENS DO EDITAL

5.1. ITEM 01: SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO:

5.1.1. **Firewall de Próxima Geração NGFW (Next Generation Firewall)**

5.1.1.1. A contratada deverá fornecer uma solução de firewall de próxima geração (NGFW – Next Generation Firewall) em alta disponibilidade com no mínimo dois equipamentos físicos idênticos;

5.1.2.1. A alta disponibilidade deve ser configurada no modo ativo-passivo, tendo no mínimo um hardware (secundário) disponível para assumir a operação, caso ocorra falha no equipamento (primário) que esteja operando;

5.1.2.2. A contratada deverá instalar e configurar os itens físicos e lógicos seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;

5.1.2.3. Prestar todos esclarecimentos a todas solicitações feitas pela contratante, referente as configurações e serviços prestados;

5.1.2.4. Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos fornecidos como serviço e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam de responsabilidade do contratante;

5.1.2.5. Os equipamentos devem estar com firmware e/ou software na versão mais recente e estável recomentada pelo fabricante da solução e com todas as licenças e funcionalidades habilitadas;

5.1.2.6. A contrata 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 evolutivo. O documento deve ser entregue para contratante, analisado e aceito pelo responsável técnico da contratante;

5.1.2.7. Ao concluir o plano de implementação, deverá ser entregue toda documentação da implementação, topologia do ambiente, arquivos de configurações;

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

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.2.9. Os equipamentos devem suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:

5.1.3.Especificações Gerais

5.1.3.1. O equipamento proposto deve fornecer logs e relatórios embarcados contendo no mínimo os itens abaixo:

5.1.3.2. Dashboard com informações do sistema:

5.1.3.3. Informações de CPU

5.1.3.4. Informações do uso da rede.

5.1.3.5. Informações de memória.

5.1.3.6. Informações de atividades de navegação.

5.1.3.7. Permitir visualizar número políticas ativas.

5.1.3.8. Visualizar número de usuários conectados remotamente.

5.1.3.9. Visualizar número de usuários conectados localmente.

5.1.3.10. Relatórios com informações sobre as conexões de origem e destino por países.

5.1.3.11. Relatórios informando as conexões dos hosts.

5.1.3.12. Visualizar relatórios por período de tempo, permitindo o agendamento e o envio destes relatórios por e-mail.

5.1.3.13. Permitir exportar relatórios para as seguintes extensões/plataformas:

5.1.3.14. PDF

5.1.3.15. HTML

5.1.3.16. Excel

5.1.3.17. Permitir visualizar relatório de políticas ativas associado ao ID da política criada.

5.1.3.18. Relatório que informe o uso IPSEC por host e usuário.

5.1.3.19. Relatório que informe o uso L2TP por host e usuário.

5.1.3.20. Relatório que informe o uso PPTP por usuários.

5.1.3.21. Relatório abordando eventos de VPN.

5.1.3.22. Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:

5.1.3.23. Logs do sistema;

5.1.3.24. Logs das políticas de segurança;

5.1.3.25. Logs de autenticação;

5.1.3.26. Logs de administração do firewall NGFW.

5.1.3.27. Permitir ocultar dos relatórios usuários e IPs cadastrados.

5.1.3.28. Possuir no mínimo 6 interfaces 10/100/1000 base-T;

5.1.3.29. Possuir no mínimo 2 interfaces SFP 1GbE base-SR;

5.1.3.30. Deve suportar adição futura de no mínimo 2 interfaces 40GbE QSFP+;

5.1.3.31. Deve possuir no mínimo 2 portas que suportem by-pass;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.3.32. A contratada deverá fornecer todos os cabos e seus acessórios necessários para atender os itens deste documento.

5.1.3.33. A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte:

5.1.3.34. Suportar no mínimo 140.000 (cento e quarenta mil) novas conexões por segundo;

5.1.3.35. Suportar no mínimo 8.000.000 (oito milhões) conexões simultâneas;

5.1.3.36. Possuir no mínimo 20 (vinte) Gbps de rendimento (throughput) do Firewall para pacotes UDP;

5.1.3.37. No mínimo 4 (quatro) Gbps de rendimento (throughput) do IPS;

5.1.3.38. Possuir no mínimo 1.7 (um inteiro e sete décimos) Gbps de throughput de VPN AES.

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

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

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

5.1.3.42. Possuir slot para adição de módulo de portas;

5.1.3.43. Possuir ao menos uma porta console RJ45 ou similar;

5.1.3.44. Número irrestrito de usuários/IP conectados.

5.1.3.45. O equipamento deve ter no máximo 2 (dois) U de altura para montagem em rack 19”.

5.1.3.46. Especificações da Administração, Autenticação e Configurações em geral

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

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

5.1.3.49. 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.

5.1.3.50. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.

5.1.3.51. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.

5.1.3.52. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.3.53. Suporte à autenticação do Chromebook.

5.1.3.54. Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.

5.1.3.55. Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.

5.1.3.56. Certificados de autenticação para iOS e Android.

5.1.3.57. 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.

5.1.3.58. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.

5.1.3.59. A solução proposta deve suportar NTP.

5.1.3.60. 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.

5.1.3.61. A solução proposta deve ter suporte multilíngue para console de administração web.

5.1.3.62. A solução proposta deverá suportar fazer um rollback de versão.

5.1.3.63. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.

5.1.3.64. A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.

5.1.3.65. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.

5.1.3.66. A solução proposta deve suportar SNMP v1, v2c.

5.1.3.67. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.

5.1.3.68. 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.

5.1.3.69. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.

5.1.3.70. 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)

5.1.3.71. A solução proposta deve ter suporte a ambientes de terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.

5.1.3.72. A solução proposta deve suportar:

5.1.3.73. Serviço de DHCP/DHCPv6;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.3.74. Serviço de DHCP/DHCPv6 Relay Agent;

5.1.3.75. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.

5.1.3.76. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.

5.1.3.77. Permitir exportar informações de troubleshooting para arquivo PCAP.

5.1.3.78. Permitir o factory reset e troca do idioma via interface gráfica.

5.1.3.79. Reutilização de definições de objetos de rede, hosts, serviços, período de tempo, usuários, grupos, clientes e servers.

5.1.3.80. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades especificas a ele.

5.1.3.81. Controle de acesso e dispositivos por zoneamento.

5.1.3.82. Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.

5.1.3.83. Traps SNMP ou e-mail para notificações do sistema.

5.1.3.84. Suportar envio de informações via Netflow e possuir informações via SNMP;

5.1.3.85. Ter funcionalidade que permita que o administrador manualmente atribua núcleos (“cores”) do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.

5.1.3.86. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

5.1.4.Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet

5.1.4.1. A solução proposta deve suportar o balanceamento de carga e redundância para no mínimo 2 (dois) links de Internet.

5.1.4.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.

5.1.4.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.

5.1.4.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.

5.1.4.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

5.1.4.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).

5.1.4.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

5.1.5.Especificações de Alta Disponibilidade

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.5.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo.

5.1.5.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.

5.1.5.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.

5.1.5.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

5.1.5.5. A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".

5.1.5.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

5.1.5.7. Proteção básica de firewall

5.1.6.Especificações do Firewall e roteamento

5.1.6.1. A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.

5.1.6.2. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-to-one", NAT Dinâmico e PAT.

5.1.6.3. 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.

5.1.6.4. 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.

5.1.6.5. A solução proposta deve suportar arquitetura de segurança baseado em Zonas.

5.1.6.6. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".

5.1.6.7. 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.

5.1.6.8. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).

5.1.6.9. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.

5.1.6.10. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.6.11. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.

5.1.6.12. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.

5.1.6.13. A solução proposta deve suportar IPv6.

5.1.6.14. A solução proposta deve suportar implementações de IPv6 Dual Stack.

5.1.6.15. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.

5.1.6.16. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.

5.1.6.17. A solução proposta deve suportar DNSv6.

5.1.6.18. A solução proposta deve oferecer proteção DoS contra ataques IPv6.

5.1.6.19. A solução proposta deve oferecer prevenção contra Spoof em IPv6.

5.1.6.20. A solução proposta deve suportar 802.3ad para Link Aggregation.

5.1.6.21. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.

5.1.6.22. 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.

5.1.6.23. Flood protection, DoS, DDoS e Portscan.

5.1.6.24. Bloqueio de Países baseados em GeoIP.

5.1.6.25. Suporte a Upstream proxy.

5.1.6.26. Suporte a VLAN DHCP e tagging.

5.1.6.27. Suporte a Multiple bridge.

5.1.6.28. Funcionalidades do portal do usuário

5.1.6.29. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).

5.1.6.30. Download dos clientes de autenticação disponibilizados pela ferramenta.

5.1.6.31. Download do cliente VPN SSL em plataformas Windows.

5.1.6.32. Download das configurações SSL em outras plataformas.

5.1.6.33. Informações de hotspot.

5.1.6.34. Autonomia de troca de senha do usuário.

5.1.6.35. Visualização do uso de internet do usuário conectado.

5.1.6.36. Acesso a mensagens em quarentena.

5.1.6.37. Opções base de VPN

5.1.6.38. Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.6.39. L2TP e PPTP.

5.1.6.40. VPN SSL, IPSEC.

5.1.6.41. 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.

5.1.7.Funcionalidades base de QoS e Quotas

5.1.7.1. QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.

5.1.7.2. Otimização em tempo real do protocolo Voip.

5.1.7.3. Suporte a marcação DSCP.

5.1.7.4. Regras associadas por usuário.

5.1.7.5. Criar regras que limitem e garantam upload e download.

5.1.7.6. Permitir criar regra de QoS individualmente e compartilhada.

5.1.7.7. Filtragem e Segurança Web

5.1.7.8. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.

5.1.7.9. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92 categorias oferecidas pela solução.

5.1.7.10. Realizar autenticação dos usuários nos modos transparente e padrão.

5.1.7.11. As autenticações devem ser feitas via NTLM.

5.1.7.12. Possuir sistema de quotas aplicado por usuários e grupos.

5.1.7.13. Permitir criar políticas por horário aplicado a usuários e grupos.

5.1.7.14. Possuir sistema de malware scanning que realize as seguintes ações:

5.1.7.15. Bloquear toda forma de vírus

5.1.7.16. Bloquear malwares web

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

5.1.7.18. Prover proteção em tempo real de todos os acessos web.

5.1.7.19. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.

5.1.7.20. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.

5.1.7.21. Fornecer Pharming Protection.

5.1.7.22. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.7.23. Permitir criação de regras customizadas baseadas em usuário e hosts.

5.1.7.24. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.

5.1.7.25. Validação de certificado.

5.1.7.26. Prover cache de navegação, contribuindo na agilidade dos acessos à internet.

5.1.7.27. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)

5.1.7.28. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.

5.1.7.29. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.

5.1.7.30. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.

5.1.7.31. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.

5.1.7.32. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.

5.1.7.33. Range aceitável de 1 a 25600KB.

5.1.7.34. Bloquear trafego que não segue os padrões do protocolo HTTP.

5.1.7.35. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.

5.1.7.36. Nas exceções, permitir definir operadores “AND” e “OR”.

5.1.7.37. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.

5.1.7.38. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.

5.1.7.39. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.

5.1.7.40. Permitir criar regras de exceções por endereços IPs de origem.

5.1.7.41. Permitir criar regras de exceções por endereços IPs de destino

5.1.7.42. Permitir criar exceções por grupo de usuários.

5.1.7.43. Permitir criar exceções por categorias de sites.

5.1.7.44. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.

5.1.7.45. 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.

5.1.7.46. Permitir editar grupos de categorias pré-estabelecidos pela solução.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.7.47. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

5.1.7.48. Nome da regra;

5.1.7.49. Permitir criar uma descrição para identificação da regra.

5.1.7.50. Ter a possibilidade de classificação de pelo menos:

5.1.7.51. Produtivo;

5.1.7.52. Não produtivo;

5.1.7.53. Permitir aplicar Traffic shaping diretamente na categoria.

5.1.7.54. Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.

5.1.7.55. 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.

5.1.7.56. 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.

5.1.7.57. Ter função para criar grupos de URLs.

5.1.7.58. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.

5.1.7.59. Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.

5.1.7.60. Deve permitir que em uma mesma política seja aplicada ações diferentes de acordo com o usuário autenticado.

5.1.7.61. 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.

5.1.7.62. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.

5.1.7.63. Permitir criar cotas de navegação com os seguintes requisitos:

5.1.7.64. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

5.1.8.Controle e Segurança de Aplicações

5.1.8.1. Prover controle para mais de 2600 aplicações diferentes.

5.1.8.2. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.

5.1.8.3. Permitir criar regras de controle por usuário e hosts.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.8.4. Permitir realizar traffic shaping por aplicação e grupo de aplicações.

5.1.8.5. Possibilitar que as regras criadas baseadas em aplicação permitam:

5.1.8.6. Bloquear o tráfego para as aplicações

5.1.8.7. Liberar o tráfego para as aplicações

5.1.8.8. Criar categorização das aplicações por risco:

5.1.8.9. Risco muito baixo

5.1.8.10. Risco baixo

5.1.8.11. Risco médio

5.1.8.12. Risco alto

5.1.8.13. Risco muito alto

5.1.8.14. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.

5.1.8.15. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.

5.1.8.16. 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.

5.1.8.17. Permitir agendar um horário e data específico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

5.1.9.Proteção de Redes

5.1.9.1. Prover funcionalidade de Intrusion Prevention System (IPS)

5.1.9.2. Proporcionar alta performance na inspeção dos pacotes

5.1.9.3. Possuir mais de 6500 assinaturas conhecidas.

5.1.9.4. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.

5.1.9.5. 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.

5.1.9.6. Possuir funcionalidade Anti-DoS.

5.1.9.7. Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:

5.1.9.8. SYN Flood

5.1.9.9. UDP Flood

5.1.9.10. TCP Flood

5.1.9.11. ICMP Flood

5.1.9.12. IP Flood

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.9.13. 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.

5.1.9.14. Possuir proteção contra spoofing.

5.1.9.15. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.

5.1.9.16. Possuir funcionalidade para o administrador poder criar by-pass de DoS.

5.1.9.17. Permitir o administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

5.1.9.18. Possuir proteção avançada contra ameaças persistentes (APT)

5.1.9.19. Detectar e bloquear tráfico 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.

5.1.9.20. Possuir logs e relatórios que informem todos eventos de APT.

5.1.9.21. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.

5.1.9.22. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.

5.1.9.23. Proteção para E-mails

5.1.9.24. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.

5.1.9.25. 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.

5.1.9.26. Bloquear SPAN e MALWARES durante a transação SMTP.

5.1.9.27. Possuir duas engines de antivírus para duplo escaneamento.

5.1.9.28. Ter proteção em tempo real, 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.

5.1.9.29. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.

5.1.9.30. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.

5.1.9.31. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customiza-los de acordo com o desejado.

5.1.9.32. Ter suporte a criptografia TLS para SMTP, POP e IMAP.

5.1.9.33. As ações dos e-mails considerados SPAN devem ser:

5.1.9.34. Drop

5.1.9.35. Warn

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.9.36. Quarantine

5.1.9.37. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: [SPAN] Marketing etc. etc. etc.

5.1.9.38. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.

5.1.9.39. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.

5.1.9.40. Possuir funcionalidade de allowlist e blocklist.

5.1.9.41. Possuir funcionalidade que rejeite e-mails com HELO invalido e/ou que não possuam RDNS.

5.1.9.42. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.

5.1.9.43. Quarentena de E-mail

5.1.9.44. Possuir quarentena para os e-mails e opções de notificações para o administrador.

5.1.9.45. E-mails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.

5.1.9.46. O usuário deve poder gerenciar sua quarentena de e-mails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.

5.1.9.47. As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.

5.1.9.48. Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.

5.1.9.49. Possuir funcionalidade de criptografia de e-mails e DLP para os dados

5.1.9.50. Possuir funcionalidade de encriptação de e-mails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.

5.1.9.51. Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF.

5.1.9.52. Ter como funcionalidade a possibilidade de o usuário poder registrar sua própria senha de segurança para que seja possível abrir os e-mails criptografados.

5.1.9.53. Possuir também funcionalidade para geração de senhas aleatórias para descriptografar o conteúdo.

5.1.9.54. Permitir enviar anexos junto aos e-mails criptografados.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.9.55. Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não se deve utilizar qualquer software adicional, plugin, ou client instalado no equipamento.

5.1.9.56. Possuir funcionalidade de DLP nos E-mails

5.1.9.57. A engine de DLP deve ser automática na hora de escanear os e-mails e anexos, assim identificando todos os dados sensíveis encontrados no e-mail sem qualquer intervenção.

5.1.9.58. Ter a opção de criar exceções individuais para cada tipo de situação.

5.1.9.59. As regras devem corresponder para as redes de origem e alvos específicos como a especificados por URLs.

5.1.9.60. Suporte a operadores lógicos

5.1.9.61. Poder definir tamanho máximo para escaneamento.

5.1.9.62. Permitir bloquear e liberar ranges IP.

5.1.9.63. Suporte para utilização de Wildcards

5.1.9.64. Anexar automaticamente um prefixo/sufixo para autenticação.

5.1.9.65. Proteção para proteção de servidores WEB (WAF)

5.1.9.66. Possuir funcionalidade de proxy reverso

5.1.9.67. Possuir engine de URL hardening e prevenção a directory traversal.

5.1.9.68. Possuir engine Form hardening.

5.1.9.69. Proteção contra SQL injection

5.1.9.70. Proteção contra Cross-site scripting

5.1.9.71. Possuir duas engines de antivírus disponíveis para análise de malware.

5.1.9.72. Permitir definir o fluxo que o antivírus irá atuar, se será no upload ou download.

5.1.9.73. Permitir limitar o tamanho máximo em que o antivírus irá atuar.

5.1.9.74. Permitir bloquear conteúdo considerado unscannable.

5.1.9.75. Possuir HTTPS (SSL) encryption offloading.

5.1.9.76. Proteção para cookie signing com assinaturas digitais.

5.1.9.77. Possuir Path-based routing.

5.1.9.78. Suporte ao protocolo do Outlook anywhere.

5.1.9.79. Possuir autenticação reversa para acesso aos servidores web.

5.1.9.80. Permitir criar templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.

5.1.9.81. Ter abstração de servidores virtuais e físicos.

5.1.9.82. Proporcionar função de load balance para que os visitantes possam ser jogados para diversos servidores de forma transparente.

5.1.9.83. Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.9.84. Bloquear clients com má reputação.

5.1.9.85. Bloquear protocolos com anomalias.

5.1.9.86. Limitar número de requisições.

5.1.9.87. Proteção de Sandbox na nuvem

5.1.9.88. Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.

5.1.9.89. Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.

5.1.9.90. Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll

5.1.9.91. Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.

5.1.9.92. Realizar analise em documentos PDF.

5.1.9.93. Realizar analise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet

5.1.9.94. Suporte a mais de 20 tipos de arquivos e extensões.

5.1.9.95. Realizar analises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.

5.1.9.96. Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.

5.1.9.97. O tempo em média das análises devem ser menores do que 120 segundos.

5.1.9.98. Suportar a análise de links de download em tempo real.

5.1.9.99. Permitir escolher pelo menos duas regiões para as quais os arquivos para analise devem ser enviados.

5.1.9.100. Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para analisa.

5.1.9.101. Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.

5.1.9.102. O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.

5.1.10. Solução de gerenciamento

5.1.10.1. A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela contratante.

5.1.10.2. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplica-los todos de uma única vez.

5.1.10.3. As políticas de configurações devem ter no mínimo as seguintes opções:

5.1.10.4. Proteção e políticas de acesso web

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.10.5. Controle de aplicativos

5.1.10.6. IPS

5.1.10.7. VPN

5.1.10.8. E-mail

5.1.10.9. Firewall

5.1.10.10. 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.

5.1.10.11. Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.

5.1.10.12. Possuir múltiplas formas de customização de warning thresholds.

5.1.10.13. Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferenciá-los como por exemplo: Região, modelo ou outro parâmetro.

5.1.10.14. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos com diferentes funções.

5.1.10.15. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

5.1.10.16. Deve ser possível integrar tanto com firewall NGFWs físicos quanto virtuais.

5.1.10.17. Possuir funcionalidade que permita o centralizador de gerência, também gerenciar os updates de firmware de ambos os firewalls NGFWs.

5.1.11. <u>Solução de Proteção para Servidores e Estações de Trabalho</u>

5.1.11.1. A solução deve ser licenciada para todo o parque de TIC da câmara, ou seja, para 300 dispositivos, servidores e estações de trabalho.

5.1.12. <u>Console</u> de Gerenciamento

5.1.12.1. O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor;

5.1.12.2. O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS);

5.1.12.3. O acesso ao Console deve suportar várias sessões simultâneas;

5.1.12.4. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

5.1.12.5. Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.12.6. Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

5.1.12.7. O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases:

5.1.12.8. Microsoft Windows 8 / 8.1 Pro

5.1.12.9. Microsoft Windows 10

5.1.12.10. Microsoft Windows 2012 R2 Server;

5.1.12.11. Microsoft Windows 2016 Server;

5.1.12.12. O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE;

5.1.12.13. Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

5.1.12.14. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

5.1.12.15. Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo;

5.1.12.16. Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso);

5.1.12.17. Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

5.1.12.18. Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento;

5.1.12.19. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;

5.1.12.20. A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente;

5.1.12.21. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador);

5.1.12.22. O log deve ser centralizado e conter, no mínimo, os seguintes itens:

5.1.12.23. Nome da ameaça

5.1.12.24. Nome do arquivo infectado

5.1.12.25. Data e hora da infecção

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.12.26. Ação tomada

5.1.12.27. Endereço IP da máquina

5.1.12.28. Usuário autenticado na máquina

5.1.12.29. Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado via rede;

5.1.12.30. O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques;

5.1.12.31. Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

5.1.13. Atualização de Vacinas

5.1.13.1. Atualização incremental e on-line das vacinas;

5.1.13.2. Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador;

5.1.13.3. Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet;

5.1.13.4. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante;

5.1.13.5. Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função;

5.1.13.6. Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução;

5.1.13.7. Qualquer atualização deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la;

5.1.13.8. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

5.1.13.9. O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

5.1.14. Cliente Gerenciado

5.1.14.1. A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits;

5.1.14.2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:

5.1.14.3. Microsoft Windows 7;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.14.4. Microsoft Windows 8;

5.1.14.5. Microsoft Windows 8.1;

5.1.14.6. Microsoft Windows 10;

5.1.14.7. Microsoft Windows 2008 server;

5.1.14.8. Microsoft Windows 2008 R2 server;

5.1.14.9. Microsoft Windows 2012 R2 server e/ou superior;

5.1.14.10. Red Hat;

5.1.14.11. SUSE.

5.1.14.12. O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede;

5.1.14.13. O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento;

5.1.14.14. Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante;

5.1.14.15. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento;

5.1.14.16. Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária;

5.1.14.17. O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas (locked) através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

5.1.15. Funcionalidade de Firewall e Sistema de Prevenção de Intrusão (IPS)

5.1.15.1. A funcionalidade deve suportar os protocolos TCP e UDP;

5.1.15.2. Reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio;

5.1.15.3. Possuir proteção contra-ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet;

5.1.15.4. Possibilidades de criação de assinaturas personalizadas para detecção;

5.1.15.5. Possibilidade de agendar a ativação de novas regras do firewall;

5.1.15.6. Possibilidade de criar regras diferenciadas por aplicações;

5.1.15.7. todos os executáveis da lista ou liberar somente os executáveis da lista;

5.1.15.8. Bloqueio de ataques baseado na exploração da vulnerabilidade;

5.1.15.9. Permitir integração com navegadores WEB para prevenção de ataques;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.15.10. Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.

5.1.16. Funcionalidade de Reconhecimento de Novas Ameaças

5.1.16.1. A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

5.1.16.2. Capacidade de detecção de keyloggers por comportamento dos processos em memória;

5.1.16.3. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts;

5.1.16.4. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção;

5.1.16.5. Possibilidade de agendar a varredura da detecção de novas ameaças.

5.1.16.6. Uso de sandboxing na nuvem para analisar o comportamento de malwares, com SLA de 5 minutos até 1 hora de resposta.

5.1.17. Funcionalidade de Controle de Dispositivos

5.1.17.1. Controlar o uso de dispositivos com comunicação infravermelha, firewire, portas seriais e paralelas, através de mecanismos de permissão e bloqueio, identificando-os pelo "Class ID" e pelo “Device ID”;

5.1.17.2. Permitir criar políticas de bloqueio de dispositivos distintas para diferentes grupos da base de estações conectadas;

5.1.17.3. Gerenciamento integrado à console de gerência da solução.

5.1.17.4. A solução deve ser capaz de permitir ou negar o uso dos dispositivos com base nos seguintes critérios:

5.1.17.5. Fabricante

5.1.17.6. Modelo

5.1.17.7. Número de Série

5.1.17.8. Funcionalidade de Controle WEB

5.1.17.9. Controlar acesso a sites, possibilitando o bloqueio do mesmo;

5.1.17.10. Permitir criar políticas de bloqueio com base em categorias e lista de URL;

5.1.17.11. Permitir gerar relatórios de sites acessados e bloqueados;

5.1.17.12. Relatórios e Monitoramento

5.1.17.13. Gerar, no mínimo, os relatórios abaixo descritos, tanto de maneira gráfica quanto em arquivos CSV, PDF, HTML ou MHTML, permitindo escolher o período de consulta desejado:

5.1.17.14. Listagem dos malwares que infectaram determinada máquina;

5.1.17.15. Listagem das máquinas que estão infectadas por determinado malware;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.17.16. Relatório dos totais de códigos maliciosos detectados, indicando aqueles de maior incidência;

5.1.17.17. Listagem das máquinas nas quais o antimalware deixou de remover algum código malicioso;

5.1.17.18. Número total de arquivos maliciosos removidos;

5.1.17.19. Relatório de máquinas cuja atualização de componentes do software antimalware e assinaturas não foi realizada, incluindo a data da última atualização;

5.1.17.20. Relatório de máquinas com maior número de infecções;

5.1.17.21. Relatório de atualização de componentes do software antimalware e assinaturas;

5.1.17.22. Relatório das máquinas que não se comunicaram com o servidor de antimalware a partir de uma determinada data.;

5.1.17.23. Possibilidade de exibir a lista de servidores e estações que possuam o antimalware instalado, contendo informações como nome da máquina, usuário autenticado, versão do engine, data da vacina, data da última verificação e status;

5.1.17.24. Sumário de eventos IPS por assinatura, por alvo, por endereço IP de origem, principais nós atacados, principais assinaturas;

5.1.17.25. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.

5.1.17.26. Deverá ter um console de administração de licenças em nuvem, de onde é possível revisar os detalhes de equipamentos aos quais foram provisionados o licenciamento.

5.1.18. Funcionalidades Tecnológicas

5.1.18.1. A console deverá funcionar também através de um Appliance Virtual.

5.1.18.2. Dentro do módulo de firewall deverá possuir a funcionalidade de bloqueio de exploits.

5.1.18.3. Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

5.1.18.4. Deverá contar com um filtro de correio para a detecção de malware e spam.

5.1.18.5. Deverá ser uma solução que pode ser utilizada e administrada através de um console de administração remota de antivírus para os sistemas operacionais Windows, Linux e Mac.

5.1.18.6. A solução Anti Malware deberá contar com a tecnologia HIPS para proteger a manipulação indevida e detectar ameaças com base na conduta do host.

5.1.18.7. O produto deverá ter um controle web para limitar o acesso a sites web por categoria, além de poder mostrar ao usuário uma notificação de bloqueio.

5.1.18.8. Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.18.9. O firewall do produto deverá ser bidirecional, assim como detectar as redes seguras.

5.1.18.10. A solução deverá realizar exploração em estado inativo para poder fornecer desta forma uma proteção pró ativa enquanto o equipamento não está em uso.

5.1.18.11. A console de administração deverá ter um Appliance Virtual aberto para instalar e utilizar em ambientes virtuais, para ter um ambiente distribuído e de fácil instalação.

5.1.18.12. O acesso ao console de administração do antivírus deve ser feito com duplo fator de autenticação integrado dentro da mesma console aonde é possível ativa-lo se a necessidade de nenhum add-on adicional.

5.1.18.13. O console de administração de licenças deve ser na nuvem, aonde é possível revisar os detalhes dos equipamentos que estão utilizando a licença do antivírus.

5.1.18.14. A versão mais atual do antivírus deve ter proteção a equipamentos com sistemas operacionais Windows XP.

5.1.18.15. A console de administração deverá suportar a instalação em ambiente com sistema operacional Linux.

5.1.18.16. Detecção do malware por DNA do vírus.

5.1.18.17. Deverá ter a capacidade de atualizar os patches do sistema operacional.

5.1.18.18. A solução deve ser capaz de definir uma lista de usuários específicos que podem fazer utilização dos dispositivos. Para dispositivos de armazenamento a solução deve permitir a configuração das seguintes permissões: Leitura e Escrita, Bloqueio, Somente Leitura e Advertência.

5.1.18.19. Quando se conectar ou utilizar um dispositivo de armazenamento a solução de antivírus deve proporcionar as seguintes opções: Escancear, não realizar nenhuma ação e se lembrar dessas ações.

5.1.18.20. Deverá permitir a execução remota de scripts, arquivos batches e pacotes personalizados através da console.

5.1.18.21. Deve permitir gerar grupos de clientes dinâmicos e grupos estáticos.

5.1.18.22. O fabricante deverá proporcionar ao menos três formas diferentes de realizar a instalação do console de administração remota: Instalação Tudo em Um, Instalação por Componentes e em Appliance Virtual.

5.1.18.23. O Appliance Virtual deverá suportar ao menos as seguintes plataformas de virtualização: VMWare vSphere, Oracle Virtual Box, Microsoft Hyper-V e Azure.

5.1.18.24. A console de administração deverá suportar a instalação em Linux.

5.1.18.25. Deve contar com desinstalador de antivírus de terceiros.

5.1.18.26. A solução de proteção Antispam deve realizar as verificações utilizando o protocolo SSL.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.18.27. A solução antivírus deve contar um Firewall pessoal com os seguintes modos de configuração: Modo automático, Modo Interativo, Modo baseado em políticas e Modo de Aprendizagem.

5.1.18.28. O fabricante deverá ter suporte local em idioma português.

5.1.18.29. O fabricante deverá ter documentação publicada na internet no idioma português.

5.1.18.30. O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.

5.1.18.31. O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.

5.1.18.32. Tenha escritório do fabricante no Brasil.

5.1.18.33. O fabricante deverá ter programas internos de Colaborador Seguro.

5.1.18.34. O fabricante deve possuir uma posição de Challenger no Quadrante Mágico do Gartner no último ano.

5.1.18.35. O fabricante não deve possuir nenhum falso positivo nas provas realizadas pelo VB100 do Virus Bulletin nos últimos dez anos.

5.1.18.36. O fabricante deve possuir mais de 70 prêmios no VB100 do Virus Bulletin e o mínimo de 80 participações no mesmo.

5.1.18.37. O fabricante deve possuir êxito em mais de 80% na participação dos prêmios do VB100 do Virus Bulletin.

5.1.18.38. O fabricante deve ter sido incluído ao menos uma vez no Top Rated do AV-Comparatives entre os aos de 2016 e 2018.

5.1.18.39. O fabricante não deve possuir nenhum falso positivo nas provas realizadas AV-Comparatives entre os anos de 2016 e 2018.

5.1.18.40. O fabricante deve ter recebido ao menos uma vez a premiação de Gold Award no quesito Desempenho do AV-Comparatives nos anos de 2016 a 2018.

5.1.18.41. Possuir proteção contra ransomware, com um módulo específico, utilizando a console para configuração e distribuição de políticas aos endpoints.

5.1.18.42. Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push (EPNS).

5.1.18.43. Funcionalidade de Inventário de Hardware (CPU, RAM, Armazenamento, Versão de Sistema Operacional e Periféricos conectados)

5.1.18.44. Possuir no mínimo 42 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.

5.1.19. Quarentena do Correio Eletrônico

5.1.19.1. Mensagens de e-mail de spam e de quarentena podem ser armazenadas em um sistema de arquivos local, não no banco de dados de caixa de correio do Exchange.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.19.2. A criptografia e a compactação de arquivos de e-mail em quarentena devem ser armazenadas localmente.

5.1.19.3. Arquivos de email em quarentena excluídos podem ser restaurados usando a interface de linha de comando do produto do fabricante do produto de proteção de email (desde que eles ainda não tenham sido excluídos do sistema de arquivos).

5.1.19.4. Os relatórios de quarentena devem ser enviados para um endereço de email especificado usando uma tarefa agendada.

5.1.19.5. É possível armazenar mensagens de destinatários inexistentes: aplica-se a mensagens marcadas para serem colocadas em quarentena por proteção antivírus, proteção antispam ou regras.

5.1.19.6. O administrador da Quarentena de e-mail deve estar disponível nos três tipos de quarentena: Quarentena local, Correio electrônico de quarentena e Quarentena de MS Exchange

5.1.19.7. Deve ter uma interface da Web da Quarentena da Web.

5.1.19.8. Deve ter validação de mensagem com SPF, DKIM e DMARC, localmente no mesmo servidor de email no aplicativo de proteção de email.

5.1.19.9. Para verificar o banco de dados por demanda, deve usar a API do EWS (Serviços Web do Exchange) para se conectar ao Microsoft Exchange Server usando HTTP / HTTPS.

5.1.19.10. A proteção de email deve ter a possibilidade de instalar por componentes, você pode escolher os componentes para adicionar ou remover.

5.1.19.11. O produto de segurança deve ter uma interface de linha de comando que ofereça aos usuários e administradores avançados opções mais profundas para gerenciar o produto.

5.1.19.12. As regras de correio devem ser classificadas em três níveis e avaliadas na seguinte ordem:

5.1.19.13. Regras de filtragem: regra avaliada antes do antispam e da verificação antivírus

5.1.19.14. Regras de processamento de anexos: regra avaliada durante a verificação antivírus

5.1.19.15. Regras de processamento de anexos: regra avaliada durante a verificação antivírus

5.1.19.16. Deve poder explorar mensagens de conexões autenticadas ou internas.

5.1.19.17. A solução deve ser capaz de excluir o cabeçalho SCL existente antes da verificação e pode ser desativada se for necessário manter o cabeçalho do nível de confiança em relação ao spam.

5.1.19.18. Regras

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.19.19. Deve-se poder excluir o anexo de uma mensagem no Transporte de Email, no banco de dados da caixa de correio e na verificação do banco de dados.

5.1.19.20. Deve-se poder adicionar uma string personalizada ao campo de cabeçalho (ao cabeçalho da mensagem).

5.1.19.21. Deve ser possível adicionar várias ações para uma regra.

5.1.19.22. Condições

5.1.19.23. Deve-se poder aplicar a mensagens enviadas a um destinatário validado no Active Directory sobre proteção de transporte de email.

5.1.19.24. Deve-se poder aplicar condições a mensagens que tenham anexos com nomes específicos.

5.1.19.25. Deve-se poder aplicar condições a mensagens de um remetente com um domínio específico no endereço de e-mail.

5.1.19.26. Deve ser possível analisar se a mensagem contém um arquivo danificado na proteção de transporte de email e na proteção de banco de dados da caixa de entrada de email.

5.1.19.27. O produto deve suportar múltiplas funções Microsoft Exchange Server 2007, 2010 e Windows SM 2008 e 2011, proteção contra spam, regras, sobre proteção de transporte de e-mail, varredura de banco de dados sob demanda, proteção de banco de dados dos dados da caixa de correio e da quarentena.

5.1.19.28. O produto deve suportar borda e caixa de correio, Windows Exchange Server 2016, proteção contra spam, regras, proteção de transporte de email, verificação de banco de dados sob demanda e quarentena de email.

5.1.20. Ferramenta de relatórios e gestão de logs:

5.1.20.1. A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;

5.1.20.2. A CONTRATADA deve disponibilizar no mínimo 1TB líquido para armazenamento de logs com proteção em RAID5 ou superior;

5.1.20.3. A solução deve suportar no mínimo 250 eventos por segundo ou 10GB de logs por dia;

5.1.20.4. A ferramenta de relatórios deverá suportar no mínimo os seguintes relatórios:

5.1.20.5. Ataques detectados;

5.1.20.6. Categorias de aplicações mais acessadas;

5.1.20.7. Categorias WEB mais acessadas;

5.1.20.8. Aplicações WEB mais utilizadas

5.1.20.9. Websites mais acessados;

5.1.20.10. Usuário ou equipamento com maior consumo de banda;

5.1.20.11. Usuário ou equipamento com maior número de sessões;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.20.12. Aplicações de Maior Risco;
5.1.20.13. Aplicações com maior vulnerabilidade;
5.1.20.14. Top Malware, Botnets, Spyware e Adware detectados;
5.1.20.15. Usuários ou dispositivos com maior risco;
5.1.20.16. Aplicações mais acessadas;
5.1.20.17. Redes sociais mais acessadas;
5.1.20.18. Aplicações de streaming de áudio e vídeo mais acessadas;
5.1.20.19. Aplicações P2P mais acessadas;
5.1.20.20. Aplicações de Game mais acessadas;
5.1.20.21. Permitir a personalização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.
5.1.20.22. Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails cadastrados.
5.1.20.23. Ter fácil identificação das atividades de rede e ataques em potencial.
5.1.20.24. Armazenar histórico dos relatórios em disco local.
5.1.20.25. Possuir relatórios únicos para cada um dos módulos ofertados pela solução.
5.1.20.26. Possuir múltiplos formatos de relatório, pelo menos tabular e gráfico.
5.1.20.27. Permitir exportar relatórios para: PDF, Excel e HTML.
5.1.20.28. Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia e Google.
5.1.20.29. Possuir relatórios que informem principais atividades em cada módulo.
5.1.20.30. Ter logs em tempo real.
5.1.20.31. Ter logs arquivados para consulta posterior.
5.1.20.32. Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.
5.1.20.33. Possuir logs de auditoria.
5.1.20.34. Ter sua gerência totalmente baseada em acesso web.
5.1.20.35. Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades especificas na ferramenta.
5.1.20.36. Possuir no mínimo 2 (duas) dashboard sendo uma exclusiva para os relatórios e outra exclusiva para visualização da saúde do equipamento (CPU e memória).
5.1.20.37. O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.
5.1.20.38. Ter total gerência sobre a retenção dos dados armazenados neste equipamento.
5.1.20.39. Ter disponibilidade em firewall NGFW virtual e software caso necessário instalar o firewall NGFW em um hardware baseado em Intel.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.20.40. Possuir suporte no mínimo aos virtualizadores:

5.1.20.41. Vmware

5.1.20.42. Hyper-V

5.1.21. <u>Gestão de Vulnerabilidades:</u>

5.1.21.1. Detectar vulnerabilidades em aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

5.1.21.2.

5.1.21.3.

5.1.21.4. Verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hot fixes, service packs, registros, peer to peer, portas de serviço habilitadas e antivírus;

5.1.21.5. Detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

5.1.21.6. Efetua descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional da câmara;

5.1.21.7. Realizar periodicamente procedimentos ou atualizações necessárias para mitigar vulnerabilidades dos componentes da solução de segurança;

5.1.21.8. Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas (inclusive instruções para aplicação de correções em produtos de terceiros);

5.1.21.9. Scanner (varredura) de rede para identificar portas TCP/UDP abertas.

5.1.21.10. Riscos baseados na pontuação CVE (Common Vulnerabilities and Exposures);

5.1.21.11. Gerar relatório nos formatos XML, PDF, CSVe HTML;

5.1.21.12. Recursos de controle de acesso:

5.1.21.13. Controle de acesso baseado em perfis;

5.1.21.14. Autenticação LDAP;

5.1.21.15. Facilidade na criação de perfis;

5.1.21.16. Visualização de problemas por categoria;

5.1.21.17. Cinco níveis de severidade: Critical, High, Medium, Low, Info;

5.1.21.18. Possuir dashboard de resultados;

5.1.21.19. Busca de vulnerabilidades em tempo real;

5.1.21.20. Possibilitar o agendamento de scans;

5.1.21.21. Escaneamento sem agentes para facilitar um scan eventual;

5.1.21.22. Programação de scans para rodar uma única vez ou de forma recorrente;

5.1.22. <u>Gestão de Incidentes de Segurança</u>

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.1.22.1. Será realizada em todos os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço, em regime 8x5 (de segunda a sexta-feira das 8:30h às 17:30h exceto feriados);

5.1.22.2. Executar as ações necessárias à resposta aos incidentes de segurança identificados de forma a manter os serviços disponíveis e operacionais;

5.1.22.3. Mapear e executar os processos de resposta dos incidentes de segurança ocorridos e documenta na base de conhecimento da câmara;

5.1.22.4. Efetuar a manutenção das regras e políticas do parque monitorado para responder a incidentes, à exceção dos ativos sob gestão exclusiva da câmara, cujos incidentes ou resultados de monitoração devem ser informados à câmara;

5.1.22.5. Verificar, quinzenalmente, a disponibilização, pelos fabricantes, de patches, correções e versões ou releases mais recentes dos softwares;

5.1.22.6. Comunicar à câmara a existência do patch juntamente com os respectivos problemas resolvidos e as novas funcionalidades disponibilizadas. A periodicidade dessa comunicação será mensal;

5.1.22.7. Serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação da câmara, tais como:

5.1.22.8. Acessos indevidos;

5.1.22.9. Instalação de códigos maliciosos;

5.1.22.10. Indisponibilidade dos serviços (DoS e DDoS);

5.1.22.11. Ataques por força bruta;

5.1.22.12. Exploração de vulnerabilidades.

5.2. ITEM 02: SERVIÇOS GERENCIADOS DE BACKUP

5.2.1. **Ferramenta de backup em nuvem e Data Center**

5.2.1.1. Será de responsabilidade da contratada implementar e configurar o software de transferência de backup local para o repositório na nuvem, de acordo com as políticas atuais da Câmara.

5.2.1.2. A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;

5.2.1.3. A contratada deverá ofertar o armazenar o backup da contratante em nuvem, com retenção mínima de 15 dias, com backups diários, com no mínimo as seguintes características:

5.2.1.4. Deverá conter um espaço mínimo liquido de 500GB de armazenamento em nuvem;

5.2.1.5. A solução deverá conter compactação e/ou aceleração WAN, para menor carga de utilização dos links de internet da contratante;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.2.1.6. O licenciamento e operação do ambiente em nuvem é de total responsabilidade da contratada;

5.2.1.7. 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;

5.2.1.8. 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;

5.2.1.9. Os backups deverão estar criptografados com um mínimo de 256 bits;

5.2.1.10. As instalações físicas do data center deverão ter os seguintes itens:

5.2.1.10.1. Sistema de piso elevado, com vias independentes de cabos de energia, lógicos e óticos;

5.2.1.10.2. Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;

5.2.1.10.3. Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento.

5.2.1.11. A estrutura de energia elétrica do data center deverá atender aos seguintes requisitos:

5.2.1.11.1. Alimentação elétrica redundante;

5.2.1.11.2. Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;

5.2.1.11.3. 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;

5.2.1.11.4. Mínimo de 2KVAs nominais;

5.2.1.11.5. Alimentação elétrica redundante e independente para os equipamentos da solução;

5.2.1.12. O data center que aloca os backups da contratante deverá atender os seguintes requisitos de climatização:

5.2.1.12.1. Sistema de climatização com controles de temperatura, umidade relativa do ar e filtros de poeira;

5.2.1.12.2. Sistema de climatização redundante (n+1), refrigerado por formas diferentes;

5.2.1.12.3. Temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/-10%.

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

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.2.1.13.1. Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);

5.2.1.13.2. 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;

5.2.1.13.3. 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;

5.2.1.13.4. Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores e de armazenamento de dados;

5.2.1.13.5. Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

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

5.2.1.14.1. Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;

5.2.1.14.2. 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;

5.2.1.14.3. Capacidade de cadastro remoto de usuários para acesso ao data center;

5.2.1.14.4. Deverá possuir a capacidade de cadastro de novo usuário local com permissão do administrador;

5.2.1.14.5. Acesso ao local através de leitura biométrica;

5.2.1.14.6. Possuir alerta por SMS e e-mail em tempo real de acesso ao ambiente;

5.2.1.14.7. Arquivar as imagens gravadas pelas câmeras de vídeo de segurança por pelo menos 30 (trinta) dias;

5.2.1.14.8. 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;

5.2.1.14.9. Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Datacenter;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.2.1.14.10. Acondicionar equipamentos e mídias geradas no ambiente do Datacenter, livres de riscos físicos;

5.2.1.14.11. Possuir rígido controle de acessos aos equipamentos do Datacenter, mesmo por pessoas credenciadas pela CONTRATANTE;

5.2.1.14.12. 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;

5.2.1.14.13. Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Datacenter, a dívida em regiões com níveis de restrição diferenciados;

5.2.1.14.14. Possuir sistema de detectores de movimento no ambiente.

5.2.2. **Gestão de backup nuvem**

5.2.2.1. A contratada deverá administrar e monitorar o sistema de backup descrito nesse documento;

5.2.2.2. Será de responsabilidade da contratada manter o pleno funcionamento da política de cópia de backup, de acordo com a rotina de backup estabelecida pela contratante;

5.2.2.3. Deverá monitorar diariamente, os relatórios de cópia de backup gerados ao concluir a tarefa, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da contratada efetuar correção ou ajuste técnico para a normalização do mesmo, garantindo o pleno funcionamento da solução;

5.2.2.4. A contratada deverá fornecer mensalmente, toda primeira segunda-feira do mês deverá ser entregue a contratante, um relatório com o resumo de execução de cada tarefa de cópia de backup, durante ao mês anterior, documento denominado “Relatório de Backup Nuvem Diário – MÊS_ANO”, a nomenclatura deverá variar de acordo com mês e ano corrente;

5.2.2.5. Deverá ser de responsabilidade da contratada garantir integridade da cópia do backup LOCAL para NUVEM;

5.2.2.6. A contratada deverá fornecer mensalmente, um relatório com o resumo da execução dos testes automáticos de integridade das cópias de backups, referente ao mês anterior, documento denominado “Relatório de Teste de Cópia de Backup - MÊS_ANO”, a nomenclatura deverá variar de acordo com mês e ano corrente;

5.2.2.7. A contratada deverá ser responsável por executar as restaurações conforme a manda da contratante;

5.2.2.8. Para controle, deverá ser entregue a contratante, um relatório de todas restaurações executadas, com data, motivo, objeto e solicitante, referente ao mês anterior,

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

documento denominado “Relatório de Restauração de Backup em Nuvem - MÊS_ANO”, a nomenclatura deverá variar de acordo com mês e ano corrente;

5.2.2.9. Deverá ser realizada de maneira mensal uma reunião presencial com o gestor do contrato, onde a contratada deverá apresentar o relatório mensal;

5.3. ITEM 03: SUPORTE TÉCNICO ESPECIALIZADO

5.3.1. Os serviços de suporte técnico especializado devem ser prestados sob a solução completa de infraestrutura de rede e firewall da contratante;

5.3.2. O suporte técnico especializado deverá ter vigência de 12 (doze) meses;

5.4. SOBRE CHAMADOS E ATENDIMENTO TÉCNICO

5.4.1. 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;

5.4.1.1. O atendimento técnico presencial deverá ocorrer de segunda a sexta-feira (exceto feriados) das 09:00h às 18:00h, sob demanda e preventivo;

5.4.1.2. O atendimento técnico remoto deverá ocorrer de segunda a sexta-feira (exceto feriados) das 08:00h às 18:00h;

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

5.4.1.4. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas no equipamento (hardware) será de plena responsabilidade da contratante.

5.4.1.5. Caso os equipamentos dessa solução estiverem garantia do fabricante a contratada poderá efetuar a tratativas com o fabricante, havendo necessidade.

5.4.1.6. 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;

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

5.4.1.8. 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;

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

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

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

5.4.1.11. Executar ações correlatas, que demandem maior esforço ou complexidade (ex: instalações e ou atualizações de software em grande quantidade de equipamentos, elaboração de roteiro específico, etc.), solicitadas diretamente pelo Gestor do Contrato por parte da Contratante e devidamente registradas no Sistema de atendimento técnico;

5.4.1.12. Deverá realizar configurações solicitadas pela contratante, tais como: regras de trafego de dados do ambiente de nuvem, rotas, políticas e demais configurações especificas dos componentes da solução;

5.4.1.13. Planejamento e aplicação de atualizações e ou correções de firmware com programação prévia de forma que não seja gerado nenhum tipo de indisponibilidade ou a mínima possível acordada com a contratante;

5.4.1.14. Manter o ambiente de infraestrutura virtual, segurança da informação e backup sempre atualizado em com as melhores práticas aplicadas;

5.4.1.15. Realização de otimizações nas configurações para melhora do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela Contratante;

5.4.1.16. Na impossibilidade de resolução de problema técnico telefônico ou acesso remoto a contratada deverá disponibilizar uma visita presencial para avaliação e resolução do problema;

5.4.1.17. Deverá garantir a atualização dos sistemas operacionais das máquinas virtuais ao quais os serviços da contratante serão alocados. Garantindo o mínimo possível de indisponibilidade;

5.4.1.18. A contratada deverá realizar manutenções preventivas nos equipamentos, a cada 90 (noventa) dias, sendo necessárias inspeções visuais, para avaliação das condições gerais. Gerando ao final um relatório com fotos a serem enviados a contratante;

5.4.1.19. A manutenção preventiva deverá contemplar todos os componentes da solução, visando manter o pleno funcionamento do ambiente de data center e infraestrutura de rede;

5.4.1.20. Deverá atualizar os softwares da solução sempre que disponíveis e homologados pelo fabricante. Acordando e alinhando as operações com a contratante;

5.4.1.21. A contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

5.4.1.22. Deverá ser fornecido relatório mensal de chamados com:

5.4.1.22.1. Categoria do chamado;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.4.1.22.2. Usuário;

5.4.1.22.3. Departamento;

5.4.1.22.4. Ativos relacionados;

5.4.1.22.5. Data de abertura e fechamento;

5.4.1.22.6. Status;

5.4.1.23. Deverá ser realizada de maneira mensal uma reunião presencial com o gestor do contrato, onde a contratada deverá apresentar o relatório mensal;

5.5. GARANTIA DE TEMPO DE RESPOSTA E NÍVEL DE SERVIÇO

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

Classe	Descrição	Início do atendimento em até:
1	Serviço indisponível	2 horas
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

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

Prioridade Descrição	
1 (Emergencial)	O serviço está for a de operação ou há um impacto crítico nas operações dos negócios.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio 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

5.5.3. As horas para primeiro atendimento e resolução de incidentes são horas úteis e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

5.6. CENTRAL DE CHAMADOS E INFORMAÇÕES

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.6.1. A contratada deverá disponibilizar e gerenciar os atendimentos técnicas da contratante através de portal de gerenciamento de atendimentos com acesso através de navegador web;

5.6.2. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;

5.6.3. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

5.6.4. 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;

5.6.5. 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;

5.6.6. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da contratada, sendo essa responsável por sua atualização e manutenção;

5.6.7. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;

5.6.8. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;

5.6.9. A solução de atendimento e informações deverá constar com a possibilidade de cadastro e organização de ativos de rede, tais como: Firewall, Switches, dispositivos de rede e demais itens com acesso à rede;

5.6.10. A contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela contratante;

5.6.11. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;

5.6.12. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a contratante;

5.6.13. 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;

5.6.14. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;

5.6.15. A solução deverá conter módulo que possibilite o inventário de racks dentro do data center;

5.6.16. Os itens de inventario da solução deverão permitir ser anexados aos atendimentos técnicos, criando assim uma relação de atendimento versus dispositivo da contratante;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.6.17. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";

5.6.18. A contratada deverá garantir que a solução de atendimento e informações tenha a possibilidade de cadastrar e organizar certificados digitais da contratante;

5.6.19. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;

5.6.20. Deverá ser possível a criação de grupos de usuários na solução;

5.6.21. A solução disponibilizada pela contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.

5.7. MONITORAMENTO DO AMBIENTE

5.7.1. O monitoramento deve contemplar todo o ambiente de infraestrutura de rede e firewall;

5.7.2. Deve monitorar até 50 (cinquenta) dispositivos de rede, link e Data Center.

5.7.3. O monitoramento deverá ter vigência de 12 (doze) meses;

5.7.4. A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;

5.7.5. Deverá ter SLA de disponibilidade da console de gerenciamento de no mínimo 99,98%;

5.7.6. A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;

5.7.7. A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a contratante;

5.7.8. Deverá ser capaz de enviar alertas de alteração de status de sensores através de e-mail, sms, push em dispositivo (s) celular (es), script, Microsoft Teams, Event Log e syslog.

5.7.9. Deverá enviar relatório via Software com customização HTML e PDF.

5.7.10. Prover aplicativos para iOS e Android

5.7.11. Todas as interfaces de usuário, devem permitir o acesso local e remoto protegido por SSL, com possibilidade de ser usadas simultaneamente.

5.7.12. Possibilidade de exportar dados de monitoramento, como históricos em PDF, HTML, XML ou CSV.

5.7.13. Ser capaz de executar áudio pré-definido em caso de alteração de sensores de monitoramento;

5.7.14. Disponibilizar sistema automático de aviso via e-mail informando ocorrências de falhas no servidor ou em quaisquer dos serviços por ele hospedados, nos endereços de e-mail definidos pela contratante;

5.7.15. Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.7.16. Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;

5.7.17. O monitoramento deverá ser compatível com os principais serviços de nuvem pública;

5.7.18. Possuir a possibilidade de integração de unidade de autenticação AD (Active Directory);

5.7.19. O sistema de monitoramento deverá contar com aplicativo de administração instalável para o sistema operacional Microsoft Windows;

5.7.20. A solução deverá ser compatível com os seguintes protocolos:

5.7.20.1. SNMPv1;

5.7.20.2. SNMPv2;

5.7.20.3. SNMPv3;

5.7.20.4. WMI;

5.7.20.5. SSH;

5.7.20.6. ICMP;

5.7.20.7. SOAP;

5.7.20.8. FTP;

5.7.20.9. SMTP;

5.7.20.10. POP3;

5.7.20.11. WBEM;

5.7.20.12. HTTP.

5.7.21. Deverá ter intervalo mínimo de verificação de 30 (trinta) segundos para os sensores monitorados;

5.7.22. Monitorar e analisar em tempo real as estatísticas de desempenho de rede para roteadores, switches, access points e outros dispositivos que suportem SNMP nas versões v1, v2 e v3, e WMI;

5.7.23. A solução deverá alertar sobre medições incomuns de sensores do ambiente, ou seja, deverá analisar padrões alertando quando houver um estado incomum no monitoramento;

5.7.24. Fornecer informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os paramentos estão ou não dentro dos limites preestabelecidos;

5.7.25. Deve permitir o monitoramento da performance com detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com carga de CPU, uso da memória, utilização de banda, status operacional de interface de rede, tempo de resposta dos dispositivos e eventos de erros;

5.7.26. Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos;

5.7.27. Permitir a configuração ou agendamento de descobrimento automático na rede;

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.7.28. Permitir a criação de relatórios de rede personalizados que possam ser exportados para pdf, impresso ou visualizado via HTTP;

5.7.29. Deve suportar IPV4 e IPV6;

5.7.30. Deve suportar NetFlow v5/v9, sFlow, jFlow, IPFIX, e packet sniffing;

5.7.31. Deverá monitorar Windows, Linux e MacOS com “Agentless”.

5.7.32. Deve permitir interação na configuração do dispositivo através de SNMP v1, v2 e v3;

5.7.33. A solução de monitoramento deverá utilizar dados históricos armazenados em seu banco de dados interno;

5.7.34. A solução deverá permitir a personalização de disparadores para sensores, tais como: intervalo de tempo de monitoramento, intervalo de tempo entre erros e alertas e quantidade de alertas consecutivos;

5.7.35. Deverá ser capaz de efetuar detecções automáticas no ambiente da contratante;

5.7.36. A solução de monitoramento deverá ser capaz de entregar e-mails utilizando Relay autenticado;

5.7.37. Deverá ser possível o monitoramento de todas as portas das soluções (hardware) deste termo de referência, mostrando através de tabela de dados e gráficos sua disponibilidade e largura de banda com o intervalo mínimo de 30 (trinta) segundos;

5.7.38. A solução deverá monitorar características físicas das soluções (hardware) desta solução, tais como: temperatura do hardware, utilização de memória volátil, utilização de armazenamento, utilização e processamento e carga total do equipamento;

5.7.39. Deverá ter sensor com a informação de quantidade de tempo ligado dos equipamentos (hardwares) das soluções;

5.7.40. A solução de monitoramento deverá abrir chamado de maneira automática junto a contratante, após a alteração de um sensor para o estado de alerta ou erro;

5.7.41. Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;

5.7.42. Deverá ser possível a criação de templates de relatórios de monitoramento;

5.7.43. A solução deverá conter sensor de “Sniffing de Pacotes”, por porta e/ou endereço IP;

5.7.44. Deverá ser capaz de detectar automaticamente sobrecargas de largura de banda em equipamentos de rede gerenciáveis;

5.7.45. A solução deverá ser capaz de monitorar a qualidade de serviço de rede “Jitter”;

5.7.46. Deverá ser capaz de monitorar a latência de um dispositivo;

5.7.47. A solução deverá ser capaz de importar arquivos “. MIB”, interpreta-los e integra-los ao sistema de monitoramento;

5.7.48. A solução de monitoramento deverá fornecer informações de disponibilidade dos equipamentos (hardwares) da solução.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

5.7.49. Deverá ser fornecido relatório mensal de monitoramento dos recursos e componentes da solução, com:

5.7.49.1. Disponibilidade;

5.7.49.2. Consumo de hardware (CPU memória, disco, rede);

5.7.49.3. Alertas e erros;

5.7.49.4. Rotinas de backups;

5.7.50. Deverá ser realizada de maneira mensal uma reunião presencial com o gestor do contrato, onde a contratada deverá apresentar o relatório mensal;

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

6.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

6.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

6.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

6.5. Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços da contratada.

7. DA SUBCONTRATAÇÃO

7.1. Não será admitida a subcontratação do objeto licitatório.

8. ALTERAÇÃO SUBJETIVA

8.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

9. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

9.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 6º do Decreto nº 9.507 de 21 de setembro de 2018.

9.2. A fiscalização dos contratos, no que se refere ao cumprimento das obrigações trabalhistas, deve ser realizada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337

9.3. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

9.4. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

9.5. O fiscal ou gestor do contrato, ao verificar o andamento da realização do serviço e a qualidade na execução do serviço, caso verifique irregularidades deverá comunicar à autoridade responsável para que esta promova a adequação.

9.6. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

10. DAS SANÇÕES ADMINISTRATIVAS

10.1. As sanções administrativas estão previstas no Item 22 do edital.

11. DA VISTORIA FACULTATIVA

11.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante PODERÁ realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 9 horas às 17 horas, devendo o agendamento ser efetuado previamente pelo e-mail, compras@osasco.sp.leg.br.

11.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até dois dias úteis anteriores à data prevista para a abertura da sessão pública.

11.3. Para a vistoria, o licitante, ou o seu representante, deverá estar devidamente identificado.

11.4. A realização da vistoria não será obrigatória, entretanto, não serão aceitas alegações posteriores quanto a desconhecimento de qualquer detalhe, incompreensão, dúvidas ou esquecimento que possam provocar empecilhos, atrasos na realização dos serviços, arcando a empresa com quaisquer ônus decorrentes destes fatos

Osasco, 20 de dezembro de 2019.

Rafael Ramos Feijó Munhoz

Diretor-Secretário

Av. dos Autonomistas, nº 2.607 – Centro – Osasco/SP – CEP: 06090-905
Telefone: (11) 3685-6336 – 3685-6337