

**DESPACHO DE HOMOLOGAÇÃO**

Processo Licitatório n° 026/2021

Modalidade: Pregão Eletrônico n° 019/2021

Tipo: Menor preço por lote

**OBJETO: REGISTRO DE PREÇO PARA FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DE REDE, IMPLANTAÇÃO E TREINAMENTO PARA POSSIBILITAR A IMPLANTAÇÃO DE SOLUÇÃO DE WI-FI NAS ESCOLAS MUNICIPAIS.**

FICHA	DOTAÇÃO
906	02.07.01.12.361.0012.2062.3.3.90.39.00
908	02.07.01.12.361.0012.2062.4.4.90.52.00

Tendo transcorrido regularmente o processo licitatório em referência, e depois de cumpridas todas as suas fases legais e administrativas com Fundamentação Legal na Lei Federal 10.520/02 no Decreto Municipal 3.989/20, subsidiados pela Lei Federal 8.666/93, HOMOLOGO o procedimento no qual foi adjudicado o lote à empresa vencedora:

EMPRESA: ALTAS NETWORKS & TELECOM LTDA CNPJ: 05.407.609/0001-01						
ITEM	QTD	UN	DESCRIÇÃO	MARCA	PREÇO UNIT.(R\$)	PREÇO TOTAL (R\$)
1	02	UN	FIREWALL 1.1. CARACTERÍSTICAS DE DESEMPENHO: 1.1.1. THROUGHPUT DE, NO MÍNIMO, 11 GBPS COM A FUNCIONALIDADE DE FIREWALL HABILITADA, INDEPENDENTEMENTE DO TAMANHO DO PACOTE 1.1.2. SUPORTE A, NO MÍNIMO, 3.000.000 CONEXÕES SIMULTÂNEAS 1.1.3. SUPORTE A, NO MÍNIMO, 280.000 NOVAS CONEXÕES POR SEGUNDO 1.1.4. THROUGHPUT DE, NO MÍNIMO, 13 GBPS DE VPN IPSEC 1.1.5. ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, 2.500 TÚNEIS DE VPN IPSEC SITE-TO-SITE SIMULTÂNEOS 1.1.6. ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, 15.000 TÚNEIS DE CLIENTES VPN IPSEC SIMULTÂNEOS 1.1.7. THROUGHPUT DE, NO MÍNIMO, 2 GBPS DE VPN SSL 1.1.8. SUPORTE A, NO MÍNIMO, 500 CLIENTES DE VPN SSL SIMULTÂNEOS 1.1.9. SUPORTE A, NO MÍNIMO, 13 GBPS DE THROUGHPUT DE APPLICATION CONTROL 1.1.10. SUPORTAR NO MÍNIMO 4 GBPS DE THROUGHPUT DE INSPEÇÃO SSL 1.1.11. THROUGHPUT DE, NO MÍNIMO 3 GBPS COM AS SEGUINTE FUNCIONALIDADES HABILITADAS SIMULTANEAMENTE PARA TODAS AS ASSINATURAS QUE A PLATAFORMA DE SEGURANÇA POSSUIR DEVIDAMENTE ATIVADAS E ATUANTES: CONTROLE DE APLICAÇÃO, IPS, ANTIVÍRUS E ANTISPYWARE. 1.1.12. CASO O FABRICANTE DIVULGUE MÚLTIPLOS NÚMEROS DE DESEMPENHO PARA QUALQUER UMA DESTAS FUNCIONALIDADES, SOMENTE O DE MENOR VALOR SERÁ ACEITO; 1.1.13. DEVE POSSUIR AO MENOS 4 INTERFACES 10 GE SFP+ 1.1.14. DEVE POSSUIR AO MENOS 16 INTERFACES 1 GE RJ-45 1.1.15. DEVE POSSUIR AO MENOS 8 INTERFACES 1 GE SFP 1.1.16. ESTAR LICENCIADO E/OU TER INCLUÍDO SEM CUSTO ADICIONAL, NO MÍNIMO, 10	FORTINET FORTIGATE -201F	R\$ 154.440,60	R\$ 308.881,20



## Prefeitura Municipal de Lagoa Santa

		<p>SISTEMAS VIRTUAIS LÓGICOS (CONTEXTOS) POR APPLIANCE 1.1.17. DEVE POSSUIR AO MENOS 1 DISCOS RÍGIDOS DE NO MÍNIMO 480GB SSD</p> <p>1.1.18. CONDIÇÕES OPERACIONAIS: 1.1.18.1. ALIMENTAÇÃO DUAL / TENSÃO DE 100-240 VAC 1.1.18.2. ALIMENTAÇÃO DUAL / FREQUÊNCIA DE 50/60 HZ 1.1.18.3. TEMPERATURA - FAIXA DE OPERAÇÃO DE 0º A 40º C 1.1.18.4. DEVE POSSUIR FONTE DE ALIMENTAÇÃO REDUNDANTE. 1.2. CARACTERÍSTICAS GERAIS 1.2.1. A SOLUÇÃO DEVE CONSISTIR EM PLATAFORMA DE PROTEÇÃO DE REDE BASEADA EM APPLIANCE COM FUNCIONALIDADES DE NEXT GENERATION FIREWALL (NGFW), E CONSOLE DE GERÊNCIA E MONITORAÇÃO; 1.2.2. POR FUNCIONALIDADES DE NGFW ENTENDE-SE: RECONHECIMENTO DE APLICAÇÕES, PREVENÇÃO DE AMEAÇAS, IDENTIFICAÇÃO DE USUÁRIOS E CONTROLE GRANULAR DE PERMISSÕES; 1.2.3. AS FUNCIONALIDADES DE PROTEÇÃO DE REDE QUE COMPÕE A PLATAFORMA DE SEGURANÇA, PODEM FUNCIONAR EM MÚLTIPLOS APPLIANCES DESDE QUE OBEDEÇAM A TODOS OS REQUISITOS DESTA ESPECIFICAÇÃO; 1.2.4. A PLATAFORMA DEVE SER OTIMIZADA PARA ANÁLISE DE CONTEÚDO DE APLICAÇÕES EM CAMADA 7; 1.2.5. O GERENCIAMENTO DA SOLUÇÃO DEVE SUPOORTAR ACESSO VIA SSH, CLIENTE OU WEB (HTTPS) E API ABERTA; 1.2.6. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A 4094 VLAN TAGS 802.1Q; 1.2.7. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A POLICY BASED ROUTING OU POLICY BASED FORWARDING; 1.2.8. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A ROTEAMENTO MULTICAST (PIM-SM E PIM-DM); 1.2.9. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A DHCP RELAY; 1.2.10. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A DHCP SERVER; 1.2.11. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A JUMBO FRAMES; 1.2.12. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM SUPOORTAR SUB-INTERFACES ETHERNET LÓGICAS 1.2.13. DEVE SUPOORTAR NAT DINÂMICO (MANY-TO-MANY); 1.2.14. DEVE SUPOORTAR NAT ESTÁTICO (1-TO-1); 1.2.15. DEVE SUPOORTAR NAT ESTÁTICO BIDIRECIONAL 1-TO-1; 1.2.16. DEVE SUPOORTAR TRADUÇÃO DE PORTA (PAT); 1.2.17. DEVE SUPOORTAR NAT DE ORIGEM; 1.2.18. DEVE SUPOORTAR NAT DE DESTINO; 1.2.19. DEVE SUPOORTAR NAT DE ORIGEM E NAT DE DESTINO SIMULTANEAMENTE; 1.2.20. DEVE IMPLEMENTAR NETWORK PREFIX TRANSLATION (NPTV6) OU NAT66, PREVENINDO PROBLEMAS DE ROTEAMENTO ASSIMÉTRICO; 1.2.21. DEVE SUPOORTAR NAT64 E NAT46; 1.2.22. DEVE IMPLEMENTAR O PROTOCOLO ECMP; 1.2.23. DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM; 1.2.24. DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM E DESTINO; 1.2.25. DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR</p>			
--	--	---	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>PESO. NESTA OPÇÃO DEVE SER POSSÍVEL DEFINIR O PERCENTUAL DE TRÁFEGO QUE SERÁ ESCOADO POR CADA UM DOS LINKS. DEVE SUPOSTAR O BALANCEAMENTO DE, NO MÍNIMO, TRÊS LINKS; 1.2.26. DEVE IMPLEMENTAR BALANCEAMENTO DE LINKS SEM A NECESSIDADE DE CRIAÇÃO DE ZONAS OU USO DE INSTÂNCIAS VIRTUAIS 1.2.27. A SOLUÇÃO DEVE PROVER RECURSOS DE ROTEAMENTO INTELIGENTE, DEFININDO, MEDIANTE REGRAS PRÉ-ESTABELECIDAS, O MELHOR CAMINHO A SER TOMADO PARA UM APLICAÇÃO; 1.2.28. A SOLUÇÃO DEVERÁ SER CAPAZ DE MONITORAR E IDENTIFICAR FALHAS MEDIANTE A ASSOCIAÇÃO DE HEALTH CHECK, PERMITINDO TESTES DE RESPOSTA POR PING, HTTP, TCP/UDP ECHO E TWAMP; 1.2.29. DEVERÁ SER PERMITIDA A CRIAÇÃO DE POLÍTICAS DE ROTEAMENTO COM BASE NOS SEGUINTE CRITÉRIOS: LATÊNCIA, JITTER, PERDA DE PACOTE, BANDA OCUPADA OU TODOS AO MESMO TEMPO; 1.2.30. DIVERSAS FORMAS DE ESCOLHA DO LINK DEVEM ESTAR PRESENTES, INCLUINDO: MELHOR LINK, MENOR CUSTO E DEFINIÇÃO DE NÍVEIS MÁXIMOS DE QUALIDADE A SEREM ACEITOS PARA QUE TAIS LINKS POSSAM SER UTILIZADOS EM UM DETERMINADO ROTEAMENTO DE APLICAÇÃO; 1.2.31. A SOLUÇÃO DEVE PROVER ESTATÍSTICAS EM TEMPO REAL A RESPEITO DA OCUPAÇÃO DE BANDA (UPLOAD E DOWNLOAD) E PERFORMANCE DO HEALTH CHECK (PACKET LOSS, JITTER E LATÊNCIA); 1.2.32. ALÉM DE POSSIBILITAR A DEFINIÇÃO DE BANDA MÁXIMA E GARANTIDA POR APLICAÇÃO, DEVE TAMBÉM SUPOSTAR O MATCH EM CATEGORIAS DE URL, IPS DE ORIGEM E DESTINO, LOGINS E PORTAS; 1.2.33. DEVE POSSIBILITAR ROTEAMENTO DISTINTO A DEPENDER DO GRUPO DE USUÁRIO SELECIONADO NA REGRA DE ROTEAMENTO; 1.2.34. DEVE PERMITIR MONITORAR VIA SNMP FALHAS DE HARDWARE, MONITORAMENTO DE CPU E MEMÓRIA, DE SEGURANÇA E INTERFACE. 1.2.35. ENVIAR LOG PARA SISTEMAS DE MONITORAÇÃO EXTERNOS, SIMULTANEAMENTE; 1.2.36. DEVE HAVER A OPÇÃO DE ENVIAR LOGS PARA OS SISTEMAS DE MONITORAÇÃO EXTERNOS VIA PROTOCOLO TCP E SSL; 1.2.37. PROTEÇÃO ANTI-SPOOFING; 1.2.38. PARA IPV4, DEVE SUPOSTAR ROTEAMENTO ESTÁTICO E DINÂMICO (RIPV2, BGP E OSPFV2); 1.2.39. PARA IPV6, DEVE SUPOSTAR ROTEAMENTO ESTÁTICO E DINÂMICO (OSPFV3); 1.2.40. SUPOSTAR OSPF GRACEFUL RESTART; 1.2.41. DEVE SUPOSTAR MODO SNIFFER, PARA INSPEÇÃO VIA PORTA ESPELHADA DO TRÁFEGO DE DADOS DA REDE; 1.2.42. DEVE SUPOSTAR MODO CAMADA - 2 (L2), PARA INSPEÇÃO DE DADOS EM LINHA E VISIBILIDADE DO TRÁFEGO; 1.2.43. DEVE SUPOSTAR MODO CAMADA - 3 (L3), PARA INSPEÇÃO DE DADOS EM LINHA VISIBILIDADE DO TRÁFEGO; 1.2.44. SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM MODO TRANSPARENTE; 1.2.45. SUPORTE A CONFIGURAÇÃO DE ALTA</p>			
--	--	---	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM LAYER 3; 1.2.46. SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM LAYER 3 E COM NO MÍNIMO 3 EQUIPAMENTOS NO CLUSTER; 1.2.47. A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: SESSÕES; 1.2.48. A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: CONFIGURAÇÕES, INCLUINDO, MAS NÃO LIMITADO AS POLÍTICAS DE FIREWALL, NAT, QOS E OBJETOS DE REDE; 1.2.49. A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: ASSOCIAÇÕES DE SEGURANÇA DAS VPNS; 1.2.50. A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR:TABELAS FIB; 1.2.51. O HA (MODO DE ALTA-DISPONIBILIDADE) DEVE POSSIBILITAR MONITORAÇÃO DE FALHA DE LINK; 1.2.52. DEVE POSSUIR SUPORTE A CRIAÇÃO DE SISTEMAS VIRTUAIS NO MESMO APPLIANCE; 1.2.53. EM ALTA DISPONIBILIDADE, DEVE SER POSSÍVEL O USO DE CLUSTERS VIRTUAIS, SEJA ATIVO-ATIVO OU ATIVO-PASSIVO, PERMITINDO A DISTRIBUIÇÃO DE CARGA ENTRE DIFERENTES CONTEXTOS; 1.2.54. DEVE PERMITIR A CRIAÇÃO DE ADMINISTRADORES INDEPENDENTES, PARA CADA UM DOS SISTEMAS VIRTUAIS EXISTENTES, DE MANEIRA A POSSIBILITAR A CRIAÇÃO DE CONTEXTOS VIRTUAIS QUE PODEM SER ADMINISTRADOS POR EQUIPES DISTINTAS; 1.2.55. CONTROLE, INSPEÇÃO E DESCRIPTOGRAFIA DE SSL PARA TRÁFEGO DE ENTRADA (INBOUND) E SAÍDA (OUTBOUND), SENDO QUE DEVE SUPORTAR O CONTROLE DOS CERTIFICADOS INDIVIDUALMENTE DENTRO DE CADA SISTEMA VIRTUAL, OU SEJA, ISOLAMENTO DAS OPERAÇÕES DE ADIÇÃO, REMOÇÃO E UTILIZAÇÃO DOS CERTIFICADOS DIRETAMENTE NOS SISTEMAS VIRTUAIS (CONTEXTOS); 1.2.56. CONTROLE POR POLÍTICA DE FIREWALL 1.2.57. DEVERÁ SUPORTAR CONTROLES POR ZONA DE SEGURANÇA 1.2.58. CONTROLES DE POLÍTICAS POR PORTA E PROTOCOLO 1.2.59. CONTROLE DE POLÍTICAS POR APLICAÇÕES, GRUPOS ESTÁTICOS DE APLICAÇÕES, GRUPOS DINÂMICOS DE APLICAÇÕES (BASEADOS EM CARACTERÍSTICAS E COMPORTAMENTO DAS APLICAÇÕES) E CATEGORIAS DE APLICAÇÕES 1.2.60. CONTROLE DE POLÍTICAS POR USUÁRIOS, GRUPOS DE USUÁRIOS, IPS, REDES E ZONAS DE SEGURANÇA 1.2.61. CONTROLE DE POLÍTICAS POR CÓDIGO DE PAÍS (POR EXEMPLO: BR, USA, UK, RUS) 1.2.62. CONTROLE, INSPEÇÃO E DESCRIPTOGRAFIA DE SSL POR POLÍTICA PARA TRÁFEGO DE ENTRADA (INBOUND) E SAÍDA (OUTBOUND) 1.2.63. DEVE SUPORTAR OFFLOAD DE CERTIFICADO EM INSPEÇÃO DE CONEXÕES SSL DE ENTRADA (INBOUND); 1.2.64. DEVE DESCRIPTOGRAFAR TRÁFEGO INBOUND E OUTBOUND EM CONEXÕES NEGOCIADAS COM TLS 1.2; 1.2.65. CONTROLE DE INSPEÇÃO E DESCRIPTOGRAFIA DE SSH POR POLÍTICA; 1.2.66. DEVE PERMITIR O BLOQUEIO DE ARQUIVO POR SUA EXTENSÃO E POSSIBILITAR A CORRETA</p>			
--	--	---	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>IDENTIFICAÇÃO DO ARQUIVO POR SEU TIPO MESMO QUANDO SUA EXTENSÃO FOR RENOMEADA; 1.2.67. TRAFFIC SHAPING QOS BASEADO EM POLÍTICAS (PRIORIDADE, GARANTIA E MÁXIMO); 1.2.68. QOS BASEADO EM POLÍTICAS PARA MARCAÇÃO DE PACOTES (DIFFSERV MARKING), INCLUSIVE POR APLICAÇÕES; 1.2.69. SUPORTE A OBJETOS E REGRAS IPV6; 1.2.70. SUPORTE A OBJETOS E REGRAS MULTICAST; 1.2.71. DEVE SUPOSTAR NO MÍNIMO DOIS TIPOS DE RESPOSTA NAS POLÍTICAS DE FIREWALL: DROP SEM NOTIFICAÇÃO DO BLOQUEIO AO USUÁRIO, DROP COM NOTIFICAÇÃO DO BLOQUEIO AO USUÁRIO, DROP COM OPÇÃO DE ENVIO DE ICMP UNREACHABLE PARA MÁQUINA DE ORIGEM DO TRÁFEGO, TCP-RESET PARA O CLIENT, TCP-RESET PARA O SERVER OU PARA OS DOIS LADOS DA CONEXÃO; 1.2.72. SUPORTAR A ATRIBUIÇÃO DE AGENDAMENTO DAS POLÍTICAS COM O OBJETIVO DE HABILITAR E DESABILITAR POLÍTICAS EM HORÁRIOS PRÉ-DEFINIDOS AUTOMATICAMENTE; 1.3. CONTROLE DE APLICAÇÕES 1.3.1. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVERÃO POSSUIR A CAPACIDADE DE RECONHECER APLICAÇÕES, INDEPENDENTE DE PORTA E PROTOCOLO 1.3.2. DEVE SER POSSÍVEL A LIBERAÇÃO E BLOQUEIO SOMENTE DE APLICAÇÕES SEM A NECESSIDADE DE LIBERAÇÃO DE PORTAS E PROTOCOLOS 1.3.3. RECONHECER PELO MENOS 1700 APLICAÇÕES DIFERENTES, INCLUINDO, MAS NÃO LIMITADO: A TRÁFEGO RELACIONADO A PEER-TO-PEER, REDES SOCIAIS, ACESSO REMOTO, UPDATE DE SOFTWARE, PROTOCOLOS DE REDE, VOIP, ÁUDIO, VÍDEO, PROXY, MENSAGEIROS INSTANTÂNEOS, COMPARTILHAMENTO DE ARQUIVOS, E-MAIL; 1.3.4. RECONHECER PELO MENOS AS SEGUINTE APLICAÇÕES: BITTORRENT, GNUTELLA, SKYPE, FACEBOOK, LINKED-IN, TWITTER, CITRIX, LOGMEIN, TEAMVIEWER, MS-RDP, VNC, GMAIL, YOUTUBE, HTTP-PROXY, HTTP-TUNNEL, FACEBOOK CHAT, GMAIL CHAT, WHATSAPP, 4SHARED, DROPBOX, GOOGLE DRIVE, SKYDRIVE, DB2, MYSQL, ORACLE, ACTIVE DIRECTORY, KERBEROS, LDAP, RADIUS, ITUNES, DHCP, FTP, DNS, WINS, MSRPC, NTP, SNMP, RPC OVER HTTP, GOTOMEETING, WEBEX, EVERNOTE, GOOGLE-DOCS; 1.3.5. DEVE INSPECIONAR O PAYLOAD DE PACOTE DE DADOS COM O OBJETIVO DE DETECTAR ASSINATURAS DE APLICAÇÕES CONHECIDAS PELO FABRICANTE INDEPENDENTE DE PORTA E PROTOCOLO; 1.3.6. IDENTIFICAR O USO DE TÁTICAS EVASIVAS, OU SEJA, DEVE TER A CAPACIDADE DE VISUALIZAR E CONTROLAR AS APLICAÇÕES E OS ATAQUES QUE UTILIZAM TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS, TAIS COMO SKYPE E UTILIZAÇÃO DA REDE TOR 1.3.7. PARA TRÁFEGO CRIPTOGRAFADO SSL, DEVE DE-CRIPTOGRAFAR PACOTES A FIM DE POSSIBILITAR A LEITURA DE PAYLOAD PARA CHECAGEM DE ASSINATURAS DE APLICAÇÕES CONHECIDAS PELO FABRICANTE; 1.3.8. DEVE REALIZAR DECODIFICAÇÃO DE PROTOCOLOS COM O OBJETIVO DE DETECTAR</p>		
--	--	---	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>APLICAÇÕES ENCAPSULADAS DENTRO DO PROTOCOLO E VALIDAR SE O TRÁFEGO CORRESPONDE COM A ESPECIFICAÇÃO DO PROTOCOLO, INCLUINDO, MAS NÃO LIMITADO A YAHOO INSTANT MESSENGER USANDO HTTP. A DECODIFICAÇÃO DE PROTOCOLO TAMBÉM DEVE IDENTIFICAR FUNCIONALIDADES ESPECIFICAS DENTRO DE UMA APLICAÇÃO, INCLUINDO, MAS NÃO LIMITADO A COMPARTILHAMENTO DE ARQUIVO DENTRO DO WEBEX 1.3.9. IDENTIFICAR O USO DE TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS; 1.3.10. ATUALIZAR A BASE DE ASSINATURAS DE APLICAÇÕES AUTOMATICAMENTE; 1.3.11. LIMITAR A BANDA (DOWNLOAD/UPLOAD) USADA POR APLICAÇÕES (TRAFFIC SHAPING), BASEADO NO IP DE ORIGEM, USUÁRIOS E GRUPOS; 1.3.12. OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR A CAPACIDADE DE IDENTIFICAR O USUÁRIO DE REDE COM INTEGRAÇÃO AO MICROSOFT ACTIVE DIRECTORY, SEM A NECESSIDADE DE INSTALAÇÃO DE AGENTE NO DOMAIN CONTROLLER, NEM NAS ESTAÇÕES DOS USUÁRIOS; 1.3.13. DEVE SER POSSÍVEL ADICIONAR CONTROLE DE APLICAÇÕES EM MÚLTIPLAS REGRAS DE SEGURANÇA DO DISPOSITIVO, OU SEJA, NÃO SE LIMITANDO SOMENTE A POSSIBILIDADE DE HABILITAR CONTROLE DE APLICAÇÕES EM ALGUMAS REGRAS; 1.3.14. DEVE SUPORTAR MÚLTIPLOS MÉTODOS DE IDENTIFICAÇÃO E CLASSIFICAÇÃO DAS APLICAÇÕES, POR PELO MENOS CHECAGEM DE ASSINATURAS E DECODIFICAÇÃO DE PROTOCOLOS; 1.3.15. PARA MANTER A SEGURANÇA DA REDE EFICIENTE, DEVE SUPORTAR O CONTROLE SOBRE APLICAÇÕES DESCONHECIDAS E NÃO SOMENTE SOBRE APLICAÇÕES CONHECIDAS; 1.3.16. PERMITIR NATIVAMENTE A CRIAÇÃO DE ASSINATURAS PERSONALIZADAS PARA RECONHECIMENTO DE APLICAÇÕES PROPRIETÁRIAS NA PRÓPRIA INTERFACE GRÁFICA DA SOLUÇÃO, SEM A NECESSIDADE DE AÇÃO DO FABRICANTE 1.3.17. A CRIAÇÃO DE ASSINATURAS PERSONALIZADAS DEVE PERMITIR O USO DE EXPRESSÕES REGULARES, CONTEXTO (SESSÕES OU TRANSAÇÕES), USANDO POSIÇÃO NO PAYLOAD DOS PACOTES TCP E UDP E USANDO DECODERS DE PELO MENOS OS SEGUINTE PROTOCOLOS: HTTP, FTP, NBSS, DCE RPC, SMTP, TELNET, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP E SSL 1.3.18. O FABRICANTE DEVE PERMITIR A SOLICITAÇÃO DE INCLUSÃO DE APLICAÇÕES NA BASE DE ASSINATURAS DE APLICAÇÕES; 1.3.19. DEVE ALERTAR O USUÁRIO QUANDO UMA APLICAÇÃO FOR BLOQUEADA; 1.3.20. DEVE POSSIBILITAR A DIFERENCIAÇÃO DE TRÁFEGOS PEER2PEER (BITTORRENT, EMULE, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS; 1.3.21. DEVE POSSIBILITAR A DIFERENCIAÇÃO DE TRÁFEGOS DE INSTANT MESSAGING (AIM, HANGOUTS, FACEBOOK CHAT, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS; 1.3.22.</p>			
--	--	--	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>DEVE POSSIBILITAR A DIFERENCIAÇÃO E CONTROLE DE PARTES DAS APLICAÇÕES COMO POR EXEMPLO PERMITIR O HANGOUTS CHAT E BLOQUEAR A CHAMADA DE VÍDEO; 1.3.23. DEVE POSSIBILITAR A DIFERENCIAÇÃO DE APLICAÇÕES PROXIES (PSIPHON, FREEGATE, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS; 1.3.24. DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS DINÂMICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: TECNOLOGIA UTILIZADA NAS APLICAÇÕES (CLIENT-SERVER, BROWSE BASED, NETWORK PROTOCOL, ETC) 1.3.25. DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS DINÂMICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: NÍVEL DE RISCO DA APLICAÇÃO 1.3.26. DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS ESTÁTICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: CATEGORIA DA APLICAÇÃO 1.4. PREVENÇÃO DE AMEAÇAS 1.4.1. PARA PROTEÇÃO DO AMBIENTE CONTRA-ATAQUES, OS DISPOSITIVOS DE PROTEÇÃO DEVEM POSSUIR MÓDULO DE IPS, ANTIVÍRUS E ANTI-SPYWARE INTEGRADOS NO PRÓPRIO APPLIANCE DE FIREWALL; 1.4.2. DEVE INCLUIR ASSINATURAS DE PREVENÇÃO DE INTRUSÃO (IPS) E BLOQUEIO DE ARQUIVOS MALICIOSOS (ANTIVÍRUS E ANTI-SPYWARE); 1.4.3. AS FUNCIONALIDADES DE IPS, ANTIVÍRUS E ANTI-SPYWARE DEVEM OPERAR EM CARÁTER PERMANENTE, PODENDO SER UTILIZADAS POR TEMPO INDETERMINADO, MESMO QUE NÃO SUBSISTA O DIREITO DE RECEBER ATUALIZAÇÕES OU QUE NÃO HAJA CONTRATO DE GARANTIA DE SOFTWARE COM O FABRICANTE; 1.4.4. DEVE SINCRONIZAR AS ASSINATURAS DE IPS, ANTIVÍRUS, ANTI-SPYWARE QUANDO IMPLEMENTADO EM ALTA DISPONIBILIDADE; 1.4.5. DEVE IMPLEMENTAR OS SEGUINTE TIPOS DE AÇÕES PARA AMEAÇAS DETECTADAS PELO IPS: PERMITIR, PERMITIR E GERAR LOG, BLOQUEAR, BLOQUEAR IP DO ATACANTE POR UM INTERVALO DE TEMPO E ENVIAR TCP-RESET; 1.4.6. AS ASSINATURAS DEVEM PODER SER ATIVADAS OU DESATIVADAS, OU AINDA HABILITADAS APENAS EM MODO DE MONITORAÇÃO; 1.4.7. DEVE SER POSSÍVEL A CRIAÇÃO DE POLÍTICAS POR USUÁRIOS, GRUPOS DE USUÁRIOS, IPS, REDES OU ZONAS DE SEGURANÇA; 1.4.8. EXCEÇÕES POR IP DE ORIGEM OU DE DESTINO DEVEM SER POSSÍVEIS NAS REGRAS OU ASSINATURA A ASSINATURA; 1.4.9. DEVE SUPORTAR GRANULARIDADE NAS POLÍTICAS DE IPS, ANTIVÍRUS E ANTI-SPYWARE, POSSIBILITANDO A CRIAÇÃO DE DIFERENTES POLÍTICAS POR ZONA DE SEGURANÇA, ENDEREÇO DE ORIGEM, ENDEREÇO DE DESTINO, SERVIÇO E A COMBINAÇÃO DE TODOS ESSES ITENS 1.4.10. DEVE PERMITIR O BLOQUEIO DE VULNERABILIDADES 1.4.11. DEVE PERMITIR O BLOQUEIO DE EXPLOITS CONHECIDOS 1.4.12. DEVE INCLUIR PROTEÇÃO CONTRA-ATAQUES DE NEGAÇÃO DE SERVIÇOS 1.4.13. DEVERÁ POSSUIR</p>			
--	--	---	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: ANÁLISE DE PADRÕES DE ESTADO DE CONEXÕES; 1.4.14. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: ANÁLISE DE DECODIFICAÇÃO DE PROTOCOLO; 1.4.15. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: ANÁLISE PARA DETECÇÃO DE ANOMALIAS DE PROTOCOLO; 1.4.16. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: ANÁLISE HEURÍSTICA; 1.4.17. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: IP DEFRAGMENTATION; 1.4.18. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: REMONTAGEM DE PACOTES DE TCP; 1.4.19. DEVERÁ POSSUIR O SEGUINTE MECANISMO DE INSPEÇÃO DE IPS: BLOQUEIO DE PACOTES MALFORMADOS 1.4.20. SER IMUNE E CAPAZ DE IMPEDIR ATAQUES BÁSICOS COMO: SYN FLOOD, ICMP FLOOD, UDP FLOOD, ETC; 1.4.21. DETECTAR E BLOQUEAR A ORIGEM DE PORTSCANS; 1.4.22. BLOQUEAR ATAQUES EFETUADOS POR WORMS CONHECIDOS; 1.4.23. POSSUIR ASSINATURAS ESPECÍFICAS PARA A MITIGAÇÃO DE ATAQUES DOS E DDOS; 1.4.24. POSSUIR ASSINATURAS PARA BLOQUEIO DE ATAQUES DE BUFFER OVERFLOW; 1.4.25. DEVERÁ POSSIBILITAR A CRIAÇÃO DE ASSINATURAS CUSTOMIZADAS PELA INTERFACE GRÁFICA DO PRODUTO; 1.4.26. DEVE PERMITIR USAR OPERADORES DE NEGAÇÃO NA CRIAÇÃO DE ASSINATURAS CUSTOMIZADAS DE IPS OU ANTI-SPYWARE, PERMITINDO A CRIAÇÃO DE EXCEÇÕES COM GRANULARIDADE NAS CONFIGURAÇÕES; 1.4.27. PERMITIR O BLOQUEIO DE VÍRUS E SPYWARES EM, PELO MENOS, OS SEGUINTE PROTOCOLOS: HTTP, FTP, SMB, SMTP E POP3; 1.4.28. IDENTIFICAR E BLOQUEAR COMUNICAÇÃO COM BOTNETS; 1.4.29. REGISTRAR NA CONSOLE DE MONITORAÇÃO AS SEGUINTE INFORMAÇÕES SOBRE AMEAÇAS IDENTIFICADAS: O NOME DA ASSINATURA OU DO ATAQUE, APLICAÇÃO, USUÁRIO, ORIGEM E O DESTINO DA COMUNICAÇÃO, ALÉM DA AÇÃO TOMADA PELO DISPOSITIVO; 1.4.30. DEVE SUPORTAR A CAPTURA DE PACOTES (PCAP), POR ASSINATURA DE IPS OU POR FILTRO PRÉ-DEFINIDO; 1.4.31. DEVE POSSUIR A FUNÇÃO DE PROTEÇÃO A RESOLUÇÃO DE ENDEREÇOS VIA DNS, IDENTIFICANDO REQUISIÇÕES DE RESOLUÇÃO DE NOME PARA DOMÍNIOS MALICIOSOS DE BOTNETS CONHECIDAS; 1.4.32. OS EVENTOS DEVEM IDENTIFICAR O PAÍS DE ONDE PARTIU A AMEAÇA; 1.4.33. DEVE INCLUIR PROTEÇÃO CONTRA VÍRUS EM CONTEÚDO HTML E JAVASCRIPT, SOFTWARE ESPÍÃO (SPYWARE) E WORMS 1.4.34. POSSUIR PROTEÇÃO CONTRA DOWNLOADS INVOLUNTÁRIOS USANDO HTTP DE ARQUIVOS EXECUTÁVEIS E MALICIOSOS 1.4.35. DEVE SER POSSÍVEL A CONFIGURAÇÃO DE DIFERENTES POLÍTICAS DE CONTROLE DE AMEAÇAS E ATAQUES BASEADO EM POLÍTICAS DO FIREWALL CONSIDERANDO USUÁRIOS, GRUPOS DE USUÁRIOS, ORIGEM, DESTINO, ZONAS DE SEGURANÇA, ETC, OU SEJA, CADA</p>		
--	--	---	--	--





## Prefeitura Municipal de Lagoa Santa

		<p>POLÍTICA DE FIREWALL PODERÁ TER UMA CONFIGURAÇÃO DIFERENTES DE IPS, SENDO ESSAS POLÍTICAS POR USUÁRIOS, GRUPOS DE USUÁRIO, ORIGEM, DESTINO, ZONAS DE SEGURANÇA 1.5. FILTRO DE URL 1.5.1. PERMITE ESPECIFICAR POLÍTICA POR TEMPO, OU SEJA, A DEFINIÇÃO DE REGRAS PARA UM DETERMINADO HORÁRIO OU PERÍODO (DIA, MÊS, ANO, DIA DA SEMANA E HORA); 1.5.2. DEVE SER POSSÍVEL A CRIAÇÃO DE POLÍTICAS POR USUÁRIOS, GRUPOS DE USUÁRIOS, IPS, REDES OU ZONAS DE SEGURANÇA; 1.5.3. DEVE POSSUIR A CAPACIDADE DE CRIAÇÃO DE POLÍTICAS BASEADAS NA VISIBILIDADE E CONTROLE DE QUEM ESTÁ UTILIZANDO QUAIS URLS ATRAVÉS DA INTEGRAÇÃO COM SERVIÇOS DE DIRETÓRIO, ACTIVE DIRECTORY E BASE DE DADOS LOCAL; 1.5.4. SUPORTAR A CAPACIDADE DE CRIAÇÃO DE POLÍTICAS BASEADAS NO CONTROLE POR URL E CATEGORIA DE URL; 1.5.5. POSSUIR PELO MENOS 60 CATEGORIAS DE URLS; 1.5.6. DEVE POSSUIR A FUNÇÃO DE EXCLUSÃO DE URLS DO BLOQUEIO, POR CATEGORIA; 1.5.7. PERMITIR A CUSTOMIZAÇÃO DE PÁGINA DE BLOQUEIO; 1.5.8. PERMITIR O BLOQUEIO E CONTINUAÇÃO (POSSIBILITANDO QUE O USUÁRIO ACESSE UM SITE POTENCIALMENTE BLOQUEADO INFORMANDO O MESMO NA TELA DE BLOQUEIO E POSSIBILITANDO A UTILIZAÇÃO DE UM BOTÃO CONTINUAR PARA PERMITIR O USUÁRIO CONTINUAR ACESSANDO O SITE); 1.6. IDENTIFICAÇÃO DE USUÁRIOS 1.6.1. DEVE INCLUIR A CAPACIDADE DE CRIAÇÃO DE POLÍTICAS BASEADAS NA VISIBILIDADE E CONTROLE DE QUEM ESTÁ UTILIZANDO QUAIS APLICAÇÕES ATRAVÉS DA INTEGRAÇÃO COM SERVIÇOS DE DIRETÓRIO, AUTENTICAÇÃO VIA LDAP, ACTIVE DIRECTORY, E-DIRECTORY E BASE DE DADOS LOCAL; 1.6.2. DEVE POSSUIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS; 1.6.3. DEVE POSSUIR INTEGRAÇÃO E SUPORTE A MICROSOFT ACTIVE DIRECTORY PARA OS SEGUINTE SISTEMAS OPERACIONAIS: WINDOWS SERVER 2008, WINDOWS SERVER 2008 R2, WINDOWS SERVER 2012 E WINDOWS SERVER 2012 R2; 1.6.4. DEVE POSSUIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS, SUPORTANDO SINGLE SIGN-ON. ESSA FUNCIONALIDADE NÃO DEVE POSSUIR LIMITES LICENCIADOS DE USUÁRIOS OU QUALQUER TIPO DE RESTRIÇÃO DE USO COMO, MAS NÃO LIMITADO À UTILIZAÇÃO DE SISTEMAS VIRTUAIS, SEGMENTOS DE REDE, ETC; 1.6.5. DEVE POSSUIR INTEGRAÇÃO COM RADIUS PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS; 1.6.6. DEVE POSSUIR</p>			
--	--	--	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>INTEGRAÇÃO COM LDAP PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS; 1.6.7. DEVE PERMITIR O CONTROLE, SEM INSTALAÇÃO DE CLIENTE DE SOFTWARE, EM EQUIPAMENTOS QUE SOLICITEM SAÍDA A INTERNET PARA QUE ANTES DE INICIAR A NAVEGAÇÃO, EXPANDA-SE UM PORTAL DE AUTENTICAÇÃO RESIDENTE NO FIREWALL (CAPTIVE PORTAL); 1.6.8. DEVE POSSUIR SUPORTE A IDENTIFICAÇÃO DE MÚLTIPLOS USUÁRIOS CONECTADOS EM UM MESMO ENDEREÇO IP EM AMBIENTES CITRIX E MICROSOFT TERMINAL SERVER, PERMITINDO VISIBILIDADE E CONTROLE GRANULAR POR USUÁRIO SOBRE O USO DAS APLICAÇÕES QUE ESTÃO NESTES SERVIÇOS; 1.6.9. DEVE IMPLEMENTAR A CRIAÇÃO DE GRUPOS CUSTOMIZADOS DE USUÁRIOS NO FIREWALL, BASEADO EM ATRIBUTOS DO LDAP/AD; 1.6.10. PERMITIR INTEGRAÇÃO COM TOKENS PARA AUTENTICAÇÃO DOS USUÁRIOS, INCLUINDO, MAS NÃO LIMITADO A ACESSO A INTERNET E GERENCIAMENTO DA SOLUÇÃO 1.6.11. PROVER NO MÍNIMO UM TOKEN NATIVAMENTE, POSSIBILITANDO AUTENTICAÇÃO DE DUPLO FATOR 1.7. QOS E TRAFFIC SHAPING 1.7.1. COM A FINALIDADE DE CONTROLAR APLICAÇÕES E TRÁFEGO CUJO CONSUMO POSSA SER EXCESSIVO, (COMO YOUTUBE, USTREAM, ETC) E TER UM ALTO CONSUMO DE LARGURA DE BANDA, SE REQUER QUE A SOLUÇÃO, ALÉM DE PODER PERMITIR OU NEGAR ESSE TIPO DE APLICAÇÕES, DEVE TER A CAPACIDADE DE CONTROLÁ-LAS POR POLÍTICAS DE MÁXIMO DE LARGURA DE BANDA QUANDO FOREM SOLICITADAS POR DIFERENTES USUÁRIOS OU APLICAÇÕES, TANTO DE ÁUDIO COMO DE VÍDEO STREAMING; 1.7.2. SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR ENDEREÇO DE ORIGEM; 1.7.3. SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR ENDEREÇO DE DESTINO; 1.7.4. SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR USUÁRIO E GRUPO; 1.7.5. SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR APLICAÇÕES; 1.7.6. SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR PORTA; 1.7.7. O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE TRÁFEGO COM BANDA GARANTIDA; 1.7.8. O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE TRÁFEGO COM BANDA MÁXIMA; 1.7.9. O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE FILA DE PRIORIDADE; 1.7.10. SUPORTAR PRIORIZAÇÃO EM TEMPO REAL DE PROTOCOLOS DE VOZ (VOIP) COMO H.323, SIP, SCCP, MGCP E APLICAÇÕES COMO SKYPE; 1.7.11. SUPORTAR MARCAÇÃO DE PACOTES DIFFSERV, INCLUSIVE POR APLICAÇÃO; 1.7.12. DISPONIBILIZAR ESTATÍSTICAS EM TEMPO REAL PARA CLASSES DE QOS OU TRAFFIC SHAPING; 1.8. FILTRO DE DADOS 1.8.1. PERMITIR IDENTIFICAR E OPCIONALMENTE PREVENIR A TRANSFERÊNCIA</p>			
--	--	---	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>DE VÁRIOS TIPOS DE ARQUIVOS (MS OFFICE, PDF, ETC) IDENTIFICADOS SOBRE APLICAÇÕES (HTTP, FTP, SMTP, ETC); 1.8.2. SUPORTAR IDENTIFICAÇÃO DE ARQUIVOS COMPACTADOS OU A APLICAÇÃO DE POLÍTICAS SOBRE O CONTEÚDO DESSES TIPOS DE ARQUIVOS; 1.8.3. SUPORTAR A IDENTIFICAÇÃO DE ARQUIVOS CRIPTOGRAFADOS E A APLICAÇÃO DE POLÍTICAS SOBRE O CONTEÚDO DESSES TIPOS DE ARQUIVOS; 1.8.4. PERMITIR IDENTIFICAR E OPCIONALMENTE PREVENIR A TRANSFERÊNCIA DE INFORMAÇÕES SENSÍVEIS, INCLUINDO, MAS NÃO LIMITADO A NÚMERO DE CARTÃO DE CRÉDITO, POSSIBILITANDO A CRIAÇÃO DE NOVOS TIPOS DE DADOS VIA EXPRESSÃO REGULAR; 1.9. GEOLOCALIZAÇÃO 1.9.1. SUPORTAR A CRIAÇÃO DE POLÍTICAS POR GEOLOCALIZAÇÃO, PERMITINDO O TRÁFEGO DE DETERMINADO PAIS/PAÍSES SEJAM BLOQUEADOS; 1.9.2. DEVE POSSIBILITAR A VISUALIZAÇÃO DOS PAÍSES DE ORIGEM E DESTINO NOS LOGS DOS ACESSOS; 1.9.3. DEVE POSSIBILITAR A CRIAÇÃO DE REGIÕES GEOGRÁFICAS PELA INTERFACE GRÁFICA E CRIAR POLÍTICAS UTILIZANDO AS MESMAS; 1.10. VPN 1.10.1. SUPORTAR VPN SITE-TO-SITE E CLIENTE-TO-SITE; 1.10.2. SUPORTAR IPSEC VPN; 1.10.3. SUPORTAR SSL VPN; 1.10.4. A VPN IPSEC DEVE SUPORTAR 3DES; 1.10.5. A VPN IPSEC DEVE SUPORTAR AUTENTICAÇÃO MD5 E SHA-1; 1.10.6. A VPN IPSEC DEVE SUPORTAR DIFFIE-HELLMAN GROUP 1, GROUP 2, GROUP 5 E GROUP 14; 1.10.7. A VPN IPSEC DEVE SUPORTAR ALGORITMO INTERNET KEY EXCHANGE (IKEV1 E V2); 1.10.8. A VPN IPSEC DEVE SUPORTAR AES 128, 192 E 256 (ADVANCED ENCRYPTION STANDARD); 1.10.9. A VPN IPSEC DEVE SUPORTAR AUTENTICAÇÃO VIA CERTIFICADO IKE PKI 1.10.10. DEVE POSSUIR INTEROPERABILIDADE COM OS SEGUINTE FABRICANTES: CISCO, CHECK POINT, JUNIPER, PALO ALTO NETWORKS, FORTINET, SONICWALL; 1.10.11. DEVE PERMITIR HABILITAR E DESABILITAR TÚNEIS DE VPN IPSEC A PARTIR DA INTERFACE GRÁFICA DA SOLUÇÃO, FACILITANDO O PROCESSO DE TROUBLESHOOTING; 1.10.12. A VPN SSL DEVE SUPORTAR O USUÁRIO REALIZAR A CONEXÃO POR MEIO DE CLIENTE INSTALADO NO SISTEMA OPERACIONAL DO EQUIPAMENTO OU POR MEIO DE INTERFACE WEB; 1.10.13. A FUNCIONALIDADES DE VPN SSL DEVEM SER ATENDIDAS COM OU SEM O USO DE AGENTE; 1.10.14. DEVE PERMITIR QUE TODO O TRÁFEGO DOS USUÁRIOS REMOTOS DE VPN SEJA ESCOADO PARA DENTRO DO TÚNEL DE VPN, IMPEDINDO COMUNICAÇÃO DIRETA COM DISPOSITIVOS LOCAIS COMO PROXIES; 1.10.15. ATRIBUIÇÃO DE DNS NOS CLIENTES REMOTOS DE VPN; 1.10.16. DEVER PERMITIR CRIAR POLÍTICAS DE CONTROLE DE APLICAÇÕES, IPS, ANTIVÍRUS, ANTIPYWARE E FILTRO DE URL PARA TRÁFEGO DOS CLIENTES REMOTOS CONECTADOS NA VPN SSL; 1.10.17. SUPORTAR AUTENTICAÇÃO VIA AD/LDAP, SECURE ID, CERTIFICADO E BASE DE USUÁRIOS LOCAL; 1.10.18. SUPORTAR LEITURA E VERIFICAÇÃO DE CRL (CERTIFICATE REVOCATION</p>			
--	--	--	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>LIST); 1.10.19. PERMITIR A APLICAÇÃO DE POLÍTICAS DE SEGURANÇA E VISIBILIDADE PARA AS APLICAÇÕES QUE CIRCULAM DENTRO DOS TÚNEIS SSL; 1.10.20. DEVE PERMITIR QUE A CONEXÃO COM A VPN SEJA ESTABELECIDAS DAS SEGUINTE FORMAS: ANTES DO USUÁRIO AUTENTICAR NA ESTAÇÃO; 1.10.21. DEVE PERMITIR QUE A CONEXÃO COM A VPN SEJA ESTABELECIDAS DAS SEGUINTE FORMAS: APÓS AUTENTICAÇÃO DO USUÁRIO NA ESTAÇÃO; 1.10.22. DEVE PERMITIR QUE A CONEXÃO COM A VPN SEJA ESTABELECIDAS DAS SEGUINTE FORMAS: SOB DEMANDA DO USUÁRIO; 1.10.23. DEVERÁ MANTER UMA CONEXÃO SEGURA COM O PORTAL DURANTE A SESSÃO; 1.10.24. O AGENTE DE VPN SSL OU IPSEC CLIENT-TO-SITE DEVE SER COMPATÍVEL COM PELO MENOS: WINDOWS 7 (32 E 64 BIT), WINDOWS 8 (32 E 64 BIT), WINDOWS 10 (32 E 64 BIT) E MAC OS X (V10.10 OU SUPERIOR);</p> <p>1.11. SUPORTE TÉCNICO E LICENCIAMENTO</p> <p>1.11.1. SUPORTE TÉCNICO DO FABRICANTE NA MODALIDADE 24X7H DURANTE 36 MESES; 1.11.2. A FUNCIONALIDADE CONTROLE DE APLICAÇÃO, IPS, GATEWAY ANTI-MALWARE, FILTRO DE CONTEÚDO WEB, ANTISPAM E O SUPORTE DEVERÃO ESTAR LICENCIADAS PARA 36 MESES; 1.11.3. DURANTE A VIGÊNCIA DO SUPORTE TÉCNICO DEVERÁ ESTAR INCLUSA ATUALIZAÇÃO DE SOFTWARE SEM NENHUM CUSTO ADICIONAL; 1.11.4. A PRESTAÇÃO DO SUPORTE TÉCNICO NÃO PODERÁ HAVER LIMITES NO QUANTITATIVO DE ABERTURA DE CHAMADOS; 1.11.5. OS CHAMADOS DEVERÃO SER ABERTOS ATRAVÉS DE PORTAL WEB E ATRAVÉS DE TELEFONE 0800, SENDO POSSÍVEL SOLICITAR ATENDIMENTO EM LÍNGUA PORTUGUESA; 1.11.6. NA APRESENTAÇÃO DA PROPOSTA COMERCIAL A EMPRESA LICITANTE DEVERÁ FORNECER DECLARAÇÃO DO FABRICANTE DOS PRODUTOS OFERTADOS ESPECÍFICA PARA ESTE CERTAME, EM PAPEL TIMBRADO, DECLARANDO QUE A LICITANTE POSSUI CREDENCIAMENTO COMO PARCEIRO AUTORIZADO E CREDENCIADO A PRESTAR SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE TÉCNICO PARA OS PRODUTOS OFERTADOS</p> <p>1.12. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO</p> <p>1.12.1. INSTALAÇÃO DEVERÁ SER REALIZADA PRESENCIALMENTE NO LOCAL DA PREFEITURA MUNICIPAL DE LAGOA SANTA, MG.</p> <p>1.12.2. CONFIGURAÇÕES BÁSICAS DE CONECTIVIDADE</p> <p>1.12.3. REGISTRO E ATIVAÇÃO DE LICENÇAS</p> <p>1.12.4. ATUALIZAÇÃO DE SOFTWARE</p> <p>1.12.5. CONFIGURAÇÃO DE ZONAS DE SEGURANÇA, VLANS E ROTEAMENTO INTERNO</p> <p>1.12.6. CONFIGURAÇÕES DOS SERVIÇOS DE SEGURANÇA COMO IPS E ANTI-MALWARE</p> <p>1.12.7. CONFIGURAÇÃO DE BALANCEAMENTO DE CARGA DE LINKS WAN</p> <p>1.12.8. MIGRAÇÃO E/OU CONFIGURAÇÃO DE REGRAS DE FIREWALL</p> <p>1.12.9. CONFIGURAÇÃO DE VPN</p> <p>1.12.10. CONFIGURAÇÃO DE REGRAS DE APLICAÇÃO</p> <p>1.12.11. INTEGRAÇÃO COM BASE LDAP OU RADIUS</p> <p>1.12.12. CONFIGURAÇÃO DE AUTENTICAÇÃO SSO</p> <p>1.12.13. CONFIGURAÇÃO DE FILTRO DE CONTEÚDO POR</p>			
--	--	---	--	--	--



Prefeitura Municipal de Lagoa Santa

			<p>GRUPO DE USUÁRIOS 1.12.13. CONFIGURAÇÃO DA UNIDADE DE ALTA DISPONIBILIDADE 1.12.14. CONFIGURAÇÃO DE QOS POR SERVIÇOS E/OU APLICAÇÕES 1.12.15. TESTES DE FUNCIONALIDADE 1.12.16. OS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DEVEM SER EXECUTADOS POR PROFISSIONAL COM CERTIFICAÇÃO TÉCNICA EMITIDA PELO FABRICANTE DA SOLUÇÃO DE FIREWALL OFERTADA. ESSA CERTIFICAÇÃO DEVERÁ SER ENVIADA JUNTAMENTE COM A PROPOSTA COMERCIAL. ESSE PROFISSIONAL DEVERÁ POSSUIR COMPROVAÇÃO DO VÍNCULO CONTRATUAL DE TRABALHO COM A LICITANTE.</p> <p>1.13. TREINAMENTO 1.13.1. TREINAMENTO REALIZADO ATRAVÉS DE FERRAMENTAS DE CONFERÊNCIA REMOTA COMO GOTOMEETING, WEBEX, TEAMS OU QUALQUER OUTRO QUE PERMITA APRESENTAÇÃO E COMUNICAÇÃO VIA VOIP COM CARGA HORÁRIA MÍNIMA DE 24 HORAS. MATERIAL DISPONIBILIZADO EM PDF PARA ACOMPANHAMENTO DO CURSO E ENTREGA DE CERTIFICADO DE CONCLUSÃO EM PAPEL OU DIGITAL. 1.13.2. TÓPICOS PARA COBERTURA DO TREINAMENTO: 1.13.3. FUNCIONALIDADES BÁSICAS DO EQUIPAMENTO: SENHA DE ADMINISTRAÇÃO, HORA E DATA, SCHEDULES E ETC 1.13.4. PROCEDIMENTO DE REGISTRO E ATIVAÇÃO DE LICENÇAS 1.13.5. PROCEDIMENTO DE ATUALIZAÇÃO DE SOFTWARE 1.13.6. ZONAS DE SEGURANÇA E OBJETOS 1.13.7. INTERFACES FÍSICAS, INTERFACES VIRTUAIS (VLANS) E ROTEAMENTO INTERNO 1.13.8. NAT 1.13.9. SERVIÇOS DE SEGURANÇA COMO IPS E ANTI-MALWARE 1.13.10. BALANCEAMENTO DE CARGA DE LINKS WAN 1.13.11. REGRAS DE FIREWALL 1.13.12. VPN 1.13.13. REGRAS DE APLICAÇÃO, INCLUINDO VISIBILIDADE DAS MESMAS 1.14. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO: 1.14.1. SUPORTE PARA O ITEM 1 - FIREWALL 1.14.2. A EMPRESA CONTRATADA DEVERÁ PRESTAR SERVIÇOS DE MANUTENÇÃO E SUPORTE TÉCNICO A TODOS OS PRODUTOS CONTRATADOS, NO LOCAL DE INSTALAÇÃO DA SOLUÇÃO, SEM ÔNUS PARA A CONTRATANTE, EM DIA ÚTEIS, 8 (OITO) HORAS POR DIA (REGIME 8X5).</p>			
2	02	UN	<p>SOFTWARE PLATAFORMA DE SOFTWARE DE ARMAZENAMENTO DE LOGS E GERAÇÃO DE RELATORIOS 2.1. DEVE SUPORTAR RECEBER LOGS DE AO MENOS 100 DISPOSITIVOS; 2.2. POSSUIR CAPACIDADE DE RECEBER AO MENOS 5 GBYTES DE LOGS DIÁRIOS; 2.3. DEVE SUPORTAR, PELO MENOS, 3 TB DE DISCO; 2.4. DEVE SER COMPATÍVEL COM VMWARE ESXI, HYPER-V, CITRIX XENSERVEN E KVM; 2.5. A SOLUÇÃO NÃO DEVE POSSUIR LIMITES DE CPU E MEMÓRIA; 2.6. A SOLUÇÃO DE RELATÓRIOS DEVE SER COMPATÍVEL COM OS FIREWALLS OFERTADOS, SENDO DO MESMO FABRICANTE; 2.7. REQUISITOS MÍNIMOS DE FUNCIONALIDADE 2.8. FUNCIONALIDADES GERAIS 2.8.1. DEVE SUPORTAR ACESSO VIA SSH, WEB (HTTPS) E TELNET PARA O GERENCIAMENTO DA SOLUÇÃO.</p>	FORTINET FORTIANALYZER-VM	R\$ 70.059,40	R\$ 140.118,80



## Prefeitura Municipal de Lagoa Santa

		<p>2.8.2. POSSUIR COMUNICAÇÃO CIFRADA E AUTENTICADA COM USUÁRIO E SENHA PARA SOLUÇÃO DE RELATÓRIOS, TANTO COMO PARA A INTERFACE GRÁFICA DE USUÁRIO E CONSOLE DE ADMINISTRAÇÃO POR LINHA DE COMANDOS (SSH); 2.8.3. PERMITIR ACESSO SIMULTÂNEO DE ADMINISTRADORES PERMITINDO A CRIAÇÃO DE AO MENOS 2 (DOIS) PERFIS PARA ADMINISTRAÇÃO E MONITORAÇÃO; 2.8.4. SUPORTAR SNMP VERSÃO 2 E VERSÃO 3 NA SOLUÇÃO DE RELATÓRIOS; 2.8.5. DEVE PERMITIR A CRIAÇÃO DE ADMINISTRADORES QUE ACESSEM A TODAS AS INSTÂNCIAS DE VIRTUALIZAÇÃO DA SOLUÇÃO DE RELATÓRIOS; 2.8.6. DEVE PERMITIR HABILITAR E DESABILITAR, PARA CADA INTERFACE DE REDE DA SOLUÇÃO DE RELATÓRIOS, PERMISSÕES DE ACESSO HTTP, HTTPS, SSH, SNMP E TELNET; 2.8.7. AUTENTICAÇÃO INTEGRADA A SERVIDOR RADIUS; 2.8.8. GERAÇÃO DE RELATÓRIOS EM TEMPO REAL, PARA A VISUALIZAÇÃO DE TRÁFEGO OBSERVADO, NOS FORMATOS: MAPAS GEOGRÁFICOS E TABELA; 2.8.9. AUTENTICAÇÃO INTEGRADA AO MICROSOFT ACTIVE DIRECTORY; 2.8.10. DEFINIÇÃO DE PERFIS DE ACESSO À CONSOLE COM PERMISSÕES GRANULARES COMO: ACESSO DE ESCRITA, ACESSO DE LEITURA, CRIAÇÃO DE USUÁRIOS, ALTERAÇÃO DE CONFIGURAÇÕES; 2.8.11. POSSUIR MECANISMO PARA QUE LOGS ANTIGOS SEJAM REMOVIDOS AUTOMATICAMENTE; 2.8.12. DEVE POSSUIR A CAPACIDADE DE CRIAR RELATÓRIOS NOS FORMATOS PDF; 2.8.13. DEVE SER POSSÍVEL EXPORTAR OS LOGS EM CSV; 2.8.14. GERAÇÃO DE LOGS DE AUDITORIA DETALHADOS, INFORMANDO A CONFIGURAÇÃO REALIZADA, O ADMINISTRADOR QUE A REALIZOU E O HORÁRIO DA ALTERAÇÃO; 2.8.15. OS LOGS GERADOS PELOS APPLIANCES DEVEM SER CENTRALIZADOS NOS SERVIDORES DE GERÊNCIA, MAS A SOLUÇÃO DEVE OFERECER TAMBÉM A POSSIBILIDADE DE UTILIZAÇÃO DE UM SYSLOG EXTERNO OU SIMILAR; 2.8.16. A SOLUÇÃO DEVE POSSUIR RELATÓRIOS PRÉ DEFINIDOS; 2.8.17. POSSUIR ENVIO AUTOMÁTICO DE LOGS PARA UM SERVIDOR FTP EXTERNO A SOLUÇÃO; 2.8.18. POSSIBILITAR A DUPLICAÇÃO DE RELATÓRIOS EXISTENTES E EDITÁ-LOS LOGO APÓS; 2.8.19. POSSUIR A CAPACIDADE DE PERSONALIZAÇÃO DE CAPAS PARA OS RELATÓRIOS; 2.8.20. PERMITIR DE FORMA CENTRALIZADA VISUALIZAR OS LOGS RECEBIDOS POR UM OU VÁRIOS DISPOSITIVOS EXTERNOS INCLUINDO A CAPACIDADE DE USO DE FILTROS NAS PESQUISAS DESTES LOGS; 2.8.21. DEVE POSSUIR LOGS DE AUDITORIA; 2.8.22. POSSUIR A CAPACIDADE DE PERSONALIZAÇÃO DE GRÁFICOS COMO BARRA, LINHA E TABELA PARA INSERÇÃO AOS RELATÓRIOS; 2.8.23. DEVE POSSUIR MECANISMO "DRILL-DOWN" PARA NAVEGAÇÃO NOS RELATÓRIOS EM REALTIME; 2.8.24. DEVER SER POSSÍVEL FAZER DOWNLOAD DOS ARQUIVOS DE LOGS RECEBIDOS; 2.8.25. DEVE POSSUIR AGENDAMENTO PARA GERAR E ENVIAR</p>			
--	--	--	--	--	--



## Prefeitura Municipal de Lagoa Santa

		<p>AUTOMATICAMENTE RELATÓRIOS; 2.8.26. PERMITIR CUSTOMIZAÇÃO DE QUAISQUER RELATÓRIOS FORNECIDOS PELA SOLUÇÃO, 2.8.27. EXCLUSIVAMENTE PELO ADMINISTRADOR, ADAPTANDO-O ÀS SUAS NECESSIDADES; 2.8.28. PERMITIR O ENVIO DE MANEIRA AUTOMÁTICA DE RELATÓRIOS POR E-MAIL; 2.8.29. DEVE PERMITIR A ESCOLHA DO E-MAIL A SER ENVIADO PARA CADA RELATÓRIO ESCOLHIDO; 2.8.30. PERMITIR PROGRAMAR A GERAÇÃO DE RELATÓRIOS, CONFORME CALENDÁRIO DEFINIDO PELO ADMINISTRADOR; 2.8.31. DEVE SER POSSÍVEL DEFINIR FILTROS NOS RELATÓRIOS; 2.8.32. DEVE SER CAPAZ DE DEFINIR O LAYOUT DO RELATÓRIO, INCLUIR GRÁFICOS, INSERIR TEXTOS E IMAGENS, ALINHAMENTO, QUEBRAS DE PÁGINAS, DEFINIR FONTES, CORES, ENTRE OUTROS; 2.8.33. GERAR ALERTAS AUTOMÁTICOS VIA EMAIL, SNMP E SYSLOG BASEADOS EM EVENTOS COMO OCORRÊNCIA COMO LOG, SEVERIDADE DE LOG, ENTRE OUTROS; 2.8.34. DEVE SER CAPAZ DE CRIAR CONSULTAS SQL OU SEMELHANTE PARA USO NOS GRÁFICOS E TABELAS DE RELATÓRIOS; 2.8.35. TER A CAPACIDADE DE VISUALIZAR NA GUI DA SOLUÇÃO DE RELATÓRIOS INFORMAÇÕES DO SISTEMA COMO MEMÓRIA, DISCO, USO DE CPU, LOGS POR SEGUNDO RECEBIDOS, TOTAL DE LOGS DIÁRIOS RECEBIDOS, ALERTAS GERADOS ENTRE OUTROS; 2.8.36. DEVE PERMITIR VER EM TEMPO REAL OS LOGS RECEBIDOS; 2.9. RELATÓRIOS: 2.9.1. DEVE PERMITIR A CRIAÇÃO DE DASHBOARDS CUSTOMIZADOS PARA VISIBILIDADES DO TRÁFEGO DE APLICATIVOS, CATEGORIAS DE URL, AMEAÇAS, SERVIÇOS, PAÍSES, ORIGEM E DESTINO; 2.9.2. DEVE POSSUIR RELATÓRIO DETALHADO DE PREVENÇÃO DE PERDA DE DADOS (DLP); 2.9.3. DEVE POSSUIR RELATÓRIO DE VPN; 2.9.4. DEVE POSSUIR RELATÓRIO DE SISTEMAS DE PREVENÇÃO DE INTRUSÃO (IPS); 2.9.5. DEVE POSSUIR RELATÓRIO DE REPUTAÇÃO DO CLIENTE; 2.9.6. DEVE POSSUIR RELATÓRIO DE ANÁLISE DE SEGURANÇA DO USUÁRIO; 2.9.7. DEVE POSSUIR RELATÓRIO DE AVALIAÇÃO DA AMEAÇA CIBERNÉTICA; 2.9.8. DEVE POSSUIR RELATÓRIO DE ANÁLISE APLICAÇÕES WEB (WAF); 2.9.9. DEVE POSSUIR RELATÓRIO DETALHADO DE NAVEGAÇÃO DE USUÁRIO; 2.9.10. DEVE POSSUIR RELATÓRIO DE EVENTOS DE SISTEMA E ADMINISTRAÇÃO; 2.9.11. DEVE POSSUIR RELATÓRIO DE AVALIAÇÃO DE AMEAÇAS CIBERNÉTICAS; 2.9.12. DEVE POSSUIR RELATÓRIO DE COMPLIANCE; 2.9.13. DEVE POSSUIR RELATÓRIO DE USO DE APLICAÇÕES SAAS; 2.10. SUPORTE TÉCNICO DO FABRICANTE NA MODALIDADE 24X7H DURANTE 36 MESES; 2.11. A CONTRATADA DEVE INSTALAR E CONFIGURAR A SOLUÇÃO DE RELATÓRIOS E LOGS EM SERVIDOR DISPONIBILIZADO PELO PMLS; 2.11.1. INSTALAÇÃO DEVERÁ SER REALIZADA PRESENCIALMENTE NO LOCAL DA PREFEITURA MUNICIPAL DE LAGOA SANTA, MG, E PARA OUTROS CLIENTES FORA DA REGIÃO</p>			
--	--	--	--	--	--



Prefeitura Municipal de Lagoa Santa

		METROPOLITANA DE BELO HORIZONTE, PODERÁ SER REALIZADA REMOTAMENTE. 2.12. TREINAMENTO 2.12.1. TREINAMENTO REALIZADO ATRAVÉS DE FERRAMENTAS DE CONFERÊNCIA REMOTA COMO GOTOMEETING, WEBEX, TEAMS OU QUALQUER OUTRO QUE PERMITA APRESENTAÇÃO E COMUNICAÇÃO VIA VOIP COM CARGA HORÁRIA MÍNIMA DE 8 HORAS. MATERIAL DISPONIBILIZADO EM PDF PARA ACOMPANHAMENTO DO CURSO E ENTREGA DE CERTIFICADO DE CONCLUSÃO EM PAPEL OU DIGITAL, COBRINDO OS ITENS A SEGUIR: 2.12.2. FUNCIONALIDADES BÁSICAS DO EQUIPAMENTO: SENHA DE ADMINISTRAÇÃO, HORA E DATA, SCHEDULES E ETC 2.12.3. PROCEDIMENTO DE REGISTRO E ATIVAÇÃO DE LICENÇAS 2.12.4. PROCEDIMENTO DE ATUALIZAÇÃO DE SOFTWARE 2.12.5. OPERACIONALIZAÇÃO DA SOLUÇÃO E HANDS-ON 2.13. SUPORTE TÉCNICO ESPECIALIZADO PARA O ITEM 2: 2.13.1. A EMPRESA CONTRATADA DEVERÁ PRESTAR SERVIÇOS DE MANUTENÇÃO E SUPORTE TÉCNICO A TODOS OS PRODUTOS CONTRATADOS, NO LOCAL DE INSTALAÇÃO DA SOLUÇÃO, SEM ÔNUS PARA A CONTRATANTE, EM DIA UTEIS, 8 (OITO) HORAS POR DIA (REGIME 8X5);			
<b>VALOR TOTAL DO LOTE : R\$ 449.000,00 (QUATROCENTOS QUARENTA E NOVE MIL).</b>					

Lagoa Santa, março de 2021.

**Nila Alves de Rezende**  
Secretária Municipal de Educação



## Homologação PE 19\_2021.pdf

Código do documento 2470bffe-d2cf-4a3d-b207-6419a469f34a



### Assinaturas



Nila Alves de Rezende  
nilarezende@lagoasanta.mg.gov.br  
Assinou

*Nila Alves de Rezende*



MONIQUE DUARTE COELHO DE OLIVEIRA  
moniquecoelho@lagoasanta.mg.gov.br  
Aprovou

*Monique Duarte Coelho de Oliveira*

### Eventos do documento

#### 15 Mar 2021, 16:26:18

Documento número 2470bffe-d2cf-4a3d-b207-6419a469f34a **criado** por MONIQUE DUARTE COELHO DE OLIVEIRA (Conta 304b0835-814a-427f-8841-36c74a67d51d). Email :moniquecoelho@lagoasanta.mg.gov.br. - DATE\_ATOM: 2021-03-15T16:26:18-03:00

#### 15 Mar 2021, 16:30:30

Lista de assinatura **iniciada** por MONIQUE DUARTE COELHO DE OLIVEIRA (Conta 304b0835-814a-427f-8841-36c74a67d51d). Email: moniquecoelho@lagoasanta.mg.gov.br. - DATE\_ATOM: 2021-03-15T16:30:30-03:00

#### 16 Mar 2021, 08:56:57

O signatário **ilcelacerda@lagoasanta.mg.gov.br DELEGOU** a assinatura para **nilarezende@lagoasanta.mg.gov.br** - DATE\_ATOM: 2021-03-16T08:56:57-03:00

#### 17 Mar 2021, 17:03:22

NILA ALVES DE REZENDE **Assinou** (Conta e947c7f3-3856-4d3e-8ec3-2a47f8e632b1) - Email: nilarezende@lagoasanta.mg.gov.br - IP: 179.134.115.68 (179-134-115-68.user.vivozap.com.br porta: 9044) - **Geolocalização: -19.637311 -43.9106554** - Documento de identificação informado: 316.278.976-15 - DATE\_ATOM: 2021-03-17T17:03:22-03:00

#### 17 Mar 2021, 17:43:07

MONIQUE DUARTE COELHO DE OLIVEIRA **Aprovou** (Conta 304b0835-814a-427f-8841-36c74a67d51d) - Email: moniquecoelho@lagoasanta.mg.gov.br - IP: 187.86.249.108 (187-86-249-108.vespanet.com.br porta: 35886) - **Geolocalização: -19.6459202 -43.914677** - Documento de identificação informado: 015.322.256-52 - DATE\_ATOM: 2021-03-17T17:43:07-03:00



Hash do documento original

(SHA256):e4861a2e8e0f1416f28010e98f16003906fdbb497366cc27bad75fdac5cf3fb3

(SHA512):5be53f6d6258ea6b9718a0b37211f0196428fa73b7738d61decda3f117ae98e86a3c8a645b29d0a5b9880872cfc74a8c8452e515c9c125d4e6a498b6f9669997

Esse log pertence **única e exclusivamente** aos documentos de HASH acima

**Esse documento está assinado e certificado pela D4Sign**