



Departamento Autônomo de Água e Esgotos
Rua Domingos Barbieri, 100 - Caixa Postal, 380 - CEP 14802-510 - Araraquara-SP
Fone: (16) 3324-9581 – DDG: 0800 602 2324
CNPJ 44.239.770/0001-67 - I.E. ISENTA
www.daaeararaquara.com.br



ANEXO I – TERMO DE REFERÊNCIA

SUMÁRIO

1. OBJETO	3
2. OBJETIVOS ESPECÍFICOS	3
3. LOCAIS DE EXECUÇÃO DOS SERVIÇOS	3
4. DO FORNECIMENTO DE PRODUTOS E SERVIÇOS E PRODUTOS:.....	5
5. LOCAÇÃO DA PLATAFORMA DE CYBERSEGURANÇA	7
5.1. APPLIANCE FIREWALL DE ÚLTIMA GERAÇÃO (UTM NGFW)	7
5.2. LICENÇAS DE ENDPOINT CONTROL.....	14
5.3. LICENÇAS DE ENDPOINT PROTECTION	17
6. LOCAÇÃO DAS PLATAFORMAS DE SOFTWARES E SERVIDORES	19
6.1. LICENÇAS DE SOFTWARE PARA GERENCIAMENTO DE VÍDEOS EM ALTA RESOLUÇÃO PARA SERVIDOR.....	19
6.2. LICENÇAS DE SOFTWARE PARA ANÁLISE DE VÍDEO (ANÁLISE FORENSE) PARA SERVIDOR	23
6.3. LOCAÇÃO DE CONJUNTO DE SERVIDORES PARA GRAVAÇÃO E BACKUP DE VÍDEOS EM ALTA RESOLUÇÃO PARA CÂMERAS IP	28
7. DAS CÂMERAS DE VIDEOMONITORAMENTO:	30
8. DO ARMAZENAMENTO DAS IMAGENS	42
9. DA PRESTAÇÃO DE SERVIÇOS DE 'INTERCONEXÃO'	42
10. DOS SERVIÇOS DE MANUTENÇÃO TÉCNICA PREVENTIVA E CORRETIVA	42
11. SUPORTE TÉCNICO CONTÍNUO DAS SOLUÇÕES	44
12. DA QUALIFICAÇÃO TÉCNICA E OPERACIONAL	45
13. DOS PRAZOS	46
14. DO VALOR ESTIMADO	46

1. OBJETO

1.1. CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM LOCAÇÃO DE PLATAFORMA DE SEGURANÇA, CÂMERAS DE VIDEOMONITORAMENTO IP, LICENÇAS DE SERVIDORES DE GESTÃO E MONITORAMENTO DE VÍDEOS EM ALTA RESOLUÇÃO DE CÂMERAS IP, SERVIDORES PARA GRAVAÇÃO E BACKUP DE VÍDEOS EM ALTA RESOLUÇÃO PARA CÂMERAS IP, PRESTAÇÃO DE SERVIÇOS DE INTERCONEXÃO DEDICADA PARA TRANSMISSÃO E RECEPÇÃO DE DADOS, SERVIÇOS DE SUPORTE TÉCNICO DA SOLUÇÃO OFERTADA, POR UM PERÍODO DE 36 MESES, INCLUINDO O FORNECIMENTO DE EQUIPAMENTOS, INSTALAÇÃO, ADEQUAÇÃO DE LOCAIS DE INSTALAÇÃO E FUNCIONAMENTO E TREINAMENTO, CONFORME ESPECIFICAÇÕES CONSTANTES NESTE ANEXO.

2. OBJETIVOS ESPECÍFICOS

2.1. SISTEMA DE MONITORAMENTO REMOTO: Instalação e locação de sistema de monitoramento remoto composto por câmeras, rede de fibra ótica e softwares de monitoramento, conforme especificado no item 3, com gravação, transmissão e gerenciamento de imagens.

2.2. CENTRAL DE MONITORAMENTO: Concentração das imagens monitoradas no Centro de Inteligência e Informação (CII) do DAAE, localizado na Av. José Parisi, 529, incluindo a instalação, o fornecimento de licenças e a integração das câmeras, comunicação e redes de dados.

2.3. MANUTENÇÃO TÉCNICA PREVENTIVA: Prestação de serviços de manutenção técnica preventiva, contemplando os serviços necessários para manter os equipamentos funcionando em condições normais, com o objetivo de diminuir as possibilidades de paralisação do sistema de monitoramento.

2.4. MANUTENÇÃO TÉCNICA CORRETIVA: Prestação de serviços de manutenção técnica corretiva, contemplando os serviços de reparo e substituição, com a finalidade de eliminar todos os defeitos existentes nos equipamentos que compõem o sistema de monitoramento remoto.

2.5. SUPORTE TÉCNICO: Prestação de serviços de suporte técnico contínuo.

3. LOCAIS DE EXECUÇÃO DOS SERVIÇOS

3.1. Os serviços, objeto deste termo, serão realizados nos seguintes locais:

Local	Nome	Endereço	Coordenadas (UTM 22K)
1	Escritório Central	Av. José Parisi, 529	E792.689m; N7.590.029m
2	Captação Anhumas I	CRT 166B, 025 Faz. Bombarda	E805.204m; N7.590.232m
3	Estação Elevatória Anhumas II	CRT 166B, 025 Faz. Bombarda	E802.003m; N7.589.890m
4	Captação das Cruzes	Rua Napoleão Selmi Dei, s/nº	E791.840m; N7.591.301m
5	Captação Águas do Paiol	Av. Augusto Bernardi, s/nº	E788.614m; N7.590.897m

3.2. Escritório Central:

3.2.1. Os serviços compreendem o fornecimento e a instalação de 45 (quarenta e cinco) câmeras do tipo IP;

3.2.2. As câmeras serão instaladas em toda a área interna do departamento, em vias internas, estacionamentos e no interior das edificações, conforme disposto no Anexo IIA – Locação das câmeras – Escritório Central;

3.2.3. Para a interligação das câmeras, deverá ser executada uma rede em fibra ótica, exclusiva para o sistema de monitoramento, conforme disposto no Anexo IIB – Implantação da rede de fibra ótica. Para a instalação da rede de fibra ótica, a CONTRATADA poderá utilizar da infraestrutura existente na Autarquia (Postes, dutos, eletrocalhas etc.);

3.2.4. Caso se necessário a instalação e/ou execução de dutos subterrâneos e caixas de interligação, elas serão executadas pela CONTRATADA;

3.2.5. A comunicação com o local, para acesso e transmissão de dados, será disponibilizada pela CONTRATADA, por meio link de interconexão clear channel (Fibra Óptica) na velocidade de 1Gb;

3.3. Captação Anhumas I:

3.3.1. Os serviços compreendem o fornecimento e a instalação de 3 (três) câmeras do tipo IP;

3.3.2. As câmeras internas deverão ser fixadas em pontos estratégicos na edificação existente no local (Casa de Bombas), permitindo a visualização das bombas e painéis elétricos;

3.3.3. As câmeras externas deverão ser fixadas em poste, de no mínimo 6,00 metros, a ser instalado em ponto estratégico do local (terreno) permitindo a visualização das áreas internas, portão de acesso e entorno da casa de bombas;

3.3.4. A comunicação com o local, para acesso e transmissão de dados, será disponibilizada pela CONTRATANTE, por meio link de internet via satélite com taxa download variável entre 25 e 200Mbps e taxa de upload variável entre 5 e 20Mbps;

3.4. Estação Elevatória de Água Anhumas II:

3.4.1. Os serviços compreendem o fornecimento e a instalação de 3 (três) câmeras do tipo IP;

3.4.2. As câmeras deverão ser fixadas em pontos estratégicos na edificação existente no local (Casa de Bombas), permitindo a visualização das bombas e painéis elétricos (câmera interna) e áreas externas, incluindo portão de acesso;

3.4.3. A comunicação com o local, para acesso e transmissão de dados, será disponibilizada pela CONTRATANTE, por meio link de internet via satélite com taxa download variável entre 25 e 200Mbps e taxa de upload variável entre 5 e 20Mbps;

3.5. Captação das Cruzes:

3.5.1. Os serviços compreendem o fornecimento e a instalação de 5 (cinco) câmeras do tipo IP;

3.5.2. As câmeras deverão ser fixadas em pontos estratégicos nas edificações existentes no local (Casa de Bombas e Museu), permitindo a visualização das bombas e painéis elétricos (câmeras internas), barramento da represa e áreas externas, incluindo portão de acesso;

3.5.3. A comunicação com o local, para acesso e transmissão de dados, será disponibilizada pela CONTRATADA, por meio link de interconexão clear channel (Fibra Óptica) na velocidade de 1Gb;

3.6. Captação Águas do Paiol:

3.6.1. Os serviços compreendem o fornecimento e a instalação de 2 (duas) câmeras do tipo IP;

3.6.2. As câmeras deverão ser fixadas em poste de iluminação existente no local, permitindo a visualização do barramento da represa, guarita e portão de acesso;

3.6.3. A comunicação com o local, para acesso e transmissão de dados, será disponibilizada pela CONTRATADA, por meio link de interconexão clear channel (Fibra Óptica) na velocidade de 1Gb;

3.7. Em todas as unidades atendidas:

3.7.1. Todas as imagens e seus eventos serão transmitidos em tempo real à central de monitoramento do DAAE;

3.7.2. Todas as imagens capturadas serão armazenadas em SD CARD de 256Gb (na própria câmera), e, simultaneamente em nuvem a partir de solução ofertada pelo licitante, sendo que elas deverão estar disponíveis para acesso via web em dispositivos móveis e fixos, mediante a disponibilização de usuários e senhas; e,

3.7.3. O sistema possibilitará a configuração de usuários e seu respectivo perfil de acesso às câmeras e a todos os eventos gerados, conforme critérios estabelecidos pela CONTRATANTE.

4. DO FORNECIMENTO DE PRODUTOS E SERVIÇOS E PRODUTOS:

4.1. Deverão ser fornecidos os seguintes produtos e quantitativos

Item	Descrição	Unidade	Quant.
1.0	Locação da Plataforma de Cibersegurança		
1.1	Appliance Firewall de Última Geração (<i>UTM NGFW</i>)	Unidade/Mês	01
1.2	Licenças de End Point Control	Unidade/Mês	10
1.3	Licenças de End Point Protection	Unidade/Mês	10
2.0	Locação das Plataformas de Softwares e Servidores		
2.1	Licenças de Softwares para Gerenciamento de Vídeos em Alta Resolução para Servidor	Unidade/Mês	58
2.2	Licenças de Softwares para Análise de Vídeo (<i>Análise Forense</i>) para Servidor	Unidade/Mês	05
2.3	Locação de Conjunto de Servidores gravação e backup de Vídeos em Alta Resolução para Câmeras IP	Unidade/Mês	01
2.4	Softwares de IAVCA para Análise de Conteúdo de Vídeo com Inteligência Artificial Embarcados nas Câmeras IP e SDCard 256Gb (C10-100MB/s) instalado	Unidade/Mês	56

2.5	Softwares de IA/LPR para Leitura de Placa Veicular com Inteligência Artificial Embarcados nas Câmeras IP e SDCard 256Gb (C10-100MB/s) instalado	Unidade/Mês	02
3.0	Locação, Manutenção e Suporte Técnico de Câmeras, Acessórios e Componentes		
3.1	Câmera IP – Tipo 01	Unidade/Mês	36
3.2	Câmera IP – Tipo 02	Unidade/Mês	15
3.3	Câmera IP – Tipo 03	Unidade/Mês	02
3.4	Câmera IP – Tipo 04	Unidade/Mês	01
3.5	Câmera IP – Tipo 05	Unidade/Mês	04
4.0	Serviços de Interconexão		
4.1	Link Clear Channel de 1Gb	Unidade/Mês	03
5.0	Serviços de instalação incluindo: a rede de interligação em fibra ótica (interna e externa), fornecimento de insumos e materiais de instalação, acessórios, componentes e os dispositivos necessários.		
5.1	Escritório Central (ETA Fonte)	Unidade/Mês	01
5.2	Captação Anhumas I	Unidade/Mês	01
5.3	Estação Elevatória de Água Anhumas II	Unidade/Mês	01
5.4	Captação das Cruzes	Unidade/Mês	01
5.5	Captação Águas do Paiol	Unidade/Mês	01

4.2. Todos os serviços de instalação técnica da infraestrutura, implantação e treinamento necessários devem estar inclusos.

4.3. As soluções de internet e interconexão para upload e gerenciamento das imagens serão fornecidas pela CONTRATADA, com exceção dos links de acesso e transmissão de dados locais “Captação Anhumas I” e “Estação Elevatória de Água Anhumas II” que serão fornecidos pelo contratante.

4.4. A CONTRATADA deverá realizar um treinamento, uma única vez e com no mínimo 8 horas de duração, para os operadores do sistema de monitoramento, devendo abordar no mínimo o uso e operação das câmeras, uso e operação da plataforma de segurança e demais itens pertinentes à operação do sistema especificados neste Termo de Referência.

4.5. A CONTRATADA deverá fornecer em versão digital e, no mínimo 1 (uma) cópia impressa, de um manual de operação do sistema, especificando o funcionamento dos equipamentos, rotinas de trabalho, parametrização e programação das rotinas de vídeo analítico, geração de relatórios, bem como de todas as funcionalidades referente a operação do sistema.

4.6. Os serviços de instalação serão pagos à CONTRATADA em 12 parcelas mensais. Para a composição destes custos a PROPONENTE deverá apresentar o custo total da instalação em cada local definido neste Termo de Referência e dividir por 12, obtendo o

valor mensal a ser pago correspondente aos serviços de instalação, conforme modelo apresentado no anexo III.

5. LOCAÇÃO DA PLATAFORMA DE CYBERSEGURANÇA

5.1. APPLIANCE FIREWALL DE ÚLTIMA GERAÇÃO (UTM NGFW)

5.1.1. Para a Interconexão e Cibersegurança dos dispositivos, na Central de Monitoramento deverá ser instalada a solução de segurança de redes de proteção perimetral, também chamado de Firewall UTM ou Firewall NG, 1(um) dispositivo possuindo no mínimo:

5.1.2. Appliance, onde não serão permitidas soluções baseadas em PC ou Servidores com sistemas operacionais como Windows, FreeBSD e GNU/Linux;

5.1.3. A solução deverá utilizar a tecnologia de Firewall Stateful Packet Inspection (Firewall por estado de conexão com inspeção profunda de pacotes);

5.1.4. A solução deverá possuir certificado ICSA para Firewall; e,

5.1.5. A solução deverá possuir todos os softwares e licenças para habilitação de todos os recursos exigidos neste termo de referência pelo período de vigência do contrato.

5.1.6. Especificações mínimas:

5.1.6.1. 1 x USB Port;

5.1.6.2. 1 x Console Port;

5.1.6.3. 2 x GE RJ45 WAN Ports;

5.1.6.4. 1 x GE RJ45 DMZ Ports;

5.1.6.5. 7 x GE RJ45 Internal Ports;

5.1.6.6. Performance mínima de 1 Gbps de throughput para Firewall;

5.1.6.7. Performance mínima de 1,4 Gbps de throughput de IPS;

5.1.6.8. Performance mínima de 6,5 Gbps de throughput de VPN;

5.1.6.9. Suporte a, no mínimo 700.000 (setecentos mil) de conexões simultâneas;

5.1.6.10. Suporte a, no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;

5.1.6.11. Suporte a, no mínimo 200 túneis Ipsec VPN;

5.1.6.12. Possuir o número irrestrito quanto ao máximo de usuários licenciados;

5.1.6.13. Deverá ser fornecido equipamento de segurança de rede gerenciada do tipo next-generation firewall com capacidade técnica suficiente para rodar sem que os limites de 80% de utilização da memória e de CPU sejam excedidos;

5.1.6.14. Na solução, o acesso redundante deverá estar ativo para uma solução hot stand-by;

5.1.6.15. Deverão estar inclusos na solução, por conta da CONTRATADA, todos os recursos de conectividade, tais como: fibras, paths cords, conversores, appliances, roteadores e outros correlatos, bem como a infraestrutura para instalação dos equipamentos de transmissão necessária à prestação dos serviços, além de dutos/eletrodutos caso necessário; e,

5.1.6.16. Deverão ser fornecidos e instalados componentes como DIO's, path cords de fibra, conversores, Gbics, todos componentes necessários ao funcionamento do link.

5.1.7. Características gerais para firewalls de última geração:

- 5.1.7.1.** A solução deve consistir em appliance de proteção de rede com funcionalidades de Next-Generation Firewall (NGFW), e console de gerência, monitoração e logs;
- 5.1.7.2.** Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 5.1.7.3.** As funcionalidades de proteção de rede que compõem a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos deste termo de referência;
- 5.1.7.4.** A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (L7);
- 5.1.7.5.** O software deverá ser fornecido em sua versão mais atualizada;
- 5.1.7.6.** Uma interface completa CLI (command-line-interface) deverá ser acessível através da interface gráfica e via porta serial;
- 5.1.7.7.** A atualização de software deverá enviar avisos de atualizações automáticos;
- 5.1.7.8.** O sistema de objetos deverá permitir a definição de redes, serviços, hosts, períodos, usuários e grupos, clientes e servidores;
- 5.1.7.9.** O backup e o restabelecimento de configuração deverão ser feitos localmente, via
- 5.1.7.10.** FTP/SFTP, com frequência diária, semanal e/ou mensal, podendo ser realizado por demanda;
- 5.1.7.11.** As notificações deverão ser realizadas via email e SNMP;
- 5.1.7.12.** Suportar SNMPv3 e Netflow;
- 5.1.7.13.** O firewall deverá ser stateful, com inspeção profunda de pacotes;
- 5.1.7.14.** As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis;
- 5.1.7.15.** As políticas de NAT deverão ser customizáveis para cada regra;
- 5.1.7.16.** A proteção contra flood deverá ter proteção contra DoS (Denial of Service). DDoS (Distributed DoS) e bloqueio de portscan;
- 5.1.7.17.** Proteção contra anti-spoofing;
- 5.1.7.18.** Suportar IPv4 e IPv6;
- 5.1.7.19.** IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969;
- 5.1.7.20.** Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGPM);
- 5.1.7.21.** Deve possibilitar o roteamento baseado em VPNs; e,
- 5.1.7.22.** Deve suportar criar políticas de roteamento.
- 5.1.8. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:**
- 1.1.1.1.** Interface de entrada do pacote;
- 1.1.1.2.** IPs de origem;
- 1.1.1.3.** IPs de destino;
- 1.1.1.4.** Portas de destino;
- 1.1.1.5.** Usuários ou grupos de usuários;
- 1.1.1.6.** Aplicação em camada 7
- 1.1.1.7.** Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento;

- 1.1.1.8. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 1q e tagging de VLAN;
- 1.1.1.9. Deve suportar Extended VLAN;
- 1.1.1.10. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso;
- 1.1.1.11. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
- 1.1.1.12. Deve permitir a configuração de jumbo frames nas interfaces de rede;
- 1.1.1.13. Deve permitir a criação de um grupo de portas layer2;
- 1.1.1.14. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;
- 1.1.1.15. O traffic shapping (QoS) deverá ser baseado em rede ou usuário;
- 1.1.1.16. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas;
- 1.1.1.17. Deve possuir otimização em tempo real de voz sobre IP; e,
- 1.1.1.18. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

5.1.9. Controle por políticas de firewall deve suportar controles por:

- 5.1.9.1. Porta;
- 5.1.9.2. Protocolos TCP/UDP;
- 5.1.9.3. Origem/destino;
- 5.1.9.4. Identificação de usuários;
- 5.1.9.5. O controle de políticas deverá monitorar as seguintes políticas de redes:
- 5.1.9.6. Usuários;
- 5.1.9.7. Grupos e tempo;
- 5.1.9.8. Identificar regras não utilizadas;
- 5.1.9.9. Identificar regras desabilitadas;
- 5.1.9.10. Identificar regras modificadas;
- 5.1.9.11. Identificar novas políticas;
- 5.1.9.12. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zona, redes e por tipos de serviços;
- 5.1.9.13. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 5.1.9.14. Controle de políticas por países via localização por IP;
- 5.1.9.15. Suporte a objetos e regras IPV6; e,
- 5.1.9.16. Suporte a objetos e regras multicast.

5.1.10. Prevenção de ameaças:

- 5.1.10.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulos de IPS, Antivírus, Anti-Malware e Firewall de Proteção WEB (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 5.1.10.2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS);

- 5.1.10.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas;
- 5.1.10.4. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;
- 5.1.10.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
- 5.1.10.6. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;
- 5.1.10.7. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise;
- 5.1.10.8. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem;
- 5.1.10.9. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails;
- 5.1.10.10. Deve ter proteção em tempo real contra novas ameaças criadas;
- 5.1.10.11. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente;
- 5.1.10.12. Deve permitir o bloqueio de vulnerabilidades;
- 5.1.10.13. Deve permitir o bloqueio de exploits conhecidos;
- 5.1.10.14. Deve detectar e bloquear o tráfego de rede que busque acesso a servidores de comando e controle conhecidos;
- 5.1.10.15. Deve incluir proteção contra ataques de negação de serviços;
- 5.1.10.16. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP flood etc.;
- 5.1.10.17. Suportar bloqueio de arquivos por tipo;
- 5.1.10.18. Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 5.1.10.19. Os eventos devem identificar o país de onde partiu a ameaça; e,
- 5.1.10.20. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança etc. Ou seja, cada política de firewall poderá ter uma configuração diferente de IPs, sendo essas políticas aplicadas por usuários, grupos de usuários, origem, destino, zonas de segurança.

5.1.11. Controle e proteção de aplicações:

- 5.1.11.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinatura e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado;
- 5.1.11.2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 0, SSL 0,
- 5.1.11.3. TLS 2 e TLS 3;
- 5.1.11.4. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA),

DH, DHE, Authentication, RSA, DAS, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384;

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

5.1.11.6. Reconhecer pelo menos 300 (duas mil e trezentas) aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de softwares, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, webmails;

5.1.11.7. Para tráfego criptografado SSL, deve decryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.1.11.8. Atualizar a base de assinaturas de aplicações automaticamente;

5.1.11.9. Reconhecer aplicações em IPv6;

5.1.11.10. Limitar a banda usada por aplicações (traffic shaping);

5.1.11.11. 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 do agente no Domain Controller, nem nas estações dos usuários;

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

5.1.11.13. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

5.1.12. Controle e proteção web:

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

5.1.12.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

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

5.1.12.4. Autenticação em 2 (dois) fatores em conjunto com a autenticação Radius;

5.1.12.5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

5.1.12.6. Possuir pelo menos 90 categorias de URLs;

5.1.12.7. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.1.12.8. Deve ser capaz de forçar o uso da opção "Safe Search" em sites de busca;

5.1.12.9. Deve ser capaz de forçar as restrições do Youtube;

- 5.1.12.10. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
- 5.1.12.11. Suportar a criação de categorias de URLs customizadas;
- 5.1.12.12. Suportar a opção de bloqueio de categoria HTTP e liberação de categoria apenas em HTTPS;
- 5.1.12.13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada;
- 5.1.12.14. Suportar a inclusão nos logs de informações das atividades dos usuários;
- 5.1.12.15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado;
- 5.1.12.16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;
- 5.1.12.17. Deve realizar caching do conteúdo web;
- 5.1.12.18. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies; e,
- 5.1.12.19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré determinados para acessar sites na internet.

5.1.13. Identificação de usuários:

- 5.1.13.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.1.13.2. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal); e,
- 5.1.13.3. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

5.1.14. Qualidade de serviço – QoS:

- 5.1.14.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de administrá-las por políticas de controle de banda quando forem solicitadas por diferentes usuários ou aplicações;
- 5.1.14.2. A solução deverá suportar Traffic Shaping (QoS) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem, endereço de destino, usuário e grupo do AD/LDAP;
- 5.1.14.3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado;
- 5.1.14.4. Suportar priorização Real-Time de protocolos de voz (VoIP); e,
- 5.1.14.5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

5.1.15. Redes virtuais privadas – VPN:

- 5.1.15.1.** Suportar VPN Site-to-Site e Client-to-Site;
- 5.1.15.2.** Suportar Ipsec VPN;
- 5.1.15.3.** Suportar SSL VPN;
- 5.1.15.4.** Suportar L2TP e PPTP;
- 5.1.15.5.** Suportar acesso remoto SSL, IPsec e VPN Client para Android e iPhone/iPAD;
- 5.1.15.6.** Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL;
- 5.1.15.7.** A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1, DiffieHellman Group 1, Group 2, Group 5 e Group 14, Algorithm Internet Key Exchange (IKE), AES 128, 192 e 256 (Advanced Encryption Standard), SHA 256, 384 e 512, Autenticação via Certificado PKI (X.509) e Pre-Shared Key (PSK);
- 5.1.15.8.** Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiMalware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 5.1.15.9.** Suportar autenticação via AD/LDAP, Token e base de usuários local;
- 5.1.15.10.** Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP; e,
- 5.1.15.11.** Active Directory, Radius, eDirectory, TACACS+ e via base de dados local.

5.1.16. Gerência administrativa centralizada:

- 5.1.16.1.** Deve possuir solução de gerenciamento integrada ou solução baseada em appliance, possibilitando o gerenciamento em um único console central, com administração de privilégios e funções;
- 5.1.16.2.** O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança; e,
- 5.1.16.3.** Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração.

5.1.17. Gerência de logs e relatórios centralizados:

- 1.1.1.1.** Deve possuir solução de logs e relatórios integrados, ou em appliance, possibilitando a consolidação total de todas as atividades da solução através de um único console central;
- 1.1.1.2.** Deve fornecer relatórios históricos para análises de mudanças e comportamentos;
- 1.1.1.3.** Deve permitir a exportação via PDF ou Excel;
- 1.1.1.4.** Deve fornecer logs em tempo real, de auditoria e arquivados; e,
- 1.1.1.5.** Deve possuir mecanismo de procura de logs arquivados.

5.1.18. A licitante deverá incluir na proposta a marca e o modelo da solução ofertada para atender esse item.

5.1.19. A licitante deverá, juntamente com a proposta, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas.

5.1.20. Os serviços de garantia, suporte técnico e manutenção deverão ser prestados pela CONTRATADA, pela fabricante dos produtos, ou por empresa credenciada à

rede nacional de assistência técnica autorizada pelo fabricante dos produtos fornecidos.

5.2. LICENÇAS DE ENDPOINT CONTROL

- 5.2.1. O sistema de controle e monitoramento Endpoint deverá ser baseada no modelo que permita monitoramento e gerenciamento centralizado em nuvem (Cloud);
- 5.2.2. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções descritas no mesmo painel de gerenciamento de segurança com objetivo de facilitar a operação e funcionar tanto de forma integrada, quanto de forma isolada ("stand alone");
- 5.2.3. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa contra códigos maliciosos e ameaças de rede (integrar uma única solução corporativa);
- 5.2.4. Todos os componentes tratados no item anterior deverão funcionar de forma integrada na solução. Não deverão ser soluções diferentes;
- 5.2.5. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de combate a código maliciosos e proteção de computadores ligados em rede;
- 5.2.6. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, possuindo ainda um recurso exclusivo somente para as versões desenvolvidas para sistemas operacionais Windows, uma versão de antimalware, status e informações CPU, MEMÓRIA, DISCO;
- 5.2.7. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- 5.2.8. Devidamente desenvolvido não somente para sistemas operacionais Windows, mas também para sistemas operacionais Linux, o acesso para ferramenta de configuração do gerenciamento em nuvem (Cloud) deverá ser com acesso seguro via HTTPS;
- 5.2.9. O Endpoint deve possuir agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões CentOS 7 e 7, Debian 8, 9 e 10, Ubuntu 14, 16 e 18 e Chrome OS última versão;
- 5.2.10. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 5.2.11. Funcionalidades de gerenciamento em nuvem (Cloud) e administração centralizada da solução, trabalhar obrigatoriamente na língua portuguesa do Brasil e inglês, o sistema de gerenciamento em nuvem deverá permitir a criação de políticas, por grupo ou território e permitir criação de regras das políticas, porém sem ser aplicadas, ou seja, permitir configurar a regra como neutra, ativa ou inativa;
- 5.2.12. A solução deverá permitir gerência granular com gerenciamento de políticas por nível hierárquico, permitindo ao usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;

- 5.2.13.** Caso possua mais de uma unidade organizacional, permitir a organização por meio de hierarquia em árvore que permita definição de permissão de acesso por cada unidade organizacional e/ou por toda a organização;
- 5.2.14.** A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal;
- 5.2.15.** No caso dos sistemas operacionais Windows, permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 5.2.16.** Possuir exclusivamente para a versão Windows recursos que possibilitem visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 5.2.17.** A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato;
- 5.2.18.** Permitir a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil. Este item é obrigatório no sistema operacional Windows;
- 5.2.19.** Para sistemas Windows, a solução deverá proteger os arquivos através de assinaturas de arquivos maliciosos já conhecidos e além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso à internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;
- 5.2.20.** Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto PUP do acrônimo em inglês Possible Unintended Programs, ou seja, programas possivelmente indesejados como exemplos Adwares e Spywares.
- 5.2.21.** Este item é obrigatório nos sistemas operacionais Windows;
- 5.2.22.** Disponibilizar na aplicação antivírus tanto no cliente da versão cliente/servidor como na versão Stand Alone ferramenta para envio de amostras para o laboratório e posterior análise, enviado da própria aplicação. Este item é obrigatório no sistema operacional Windows;
- 5.2.23.** A solução deverá prover proteção quanto a navegação, para sistemas Windows. Essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 5.2.24.** Para a proteção de navegação nos sistemas Windows, a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (PUP - Possible Unintended Programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- 5.2.25.** A solução deverá permitir agendamento de scan na rede, podendo criar mais do que uma regra de agendamento como por exemplo um agendamento de scan rápido em um determinado horário do dia e um agendamento completo durante a noite, a solução deverá conter tecnologia de identificação de condição de carga do equipamento para que nessa

condição o scan seja colocado em segundo plano evitando aplicar lentidão ao equipamento, essa tecnologia deverá ser configurada para ocorrer ou não em cada tarefa de agendamento de scan, para o agendamento deverá permitir no mínimo frequência diária, semana ou mensal podendo definir o horário para execução, para sistemas Windows;

5.2.26. A solução deverá permitir executar comandos remotos na estação, deverá permitir no mínimo desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo e permitir gerenciamento de inventário de software e hardware, deverá conter no mínimo os seguintes itens, nos sistemas Windows;

5.2.27. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;

5.2.28. Nos sistemas Windows, permitir acessar remotamente o equipamento direto do painel cloud, a solução deverá solicitar autorização da estação de trabalho a ser acessada quanto a autorização do acesso, remover o software remotamente direto do painel cloud e ativar ou desativar recebimento de alerta dos dispositivos e a solução deverá permitir bloquear o uso de pendrive ou storage externo, essa restrição deverá ser granular;

5.2.29. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, MEMÓRIA e DISCO e tais informações deverão estar disponíveis em um painel ou dash board específico para monitoramento;

5.2.30. Trazer as informações de cada dispositivo com status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de atividade, consumo e total de CPU, consumo e total de memória RAM, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo CPU, processos que estão mais consumindo memória, informações de hardware como drivers de impressora, CD-ROM, Dispositivos gerais, IDE, USB, SOM, VÍDEO, Adaptador de Rede, Processador, BIOS, MEMÓRIA, PLACA DE SOM, DISCO, MEMÓRIA e informações dos softwares instalados, tais como: fabricantes, software e versão;

5.2.31. A solução deverá prover modulo de relatórios com no mínimo relatório de inventário de software e hardware, relatório de licenças do Windows com seu status e relatórios de ameaças encontradas, os relatórios deverão ao menos ser gerados no formato PDF, CSV e HTML;

5.2.32. O console de gerenciamento Web deverá prover na tela principal um Dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;

5.2.33. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações, estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados SQLServer, MySQL, PostgreSQL, Oracle, monitoramento do serviço do Microsoft Active Directory e DNS, informações quanto aos sistemas operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não validas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;

5.2.34. Destinado não somente ao sistema operacional Windows, mas também para Linux, um painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema;

5.2.35. Ter painel de visualização que permita verificar somente o status dos servidores por meio visual;

5.2.36. Tendo em vista o sistema operacional Windows como referência, a solução deverá prover relatórios referente as informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco dela;

5.2.37. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;

5.2.38. No caso de sistema operacional da família Windows, ter controle e relatório de uso de aplicação por horário, quantidade de dados trafegados por usuário com possibilidade de bloqueio de uso de determinadas aplicações e sistemas;

5.2.39. Disponibilizar recursos que permitam inclusão de hostname e serial do dispositivo, abertura de ticket via agente, configurar e-mail em nuvem para direcionamento de informações disponíveis via formulário via agente (solicitação de abertura de ticket) e que o e-mail seja enviado com os dados do dispositivo em que foi aberto o ticket; e ainda o link para visualização dos detalhes do dispositivo em nuvem;

5.2.40. Enviar e-mail informando o usuário requerente da solicitação de atendimento, informando detalhes do ticket, e ainda com a possibilidade de personalizar com logomarca no e-mail de retorno;

5.2.41. Possuir QR Code no agente local, com direcionamento para o dispositivo direto para a gestão em nuvem, exibição de log, mostrar informações do dispositivo diretamente no agente local com acesso rápido e facilitado e que as informações do device ID sejam copiadas, informações de serial ou hostname do dispositivo com duplo clique;

5.2.42. A licitante deverá incluir na proposta a marca e o modelo da solução ofertada para atender esse item;

5.2.43. A licitante deverá, juntamente com a proposta, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas; e,

5.2.44. Os serviços de garantia, suporte técnico e manutenção deverão ser prestados pela CONTRATADA, pela fabricante dos produtos, ou por empresa credenciada à rede nacional de assistência técnica autorizada pelo fabricante dos produtos fornecidos.

5.3. LICENÇAS DE ENDPOINT PROTECTION

5.3.1. O sistema de controle e monitoramento Endpoint deverá ser baseada no modelo que permita monitoramento e gerenciamento centralizado em nuvem (Cloud);

5.3.2. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas e vermes (worms). Salvo a versão para Linux, a solução deverá também fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações),

bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware", "keylogger", "screenlogger" etc.), códigos de apoio à invasão e escalada de privilégio ("rootkit", "backdoor" etc.), código e conteúdo indesejado ("dialer", "adware", "joke" etc.

5.3.3. Permitir a execução de escaneamentos nos servidores, nas estações de trabalho (programada ou não) e um sistema avançado de limpeza que reduza risco de estabilidade do sistema operacional;

5.3.4. As versões para sistemas operacionais Windows, deverão apresentar a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;

5.3.5. A solução precisa possuir como recurso, camada de proteção contra acesso a sites fraudulentos e perigosos no sistema Windows;

5.3.6. No sistema Windows, deverá negar acesso ao arquivo infectado antes que ele seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);

5.3.7. A versão do agente Endpoint para sistemas operacionais Windows possui proteção avançada de mídias removíveis ("CD", "DVD", "pendrive", "HD" externo), sem a necessidade de configurações adicionais e permitir detecção de ameaças em arquivos compactados nos principais algoritmos ("ZIP", "RAR", "7zip");

5.3.8. A solução precisa dispor de comunicação via protocolo SNMP nos sistemas Windows assim como também anti-ransomware ativo e inteligência artificial trabalhando de forma passiva na detecção de comportamento suspeito;

5.3.9. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente;

5.3.10. Em sua camada de proteção de arquivos contra sequestro de informações deverá ainda ter como adicional, camada de proteção comportamental contra programas e/ou comportamentos suspeitos;

5.3.11. O seu módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware precisa ser integrado com geração de "kit de emergência" para sistemas Windows, que permitirá usuário dar boot na máquina e efetuar limpeza manual; e ainda possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;

5.3.12. Todos os itens acima deverão atender sistemas operacionais da família Windows da versão Windows 7 e servidores Windows Server 2008 R2 em diante e dispor de opção para ativar ou desativar recebimento de alerta dos dispositivos, desde que tais sistemas ainda estejam na lista de sistemas oficiais com suporte e atualização do fabricante;

5.3.13. Trazer as seguintes informações de cada dispositivo como status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo e consumo geral e total de CPU;

5.3.14. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, MEMÓRIA e DISCO e tais informações deverão estar disponíveis em um painel ou Dash Board específico para monitoramento;

5.3.15. Mostrar o consumo total de memória RAM, memória Swap e volume de disco e partições, de todas as interfaces de rede, os serviços que estão em execução, os serviços que estão parados, os processos que estão mais consumindo CPU, os processos que estão

mais consumindo memória, o histórico de comandos executados e por fim localização do dispositivo em mapa georreferenciado; A solução deverá permitir configurar quais serviços o agente irá monitorar, em caso de parada do serviço o agente deverá reiniciar o mesmo e ainda mediante compatibilidade única com sistemas operacionais Windows, o sistema deverá permitir monitoramento por meio de protocolo

5.3.16. SNMP de qualquer dispositivo conectado na rede;

5.3.17. Possuir proteção contra sequestro de informações, artefatos maliciosos, proteção contra invasão através de dispositivos desprotegidos e proteção contra criptografia de arquivos;

5.3.18. Deve possuir inteligência heurística para dentro dos sistemas Windows, desencapsular e analisar todas as informações contidas em artefatos maliciosos (ransomware) que cheguem oriundos da rede externa para a rede interna. Todos os pacotes de dados devem ser descapsulados e todas as informações contidas nos mesmos devem ser lidas e analisadas;

5.3.19. Deve trabalhar com o recurso Sandbox, para que as informações lidas sejam simuladas em um ambiente de testes para prever e estudar o comportamento do artefato malicioso (ransomware), uma vez que for alocado na rede interna;

5.3.20. Deve conter o recurso para, após a leitura e simulação como nos passos anteriores, nomeação do artefato malicioso (ransomware) onde o mesmo deverá ser posto fora do ambiente de produção para que um banco de informações próprias seja criado com dados sobre o artefato malicioso (ransomware) e seu possível funcionamento, o que manterá a segurança contra novas ameaças; e

5.3.21. O monitoramento comportamental personalizado para detecção de criptografia em massa deve impedir a propagação do artefato malicioso (ransomware) antes de ocorrer o sequestro de dados. Identificando comportamento suspeito e variações nas funções de aplicações, mesmo as mais sutis;

5.3.22. A licitante deverá incluir na proposta a marca e o modelo da solução ofertada para atender esse item.

5.3.23. A licitante deverá, juntamente com a proposta, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas; e,

5.3.24. Os serviços de garantia, suporte técnico e manutenção deverão ser prestados pela CONTRATADA, pela fabricante dos produtos, ou por empresa credenciada à rede nacional de assistência técnica autorizada pelo fabricante dos produtos fornecidos.

6. LOCAÇÃO DAS PLATAFORMAS DE SOFTWARES E SERVIDORES

6.1. LICENÇAS DE SOFTWARE PARA GERENCIAMENTO DE VÍDEOS EM ALTA RESOLUÇÃO PARA SERVIDOR

6.1.1. As descrições elencadas neste item referem-se apenas as características mínimas a serem atendidas pela Contratada. Todavia, esta deve garantir o funcionamento pleno de toda a solução, sendo utilizada em sua capacidade máxima, baseada no modelo que permita monitoramento e gerenciamento centralizado e em nuvem (Cloud), com todas as descrições constantes neste Termo de Referência.

6.1.2. A plataforma deverá ser uma solução de segurança de classe empresarial habilitada em tecnologia IP, com capacidade de comportar a interação com todas as licenças de softwares necessários para gerenciamento e videomonitoramento de câmeras em alta resolução para servidor.

6.1.3. O modulo de software deve ser compatível com sistemas operacionais de 64-bit, incluindo Windows Vista, Windows 7, Windows 8.1 e 10, além de Windows Server 2008, Windows Server 2012, Windows Server 2016 e Windows Server 2019.

6.1.4. O sistema deve suportar e operar com dispositivos H.265, H.264, M-JPEG, MPEG-4

6.1.5. A base do software proposto deve ser fornecida suportando todas as câmeras IP previstas neste Termo de Referência, devidamente habilitadas, porém futuras licenças adicionais não devem alterar a versão da base fornecida, devendo esta possuir uma capacidade ilimitada de câmeras/servidores ou limitada a no mínimo 1000 câmeras.

6.1.6. O sistema deve ser fornecido com atualização gratuita por até 1 ano, o licenciamento será renovado automaticamente em caso de prorrogação contratual.

6.1.7. Incluir na proposta marca e modelo dos componentes ofertados para atender esse item, juntamente com catálogo(s) e/ou manual(ais) que comprovem as características solicitadas.

6.1.8. Cliente remoto de administração:

6.1.8.1. O cliente remoto para administração deve possuir as características mínimas solicitadas abaixo:

6.1.8.2. Permitir a gestão centralizada de todos os dispositivos compatíveis, servidores, alarmes e usuários; e,

6.1.8.3. Permitir a configuração de qualquer servidor conectado à rede.

6.1.8.4. Permitir agregar permissões e acessos de usuários, e as seguintes configurações:

6.1.8.5. Suportar a criação de usuários e atribuir suas permissões por serviço de autenticação do próprio software; e,

6.1.8.6. Suportar leitura de usuários e grupos de usuários do Microsoft Active Directory, para poder atribuir suas permissões no software.

6.1.8.7. Deve permitir a adição e programação de dispositivos compatíveis, permitindo:

6.1.8.8. Detectar automaticamente na rede os dispositivos compatíveis;

6.1.8.9. Configuração da detecção de movimento e analíticos em vídeo ilimitado por servidor; e,

6.1.8.10. Configuração do monitoramento de estado e saúde do software.

6.1.8.11. Suportar permissões de usuários com, no mínimo, as seguintes funcionalidades:

6.1.8.12. Privilégio de usuário para acesso por câmera;

6.1.8.13. Controle de privilégios por grupos de usuários customizados;

6.1.8.14. Suportar diferentes perfis de segurança, que permitem ao administrador mudar em tempo real as permissões de usuários dependendo do perfil escolhido, como por exemplo, em casos de emergência;

6.1.8.15. Suportar diferentes perfis de segurança, que permitem ao administrador mudar em tempo real as permissões de usuários dependendo do perfil escolhido, como por exemplo, em casos de emergência; e,

- 6.1.8.16. Deve ser possível, ao cliente remoto, definir locais de armazenamento, configuração do failover e redundância, sem custos adicionais de licenciamento.
- 6.1.8.17. Permitir a configuração de regras/macros, com pelo menos:
- 6.1.8.18. Início do alarme, podendo ser por detecção de movimento, analíticos, entradas de alarme ou integração com terceiros;
- 6.1.8.19. Programação de quando a regra/macro deverá estar habilitada;
- 6.1.8.20. Ações que o sistema deve realizar, tais como: enviar um email/SMS, avisar o operador pela tela do Client Windows de Monitoramento, gravar uma ou mais câmeras, envio de fotos por e-mail, enviar requisições HTTP e SNMP Trap, movimentar uma câmera PTZ para um preset.
- 6.1.8.21. Implementar mapas sinóticos (ou 3D) e hierárquicos com, no mínimo, os seguintes requisitos:
- 6.1.8.22. Importar imagens para a função mapa sinótico nos seguintes formatos: BMP, GIF, PNG, TIF/TIFF e JPEG;
- 6.1.8.23. O sistema deve suportar imagens com até 8.25 megapixels;
- 6.1.8.24. Deve suportar mapa georreferenciados baseado no Open Street Map;
- 6.1.8.25. Apresentar ícones para layout compartilhado, atalho para outros sites da organização, além de ícones para os seguintes dispositivos: câmeras fixas, câmeras moveis, entradas de alarme, saídas de alarme e sinalização de portas;
- 6.1.8.26. Criar múltiplos mapas;
- 6.1.8.27. Criar hierarquia e links entre mapas;
- 6.1.8.28. Habilitar e desabilitar entradas e saídas de alarme diretamente do mapa.
- 6.1.8.29. Permitir criar permissões diferentes para múltiplos vídeo walls num mesmo sistema; e,
- 6.1.8.30. Permitir criar uma única coleção de monitores (gráfica) na tela, representando diferentes localidades físicas (diferentes vídeos walls).

6.1.9. Cliente de monitoramento:

- 6.1.9.1. O cliente para monitoramento deve possuir as características mínimas solicitadas abaixo
- 6.1.9.2. Ser compatível com computadores e estações de trabalho de prateleira, instalável em sistemas operacionais Windows;
- 6.1.9.3. Todas as funcionalidades do sistema devem ser acessíveis a partir de uma única interface de usuário, ou seja, de um único programa, sem ser necessário assim utilizar várias interfaces/programas para o monitoramento do vídeo e áudio ao vivo, gravado, visualização de alarmes e mapas, além de visualização de metadados de analíticos e resultados de reconhecimento facial e LPR;
- 6.1.9.4. Possuir uma tela de monitoramento de vídeo e áudio ao vivo e gravado.
- 6.1.9.5. Aplicar zoom digital no vídeo ao vivo e gravado.
- 6.1.9.6. Permitir os seguintes comandos para navegação:
- 6.1.9.7. Selecionar e disparar a um pré-posicionamento de uma câmera PTZ
- 6.1.9.8. Selecionar e mostrar uma câmera em específico;
- 6.1.9.9. Copiar uma imagem estática de uma câmera (ao vivo ou gravado) para colar em outro documento;
- 6.1.9.10. Enviar uma imagem estática de uma câmera (ao vivo ou gravado) para impressão;
- 6.1.9.11. Salvar uma imagem estática de uma câmera (ao vivo ou gravado) numa pasta;

- 6.1.9.12. Configuração matricial de câmeras.
- 6.1.9.13. Suportar múltiplos monitores, com as seguintes funcionalidades:
- 6.1.9.14. Tela cheia;
- 6.1.9.15. Telas flutuantes ou configuráveis por posicionamento em cada desktop;
- 6.1.9.16. Componentes da tela principal tais como a tela dos mapas, árvore de dispositivos, lista de eventos/alarmes;
- 6.1.9.17. Suportar layouts de câmeras com as seguintes funcionalidades:
- 6.1.9.18. Mostrar layouts criados na árvore de dispositivos para fácil navegação;
- 6.1.9.19. Customização da árvore de dispositivos mostrando as câmeras de todos os servidores;
- 6.1.9.20. Customização da interface de usuário, podendo posicionar o log de eventos/alarmes, lista de servidores, árvore de dispositivos, mapas e log do Sistema;
- 6.1.9.21. Possibilidade de salvar e nomear as telas customizadas para uso futuro.
- 6.1.9.22. Acionar através do ícone a visualização de um quadrante numa câmera ou a gravação do vídeo ou áudio; e,
- 6.1.9.23. Acionar através do ícone o relé ou coletor aberto de câmeras.
- 6.1.9.24. Suportar as seguintes opções de busca de vídeo e áudio:
- 6.1.9.25. Busca básica igual a VHS/VCR (pause, reproduzir à frente e atrás, aumentar a velocidade de reprodução);
- 6.1.9.26. Busca por data e hora;
- 6.1.9.27. Busca na linha de tempo;
- 6.1.9.28. A linha de tempo deve apresentar cores diferentes para indicar gravação contínua, por evento (alarme, detecção de movimento), com áudio, e marcações de bookmark;
- 6.1.9.29. Busca inteligente, por detecção de movimento numa área desenhada na visão da câmera, com possibilidade de:
- 6.1.9.30. Incluir trechos de pré e pós-alarme com tempo predeterminado;
- 6.1.9.31. Fornecer ou exportar imagens JPG de cada trecho de alarme;
- 6.1.9.32. Anunciar os eventos da seguinte forma, como mínimo:
- 6.1.9.33. Disparar manualmente eventos e saídas de alarme;
- 6.1.9.34. Permitir alarmes audíveis continuamente até ser reconhecidos.
- 6.1.9.35. Comandar câmeras móveis da seguinte forma, como mínimo:
- 6.1.9.36. Assignar comandos a botões do teclado ou do joystick;
- 6.1.9.37. Controle de PTZ por "point and click", ou seja, movimentar a câmera para o ponto selecionado no clique, na imagem;
- 6.1.9.38. Controle de zoom ao selecionar a área a ser focada;
- 6.1.9.39. Controle de zoom utilizando a rodinha do mouse;
- 6.1.9.40. Criar ilimitados tours/patterns com ilimitados preposicionamentos;
- 6.1.9.41. Direcionar a câmera para preposicionamentos em eventos;
- 6.1.9.42. Criar múltiplos tours/patterns limitados apenas pelas câmeras.
- 6.1.9.43. Permitir exportar trechos de vídeo selecionados com recursos que garantam a autenticidade dele, seja através de marca d'água ou detecção de violação;
- 6.1.9.44. Permitir exportar relatórios das seguintes informações:
- 6.1.9.45. Relatório do resumo de eventos;
- 6.1.9.46. Os relatórios podem ser exportados em arquivos CSV e PDF;
- 6.1.9.47. Sincronizar a navegação de todas as câmeras mostradas em diferentes quadrantes de uma tela.

- 6.1.9.48. A sincronização serve para imagens estáticas (pause) e para vídeo gravado;
- 6.1.9.49. Não deve limitar o número de monitores por sistema, o limite deve ser ditado pelas limitações das configurações de hardware.
- 6.1.9.50. Realizar a gestão de alarmes recebidos, atendendo os seguintes requerimentos, como mínimo:
- 6.1.9.51. Gestão centralizada dos eventos gerados por múltiplos sistemas, tais como: detecção de movimento no servidor ou nas câmeras, controle de acesso, sensores ligados ou embarcados nas câmeras; e,
- 6.1.9.52. Feedback automático, em tempo real, a todos os operadores dos clientes uma vez que um operador em outra estação reconheceu o alarme, e dos comentários deixados para este evento.
- 6.1.9.53. Incluir na proposta a marca e o modelo da solução ofertada para atender esse item. O vencedor do certame deverá, juntamente com a proposta arrematada, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas, além de carta do fabricante declarando que a licitante está autorizada a comercializar e prestar assistência técnica do produto proposto.

6.2. LICENÇAS DE SOFTWARE PARA ANÁLISE DE VÍDEO (ANÁLISE FORENSE) PARA SERVIDOR

6.2.1. As descrições elencadas neste item referem-se apenas as características mínimas a serem atendidas pela Contratada. Todavia, esta deve garantir o funcionamento pleno de toda a solução, sendo utilizada em sua capacidade máxima, baseada no modelo que permita monitoramento e gerenciamento centralizado e em nuvem (Cloud), com todas as descrições constantes neste Termo de Referência.

6.2.2. O sistema de vídeo analítico, instalado em plataforma cliente servidor, deve suportar no mínimo as seguintes especificações:

6.2.3. Câmeras suportadas:

- 6.2.3.1. ONVIF / RTSP: A solução deve suportar a análise de quaisquer transmissões de vídeo ONVIF / RTSP de câmeras fixas, angulares ou aéreas. Estas podem ser câmeras IP ou câmeras analógicas através de codificadores.
- 6.2.3.2. CÂMERAS ÓPTICAS: A solução deve suportar a análise de fluxos de vídeo de câmeras ópticas.
- 6.2.3.3. A solução deve suportar resolução mínima de 480p e deve ser capaz de suportar fluxos de maior resolução, para melhorar a distância e a precisão da detecção.
- 6.2.3.4. A resolução máxima suportada deve ser de até 4k.
- 6.2.3.5. A solução deve suportar a análise de fluxos de vídeo com taxa mínima de quadros de 8 FPS.

6.2.4. Tecnologia de análise de vídeo:

- 6.2.4.1. A solução deve ser baseada na tecnologia de aprendizagem profunda (Deep Learning) para detecção e classificação de alvos, suportando a detecção automática e a classificação dos seguintes tipos:
- 6.2.4.2. Pessoa: Em pé e/ou caída no chão;
- 6.2.4.3. Veículo de duas rodas: Motocicleta, Bicicleta;

- 6.2.4.4. Veículo: Carro, Caminhonete, Van, Ônibus, Caminhão;
- 6.2.4.5. Objeto: Malas, Bolsas, Mochilas, Caixas; E,
- 6.2.4.6. Fumaça e Fogo Fumaça, Fogo.
- 6.2.4.7. A solução deve ser capaz de detectar e ignorar automaticamente os seguintes objetos:
- 6.2.4.8. Nuvem;
- 6.2.4.9. Pássaros;
- 6.2.4.10. Cães/gatos;
- 6.2.4.11. Vegetação ;
- 6.2.4.12. A solução deve suportar a detecção da existência ou ausência de tipos de objetos personalizados.

6.2.5. Recursos de detecção e análise de eventos baseados em regras:

- 1.1.1.1. A solução deve oferecer um conjunto de regras analíticas para fornecer detecção em tempo real dos seguintes comportamentos:
- 1.1.1.2. Alvos movendo-se em uma área / vadiagem – o alvo está se movendo na região de interesse por um período, definido pelo usuário;
- 1.1.1.3. Alvo/s cruzando uma linha – o alvo cruzou uma linha definida pelo usuário em uma direção específica ou em qualquer direção;
- 1.1.1.4. Veículo parado – o alvo parou na região de interesse por um período definido pelo usuário;
- 1.1.1.5. Excesso de velocidade do veículo – o veículo alvo cruza uma linha a uma velocidade maior do que a determinada;
- 1.1.1.6. Agrupamento – detecção de um grupo denso de pessoas (quantidade configurável) na região de interesse, detectado por um período definido pelo usuário;
- 1.1.1.7. Ocupação – detecção de pessoas (quantidade configurável) na região de interesse, detectada por um período definido pelo usuário;
- 1.1.1.8. Objeto abandonado - detecção de mala/bolsa/mochila abandonada na região de interesse por um período definido pelo usuário;
- 1.1.1.9. Proteção patrimonial – marque um objeto no campo de exibição e receba um alerta quando esse objeto for removido;
- 1.1.1.10. Contramão – um veículo está viajando na direção oposta;
- 1.1.1.11. Deslizamento & queda – uma pessoa escorrega ou cai no chão ou é detectada deitada no chão;
- 1.1.1.12. Cada regra de detecção deve ser aplicável aos tipos de destino relevantes.
- 1.1.1.13. O usuário deve ser capaz de selecionar vários tipos de destino relevantes para cada regra de detecção.
- 1.1.1.14. A solução deve ser capaz de detectar a existência ou desaparecimento de objetos personalizados dentro de uma região de interesse definida pelo usuário.

6.2.6. Configuração de regras e parâmetros:

- 6.2.6.1. A solução deve fornecer a capacidade de executar operações em massa para ativar, desativar e agendar várias regras de análise.
- 6.2.6.2. A solução deve permitir que qualquer combinação de regras de análise seja executada na mesma câmera simultaneamente, sem limitações.
- 6.2.6.3. A solução deve permitir que o operador defina várias regiões de detecção por câmera.

6.2.7. Calibração da cena:

6.2.7.1. Calibração refere-se à tradução de pixels na imagem para tamanho real (metros/pés) em diferentes partes da imagem;

6.2.7.2. O sistema deve calibrar automaticamente os tamanhos dos objetos na imagem com base nos tamanhos padrão dos alvos classificados segundo modelo de rede neural profunda (DNN) na cena, ao longo do tempo;

6.2.7.3. O sistema deve ter a possibilidade de substituir a calibração automática, ou calibrar cenas em que não ocorre movimento. A calibração manual deve suportar diferentes traduções de pixel para diferentes partes da imagem, criando uma malha de calibração flexível através do quadro de imagem; e,

6.2.7.4. Todos os métodos de calibração devem suportar traduções precisas em ambientes desafiadores resultantes, por exemplo, da distorção de imagens de câmeras do tipo olho de peixe (fisheye) e cenas com múltiplos níveis.

6.2.8. Geração de eventos:

6.2.8.1. A solução deve possibilitar a geração de eventos em tempo real para alertar os operadores quando um comportamento que corresponda à regra definida pelo usuário for detectado.

6.2.8.2. A solução deve suportar o rastreamento simultâneo de vários alvos dentro das regiões de detecção e/ou das linhas de perímetro interno e/ou externo.

6.2.8.3. A solução deve gerar um vídeo curto de evento para cada detecção, mostrando vários segundos antes e depois do evento, e incluir uma caixa de limites ao redor do alvo que acionou o evento.

6.2.9. Integração:

6.2.9.1. A solução deve estar integrada e ser capaz de enviar os eventos para os seguintes sistemas externos:

6.2.9.2. Milestone XProtect VMS.

6.2.9.3. Genetec Security Center VMS.

6.2.9.4. Immix CS e Immix GF.

6.2.9.5. Sentinela.

6.2.9.6. Mobotix MxHub e Mx Management Center.

6.2.9.7. Outros sistemas baseados no protocolo WebHooks (HTTP Push); e,

6.2.9.8. Outros sistemas baseados no protocolo SMTP.

6.2.10. Detecção de anomalias:

6.2.10.1. O sistema deve ser capaz de "aprender" continuamente o comportamento típico da cena, sendo capaz de detectar automaticamente comportamentos anormais de alvos detectados e gerar eventos de anomalia em tempo real.

6.2.10.2. O sistema deve gerar um evento de anomalia, incluindo um clipe de evento com vários segundos antes e depois da data e hora do evento, delimitando caixas em torno dos alvos relevantes e descrição da anomalia detectada.

6.2.11. Investigação de vídeo:

6.2.11.1. O sistema deve analisar todas as câmeras em tempo real e criar metadados que serão armazenados em um banco de dados. Deve ser possível procurar qualquer câmera com um atraso de no máximo 10 segundos em tempo real.

6.2.11.2. Deve ser possível pesquisar qualquer ou todas as câmeras na instalação simultaneamente e sem a necessidade de processar as câmeras em pequenos lotes, independentemente do número de câmeras instaladas no sistema.

6.2.12. Definição de critérios de pesquisa:

6.2.12.1. A solução não deve exigir que o operador aplique qualquer regra ou configuração de comportamento com antecedência como pré-requisito para a realização de investigação de vídeo.

6.2.12.2. A investigação de vídeo deve ser conduzida simultaneamente em câmeras selecionadas únicas ou múltiplas, seja a partir de uma lista ou mapa.

6.2.12.3. A solução deve oferecer a busca pelos seguintes conjuntos de comportamentos, seja no campo de visão da câmera ou de uma área de interesse pré-definida:

6.2.12.4. Pessoa / Veículo de Duas Rodas (Motocicleta/Bicicleta) / Veículo (Carro, Picape, Van, Ônibus, Caminhão) movendo-se por um tempo especificado;

6.2.12.5. Pessoa / Veículo de Duas Rodas (Motocicleta/Bicicleta) / Veículo (Carro, Caminhonete, Van, Ônibus, Caminhão) cruzando uma linha para um sentido específico ou em ambos os sentidos

6.2.12.6. Pessoas agrupando-se em uma área de interesse por um tempo especificado;

6.2.12.7. Pessoas ocupando uma área de interesse por um tempo especificado;

6.2.12.8. Veículo de Duas Rodas (Motocicleta/Bicicleta) / Veículo (Carro, Picape, Van, Ônibus, Caminhão) que parou por um tempo especificado;

6.2.12.9. Bolsas/mochilas/malas que foram adicionadas por um tempo especificado;

6.2.12.10. A solução deve permitir filtragem de resultados de pesquisa com base nas características de cor alvo. Para as pessoas, a solução deve permitir especificar a cor superior do corpo e a cor inferior do corpo;

6.2.12.11. A solução deve ser capaz de pesquisar ao longo de várias opções de intervalo de tempo:

6.2.12.12. Ao longo dos últimos minutos, horas ou dias (por exemplo, nas últimas 3 horas; últimos 7 dias)

6.2.12.13. Desde uma data e hora de início até uma data e hora de término

6.2.12.14. Durante um intervalo de tempo recorrente em um intervalo de data (por exemplo, entre 8-9 da manhã, todos os dias entre 1 e 10 de janeiro)

6.2.12.15. A solução deve fornecer a capacidade de procurar alvos semelhantes: Se um alvo for encontrado, outra pesquisa pode ser realizada no vídeo gravado (gerado a partir da mesma câmera ou qualquer grupo de câmeras) para encontrar alvos que sejam iguais ou semelhantes ao alvo encontrado.

6.2.13. Visualização de resultados de pesquisa:

6.2.13.1. A solução deve ser capaz de exibir gravação de vídeo para qualquer resultado de pesquisa, sem exigir integração a uma solução de gravação de terceiros, fornecendo várias opções para visualizar resultados de pesquisa: Miniaturas do evento, Caminho de destino, Localização e Mapa de Calor.

6.2.14. Recursos de processo de investigação:

- 6.2.14.1. A solução deve fornecer os seguintes recursos de processo e investigação:
- 6.2.14.2. Os usuários devem ser capazes de salvar uma consulta de pesquisa com um nome dado para reutilização posterior.
- 6.2.14.3. Os usuários devem ser capazes de salvar resultados de pesquisa com instantâneos das detecções e informações de identificação dos resultados (ID da câmera, tempo).
- 6.2.14.4. A solução deve permitir que os usuários exportem um resultado de pesquisa para um arquivo de vídeo.

6.2.15. Estatística:

- 6.2.15.1. A solução deve oferecer regras de análise estatística para vários tipos de destino, incluindo, mas não se limitando a:
- 6.2.15.2. Contagem do número de alvos se movendo em direção, distinguindo alvos individuais em um cluster. Se um aglomerado de 4 pessoas cruzar uma linha (por exemplo), uma contagem de 4 ocorrerá em vez de 1.
- 6.2.15.3. Cálculo da velocidade média dos veículos que cruzam uma linha.
- 6.2.15.4. A solução deve oferecer estatísticas de alertas de saúde gerados no sistema, ao longo do tempo.
- 6.2.15.5. Os dados estatísticos devem estar disponíveis diretamente na aplicação ou usando APIs.

6.2.16. Georreferenciamento:

- 6.2.16.1. A solução deve permitir que o usuário configure os seguintes dados geoespaciais por fonte de vídeo conectada à solução:
- 6.2.16.2. A localização da fonte de vídeo em um mapa;
- 6.2.16.3. O registro do campo de visão da fonte de vídeo e a correlação de vários pontos em um mapa;
- 6.2.16.4. A solução deve ser capaz de apresentar eventos em tempo real ou resultados de pesquisa de investigação de vídeo em um mapa.
- 6.2.16.5. A solução deve permitir a seleção de câmeras relevantes, dentro de uma zona definida pelo usuário no mapa, para investigação de vídeo.
- 6.2.16.6. A solução deve ser capaz de apresentar um caminho de destino rastreado sobre um mapa.

6.2.17. Arquitetura do sistema:

- 6.2.17.1. A solução deve ser baseada nos seguintes componentes principais:
- 6.2.17.2. Servidores de análise:
- 6.2.17.3. O servidor realiza a análise inicial de vídeo.
- 6.2.17.4. O servidor de análise deve suportar conexão de baixa largura de banda para os serviços principais, até ~5 kbps por câmera.
- 6.2.17.5. O servidor de análise deve ser dimensionado para suportar qualquer número de câmeras.
- 6.2.17.6. O uso de GPU não deve ser necessário.
- 6.2.17.7. O servidor de análise deve suportar implantações baseadas em nuvem, on-premise e híbridas. As instalações no local sem acesso à internet ("totalmente offline") devem ser suportadas.

6.2.17.8. Servidor principal:

6.2.17.9. O servidor principal deve fornecer gerenciamento central para todas as análises de vídeo, configuração de regras e parâmetros.

6.2.17.10. Os servidores principais devem suportar implantações baseadas em nuvem e no local. As instalações no local sem acesso à internet ("totalmente offline") devem ser suportadas.

6.2.17.11. O servidor principal deve ser dimensionado para suportar qualquer número de câmeras.

6.2.17.12. Os servidores principais devem suportar implantações de alta disponibilidade.

6.2.17.13. A solução deve suportar um número ilimitado de localidades separadas que devem ser completamente isoladas umas das outras.

6.2.17.14. Cada localidade no sistema deve permitir a configuração de um número ilimitado de usuários.

6.2.17.15. Cada usuário no sistema deve receber uma função com permissões de acesso específicas a diferentes módulos da solução.

6.2.17.16. Integrações de eventos em tempo real do servidor principal com sistemas de terceiros.

6.2.17.17. Os alertas de saúde em tempo real para a integração com sistemas de terceiros devem ser suportados.

6.2.18. A licitante deverá incluir na proposta a marca e o modelo da solução ofertada para atender esse item. O licitante deverá, juntamente com a proposta, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas.

6.2.19. Os serviços de garantia, suporte técnico e manutenção deverão ser prestados pela CONTRATADA, pela fabricante dos produtos, ou por empresa credenciada à rede nacional de assistência técnica autorizada pelo fabricante dos produtos fornecidos.

6.3. LOCAÇÃO DE CONJUNTO DE SERVIDORES PARA GRAVAÇÃO E BACKUP DE VÍDEOS EM ALTA RESOLUÇÃO PARA CÂMERAS IP

6.3.1. As descrições elencadas neste item referem-se apenas as características mínimas a serem atendidas pela Contratada. Todavia, esta deve garantir o funcionamento pleno de toda a solução, sendo utilizada em sua capacidade máxima, baseada no modelo que permita monitoramento e gerenciamento centralizado e em nuvem (Cloud), com todas as descrições constantes neste Termo de Referência.

6.3.2. Suportar todas as câmeras IP e todos os seus fluxos de vídeo e áudio, com as seguintes características mínimas:

6.3.3. É de responsabilidade da CONTRATADA, o dimensionamento e a quantidade de servidores de vídeo, para atender as todas as câmeras com resolução de 2MP, utilizando 60FPS, com H.265;

6.3.4. Possuir a capacidade conjunta mínima total de gravação de 80TB;

6.3.5. Capacidade mínima de suportar 320Mbps de entrada e 250Mbps de saída;

6.3.6. Suporte compressão H.265+/H.265 (HEVC)/H.264;

6.3.7. Deverá ser capaz de fazer gravações de forma contínua, agendamento, manual, por evento totalmente integrada ao software de gerenciamento;

6.3.8. Deverá permitir configuração de DDNS;

- 6.3.9. O DDNS a ser utilizado deverá estar integrado à plataforma de gravação de vídeo em rede;
- 6.3.10. Deverá ser capaz de exportar as imagens nos formatos .EXE de forma a facilitar a visualização das imagens exportadas;
- 6.3.11. Deverá disponibilizar diferentes níveis de usuários de forma a criar diferentes privilégios de acordo com a autorização de acesso de cada usuário;
- 6.3.12. Possibilitar o armazenamento de logs de sistema, operação e eventos provenientes das câmeras;
- 6.3.13. Deverá ser do mesmo fabricante das câmeras, ou as câmeras estarem totalmente integradas mediante comprovação no site do fabricante;
- 6.3.14. Suportar padronização ONVIF profile S & T. Caso a solução seja baseada em dispositivo dedicado, tal comprovação deverá ser realizada através do site <https://www.onvif.org/conformant-products>. Não será aceito carta do fabricante para comprovação deste item, bem como não será aceito a simples indicação no catálogo comercial;
- 6.3.15. Deverá suportar e reconhecer todos os analíticos disponibilizados pelas câmeras do sistema de forma integral;
- 6.3.16. Possibilitar o backup e restauração da configuração;
- 6.3.17. Deverá ser capaz procurar as câmeras na mesma rede de domínio de broadcast;
- 6.3.18. Na tela de apresentação da câmera deverá ser capaz de mostrar informações provenientes das câmeras tais como, tipo de compressão utilizada, resolução, taxa de atualização de quadros por segundo e qualidade de vídeo;
- 6.3.19. Enviar e-mail de acordo com eventos gerados pelas câmeras;
- 6.3.20. Adicionalmente deverá suportar câmeras com protocolo Onvif;
- 6.3.21. Protocolos suportados: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, SMTP, DHCP, NTP, DNS, DDNS, SNMP, UDP, ANR e NFS;
- 6.3.22. Deverá gravar simultaneamente todas as câmeras do sistema;
- 6.3.23. Deverá ser capaz de autoconfigurar as câmeras conectadas conforme sua resolução, taxa de frames; e,
- 6.3.24. A pesquisa de gravações deverá ser feita por: evento, período e através de sistema inteligente definida por área.
- 6.3.25. Incluir na proposta a marca e o modelo da solução ofertada para atender esse item.
- 6.3.26. O vencedor do certame deverá, juntamente com a proposta arrematada, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas, além de carta do fabricante declarando que a licitante está autorizada a comercializar e prestar assistência técnica do produto proposto.

6.4. Quantitativo de Câmeras e Plataformas de Gestão:

N ^o	Unidades / Localidades	PLATAFORMAS DE GESTÃO				
		Quantidade de Câmeras IP	Software para Gerenciamento de Vídeos de Alta Resolução para Servidor (Cloud Server)	Software para Análise de Vídeo (Análise e Forense) para Servidor (Cloud Server)	Software de IA / VCA (Embarcado em IP-Cam)	Software de IA / *LPR (Embarcado em IP-Cam)
1	Escritório Central	45	45	5	43	2
2	Captação Anhumas I	3	3		3	
3	Estação Elevatória de Água Anhumas II	3	3		3	
4	Captação das Cruzes	5	5		5	
5	Captação Águas do Paiol	2	2		2	
Total:		58	58	5	56	2

* LPR para Entrada Principal de Veículos (Escritório Central)

7. DAS CÂMERAS DE VIDEOMONITORAMENTO:

7.1. Para o fornecimento das câmeras, a empresa deverá atender, no mínimo ao disposto abaixo:

7.1.1. Todos os equipamentos deverão ser novos, de primeiro uso, originais dos fabricantes e fornecidos de forma completa, ou seja, com todos os insumos necessários à sua correta instalação e operação, tais como cabos de força, manuais, acessórios de fixação etc.

7.1.2. Todas as câmeras ofertadas, deverão ser no mesmo fabricante garantindo a total compatibilidade, em todos os aspectos, para fins de facilidade operacional e perfeita integração entre componentes.

7.1.3. Todas as câmeras ofertadas, deverão possuir capacidade de armazenamento interno.

7.1.4. Para este armazenamento, todas as câmeras ofertadas, possuirão capacidade mínima de armazenamento local através de Micro SD/SDHC/SDXC de 256Gb.

7.1.5. Todas as câmeras ofertadas, deverão possuir SD Card de no mínimo 256Gb incluso e devidamente instalado e configurado para gravação simultânea.

7.1.6. Todos os serviços de garantia, suporte técnico e manutenção deverão ser prestados pela CONTRATADA, pela fabricante dos produtos, ou por empresa credenciada à rede nacional de assistência técnica autorizada pelo fabricante dos produtos fornecidos.

7.1.7. A licitante deverá incluir na proposta a marca e o modelo das câmeras ofertadas.

7.1.8. A licitante deverá, juntamente com a proposta, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas.

7.1.9. O vencedor do certame deverá, juntamente com a proposta arrematada, apresentar catálogo(s) e/ou manual(ais) que comprovem as características solicitadas, além de carta do fabricante declarando que a licitante está autorizada a comercializar e prestar assistência técnica do produto proposto.

7.2. Especificações mínimas das câmeras de monitoramento:

7.2.1. As descrições elencadas neste item referem-se apenas as características mínimas a serem atendidas pela Contratada. Todavia, esta deve garantir o funcionamento pleno de toda a solução, sendo utilizada em sua capacidade máxima, baseada no modelo que permita monitoramento e gerenciamento centralizado e em nuvem, e com processamento local através de IA embarcada diretamente nos dispositivos (câmeras), conforme todas as descrições constantes neste Termo de Referência.

7.2.2. Todas as câmeras IP previstas no neste Termo de Referência deverão possuir padronização mínima ONVIF, com validação verificável através do site www.onvif.org.

CÂMERA:		TIPO 01
Câmera	Descrição	Câmera IP Tipo bullet com lente fixa para utilização em ambientes externos. Resolução: 2MP
	Sensor de imagem	Sensor de imagem em estado sólido do tipo CMOS ou CCD de 1/2.8" ou maior e com escaneamento progressivo.
	Iluminação mínima	Sensibilidade à iluminação igual ou inferior a 0,005 lux em modo colorido considerando F1.6 ou melhor. Filtro de bloqueio de iluminação infra-vermelha (IR) removível automaticamente.
	WDR	Wide Dynamic Range de, no mínimo 120 dB.
	Lentes	Lente fixa com comprimento focal entre de 4mm com no mínimo F1.6 e correção de IR
	Campo de visão	Deve proporcionar ângulo de visualização mínimo de 90°(Horizontal).
	Dia e noite / Distância IR	Possuir Infravermelho Integrado com capacidade de no mínimo 30mts
Vídeo	Resolução da Imagem e fluxo principal	Resolução de 1920 x 1080 pixels a 60fps em fluxo principal.
	Compressão de vídeo	Implementar no mínimo os formatos de compressão H.265 (HEVC), H.264; MJPEG.
Rede	Interface de comunicação	Saída UTP para conexão em rede TCP/IP RJ-45 100BASE-TX conector RJ-45.
	Protocolos suportados	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, Bonjour, DNS, DDNS, PPPoE, QoS, SNMP, 802.1X, ICMP, SSL e SIP.
	Armazenamento em rede	Capacidade de armazenamento em rede (NAS ou Servidor de Arquivos) através da câmera;
Sistema	Armazenamento interno	Capacidade de armazenamento local através de MicroSD/SDHC/SDXC até 256G, com SD Card de 256Gb incluso;
	Acionamento de alarme	Possuir gatilhos em caso de detecção de movimento, disparo manual, ativação de dispositivo de entrada, disparo programado, inicialização do sistema, notificação de disco/cartão cheio, violação da câmera;

Configurações gerais	Ações de eventos	Permitir geração de alarmes por notificação de evento usando saída digital, HTTP, SMTP, FTP;
	Funções inteligentes	possuir vídeo analítico embarcado diretamente na câmera, com no mínimo as seguintes condições: área de entrada, área de saída, detecção de movimento, detecção de obstrução da câmera, detecção de humano, contagem de pessoas, objetos abandonados e removidos e cruzamento de linha;
	Compatibilidade	Possui padronização mínima ONVIF profile S, T & G, com validação no site www.onvif.org
	Temperatura de trabalho	Deve suportar temperatura de operação de -40° C a 60/C;
	Fonte de energia	Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais.
	Grau de proteção	Caixa de proteção do tipo Bullet resistente a vandalismo com classificação IK10 e resistente a água com classificação IP67;
	Configurações gerais	Deve ser fornecida com capacidade embarcada para a configuração de no mínimo 04 máscaras de privacidade na própria câmera.
		Tecnologia de redução de ruído 3D;
		Deve possuir no mínimo 3 fluxos de vídeo com configuração de vídeo independentes;
		Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo.
		Possibilitar compensação automática para tomada de imagem contra luz de fundo.
		Formato tipo Bullet e permitindo ajustes triaxiais de posicionamento do suporte;
		Possuir caixa de junção para proteção de conexão;
Caixa de componentes		PoE incluso;
		Relação sinal ruído superior a 55dB;
Garantia		Recurso para ajuste de limite de largura de banda e taxa de frames.
	Caixa de componentes	Caixa de componentes contendo: Nobreak 600VA com auto start, bateria 12v 7A, protetores de surto, switch; postes metálicos e suportes de fixação quando necessários;
	Garantia	Garantia mínima de 12 meses, renovados por iguais e sucessivos períodos contratuais

CÂMERA:		TIPO 02
Câmera	Descrição	Câmera IP Tipo dome com lente fixa para utilização em ambientes internos. Resolução: 2MP
	Sensor de imagem	Sensor de imagem em estado sólido do tipo CMOS ou CCD de 1/2.8" ou maior e com escaneamento progressivo.
	Iluminação mínima	Sensibilidade à iluminação igual ou inferior a 0,005 lux em modo colorido considerando F1.6 ou melhor; Filtro de bloqueio de iluminação infra-vermelha (IR) removível automaticamente.
	WDR	Wide Dynamic Range de, no mínimo 120 dB.

	Lentes	Lente fixa com comprimento focal entre de 4mm com no mínimo F1.6 e correção de IR
	Campo de visão	Deve proporcionar ângulo de visualização mínimo de 90°(Horizontal).
	Dia e noite/Distância IR	Possuir Infravermelho Integrado com capacidade de no mínimo 20mts
Vídeo	Resolução da Imagem e fluxo principal	Resolução de 1920 x 1080 pixels a 60 fps em fluxo principal.
	Compressão de vídeo	Implementar no mínimo os formatos de compressão H.265 (HEVC), H.264; MJPEG.
Rede	Interface de comunicação	Saída UTP para conexão em rede TCP/IP RJ-45 100BASE-TX conector RJ-45.
	Protocolos suportados	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, Bonjour, DNS, DDNS, PPPoE, QoS, SNMP, 802.1X, ICMP, SSL e SIP.
	Armazenamento em rede	Capacidade de armazenamento em rede (NAS ou Servidor de Arquivos) através da câmera;
Sistema	Armazenamento interno	Capacidade de armazenamento local através de MicroSD/SDHC/SDXC até 256G, com SD Card de 256Gb incluso;
	Acionamento de alarme	Possuir gatilhos em caso de detecção de movimento, disparo manual, ativação de dispositivo de entrada, disparo programado, inicialização do sistema, notificação de disco/cartão cheio, violação da câmera;
	Ações de eventos	Permitir geração de alarmes por notificação de evento usando saída digital, HTTP, SMTP, FTP;
	Funções inteligentes	Deve possuir a capacidade receber vídeo analítico embarcado diretamente na câmera, com no mínimo as seguintes condições: área de entrada, área de saída, detecção de movimento, detecção de obstrução da câmera, detecção de humano, contagem de pessoas, objetos abandonados e removidos e cruzamento de linha;
	Compatibilidade	Possui padronização mínima ONVIF profile T, S & G, com validação no site www.onvif.org
Configurações gerais	Temperatura de trabalho	Deve suportar temperatura de operação de -40°C a 60°C;
	Fonte de energia	Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais.
	Grau de proteção	Caixa de proteção do tipo dome resistente a vandalismo com classificação IK10 e resistente a água no mínimo com classificação IP66;
	Configurações gerais	Deve ser fornecida com capacidade embarcada para a configuração de máscaras de privacidade na própria câmera.
		Tecnologia de redução de ruído 3D;
		Deve possuir no mínimo 3 fluxos de vídeo com configuração de vídeo independentes;
		Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo.
		Possibilitar compensação automática para tomada de imagem contra luz de fundo.
		Formato tipo dome e permitindo ajustes triaxiais de posicionamento da câmera;

	Possuir suporte para instalação;
	PoE incluso;
	Relação sinal ruído superior a 55dB;
	Recurso para ajuste de limite de largura de banda e taxa de frames.
Caixa de componentes	Caixa de componentes contendo: Nobreak 600VA com auto start, bateria 12v 7A, protetores de surto, switch; postes metálicos e suportes de fixação quando necessários;
Garantia	Garantia mínima de 12 meses, renovados por iguais e sucessivos períodos contratuais

CÂMERA:		TIPO 03
Câmera	Descrição	Camera IP tipo Bullet LPR com lente motorizada. Resolução: 2MP
	Sensor de imagem	Sensor de imagem em estado sólido do tipo CMOS ou CCD de 1/2.8" ou maior e com escaneamento progressivo.
	Iluminação mínima	Sensibilidade à iluminação igual ou inferior a 0,005 lux em modo colorido considerando F1.4 ou melhor Filtro de bloqueio de iluminação infra-vermelha (IR) removível automaticamente.
	WDR	Wide Dynamic Range de, no mínimo 120dB
	Lentes	Lente motorizada com comprimento focal de 2.7mm ~ 13,5mm com F1.4 e correção de IR, ou outra medida que proporcione o ângulo desejado.
	Campo de visão	Deve proporcionar ângulo de visualização de 115° ~ 34°(Horizontal).
	Dia e noite / Distância IR	Possuir Infravermelho Integrado com capacidade de no mínimo 50mts.
Vídeo	Resolução e fluxo principal	Resolução de 1920 x 1080 pixels a 60 fps em fluxo principal.
	Compressão de vídeo	Implementar no mínimo os formatos de compressão H.265 (HEVC), H.264; MJPEG.
Rede	Interface de comunicação	Saída UTP para conexão em rede TCP/IP RJ-45 100BASE-TX conector RJ-45.
	Protocolos suportados	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, Bonjour, DNS, DDNS, PPPoE, QoS, SNMP, 802.1X, ICMP, SSL e SIP.
	Armazenamento em rede	Capacidade de armazenamento em rede (NAS suportando NFS, SMB/CIFS e ANR) através da câmera;
Sistema	Armazenamento interno	Capacidade de armazenamento local através de MicroSD/SDHC/SDXC até 1Tb, com SD Card de 256Gb incluso;
	Acionamento de alarme	Possuir gatilhos em caso de detecção de movimento, disparo manual, ativação de dispositivo de entrada, disparo programado, inicialização do sistema, notificação de disco/cartão cheio, violação da câmera;
	Ações de eventos	Permitir geração de alarmes por notificação de evento usando saída digital, HTTP, SMTP, FTP;
	Funções inteligentes	Deve possuir a capacidade receber vídeo analítico com no mínimo as seguintes condições: Leitura de placa veicular (LPR) até 100Km/h; Acuracidade de até 98%; identificação e contagem de veículos;

		Identificação de 2 faixas simultâneas.
	Compatibilidade	Possui padronização mínima ONVIF profile M, T, S & G com validação no site www.onvif.org ;
	Temperatura de trabalho	Deve suportar temperatura de operação de -40° C a 60°C;
	Fonte de energia	Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de adicionais.
	Grau de proteção	Caixa de proteção do tipo Bullet resistente a vandalismo com classificação IK10 e resistente a água com classificação IP67;
Configurações gerais	Configurações gerais	Deve ser fornecida com capacidade embarcada para a configuração de no mínimo 08 máscaras de privacidade na própria câmera.
		Tecnologia de redução de ruído 3D;
		Deve possuir no mínimo 3 fluxos de vídeo com configuração de vídeo independentes.
		Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo.
		Deve possuir função de BLC, HLC, AWB, AGC, filtro de IP e modelo corredor;
		Possibilitar compensação automática para tomada de imagem contra luz de fundo;
		Formato tipo Bullet e permitindo ajustes triaxiais de posicionamento do suporte;
		Possuir caixa de junção integrada ao corpo da camera para proteção de conexões;
		PoE incluso;
		Relação sinal ruído superior a 55dB;
	Caixa de componentes	Recurso para ajuste de limite de largura de banda e taxa de frames. Caixa de componentes contendo: Nobreak 600VA com auto start, bateria 12v 7A, protetores de surto, switch; postes metálicos e suportes de fixação quando necessários;
	Garantia	Garantia mínima de 12 meses, renovados por iguais e sucessivos períodos contratuais

CÂMERA:		TIPO 04
Câmera	Descrição	Câmera IP Panorâmica, com campo de visão de 360° em horizontal. Resolução: 12MP
	Sensor de imagem	Sensor de imagem em estado sólido do tipo CMOS ou CCD de 1/1,7" ou maior e com escaneamento progressivo.
	Iluminação mínima	Sensibilidade à iluminação igual ou inferior a 0,05 lux em modo colorido, considerando F2.8 ou melhor; Filtro de bloqueio de iluminação infra-vermelha (IR) removível automaticamente.
	WDR	Wide Dynamic Range de, no mínimo 120 dB.
	Lentes	Lente fixa de 1,98mm com F2.8 e correção de IR.
	Campo de visão	Deve proporcionar ângulo de visualização mínimo de 360°(Horizontal).

Vídeo	Dia e noite / Distância IR	Possuir Infravermelho Integrado com capacidade de no mínimo 15mts
	Resolução da Imagem e fluxo principal	Resolução de no mínimo 3000 x 3000 pixels a 30 fps em fluxo principal.
	Compressão de vídeo	Implementar no mínimo os formatos de compressão H.265 (HEVC), H.264; MJPEG.
Rede	Interface de comunicação	Saída UTP para conexão em rede TCP/IP RJ-45 100BASE-TX conector RJ-45.
	Protocolos suportados	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, QoS, SNMP, 802.1X, ICMP, SSL e SIP.
	Armazenamento em rede	Capacidade de armazenamento em rede (NAS suportando NFS, SMB/CIFS e ANR) através da câmera;
Sistema	Armazenamento interno	Capacidade de armazenamento local através de MicroSD/SDHC/SDXC até 256G, com SD Card de 256Gb incluso;
	Acionamento de alarme	Possuir gatilhos em caso de detecção de movimento, disparo manual, ativação de dispositivo de entrada, disparo programado, inicialização do sistema, notificação de disco/cartão cheio, violação da câmera;
	Ações de eventos	Permitir geração de alarmes por notificação de evento usando saída digital, HTTP, SMTP, FTP;
	Funções inteligentes	Deve possuir a capacidade receber vídeo analítico embarcado diretamente na câmera, com no mínimo as seguintes condições: área de entrada, área de saída, detecção de movimento, detecção de obstrução da câmera, detecção de humano, contagem de pessoas, objetos abandonados e removidos e cruzamento de linha;
	Compatibilidade	Possui padronização ONVIF profile T, S & G, com validação no site www.onvif.org ;
Configurações gerais	Temperatura de trabalho	Deve suportar temperatura de operação de -40° C á 60/C;
	Fonte de energia	Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais e 12 VDC +/-10%
	Grau de proteção	Caixa de proteção do tipo Bullet resistente a vandalismo com classificação IK10 e resistente a água com classificação IP67;
	Configurações gerais	Deve ser fornecida com capacidade embarcada para a configuração de no mínimo 24 máscaras de privacidade na própria câmera.
		Tecnologia de redução de ruído 3D;
		Deve possuir no mínimo 2 fluxos de vídeo com configuração de vídeo independentes;
		Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo.
		Possibilitar compensação automática para tomada de imagem contraluz de fundo.
		Deve possuir interface de rede RJ45 10/100/1000 Mb
		Possuir suporte para instalação;
		PoE incluso;
		Relação sinal ruído superior a 55dB;
		Recurso para ajuste de limite de largura de banda e taxa de frames.

Caixa de componentes	Caixa de componentes contendo: Nobreak 600VA com auto start, bateria 12v 7A, protetores de surto, switch; postes metálicos e suportes de fixação quando necessários;
Garantia	Garantia mínima de 12 meses, renovados por iguais e sucessivos períodos contratuais

CÂMERA:		TIPO 05
Câmera	Descrição	Câmera PTZ IP com ZOOM OPTICO de no mínimo 23x. Resolução: 2MP
	Sensor de imagem	Sensor de imagem em estado sólido do tipo CMOS ou CCD de 1/2.8" ou maior e com escaneamento progressivo.
	Iluminação mínima	Sensibilidade à iluminação igual ou inferior a 0,005 lux em modo colorido, considerando F1.5 ou melhor; Filtro de bloqueio de iluminação infra-vermelha (IR) removível automaticamente para função day/night.
	WDR	Wide Dynamic Range de, no mínimo 120 dB.
	Lentes	Lente motorizada de 5 - 117mm ou superior, com zoom óptico de no mínimo 23x e zoom digital de 16x, ou superior, com ajuste de foco e zoom remoto
	Campo de visão	Abertura Horizontal maior ou igual a 3° ~ 60° ou superior; Recurso de 360° contínuo, com velocidade manual de 0.1° ~ 250°/s e até 250°/s em preset.
	Dia e noite / Distância IR	Possuir Infravermelho Integrado com capacidade de no mínimo 200m.
Vídeo	Resolução e fluxo principal	Resolução de no mínimo 1920 x 1080 pixels a 60 fps em fluxo principal.
	Compressão de vídeo	Implementar no mínimo os formatos de compressão H.265 (HEVC), H.264; MJPEG.
Rede	Interface de comunicação	Possuir interface de rede 10/100 Mbps Ethernet, RJ-45;
	Protocolos suportados	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, QoS, SNMP, 802.1X, ICMP, SSL e SIP.
	Armazenamento em rede	Capacidade de armazenamento em rede (NAS ou Servidor de Arquivos) da câmera;
Sistema	Armazenamento interno	Capacidade de armazenamento local através de MicroSD/SDHC/SDXC até 256G, com SD Card de 256Gb incluso;
	Acionamento de alarme	Possuir gatilhos em caso de detecção de movimento, disparo manual, ativação de dispositivo de entrada, disparo programado, inicialização do sistema, notificação de disco/cartão cheio, violação da câmera;
	Ações de eventos	Permitir geração de alarmes por notificação de evento usando saída digital, HTTP, SMTP, FTP;
	Funções inteligentes	Deve possuir a capacidade receber vídeo analítico embarcado diretamente na câmera, com no mínimo as seguintes condições: área de entrada, área de saída, detecção de movimento, detecção de obstrução da câmera, detecção de humano, contagem de pessoas, objetos abandonados e removidos e cruzamento de linha, deve possuir função auto tracking para rastreamento de pessoas;

	Compatibilidade	Possui padronização mínima ONVIF profile T, S & G, com validação no site www.onvif.org ;
	Temperatura de trabalho	Deve suportar temperatura de operação de -30° C a 60°C;
	Fonte de energia	Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais e 12 VDC +/-10%
	Grau de proteção	Resistente a vandalismo com classificação IK10 e resistente a água no mínimo com classificação IP66;
Configurações gerais	Configurações gerais	Deve ser fornecida com capacidade embarcada para a configuração de no mínimo 24 máscaras de privacidade na própria câmera.
		Tilt com alcance variando entre -5° e 90°, com velocidade manual de 0.1° ~ 160°/s e até 160°/s em preset; deve possuir, no mínimo 300 presets; deve possuir a capacidade embarcada de realizar até 8 rondas com no mínimo 48 presets em cada ronda.
		Deve possuir no mínimo 3 fluxos de vídeo com configuração de vídeo independentes;
		Tecnologia de redução de ruído 3D;
		Permite o acesso remoto por dispositivos móveis através do protocolo RTSP;
		Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo.
		Alternar automaticamente, manualmente ou sob predefinição entre o modo colorido e monocromático em função do nível de luminosidade incidente na câmera (day/night)
		Formato tipo Bullet e permitindo ajustes triaxiais de posicionamento do suporte;
		Possuir suporte para instalação;
		PoE incluso;
		Possuir tecnologia de Redução de ruído noturno 2D e 3D;
		Deve possuir BLC, HLC, AWB, AGC, Modo corredor e filtro de IP.
	Caixa de componentes	Caixa de componentes contendo: Nobreak 600VA com auto start, bateria 12v 7A, protetores de surto, switch; postes metálicos e suportes de fixação quando necessários;
	Garantia	Garantia mínima de 12 meses, renovados por iguais e sucessivos períodos contratuais

7.3. LOCAIS, POSICIONAMENTO E QUANTIDADES POR TIPO DE CÂMERAS:

LOCAL		DESCRIÇÃO	QUANTIDADE DE CÂMERAS					
			TIPO 01	TIPO 02	TIPO 03	TIPO 04	TIPO 05	
1.0		Escritório central, Av. José Parisi, 529.						
1.1	Local 01 - Prédio da Gerência de Inteligência e Informação	01 câmera fixada na parte superior do prédio com visada para a porta de entrada e fachada pelo lado da Rua José Parisi; 01 câmeras internas na sala do Centro de Inteligência e Informação.	1	1	0	0	0	
1.2	Local 02 - Garagem	01 câmera com visada para a garagem de tratores, fixada em poste de energia existente no local; 01 com visada para as "celas" do almoxarifado e garagem de motos fixada em poste de energia existente no local; 01 câmera fixada na parede lateral da oficina com visada para a via de acesso à Gerência de Redes.	3	0	0	0	0	
1.3	Local 03 - Entrada e Saída de veículos	02 câmeras LPR com Lente motorizada para leitura de placa, controlando o fluxo de entrada e saída de veículos.	0	0	2	0	0	
1.4	Local 04 - ETA Fonte	01 Câmeras fixada na parte superior do prédio da ETA Fonte com visada para a praça, sendo uma de cada lado, proporcionando uma visão ampla da área em frente a fachada; 02 câmeras na parte interna da ETA com visada para acessos ao prédio.	0	2	0	0	1	
1.5	Local 05 - Gerência de redes	01 Câmera fixada no prédio da gerência de redes com visada para o lavador de veículos e demais movimentações no entorno; 01 Câmera fixada no prédio da gerência de redes com visada para as duas laterais do CAUD e escada de incêndio; 01 câmera interna com visada para o relógio de ponto.	2	1	0	0	0	
1.6	Local 06 - Oficina de elétrica	01 câmera fixada em poste existente no local com visada para via de acesso sentido reservatório de chapa; 01 câmera fixada em poste existente no local com visada para poço e acesso ao estacionamento da frota.	2	0	0	0	0	
1.7	Local 07- Bloco administrativo	04 Câmeras internas fixadas nas paredes e tetos, posicionadas de forma a visualizar a área do hall da superintendência e corredor do auditório, corredor das diretorias, hall do xerox sentido porta frontal; hall do xerox sentido portas centrais e corredor do RH; 01 câmera externa fixada na parede lateral de forma a visualizar o acesso de pessoas e veículos pela	1	4	0	1	0	

		passagem entre o estacionamento e o bloco administrativo; 01 Câmera Auditório						
1.8	Local 08 - Frota Estacionamento	01 Câmera PTZ com visada para o pátio de veículos e baias do almoxarifado.	0	0	0	0	0	1
1.9	Local 09 - CAUD	02 câmeras internas fazendo a cobertura da área de atendimento e acessos internos; 03 câmeras externas fixadas nas paredes do CAUD com visada para o acesso principal, estacionamento fachada lateral e estacionamento e portão de acesso.	3	2	0	0	0	0
1.10	Local 10 - Almoxarifado	01 câmera com visada para o portão de acesso e balcão do almoxarifado; 01 câmera fixada na parede lateral da oficina de eletromecânica com visada para portão de acesso e pátio interno; 01 câmera fixada na casa de bombas do tanque de lodo com visada a fachada lateral do almoxarifado.	2	1	0	0	0	0
1.11	Local 11 - Portaria Central	02 câmeras posicionadas no interior da portaria de forma a visualizar a catraca, porta de acesso e relógio de ponto, interior da guarita; 02 câmeras externas posicionadas de forma a visualizar a porta de entrada, escadaria e balcão de atendimento frontal e balcão de atendimento lateral e via de acesso de veículos.	2	2	0	0	0	0
1.12	Local 12 - Área livre entre o laboratório e a ETA Fonte.	01 câmera fixada em poste existente no local, com visada para a para entrada da ETA, portão lateral de acesso à praça e área livre; 01 câmera fixada em poste existente no local, com visada para acesso do laboratório e área de estacionamento.	2	0	0	0	0	0
1.13	Local 13 - Estacionamento bloco administrativo	02 câmeras fixadas em poste metálico existente com visada para o estacionamento interno e acesso do prédio administrativo.	2	0	0	0	0	0
1.14	Local 14 - Restaurante e área de convívio.	01 câmera fixada na parte interna do restaurante com visada para a área do buffet e acesso lateral; 01 câmera na varanda do restaurante com visada para as catracas de entrada e saída de pessoas.	1	1	0	0	0	0
1.15	Local 15 - Unidade de Supressão e Reabertura	01 câmera com visada reta para o estacionamento logo a frente e divisa com a rua;	1	0	0	0	0	0
1.16	Local 16 - Laboratório e GTI	01 câmera com visada para o estacionamento e porta de acesso do prédio GTI e prédio do laboratório; 01 câmera com visada para o estacionamento e portão de acesso pelo estacionamento frontal.	2	0	0	0	0	0
1.17	Local 17 - Reservatório elevado	01 câmera fixada na estrutura do reservatório elevado com visada para as vias de acesso existente no local, sentido divisas com a CTA.	0	0	0	0	0	1

1.18	Local 18 – Entorno do Escritório Central	01 câmera fixada em poste existente no local, no cruzamento da Rua Domingos Barbieri com a Avenida José Parisi, com visada para as fachadas frontal e lateral da autarquia (lado externo).	0	0	0	0	1
2.0	Outros Locais						
2.1	Captação Anhumas I	As câmeras internas deverão ser fixadas em pontos estratégicos na edificação existente no local (Casa de Bombas), permitindo a visualização das bombas e painéis elétricos; A câmera motorizada externa deverá ser fixada em poste, de no mínimo 6,00 metros, a ser instalado em ponto estratégico do local (terreno) permitindo a visualização das áreas internas, portão de acesso e entorno da casa de bombas.	2	1	0	0	0
2.2	Estação Elevatória de Água Anhumas II	As câmeras deverão ser fixadas em pontos estratégicos na edificação existente no local (Casa de Bombas), permitindo a visualização das bombas e painéis elétricos (câmera interna) e áreas externas, incluindo portão de acesso.	3	0	0	0	0
2.3	Captação das Cruzes	As câmeras deverão ser fixadas em pontos estratégicos nas edificações existentes no local (Casa de Bombas e museu), permitindo a visualização das bombas e painéis elétricos (câmeras internas), barramento da represa e áreas externas, incluindo portão de acesso.	5	0	0	0	0
2.4	Captação Águas do Paiol	As câmeras deverão ser fixadas em poste de iluminação existente no local, permitindo a visualização do barramento da represa, guarita e portão de acesso.	2	0	0	0	0
TOTAL POR TIPO:			36	15	2	1	4
TOTAL GERAL:			58				

7.4. TABELA RESUMO:

CÂMERA	DESCRIÇÃO	TOTAL
TIPO 01	Câmera IP Tipo bullet com lente fixa para utilização em ambientes externos; Resolução: 2MP; Possuir Infravermelho Integrado com capacidade de no mínimo 30mts.	36
TIPO 02	Câmera IP Tipo dome com lente fixa para utilização em ambientes internos; Resolução: 2MP; Possuir Infravermelho Integrado com capacidade de no mínimo 20mts.	15
TIPO 03	Câmera IP Tipo bullet com lente motorizada para utilização em ambientes externos; Resolução: 2MP; Possuir Infravermelho Integrado com capacidade de no mínimo 20mts para LPR	2
TIPO 04	Câmera IP 360° com lente fixa ambientes externos; Resolução: 12MP; deve proporcionar ângulo de visualização de 360°(Horizontal); Possuir Infravermelho Integrado com capacidade de no mínimo 15mts.	1
TIPO 05	Câmera PTZ IP com ZOOM OPTICO de 23x; Resolução: 2MP; Recurso de 360° contínuo; Possuir Infravermelho Integrado com capacidade de no mínimo 200mts	4
TOTAL:		58

8. DO ARMAZENAMENTO DAS IMAGENS

8.1. A CONTRATADA deverá fornecer solução para a guarda e armazenamento em nuvem das imagens gerada pelo Sistema de Monitoramento, com disponibilidade de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

8.2. As imagens captadas de todos os dispositivos presentes em todas as unidades monitoradas, deverão ser gravadas e armazenadas pelo com resolução mínima de 1080p, 30fps, pelo período mínimo de 20 (vinte) dias;

8.3. Em Cloud Server, em seu conjunto, em espaço de até 80Tb; e de maneira simultânea,

8.4. Em cada uma das câmeras, individualmente, em SD Card com no mínimo 256Gb.

9. DA PRESTAÇÃO DE SERVIÇOS DE 'INTERCONEXÃO'

9.1. A Fornecimento de Link clear channel (fibra-óptica), com velocidade de 1 Gbps (1 Giga), sem limite de tráfego, com garantia mínima de 99% da banda, com VLAN privativa L3 em bloco IPV4 privado, compreendendo suporte técnico, incluindo serviço de cabeamento, instalação, gerenciamento, manutenção, fornecimento e configuração dos equipamentos a serem utilizados para a prestação do serviço contratado.

10. DOS SERVIÇOS DE MANUTENÇÃO TÉCNICA PREVENTIVA E CORRETIVA

10.1. A Manutenção Técnica Preventiva contempla os serviços efetuados para manter os equipamentos funcionando em condições normais, tendo como objetivo diminuir as possibilidades de paralisações, compreendendo: manutenção do bom estado de conservação, substituição ou reparo de pequenos componentes que comprometam o bom funcionamento, modificações necessárias com objetivo de atualização dos aparelhos,

limpeza, regulagem, inspeção, calibração e simulação de testes mecânicos e eletroeletrônicos em todo sistema interno e externo, entre outras ações que garantam que o conjunto dos equipamentos esteja em permanente condição de operação.

10.2. A Manutenção Técnica Corretiva contempla os serviços de reparo com a finalidade de eliminar todos os defeitos existentes nos equipamentos identificados por meio de diagnóstico, bem como da correção de anormalidades, da realização de testes e regulagens que sejam necessárias para garantir o retorno do equipamento às condições normais de funcionamento, e na substituição do equipamento sem que haja prejuízo ao funcionamento do sistema.

10.3. Caberá à CONTRATADA manter o sistema em perfeitas condições de uso durante todo o período de duração do contrato, comprometendo-se a reparar ou substituir, se for o caso, os acessórios ou componentes que apresentarem falhas e que caracterizarem ou não perda das funções básicas do sistema.

10.4. As falhas constatadas deverão ser sanadas de imediato, observando os prazos previstos no acordo de nível de serviço integrante neste Termo de Referência.

10.5. A CONTRATADA deverá elaborar e entregar ao DAAE, após a execução de cada manutenção preventiva e/ou corretiva, um relatório do serviço prestado onde deverão constar: a data da manutenção, os itens verificados, as anomalias encontradas, medidas corretivas adotadas (quando for o caso), peças ou equipamentos substituídos e nome do técnico responsável pela manutenção.

10.6. Para a gestão dos serviços de manutenção preventiva e corretiva, a CONTRATADA deverá utilizar software de gerenciamento que permita: abertura de chamados de manutenção; acompanhamento do planejamento e execução das manutenções preventivas e corretivas; flexibilidade e simplicidade na organização dos dados e informações; apresentação de resultados em formas de tabelas e gráficos; consultas e relatórios com recursos de ordenação, filtro e localização; criação de relatórios personalizados; distinção de níveis de permissão.

10.7. A CONTRATADA deverá fornecer ao DAAE acesso irrestrito e em tempo real ao software de gerenciamento de manutenções, com possibilidade de abertura de chamados e acompanhamento de todos os dados lançados no sistema, realização de consultas em toda a base de dados e geração de relatórios.

10.8. Quando necessária a substituição de materiais do sistema de vigilância eletrônica, a CONTRATADA deverá instalar equipamentos de primeira linha de fabricação, de acordo com as especificações do fabricante, nunca inferiores.

10.9. Caberá à CONTRATADA, durante a vigência do contrato, garantir o funcionamento dos equipamentos fornecidos realizando, sem custo extra à DAAE, toda a manutenção destes equipamentos, inclusive realizando a substituição de peças desgastadas e/ou danificadas dos equipamentos.

10.10. Caberá à CONTRATADA, durante a vigência do contrato, atender ao disposto neste termo de referência, inclusive quanto ao quantitativo de câmeras e equipamentos disponíveis, se responsabilizando por sua reposição e pelo restabelecimento das condições de funcionamento estabelecidas neste edital, em caso de furto, roubo ou danos decorrentes de vandalismo, caso fortuito ou de força maior.

10.11. A CONTRATADA deverá comunicar ao fiscal e ao gestor do contrato todas as ocorrências nos equipamentos instalados, que possam comprometer ou não os serviços.

10.12. Os custos da Manutenção Técnica Preventiva e Corretiva devem ser referentes a cada um dos equipamentos e sistemas locados.

11. SUPORTE TÉCNICO CONTÍNUO DAS SOLUÇÕES

11.1. A CONTRATADA deverá disponibilizar suporte técnico contínuo ao CONTRATANTE com o objetivo de restaurar os serviços dos usuários o mais rápido possível, provendo soluções definitivas e soluções de contorno minimizando assim o impacto causado pelas possíveis falhas das soluções contratadas.

11.2. A fim de prestar seus serviços, a CONTRATADA deverá possuir um CANAL DE ATENDIMENTO aos chamados em 1º Nível, por telefone e/ou sistema Web com disponibilidade de 24x7, ou seja, de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com SLA (Service Level Agreement) de até 2 (duas) horas para o atendimento e até 4 (quatro) horas para resolução de problemas de alta severidade e alto impacto, remota ou presencialmente.

11.3. Para a abertura de um chamado técnico, aqui denominado OCORRÊNCIA, a CONTRATANTE informa à CONTRATADA a ocorrência de falha de funcionamento ou o não funcionamento geral ou parcial dos equipamentos ou softwares. Imediatamente após este procedimento, deverá a CONTRATADA informar a CONTRATANTE o identificador da ocorrência com data de abertura para referência no acompanhamento dos serviços de assistência técnica.

11.4. Uma vez registrada a OCORRÊNCIA, a CONTRATADA iniciará o atendimento primeiramente em nível 1, Service Desk, e caso exista necessidade, em nível 2, Atendimento de Campo, cabendo à CONTRATADA o fornecimento de aplicação para acompanhamento de aberturas e tratamentos das OCORRÊNCIAS, o qual deverá possuir interface web para o acompanhamento e emissão de relatórios destes chamados por parte da CONTRATANTE.

11.5. O serviço de atendimento de 1º Nível prestado pelo Service Desk deverá seguir as boas práticas preconizadas pelo ITILv3.

11.6. O serviço de atendimento de 2º Nível deverá ser prestado por técnico(s) especializado(s), com formação e/ou certificação adequada ao problema a ser tratado. Estes técnicos serão acionados sempre que houver a necessidade. O atendimento especializado prestado no local da ocorrência é denominado Atendimento de Campo.

11.7. A CONTRATADA deverá prever o atendimento de campo para realização de manutenções preventivas, realizadas conforme agendamento prévio, e corretivas, tratamento de chamado de visitas corretivas.

11.8. Os atendimentos e visitas preventivas deverão ser realizadas para atuações de até 60h (sessenta horas) mensais para rotinas remotas e/ou presenciais, com ações de checagem, limpeza, regulagem, ajustes, reconfigurações realizadas pela CONTRATADA, para atendimentos e visitas técnica preventivas com disponibilidade de 8x5, ou seja, de 8 (oito) horas por dia e 5 (cinco) dias por semana em horário comercial em intervalos predeterminados de forma a reduzir a probabilidade de falha ou a degradação do funcionamento, nos locais e horários programados previamente, em conjunto com a CONTRATANTE, para verificação, identificação e prevenção de possíveis defeitos de funcionamento ou performance dos equipamentos ou soluções conforme descrito a seguir:

11.8.1. Verificação das câmeras;

11.8.2. Verificação dos conectores e cabos;

11.8.3. Verificação das tensões de alimentação e protetores de surto;

11.8.4. Verificação das instalações físicas (suporte e fiação);

- 11.8.5. Reinstalação, remoção e/ou substituição quando necessário.
- 11.8.6. Conjunto de servidores;
- 11.8.7. Testes de respostas e comandos;
- 11.8.8. Revisão geral das configurações e ajustes necessários;
- 11.8.9. Reinstalação ou reconfiguração quando necessário;
- 11.8.10. Rack, patch panels, switches, roteadores e acessórios;
- 11.8.11. Checagem das conexões;
- 11.8.12. Revisão geral das configurações e ajustes necessários; e,
- 11.8.13. Reinstalação, remoção e/ou substituição quando necessário.
- 11.9. Os equipamentos e soluções deverão ser checados e/ou ajustados, preferencialmente no local onde estiverem instalados, ou seja, onde estão funcionando, com a devida orientação e autorização de acesso dos responsáveis da CONTRATANTE.
- 11.10. Os atendimentos e visitas corretivas não possuirão limitações em suas quantidades, no entanto, deverão ser realizadas mediante abertura de chamado, sendo que o atendimento a estes chamados, deverão ocorrer de acordo com a severidade e/ou prioridade apontada pela CONTRATANTE, de até 2 horas para atendimento, até 4 horas para resolução em casos de alta severidade, e em no máximo um dia útil (Next Business Day), de acordo com a prioridade e deverão atender aos fluxos definidos abaixo.
- 11.11. Para que a execução dos serviços corra de forma satisfatória, sem comprometer o bom funcionamento dos serviços prestados devem ser observados os seguintes itens:
 - 11.11.1. Para atuação do Atendimento de Campo, poderão ocorrer execuções de serviços em horários não comerciais, devendo estes ser acordados com a CONTRATANTE para liberação dos locais e acompanhamento dos trabalhos.
 - 11.11.2. Os trabalhadores da CONTRATADA deverão estar uniformizados e portando crachás de identificação com foto durante todo o período de atividades.
 - 11.11.3. Os trabalhadores da CONTRATADA deverão portar e utilizar equipamentos de proteção individual de acordo com a atividade desempenhada.
- 11.12. Os trabalhadores da CONTRATADA deverão possuir habilitação técnica para prestar os serviços aqui requisitados apresentando à CONTRATANTE cópia dos seguintes documentos, referentes a segurança do trabalho:
 - 11.12.1. PPRA / PCMSO / CND Federal, Estadual e Municipal em nome de CONTRATADA.
 - 11.12.2. Exames Médicos conforme prescrito no PCMSO.
 - 11.12.3. Certificados de Conclusão de Curso da NR-10 e NR-35, de no mínimo dois funcionários, os quais obrigatoriamente serão os prestadores de serviços.
 - 11.12.4. Ficha de EPI.
 - 11.12.5. Ordem de Serviço em nome de cada empregado prestador de serviço.
 - 11.12.6. Ficha de registro do empregado acompanhado do comprovante de recolhimento do INSS e FGTS mensalmente.
 - 11.12.7. Ocorrendo a solução satisfatória de uma OCORRÊNCIA, com o retorno ao perfeito funcionamento, será devidamente registrada no relatório técnico da CONTRATADA como CONCLUÍDO.

12. DA QUALIFICAÇÃO TÉCNICA E OPERACIONAL

- 12.1. A licitante deverá apresentar no mínimo 1 (um) profissional de nível superior – ENGENHEIRO ELETRÔNICO, ENGENHEIRO ELETRICISTA ou ENGENHEIRO DE

COMUNICAÇÃO ou outro que possua atribuições equivalentes, responsável pelo projeto, devidamente reconhecido pela entidade competente, para execução de serviços eletrônicos e/ou eletrotécnicos e para a emissão de Anotação de Responsabilidade Técnica (A.R.T.) referente a esta prestação de serviço, com data posterior à emissão da Ordem de Serviço Inicial. O licitante podendo apresentar, para tanto, contrato social, registro na carteira profissional, ficha de empregado ou contrato de trabalho, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços. (Súmula 25 do TCESP);

12.2. A licitante deverá apresentar 01 (um) ou mais atestado (s) sendo admitida a soma das quantidades, expedido(s) por pessoa jurídica de direito público ou privado, comprovando o desempenho de atividade pertinente e compatível com 50% do objeto dessa licitação, que tem como parcela de maior relevância:

12.3. Locação e instalação de 58 câmeras de monitoramento;

12.4. A empresa vencedora do processo licitatório deverá apresentar Declaração de Conformidade "Onvif Client", comprovando do registro do protocolo Onvif (Open Network Video Interface Forum), para os perfis M, S, T e G individualizada para as câmeras dos tipos 1 e 4 e para os perfis S, T e G individualizada para as câmeras dos tipos 2, 3 e 5, podendo ser emitidas através do site <https://www.onvif.org/conformant-products> não sendo aceitos protocolos Onvif cuja aprovação não seja superior a 12(doze) meses.

12.5. Tal solicitação se justifica e torna-se necessária para demonstrar que é um equipamento novo e de tecnologia atualizada; evitando que o DAAE adquira produtos desatualizados e/ou obsoletos que venham causar prejuízos ao bom andamento dos serviços ora locados.

13. DOS PRAZOS

13.1. O prazo máximo para entrega do objeto será de 60 (SESSENTA DIAS) dias corridos, contados a partir do recebimento da ORDEM DE SERVIÇOS, a ser emitida pela DAAE.

13.2. A entrega do objeto será formalizada através do recebimento e assinatura pela DAAE, do seguintes TERMOS DE ENTREGA:

13.3. TERMO DE ENTREGA DA PLATAFORMA DE SEGURANÇA, com as respectivas senhas de acesso ativadas;

13.4. TERMO DE ENTREGA DAS CÂMERAS DE VIDEOMONITORAMENTO relacionando todos os itens disponibilizados; e,

13.5. TERMO DE ENTREGA PARA OS SERVIÇOS DE SUPORTE TÉCNICO DA SOLUÇÃO OFERTADA, com suas respectivas senhas de acesso ativadas, telefones e e-mail (s) para atendimento pela CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO.

13.6. Caberá ao DAAE, sem prejuízo dos prazos de emissão da ORDEM DE SERVIÇO, por escrito e previamente, a determinação dos responsáveis pelo acompanhamento e gestão por parte da DAAE, e a confirmação dos locais onde serão instalados os equipamentos, fornecimento energia elétrica e a indicação dos dispositivos ou monitores para visualização das imagens.

13.7. O prazo de vigência contratual será de 36 (trinta e seis) meses, contados a partir da data da assinatura do contrato pertinente, considerando as possíveis prorrogações, nos termos da Lei nº 14.133/2021.

14. DO VALOR ESTIMADO



14.1. A contratação será pelo VALOR GLOBAL estimado que é de **R\$ 2.929.296,00. (dois milhões, novecentos e vinte e nove mil, duzentos e noventa e seis reais)**

14.2. O VALOR GLOBAL é composto pela somatória:

14.2.1. dos valores correspondentes aos serviços de locação, prestação de serviços de interconexão, manutenção corretiva e preventiva e suporte técnico, para um período de 36 meses;

14.2.2. dos valores correspondentes aos serviços de instalação das câmeras e plataforma de segurança, para um período de 12 meses.

14.3. O VALOR ESTIMADO para os serviços de locação, prestação de serviços de interconexão, manutenção corretiva e preventiva e suporte técnico, para um período de 36 meses é **R\$ 2.906.496,00 (dois milhões, novecentos e seis mil, quatrocentos e noventa seis reais).**

14.4. O VALOR ESTIMADO para os serviços de instalação das câmeras e plataforma de segurança, para um período de 12 meses é **R\$ 22.800,00 (vinte e dois mil e oitocentos reais).**

14.5. Para a composição das propostas deverão ser observados como valores máximos os valores estipulados no item 14.1 (VALOR GLOBAL) e nos itens 14.3, para os serviços de locação e 14.4 para os serviços de instalações.

14.6. O pagamento à CONTRATADA será executado em 36 parcelas mensais, sendo que nos primeiros 12 meses o valor da parcela será a somatória dos valores correspondentes aos serviços descritos nas letras "a" e "b" do item 17.1.1 e, nos demais meses, o valor da parcela será correspondente apenas aos serviços descritos na letra "a" do item 17.1.1.

Araraquara, 10 de maio de 2024.


Helton Alves de Galvão
Gerencia de Administrativo