ANEXO II

ESPECIFICAÇÕES TÉCNICAS

REGISTRO DE PREÇOS PARA FORNECIMENTO DE SOLUÇÃO DE CONTROLE DE ACESSO E CFTV PARA O SESC CIDADANIA

1. DEFINIÇÃO DO OBJETO

1.1. Registro de preços para fornecimento de solução de controle de acesso para o SESC Cidadania, conforme especificações técnicas, quantidades e condições constantes desta especificação técnica.

2. QUADRO DESCRITIVO E QUANTITATIVOS

LOTE			
ITEM	DESCRIÇÃO	QTD	UNI. MED.
1.	CÂMERA SPEED DOME	10	Und.
2.	CÂMERA DE REDE	300	Und.
3.	MESA CONTROLADORA	1	Und.
4.	MONITOR	4	Und.
5.	SERVIDOR TIPO I	1	Und.
6.	SERVIDOR TIPO II	1	Und.
7.	SERVIDOR TIPO III	1	Und.
8.	COLETOR DE ACESSO PARA PORTAS	3	Und.
9.	LEITOR GRAVADOR DE CARTÕES USB	20	Und.
10.	CATRACA DE BLOQUEIO FISICO	40	Und.
11.	CATRACA DE BLOQUEIO FISICO PNE	8	Und.
12.	BOTOEIRA	3	Und.
13.	LEITOR BIOMÉTRICO USB PARA CADASTRO	10	Und.
14.	FECHADURA ELETRÔNICA	5	Und.
15.	CARTÃO DE PROXIMIDADE	1000	Und.
16.	CANCELA DE BLOQUEIO FISICO	3	Und.
17.	GUARDA-CORPO	10	Metros
18.	PORTÃO DE FECHAMENTO DE VIDRO	4	Und.
19.	SERVIÇO DE INSTALAÇÃO DE EQUIPAMENTOS	424	Svç.
20.	SOFTWARE	1	Svç.
21.	SOFTWARE	1	Svç.
22.	SERVIÇO DE INSTALAÇÃO DE SOFTWARE	2	Svç.
23.	TREINAMENTO DA SOLUÇÃO - SOFTWARE	10	Svç.
24.	SUPORTE E MANUTENÇÃO PREVENTIVA, CORRETIVA, ADAPTATIVA E SUPORTE TÉCNICO DE SOFTWARE	12	Meses

3. CARACTERÍSTICAS GERAIS DOS EQUIPAMENTOS

3.1. CÂMERA SPEED DOME

3.1.1.	Câmera IP de alta definição, tipo speed dome, policromática e com sensor de imagem CMOS maior ou igual a 1/2.8" com varredura progressiva para vídeo monitoramento;
3.1.2.	Permitir captação de imagens em situação de baixa luminosidade, com sensibilidade mínima no modo Colorido igual ou inferior a 0.005Lux (para F1.5,AGC ON), no modo Preto&Branco a 0.001Lux (para F1.5,AGC ON);
3.1.3.	Resolução máxima de, no mínimo, 2MP (1920x1080) operando com uma taxa mínima de 30 quadros por segundo;
3.1.4.	Deve possuir compressão de vídeo padrão H.264 e, ao menos, um padrão compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265 ou similares), com alta relação de compressão;
3.1.5.	Permitir ajuste de PAN na faixa de 360O contínuos, ajuste de TILT na faixa de -10O a 90O com autoflip;
3.1.6.	Possuir velocidade máxima de PAN de no mínimo 100°/s e de TILT de no mínimo 80°/s;
3.1.7.	Possuir tempo do obturador configurável de 1seg a 1/30.000seg;
3.1.8.	Possuir IR embutido para uma distância de no mínimo 150m;
3.1.9.	Permitir zoom óptico máximo, de no mínimo, 40x;
3.1.10.	Possuir zoom digital de até, no mínimo, 16x;
3.1.11.	Possuir configuração de ajuste de foco para automático / semiautomático / manual;
3.1.12.	Permitir configuração de até 300 presets;
3.1.13.	Permitir configuração de até 8 patrulhas com, no mínimo, 32 presets cada.
3.1.14.	Possuir Modo Dia&Noite com acionamento do filtro de IR;
3.1.15.	Possuir função de balanço de branco automático ajustável pelo usuário;
3.1.16.	Deve possuir WDR de no mínimo 120db, não sendo aceito WDR digital;
3.1.17.	Possuir função de máscara de privacidade de no mínimo, 20 zonas;
3.1.18.	Possuir função controle de ganho automático (AGC);
3.1.19.	Possuir funções inteligentes de detecção de cruzamento de linha, detecção de entrada e saída de ambiente, detecção de bagagem retirada ou esquecida no local, detecção de face e detecção de intrusão;
3.1.20.	Possuir proteção total contra poeira e jatos fortes d'água – grau de proteção IP66 ou superior;
3.1.21.	Suportar os protocolos de rede TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP;
3.1.22.	Possuir compatibilidade com os padrões ONVIF, PSIA e ainda possuir SDK para integração com software de terceiros;
3.1.23.	Possuir função de autenticação segura baseado em usuário, via MAC, IEEE 802.1x e filtro de endereço IP;
3.1.24.	Permitir gravação em cartão de memória Micro SD/SDHC/SDXC de no mínimo, 256GB, com função automática de gravação local ou remota, com transferência automática após restabelecimento da rede;
3.1.25.	Possuir suporte para instalação em postes;
3.1.26.	Permitir tensão de alimentação de 24Vdc;
3.1.27.	Permitir alimentação via POE 802.3 at;

3.1.28. Permitir trabalhar entre temperaturas na faixa de -20oC a +60oC e humidade na faixa de 90% ou inferior;

3.1.29. Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia.

3.2. CÂMERA DE REDE

3.2.1. Câmera de rede IP tipo dome para vídeo monitoramento outdoor ou indoor;

3.2.2. Resolução mínima de 4MP (2688 × 1520) operando com uma taxa mínima de 30 quadros por segundo em todas as resoluções;

3.2.3. Sensor de imagem CMOS 1/3" ou maior, com varredura progressiva;

3.2.4. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão;

3.2.5. Suportar velocidade de shutter de 1/3s a 1/30.000s;

3.2.6. Suporte para três streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo;

3.2.7. Deve possuir iluminadores IR integrados, com alcance mínimo de 30 metros.

3.2.8. Lente fixa embutida de 2.8 ou 2.9 mm com ângulo de visualização horizontal mínimo de 103°

3.2.9. Função Dia & Noite com filtro de IR com troca automática;

3.2.10. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI);

3.2.11. Possuir funções blc (compensação de luz de fundo) e redução digital de ruídos 3d (3DNR), Scalable Video Coding (SVC) e HLC;

3.2.12. Possuir sensor de imagem com gama dinâmica ampla (WDR) de, no mínimo 115 dB, não sendo aceito WDR digital ou similar;

3.2.13. Deve possuir detecção de exceções de hardware para: Desconexão de Rede, Conflito de Endereço IP, Tentativa de Login Irregular;

3.2.14. Possuir analíticos inteligentes embarcados para detecção de cruzamento de linha, detecção de intrusos em uma determinada área e detecção de faces;

3.2.15. Deve possuir ativação de alarmes para as exceções e regras de analítico;

3.2.16. Ser compatível com os padrões de fóruns mundiais integrações aberto;

3.2.17. Compatível com os protocolos de rede: TCP/IP, IPV4, IPV6, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, NTP, UPnP, SMTP, IGMP, 802.1X e QoS;

3.2.18. Possuir capacidade de armazenamento local através de SD/MicroSD card, com capacidade de no mínimo 64 GB;

3.2.19. Suportar filtro de endereço IP;

3.2.20. Ser apto a operações em temperaturas de -20 °C a 50 °C com humidade não superior a 95% (sem condensação);

3.2.21. Possuir resistência contra vandalismo e impactos com grau de proteção IK10 ou superior;

3.2.22. Possuir proteção total contra poeira e jatos fortes d'água – grau de proteção IP67 ou superior;

3.2.23. O item deverá acompanhar caixa de junção para o local da instalação, todos os acessórios do mesmo fabricante da câmera com o objetivo de garantir a integridade, funcionamento e garantia do equipamento;

3.2.24. Possuir, no mínimo, 1 entrada e 1 saída de alarme;

3.2.25. Possuir entrada RJ45 10/100/1000M auto adaptável;

3.2.26. Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia;

3.2.27. Possuir alimentação compatível para 12Vdc e PoE (802.3af).

3.3. MESA CONTROLADORA

3.3.1. Mesa controladora USB para controle de câmeras Speed Dome IP via NVR ou Software de Gerenciamento de Imagens;

3.3.2. Possuir joystick para controle Pan, Tilt e zoom (PTZ 3D) das câmeras Speed Domes;

3.3.3. Possuir botões pré-ajustáveis pelo usuário, acima de 15 botões;

3.3.4. Ser compatíveis com variados tipos de Software de Gerenciamento de Imagens;

3.3.5. Suporte ao protocolo USB HID;

3.3.6. Compatível com o Sistema Operacional Windows 10/11;

3.3.7. Alimentação 5Vdc via porta USB.

3.4. MONITOR

3.4.1. Deve possuir no mínimo 4 telas de 55" LED padrão monitor para funcionamento 24/7;

3.4.2. Deve possuir desktop de monitoramento que suporte saída de vídeo independente para 4 monitores;

3.4.3. Requisitos mínimos da máquina:

3.4.4. Processador Core i5-9400F ou superior;

3.4.5. Memória 8GB RAM;

3.4.6. Sistema operacional Windows Server 2012 ou versão mais atual;

3.4.7. Deverá ter disco SSD com no mínimo 512GB de capacidade total;

3.4.8. Placa de rede Gibabit Ethernet.

3.5. SERVIDOR TIPO I

3.5.1. Deve ser fornecido processador com no mínimo 8 núcleos;

3.5.2. Deve suportar no mínimo dois processadores;

3.5.3. Deve ter cache mínimo de 11 MB L3;

3.5.4. Deve possuir velocidade escalável e ter no mínimo velocidade de 2,1 GHz até 3.20 GHz ou superior;

3.5.5. Deve possuir memória DDR4 padrão;

3.5.6. Deve suportar no mínimo 24 slots de memória podendo ser 12 slots para cada processador;

3.5.7. Deve possuir no mínimo 32 GB de memória RDIMM;

3.5.8. Deve possuir armazenamento em SSD de no mínimo 240GB;

3.5.9. Deve possuir 8 discos de HD 10TB SATA ENTERPRISE;

3.5.10. Deve suportar no mínimo 12 unidades LFF 3,5"

3.5.11. Deve possuir uma fonte de alimentação, hot-plug Universal com potência mínima de 800W;

3.5.12. Deve possuir controlador de rede Ethernet com 1 Gb 4 portas;

3.5.13. Deve possuir controlador de vídeo com no mínimo 1920 x 1200 a 60 Hz (32 bpp) com 16 MB de memória dedicada;

3.5.14. Deve suportar RAID: 0, 1, 5, 6, 10, 50, 60, 1TP/10TP Opera em (RAID & HBA/JBOD);

3.5.15. Deve possuir gerenciamento de infraestrutura inteligente integrado;

3.5.16. Deve possuir no mínimo 6 ventiladores hot-plug de desempenho;

3.5.17. Deve ocupar no máximo 2U no rack;

3.5.18. Deve suportar tensão 110 ou 220v (Bivolt);

3.5.19. Deve possuir no mínimo 3 slots de expansão PCIe 3.0;

3.5.20. Deve fornecer garantia de 3 anos para peças, serviço e suporte local.

3.6. SERVIDOR TIPO II

3.6.1. Processador Core i5-9400F ou superior;

3.6.2. Memória 8GB RAM;

3.6.3. Sistema operacional Windows Server 2012 ou versão mais atual;

3.6.4. Deverá ter disco SSD com no mínimo 512GB de capacidade total;

3.6.5. Placa de rede Gigabit Ethernet.

3.7. SERVIDOR TIPO III

3.7.1. Processador Core i5-9400F ou superior;

3.7.2. Memória 16GB RAM;

3.7.3. Sistema operacional Windows Server 2012 ou versão mais atual;

3.7.4. Deverá ter disco SSD com no mínimo 512GB de capacidade total;

3.7.5. Placa de rede Gigabit Ethernet.

3.8. COLETOR DE ACESSO PARA PORTAS

3.8.1. Deve possuir estrutura do corpo em aço inox;

3.8.2. Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia.

3.8.3. Deve possuir estrutura do corpo em aço inox;

3.8.4. Deve possuir indicação visual para a indicação de entrada e saída autorizada e acesso negado;

3.8.5. Deve possuir sinalização sonora para indicar falha ou êxito de registros através de "beeps" ou da reprodução de mensagens faladas pré-configuradas enviadas pelo computador servidor da aplicação;

3.8.6. Deve possuir leitor de impressões digitais, com as seguintes características:

a) Leitor ótico com geração da imagem por emissão de luz (LE Sensor) ou reflexão em prisma;

b) Resolução mínima de 500 dpi;

c) Área de captura mínima de 16 x 14 mm;

d) Detecção automática da presença do dedo sobre o dispositivo;

e) Capaz de desconsiderar impressões latentes;

f) Capaz de operar em ambientes externos e internos, independentemente da luminosidade do ambiente;

g) Captura em tempo real;

h) Liberação por controle remoto ou software de computador;

i) Comunicação TCP/IP;

j) Memória RAM: 512 MB;

k) Armazenamento: 8 GB Flash;

l) Portas multifunção 2 portas, 4 pinos (Wiegand / Abatrack Entradas ou Saídas digitais);

m) Display de cristal líquido texto, capaz de exibir as seguintes mensagens: nome ou parte do nome da pessoa identificada, data do acesso (dia e mês), hora do registro de (hora e minuto);

n) Interface padrão Ethernet (10/100 Mbps), com conector RJ45 fêmea diretamente no equipamento, sendo proibida a utilização de quaisquer tipos de conversores (USB - Ethernet, Serial-Ethernet, etc.);

o) Protocolo de comunicação TCP/IP;

p) Captura em tempo real;

q) Possuir saídas digitais para acionamentos eletrônicos de dispositivos externos como sirene, catracas, portas giratórias fechaduras, cancelas ou centrais de alarme e incêndio;

r) Possuir entradas digitais (sensores) para monitorações diversas;

s) Dispositivo de marcação em tempo real (relógio), com bateria própria de lítio + RAM não volátil;

t) Trabalhar em modo on-line e off-line;

u) Na operação off-line o tempo máximo de 1,5 segundos para identificação biométrica deve ser respeitado para bases com até 65.000 (Sessenta e cinco mil) amostras armazenadas no próprio equipamento. Este limite deverá ser respeitado tanto para identificação positiva (aceite), quanto para negativa (rejeição);

v) Display de cristal líquido texto;

w) Teclado com no mínimo 12 teclas;

x) Permitir realizar o cadastro das impressões digitais no próprio equipamento;

y) Dispositivo alternativo para substituir a impressão digital de pessoas que não possuem traços biométricos suficientes para realizar uma identificação ou uma verificação. Este dispositivo deve ser um leitor de cartões padrão ISO 14443 A/B.

3.8.7. Deverá ser realizado o cadastro da impressão digital. A confirmação 1:N exigirá um processamento enorme para realizar a identificação 1:N, desta forma, exige-

se que sejam confirmados via verificação (1:1), onde a pessoa utiliza o cartão descrito acima e coloca sua digital como forma de confirmação da identidade. Nos casos onde o procedimento de verificação não funcionar corretamente, em função dos traços biométricos insuficientes da pessoa, a mesma utilizará apenas o cartão de acesso;

3.8.8. Deve possuir integração com o software de controle de acesso existente;

3.8.9. Deve possuir comunicação Bluetooth com as seguintes características:

a) Deve ser compatível com os hardwares das leitoras e controladoras das catracas, cancelas e portas;

b) Deve permitir o acesso seguro através de um dispositivo móvel e tecnologias de comunicação padrão que funcionem com ambos sistemas operacionais iOS® e Android™;

c) Suportar Identidades Digitais Móveis (IDs Móveis) novas e grupos de cartões existentes para migração sem interrupções para um padrão mais seguro;

d) Configurações de leitura ajustáveis que permitam controlar a operação geral e o alcance de leitura dos IDs móveis, possibilitando a flexibilidade em distâncias menores;

e) Deve possuir capacidade de leitura para distâncias de pelo menos 2 metros entre o smartphone e a leitora;

f) Devem possuir certificação da Anatel para uso no país.

3.9. LEITOR GRAVADOR DE CARTÕES USB

3.9.1. Leitor USB padrão MIFARE, para leitura e gravação sem contato (a distância) de cartões de Proximidade SmartCard, conforme ISO 14443 A (ProximityCards);

3.9.2. Deve ser compatível e integrado com software existente;

3.9.3. Deve ser fornecida a licença para funcionamento no software de controle de acesso já existente.

3.10. CATRACA DE BLOQUEIO FISICO

3.10.1. Deve possuir estrutura do corpo em aço com pintura epóxi preta;

3.10.2. Deve possuir as seguintes dimensões: altura: 1000 mm; comprimento total (incluindo o braço): 78,3 mm, podendo sofrer variações de 10%;

3.10.3. Deve possuir 3 braços em aço;

3.10.4. Modelo referência pedestal;

3.10.5. Deve possuir alimentação elétrica dos mecanismos eletromecânicos com fonte chaveada – full range ou similar;

3.10.6. Deve possuir fluxo bidirecional (sentido do giro dos braços);

3.10.7. Deve possuir sensores óticos para detecção de giro;

3.10.8. Deve possuir sistema de travamento mecânico por solenoide ou eletroímã;

3.10.9. Deve possuir giro mecânico leve;

3.10.10. Deve possuir tempo médio entre falhas - MTBF de, no mínimo, 30.000 horas.

3.10.11. Deve possuir número de ciclos entre falhas - MCBF de, no mínimo,1.000.000 ciclos.

3.10.12. Deve possuir tempo médio para reparo - MTTR máximo 30 minutos;

3.10.13. Deve suportar alto fluxo de pessoas;

3.10.14. Deve possuir, memória RAM de 512 MB, armazenamento de 8 GB Flash.

3.10.15. Deve possuir 2 postas, 4 pinos (Wiegand/ Abatrack entradas ou saídas digitais).

3.10.16. Deve possuir conexões auxiliares, 2 portas seriais RS 232 para conexão de leitores de código de barras, RFID;

3.10.17. Deve possuir sinalização sonora para indicar falha ou êxito de registros através de "beeps";

3.10.18. Deve possuir saídas digitais para acionamentos eletrônicos de dispositivos externos; como sirene, catracas, fechaduras, cancelas ou centrais de alarme e incêndio;

3.10.19. Deve possuir entradas digitais (sensores) para monitorações diversas;

3.10.20. Deve possuir dispositivo de marcação em tempo real (relógio), com bateria própria;

3.10.21. Trabalhar em modo on-line e off-line;

3.10.22. Na operação off-line o tempo máximo de 2 segundos para identificação biométrica deve ser respeitado para bases com até 65.000 (Sessenta e cinco mil) amostras de digitais armazenadas no próprio equipamento. Este limite deverá ser respeitado tanto para identificação positiva (aceite), quanto para negativa(rejeição).

3.10.23. Deve possuir leitor óptico com geração da imagem por emissão de luz (LESensor) ou reflexão em prisma ou similar, com as seguintes características mínimas:

3.10.24. Resolução mínima de 500 dpi;

3.10.25. Área de captura mínima de 16 x 14 mm;

3.10.26. Detecção automática da presença do dedo sobre o dispositivo;

3.10.27. Capaz de desconsiderar impressões latentes;

3.10.28. Capaz de operar em ambientes externos e internos, independentemente da luminosidade do ambiente;

3.10.29. Deverá possuir captura em tempo real;

3.10.30. Deve possuir display de cristal líquido capaz de exibir as seguintes mensagens: nome ou parte do nome da pessoa identificada, data do registro de frequência (dia e mês), hora do registro de frequência (hora e minuto);

3.10.31. Deverá possuir teclado numérico e de funções com no mínimo 12 teclas;

3.10.32. Deverá possuir interface de comunicação padrão Ethernet (10 ou 100 Mbps) com conector RJ45 fêmea, protocolo de comunicação TCP/IP com IP fixo a ser estabelecido pelo CONTRATANTE e alimentação exclusiva para o sistema de leitura de registros (biometria, cartão de proximidade e teclado) fornecida pelo padrão IEEE 802.3af (Power over Ethernet - PoE) ou IEEE 802.3at (Power over Ethernet Plus - PoE+);

3.10.33. Os coletores biométricos de impressão digital, e teclado deverão formar um único conjunto de identificação, sendo utilizados embarcados na catraca, de modo a efetuar o controle de acesso, devendo ainda, prover comunicação criptografada configurável;

3.10.34. O controle de acesso deve ser composto de forma que possa realizar, primeiramente, a identificação por biometria seja ela impressão digital ou facial, 1:N, em segundo momento, trabalhando com a verificação 1:1 (código digitado) ou 1:N. Em ambos os casos, a captura biométrica será comparada com registros de um banco de dados. Este sistema deverá, ainda, possibilitar a liberação de acesso digitação de senha em função dos traços biométricos insuficientes da pessoa ou por comando do administrador;

3.10.35. O coletor de controle de acesso deve ser capaz de, em média, realizar a leitura biométrica ou por face ou impressão digital a liberação/negação do acesso em menos de 01 (um) segundos, desconsiderando-se o tempo gasto pelo software de controle e da estrutura de rede Ethernet;

3.10.36. Deve possuir coletor de reconhecimento facial com no mínimo as seguintes características:

a) Processador com dois núcleos ou superior;

b) Memória de 1GB ou superior;

c) Memória flash de 8GB ou superior;

d) Deve possuir sistema operacional Linux;

e) Capacidade mínima de 10.000 faces, 60.000 eventos;

f) Deve realizar verificação de máscara;

g) Sensor 1/2.8" Progressive Scan CMOS ou superior;

h) Lentes de 6mm ou superior.

3.10.37. PERFORMANCE:

a) Deve permitir ajuste de ângulo da altura de reconhecimento de 1.2 a 2.2 metros ou superior;

b) Deve permitir o reconhecimento com a distância mínima de 0,5 a 1,5 metros;

c) Deve permitir o ângulo de captura de 30 graus (esquerda e direita) 30 graus (para cima e para baixo) ou superior;

d) O tempo de reconhecimento não deve exceder 1 segundo.

3.10.38. INTERFACE:

a) Deve possuir alimentação elétrica de DC12V com no máximo 2A;

b) Deve possuir uma interface de rede com entrada RJ45 com velocidade de no mínimo 10/100

c) Deve possuir uma interface wiegand IN e wiegand OUT (26bits ou 34bits)

d) Deve possuir uma interface de alarme de emergência INPUT e outra OUTPUT;

e) Deve possuir uma interface de porta magnética;

f) Deve possuir uma interface de sensor de abertura;

g) Deve possuir uma interface de campainha;

h) Deve possuir uma interface de fechadura;

i) Deve possuir uma interface de comunicação com saída RS485;

j) Deve possuir um relé com saída NF.

3.10.39. CÂMERA

a) Deve possuir no mínimo duas câmeras: 1x câmera P/B e 1x câmera colorida;

b) Deve possuir no mínimo a resolução 2MP 1920 x 1080;

c) Mínimo de Iluminação Color 0.01Lux @F1.2(ICR);P/B 0.001Lux @F1.2 (ICR);

d) Codificação de Vídeo Main Profile H.265 /H.264 BP / MP / HP / MJPEG;

e) Resolução Main Stream: 50Hz: 25fps (1920×1080,1280×720) 60Hz: 30fps (1920×1080,1280×720);

f) Sub Stream: 720*576, 1-25(30)fps/640*480, 1-25(30)fps, 320*240, 1-25(30)fps.

3.10.40. OPERAÇÃO

a) Deve ser capaz de operação em temperaturas de -30° C a + 60° C;

b) Deve suportar umidade de operação 0-90% de umidade relativa, sem condensação;

c) Possuir no máximo 10W de potência;

d) Tamanho do dispositivo 205(C) * 95(L) *20(H)mm

e) Deve possuir suporte para fixação;

f) Deve possuir proteção mínima IP54;

g) Deve possuir tele de no mínimo 5 Polegadas;

h) Deve possuir peso máximo 0,4 Kg;

i) Deve possuir integração com o software de controle de acesso existente;

j) Deve possuir comunicação Bluetooth com as seguintes características:

k) Deve ser compatível com os hardwares das leitoras e controladoras das catracas, cancelas e portas.

l) Deve permitir o acesso seguro através de um dispositivo móvel e tecnologias de comunicação padrão que funcionem com ambos sistemas operacionais iOS® e Android™;

m) Suportar Identidades Digitais Móveis (IDs Móveis) novas e grupos de cartões existentes para migração sem interrupções para um padrão mais seguro;

n) Configurações de leitura ajustáveis que permitam controlar a operação geral e o alcance de leitura dos IDs móveis, possibilitando a flexibilidade em distâncias menores;

o) Deve possuir capacidade de leitura para distâncias de pelo menos 2 metros entre o smartphone e a leitora;

p) Devem possuir certificação da Anatel para uso no país.

3.11. CATRACA DE BLOQUEIO FÍSICO PNE

3.11.1. Deve possuir estrutura do corpo em aço com pintura epóxi preta;

3.11.2. Deve possuir as seguintes dimensões: altura: 1000 mm; comprimento total (incluindo o braço);

3.11.3. Deve possuir 1 braços em aço com formato de clip;

3.11.4. Modelo referência pedestal;

3.11.5. Deve possuir alimentação elétrica dos mecanismos eletromecânicos com fonte chaveada – full range ou similar;

3.11.6. Deve possuir fluxo bidirecional (sentido do giro do braço);

3.11.7. Deve possuir sensores óticos para detecção de giro;

3.11.8. Deve possuir sistema de travamento mecânico por solenoide ou eletroímã;

3.11.9. Deve possuir giro mecânico leve;

3.11.10. Deve possuir tempo médio entre falhas - MTBF de, no mínimo, 30.000horas.

3.11.11. Deve possuir número de ciclos entre falhas - MCBF de, no mínimo,1.000.000 ciclos;

3.11.12. Deve possuir tempo médio para reparo - MTTR máximo 30 minutos;

3.11.13. Deve suportar alto fluxo de pessoas;

3.11.14. Deve possuir, memória RAM de 512 MB, armazenamento de 8 GB Flash;

3.11.15. Deve possuir 2 postas, 4 pinos (Wiegand/ Abatrack entradas ou saídas digitais);

3.11.16. Deve possuir conexões auxiliares, 2 portas seriais RS 232 para conexão de leitores de código de barras, RFID;

3.11.17. Deve possuir sinalização sonora para indicar falha ou êxito de registros através de "beeps";

3.11.18. Deve possuir saídas digitais para acionamentos eletrônicos de dispositivos externos; como sirene, catracas, fechaduras, cancelas ou centrais de alarme e incêndio;

3.11.19. Deve possuir entradas digitais (sensores) para monitorações diversas;

3.11.20. Deve possuir dispositivo de marcação em tempo real (relógio), com bateria própria;

3.11.21. Trabalhar em modo on-line e off-line;

3.11.22. Na operação off-line o tempo máximo de 2 segundos para identificação biométrica deve ser respeitado para bases com até 65.000 (Sessenta e cinco mil) amostras de digitais armazenadas no próprio equipamento. Este limite deverá ser respeitado tanto para identificação positiva (aceite), quanto para negativa(rejeição).

3.11.23. Deve possuir leitor ótico com geração da imagem por emissão de luz (LESensor) ou reflexão em prisma ou similar, com as seguintes características:

a) Resolução mínima de 500 dpi;

b) Área de captura mínima de 16 x 14 mm;

c) Detecção automática da presença do dedo sobre o dispositivo;

d) Capaz de desconsiderar impressões latentes;

e) Capaz de operar em ambientes externos e internos, independentemente da luminosidade do ambiente;

f) Deverá possuir captura em tempo real;

g) Deverá possuir interface de comunicação padrão Ethernet (10 ou 100 Mbps) com conector RJ45 fêmea, protocolo de comunicação TCP/IP com IP fixo a ser estabelecido pelo CONTRATANTE e alimentação exclusiva para o sistema de leitura de registros (biometria, cartão de proximidade e teclado) fornecida pelo padrão IEEE 802.3af (Power over Ethernet - PoE) ou IEEE 802.3at (Power over Ethernet Plus - PoE+).

h) Os coletores biométricos de impressão digital deverão formar um único conjunto de identificação, sendo utilizados embarcados na catraca, de modo a efetuar o controle de acesso, devendo ainda, prover comunicação criptografada configurável;

i) O controle de acesso deve ser composto de forma que possa realizar, primeiramente, a identificação por biometria seja ela impressão digital ou facial , 1:N, em segundo momento, trabalhando com a verificação 1:1 (código digitado) ou 1:N. Em ambos os casos, a captura biométrica será comparada com registros de um banco de dados. Este sistema deverá, ainda, possibilitar a liberação de acesso digitação de senha em função dos traços biométricos insuficientes da pessoa ou por comando do administrador.

j) O coletor de controle de acesso deve ser capaz de, em média, realizar a leitura biométrica ou por face ou impressão digital a liberação/negação do acesso em menos de 01 (um) segundos, desconsiderando-se o tempo gasto pelo software de controle e da estrutura de rede Ethernet.

3.11.24. Deve possuir 2 coletores de reconhecimento facial com no mínimo as seguintes características cada:

a) Processador com dois núcleos ou superior;

b) Memória de 1GB ou superior;

c) Memória flash de 8GB ou superior;

d) Deve possuir sistema operacional Linux;

e) Capacidade mínima de 10.000 faces, 60.000 eventos;

f) Deve realizar verificação de máscara;

g) Sensor 1/2.8" Progressive Scan CMOS ou superior;

h) Lentes de 6mm ou superior.

3.11.25. PERFORMANCE

a) Deve permitir ajuste de ângulo da altura de reconhecimento de 1.2 a 2.2 metros ou superior;

b) Deve permitir o reconhecimento com a distância mínima de 0,5 a 1,5 metros;

c) Deve permitir o ângulo de captura de 30 graus (esquerda e direita) 30 graus (para cima e para baixo) ou superior;

d) O tempo de reconhecimento não deve exceder 1 segundo.

3.11.26. INTERFACE

a) Deve possuir alimentação elétrica de DC12V com no máximo 2A;

b) Deve possuir uma interface de rede com entrada RJ45 com velocidade de no mínimo 10/100

c) Deve possuir uma interface wiegand IN e wiegand OUT (26bits ou 34bits)

d) Deve possuir uma interface de alarme de emergência INPUT e outra OUTPUT;

e) Deve possuir uma interface de porta magnética;

f) Deve possuir uma interface de sensor de abertura;

g) Deve possuir uma interface de campainha;

h) Deve possuir uma interface de fechadura;

i) Deve possuir uma interface de comunicação com saída RS485;

j) Deve possuir um relé com saída NF.

3.11.27. CÂMERA

a) Deve possuir no mínimo duas câmeras: 1x câmera P/B e 1x câmera colorida;

b) Deve possuir no mínimo a resolução 2MP 1920 x 1080;

c) Mínimo de Iluminação Color 0.01Lux @F1.2(ICR);P/B 0.001Lux @F1.2 (ICR)

d) Codificação de Vídeo Main Profile H.265 /H.264 BP / MP / HP / MJPEG

e) Resolução Main Stream: 50Hz: 25fps (1920×1080,1280×720) 60Hz: 30fps (1920×1080,1280×720)

f) Sub Stream: 720*576, 1-25(30)fps/640*480, 1-25(30)fps, 320*240, 1-25(30)fps.

3.11.28. OPERAÇÃO

a) Deve ser capaz de operação em temperaturas de -30° C a + 60° C;

b) Deve suportar umidade de operação 0-90% de umidade relativa, sem condensação;

c) Possuir no máximo 10W de potência;

d) Tamanho do dispositivo 205(C) * 95(L) *20(H)mm

e) Deve possuir suporte para fixação;

f) Deve possuir proteção mínima IP54;

g) Deve possuir tele de no mínimo 5 Polegadas;

h) Deve possuir peso máximo 0,4 Kg;

i) Deve ser compatível com o controle de acesso existente;

j) Deve possuir integração com o software de controle de acesso existente;

k) Deve possuir comunicação Bluetooth com as seguintes características:

l) Deve ser compatível com os hardwares das leitoras e controladoras das catracas, cancelas e portas.

m) Deve permitir o acesso seguro através de um dispositivo móvel e tecnologias de comunicação padrão que funcionem com ambos sistemas operacionais iOS® e Android™;

n) Suportar Identidades Digitais Móveis (IDs Móveis) novas e grupos de cartões existentes para migração sem interrupções para um padrão mais seguro;

o) Configurações de leitura ajustáveis que permitam controlar a operação geral e o alcance de leitura dos IDs móveis, possibilitando a flexibilidade em distâncias menores;

p) Deve possuir capacidade de leitura para distâncias de pelo menos 2 metros entre o smartphone e a leitora;

q) Devem possuir certificação da Anatel para uso no país.

3.12. BOTOEIRA

3.12.1. Botoeira para acionamento de contato seco em espelho padrão 4x2 de embutir;

3.12.2. Confeccionado em aço inoxidável.

3.13. LEITOR BIOMÉTRICO USB PARA CADASTRO

3.13.1. Leitor de impressões digitais, para ser instalado a micro padrão PC, para utilização no cadastramento de pessoas, com as seguintes características:

3.13.2. Leitor ótico com geração da imagem por emissão de luz (LE Sensor) ou reflexão em prisma;

3.13.3. Resolução mínima de 500 dpi;

3.13.4. Área de captura mínima de 16 x 14 mm;

3.13.5. Capaz de operar em ambientes externos e internos, independentemente da luminosidade do ambiente;

3.13.6. Protocolo de comunicação TCP/IP;

3.13.7. Cabo com conector para porta USB de micros PC;

3.13.8. Deve rejeitar dedos falsos de silicone, borracha e cola branca;

3.13.9. Integrado com software de controle de acesso já existente.

3.14. FECHADURA ELETRÔNICA

3.14.1. O equipamento deverá apresentar no mínimo as seguintes especificações ou superior:

3.14.2. Versão: "Fail-Safe" / "Falha-Aberta" (energia para travar);

3.14.3. Design estreito para instalação de embutir: 32mm (L);

3.14.4. Monitoramento de status NA/NF - real posição do pino;

3.14.5. Esfera de auto-alinhamento ajustável;

3.14.6. Sensor magnético ajustável;

3.14.7. Projetado para portas normais ou vai-vém;

3.14.8. Acabamento frontal em aço inox escovado;

3.14.9. Circuito de proteção;

3.14.10. Circuito anti-tamper

3.14.11. Circuito lógico de auto-detecção;

3.14.12. Configuração de temporização 0, 3, 6 e 9s;

3.14.13. Solenóides de vida longa testados com 500.000 ciclos;

3.14.14. Instalação horizontal ou vertical com acabamento impecável;

3.14.15. Suporte para instalação em porta de vidro ou porta de madeira:

3.14.16. Temperatura de operação: -10~+45 ºC;

3.14.17. Umidade: 0~95%;

3.14.18. Equipamento integrado com o sistema de acesso existente.

3.15. CARTÃO DE PROXIMIDADE

3.15.1. Deve ser um cartão na frequência 13,56Mhz com microprocessador residente para armazenar e processar dados, efetuar cálculos, gerenciar arquivos e executar algoritmos de criptografia;

3.15.2. Deve permitir a leitura dos dados através da tecnologia de Rádio Frequência, sem a necessidade de contato físico entre o leitor e o cartão;

3.15.3. Deve permitir a reutilização de memória, regravando novos dados por cima dos existentes, possuindo um sistema de criptografia que protege os dados do cartão;

3.15.4. Deve possuir as seguintes especificações:

3.15.5. Cartão laminado em PVC ou ABS, tipo ID-1 (ISO/IEC 7816);

3.15.6. Sem Contato – "Contactless" (ISO/IEC 10536);

3.15.7. Deve possuir memória protegida;

3.15.8. Deve possuir tecnologia Smart Card Standard (Chip Fudan FM11RF08 ou compatível), com capacidade de memória EEPROM de 1Kb.

3.16. CANCELA DE BLOQUEIO FISICO

3.16.1. Deve possuir base em aço;

3.16.2. Deve possuir corpo em chapa de aço galvanizado com pintura eletrostática ou similar, que garanta maior durabilidade contra corrosão.

3.16.3. Deve possuir haste em alumínio estruturado ou plástico resistente, pintada zebrado e refletiva;

3.16.4. Deve possuir haste articulada com comprimento de 3,0 metros;

3.16.5. A haste, quando retraída (levantada) não deve ter seu comprimento maior que 2,50 m;

3.16.6. Deve possuir alimentação elétrica dos mecanismos eletromecânicos com fonte chaveada – full range ou similar;

3.16.7. Deve possuir interfaces para saídas digitais ou analógicas para acionamentos eletrônicos de dispositivos externos como sirene, alarme luminoso e sistema de laço indutivo, incluindo os respectivos relés ou acionadores destes dispositivos;

3.16.8. Deve possuir entradas digitais (sensores) ou analógicas para monitoração de sistema de laço indutivo;

3.16.9. Deve possuir sistema completo antiesmagamento por detecção indutiva de veículos (massa metálica) instalado no solo, sendo composto por módulo indutivo e looping, permitindo diversas regulagens de sensibilidade de campos magnéticos, trabalhando nas seguintes funções:

a) Protegendo o veículo quando este está sobre o looping, não deixando a cancela automática fechar sobre o veículo;

b) Fechando automaticamente a cancela após a passagem do veículo, impedindo que a mesma fique aberta desnecessariamente ou que outro veículo entre logo em seguida.

3.16.10. Deve possuir ciclo diário de no mínimo de 3.000 acessos;

3.16.11. Deve possuir velocidade mínima de abertura de 2,5 seg.

3.16.12. Deve possuir tecnologia de inversor de frequência;

3.16.13. Deve possuir partida e freio suaves;

3.16.14. Deve ser fornecido 01 coletor de acesso com biometria e proximidade com as seguintes especificações:

a) Estrutura do corpo em aço inox;

b) Indicação visual para a indicação de entrada e saída autorizada e acesso negado;

c) Sinalização sonora para indicar falha ou êxito de registros através de "beeps" ou da reprodução de mensagens faladas pré-configuradas enviadas pelo computador servidor da aplicação;

3.16.15. Leitor de impressões digitais, com as seguintes características:

a) Leitor ótico com geração da imagem por emissão de luz (LE Sensor) ou reflexão em prisma;

b) Resolução mínima de 500 dpi;

c) Área de captura mínima de 16 x 14 mm;

d) Detecção automática da presença do dedo sobre o dispositivo;

e) Capaz de desconsiderar impressões latentes;

f) Capaz de operar em ambientes externos e internos, independentemente da luminosidade do ambiente;

g) Captura em tempo real;

3.16.16. Liberação por controle remoto ou software de computador.

3.16.17. Protocolo de comunicação TCP/IP.

3.16.18. Memória RAM: 512 MB.

3.16.19. Armazenamento: 8 GB Flash.

3.16.20. Portas multifunção 2 portas, 4 pinos (Wiegand / Abatrack Entradas ou Saídas digitais).

3.16.21. Display de cristal líquido texto, capaz de exibir as seguintes mensagens: nome ou parte do nome da pessoa identificada, data do acesso (dia e mês), hora do registro de (hora e minuto);

3.16.22. Interface padrão Ethernet (10/100 Mbps), com conector RJ45 fêmea diretamente no equipamento, sendo proibida a utilização de quaisquer tipos de conversores (USB - Ethernet, Serial-Ethernet, etc.);

3.16.23. Protocolo de comunicação TCP/IP;

3.16.24. Captura em tempo real;

3.16.25. Possuir saídas digitais para acionamentos eletrônicos de dispositivos externos como sirene, catracas, portas giratórias fechaduras, cancelas ou centrais de alarme e incêndio;

3.16.26. Possuir entradas digitais (sensores) para monitorações diversas;

3.16.27. Dispositivo de marcação em tempo real (relógio), com bateria própria de lítio + RAM não volátil;

3.16.28. Trabalhar em modo on-line e off-line;

3.16.29. Na operação off-line o tempo máximo de 1,5 segundos para identificação biométrica deve ser respeitado para bases com até 65.000 (Sessenta e cinco mil) amostras armazenadas no próprio equipamento. Este limite deverá ser respeitado tanto para identificação positiva (aceite), quanto para negativa (rejeição).

3.16.30. Display de cristal líquido texto;

3.16.31. Teclado com no mínimo 12 teclas;

3.16.32. Permitir realizar o cadastro das impressões digitais no próprio equipamento;

3.16.33. Dispositivo alternativo para substituir a impressão digital de pessoas que não possuem traços biométricos suficientes para realizar uma identificação ou uma verificação. Este dispositivo deve ser um leitor de cartões padrão ISO 14443 A/B;

3.16.34. Observação: mesmo para as pessoas enquadradas neste item, deve ser feito o cadastro da impressão digital. No entanto, a identificação 1:N ficará prejudicada e o seu acesso deve ser confirmado via verificação (1:1), onde a pessoa utiliza o cartão descrito acima e coloca sua digital como forma de confirmação da identidade. Nos casos onde o procedimento de verificação não funcionar corretamente, em função dos traços biométricos insuficientes da pessoa, a mesma utilizará apenas o cartão de acesso;

3.16.35. Deve ser fornecido 01 (um) totem (poste externo) com altura máxima de 1,10 m para fixação do coletor de acesso com proteção contra intempéries;

3.16.36. Deve possuir coletor de reconhecimento facial com no mínimo as seguintes características:

a) Processador com dois núcleos ou superior;

b) Memória de 1GB ou superior;

c) Memória flash de 8GB ou superior;

d) Deve possuir sistema operacional Linux;

e) Capacidade mínima de 10.000 faces, 60.000 eventos;

f) Deve realizar verificação de máscara;

g) Sensor 1/2.8" Progressive Scan CMOS ou superior;

h) Lentes de 6mm ou superior.

3.16.37. PERFORMANCE

a) Deve permitir ajuste de ângulo da altura de reconhecimento de 1.2 a 2.2 metros ou superior;

b) Deve permitir o reconhecimento com a distância mínima de 0,5 a 1,5 metros;

c) Deve permitir o ângulo de captura de 30 graus (esquerda e direita) 30 graus (para cima e para baixo) ou superior;

d) O tempo de reconhecimento não deve exceder 1 segundo.

3.16.38. INTERFACE

a) Deve possuir alimentação elétrica de DC12V com no máximo 2A;

b) Deve possuir uma interface de rede com entrada RJ45 com velocidade de no mínimo 10/100

c) Deve possuir uma interface wiegand IN e wiegand OUT (26bits ou 34bits)

d) Deve possuir uma interface de alarme de emergência INPUT e outra OUTPUT;

e) Deve possuir uma interface de porta magnética;

f) Deve possuir uma interface de sensor de abertura;

g) Deve possuir uma interface de campainha;

h) Deve possuir uma interface de fechadura;

i) Deve possuir uma interface de comunicação com saída RS485;

j) Deve possuir um relé com saída NF.

3.16.39. CÂMERA

a) Deve possuir no mínimo duas câmeras: 1x câmera P/B e 1x câmera colorida;

b) Deve possuir no mínimo a resolução 2MP 1920 x 1080;

c) Mínimo de Iluminação Color 0.01Lux @F1.2(ICR);P/B 0.001Lux @F1.2 (ICR);

d) Codificação de Vídeo Main Profile H.265 /H.264 BP / MP / HP / MJPEG;

e) Resolução Main Stream: 50Hz: 25fps (1920×1080,1280×720) 60Hz: 30fps (1920×1080,1280×720);

f) Sub Stream: 720*576, 1-25(30)fps/640*480, 1-25(30)fps, 320*240, 1-25(30)fps.

3.16.40. OPERAÇÃO

a) Deve ser capaz de operação em temperaturas de -30° C a + 60° C;

b) Deve suportar umidade de operação 0-90% de umidade relativa, sem condensação;

c) Possuir no máximo 10W de potência;

d) Tamanho do dispositivo 205(C) * 95(L) *20(H)mm

e) Deve possuir suporte para fixação;

f) Deve possuir proteção mínima IP54;

g) Deve possuir tele de no mínimo 5 Polegadas;

h) Deve possuir peso máximo 0,4 Kg;

i) Deve possuir integração com o software de controle de acesso existente;

j) Deve possuir comunicação Bluetooth com as seguintes características:

k) Deve ser compatível com os hardwares das leitoras e controladoras das catracas, cancelas e portas.

l) Deve permitir o acesso seguro através de um dispositivo móvel e tecnologias de comunicação padrão que funcionem com ambos sistemas operacionais iOS® e Android™;

m) Suportar Identidades Digitais Móveis (IDs Móveis) novas e grupos de cartões existentes para migração sem interrupções para um padrão mais seguro;

n) Configurações de leitura ajustáveis que permitam controlar a operação geral e o alcance de leitura dos IDs móveis, possibilitando a flexibilidade em distâncias menores;

o) Deve possuir capacidade de leitura para distâncias de pelo menos 2 metros entre o smartphone e a leitora;

p) Devem possuir certificação da Anatel para uso no país.

3.17. GUARDA-CORPO

3.17.1. Tubos em aço inox polido - diâmetro de 76 mm;

3.17.2. Base de aço inox, chumbado em 3 pontos com Parabolt 100mm;

3.17.3. Suportes resistentes para fixação dos vidros com acabamento cromado;

3.17.4. Vidro transparente incolor de 8mm;

3.17.5. Dimensionamento conforme a necessidade do projeto;

3.17.6. Deverá ser fornecido com os acessórios necessários para a instalação;

3.17.7. Deverá ser fornecido instalado.

3.18. PORTÃO DE FECHAMENTO DE VIDRO

3.18.1. Fabricado em vidro incolor;

3.18.2. Com medidas adaptadas para pessoas portadoras de necessidades especiais (cadeirante).

3.18.3. Deverá conter fechadura com chave;

3.18.4. Deverá ser ajustado de acordo com as necessidades do projeto (altura, largura e etc);

3.18.5. Deverá ser fornecido com os acessórios necessários para a instalação e fixação.

3.19. SERVIÇO DE INSTALAÇÃO DOS EQUIPAMENTOS

3.19.1. SERVIÇO DE INSTALAÇÃO DE CÂMERA SPEED DOME

a) Deverá ser realizada a instalação da câmera com os ajustes de foco e zoom utilizando ferramentas disponibilizada pelo fabricante da solução para descoberta dos dispositivos instalados em rede, ou através do VMS;

b) As câmeras deverão ser instaladas e renomeadas conforme padronização do CONTRATANTE;

c) As câmeras deverão ser instaladas e configuradas para serem controladas via VMS.

3.19.2. SERVIÇO DE INSTALAÇÃO DE CAMÊRA DE REDE

a) Deverá ser realizada a instalação da câmera com os ajustes de foco e zoom utilizando ferramentas disponibilizada pelo fabricante da solução para descoberta dos dispositivos instalados em rede, ou através do VMS;

b) As câmeras deverão ser instaladas e renomeadas conforme padronização do CONTRATANTE;

c) As câmeras deverão ser instaladas e configuradas para serem controladas via VMS.

3.19.3. SERVIÇO DE INSTALAÇÃO DE MESA CONTROLADORA

a) Deverá ser instalado utilizando ferramentas disponibilizada pelo fabricante da solução para descoberta do dispositivo instalado em rede, ou através do VMS;

b) Deverá ser instalado e configurado para ser utilizado como controle via VMS.

3.19.4. SERVIÇO DE INSTALAÇÃO DE MONITORES

a) Deverá ser instalada as 4 telas de 55" com suporte e acessórios de instalação inclusos;

b) Deverá ser configurado o Desktop para visualização das telas no VMS;

c) Deverá ser configurado o mosaico de telas com no mínimo 16 telas em cada televisor.

3.19.5. SERVIÇO DE INSTALAÇÃO DE SERVIDORES

a) Instalação física e configurações dos servidores conforme manual do fabricante;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA;

c) O ponto elétrico e conectividade é de responsabilidade da CONTRATANTE;

3.19.6. INSTALAÇÃO E CONFIGURAÇÃO CONJUNTO IDENTIFICADOR BIOMÉTRICO (Coletor de acesso, fechadura e botoeira)

a) Instalação física e configurações dos equipamentos de controle de acesso, fechadura e botoeira no Software de controle de acesso já existente;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA;

c) O ponto de elétrica e conectividade é de responsabilidade da CONTRATANTE;

d) Capacitação para os operadores do sistema, cadastro de novos usuários e configuração do sistema.

3.19.7. SERVIÇO DE INSTALAÇÃO DE LEITOR BIOMÉTRICO USB

a) Instalação física e configurações dos coletores conforme manual do fabricante;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA;

3.19.8. SERVIÇO DE INSTALAÇÃO DE LEITOR GRAVADOR DE CARTÕES USB

a) Instalação física e configurações dos leitores conforme manual do fabricante;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA;

3.19.9. INSTALAÇÃO E CONFIGURAÇÃO CATRACA

a) Instalação física e configurações dos equipamentos de controle de acesso e no Software de controle de acesso já existente;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA.

c) O ponto de elétrica e conectividade é de responsabilidade da CONTRATANTE.

d) capacitação para os operadores do sistema, cadastro de novos usuários, configuração do sistema.

3.19.10. INSTALAÇÃO E CONFIGURAÇÃO CANCELA

a) Instalação física e configurações dos equipamentos de controle de acesso e no Software de controle de acesso já existente;

b) Todo material referente a instalação é de responsabilidade da CONTRATADA.

c) O ponto de elétrica e conectividade é de responsabilidade da CONTRATANTE.

d) Capacitação para os operadores do sistema, cadastro de novos usuários, configuração do sistema.

3.19.11. SERVIÇO DE INSTALAÇÃO DE GUARDA-CORPO

a) Serviço de instalação dos metros do guarda-corpo fixado com todos os acessórios necessários inclusos.

3.19.12. SERVIÇO DE INSTALAÇÃO DE PORTÃO DE FECHAMENTO DE VIDRO

a) Serviço de instalação de portão de fechamento de vidro contendo todos os acessórios necessários, limpeza e fixação.

3.19.13. SERVIÇO DE INTEGRAÇÃO DO VMS COM O CONTROLE DE ACESSO

a) As soluções de controle de acesso e monitoramento eletrônico devem estar integradas com os seguintes requisitos:

b) O sistema de controle de acesso deve enviar os eventos relacionados aos pontos controlados (acesso permitido, bloqueado, porta forçada etc.) e o evento deve ser vinculado com a câmera associada àquele evento sendo possível uma auditoria através dessa intercomunicação;

c) Deve permitir escolher em um determinado evento em uma lista e ao clicar no evento levar diretamente ao vídeo;

d) Deve permitir fazer pesquisas por tipo de evento, baseada nos nomes definidos para cada um deles;

e) O VMS deve disponibilizar a imagens e gravações para o controle de acesso, nos casos onde a interface de monitoramento usado for a do controle de acesso.

4. SOFTWARE - CARACTERÍSTICAS GERAIS DOS SOFTWARES

4.1. O software de monitoramento e armazenamento (VMS) deve suportar:

4.1.1. Solução de sistema de vídeo segurança multiusuário e multi-site com capacidade de integrar múltiplos servidores de vídeo em uma rede unificada, com cada servidor capaz de se comunicar com os outros servidores da rede. Vídeos e eventos de qualquer servidor devem ser transparente e visíveis de outros e para outros servidores;

4.1.2. Deverá apresentar carta do fabricante do VMS junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia;

4.1.3. Gerenciamento otimizado de armazenamento de vídeo, para dispor de arquivamento único, gravação de longa duração de bom desempenho, escalabilidade e custo-eficiente;

4.1.4. Lista de dispositivos homologados com mais de 7000 modelos de câmeras IP, codificadores de vídeo IP, e mais de 60 fabricantes diferentes entre todas as soluções, utilizando métodos como varredura manual e varredura de IP para adição destes;

4.1.5. Até 640 câmeras por servidor de gravação contínua ou ativada por movimento, evento ou agendamento e apareçam como um único site para o usuário;

4.1.6. Deve permitir que os servidores, estações de trabalho, câmeras e contas de usuários sejam configurados em uma implementação corporativa lógica com uma única interface gráfica de usuário (GUI).

4.1.7. Rede e armazenamento otimizados, por multi-streaming, que otimiza a banda usando novos métodos de compressão, com H.264, H.265 além MJPEG e MPEG4;

4.1.8. Multi-live Streaming, que possibilita definir múltiplos fluxos de vídeo ao vivo com diferentes configurações, otimizando a performance de visualização do Cliente de Monitoramento de acordo com os layouts de visualização.

4.2. Deve possuir um modulo de arquivamento de longo prazo que será utilizado especificamente para gravação e backups de longo prazo de arquivos de vídeo:

4.2.1. Os backups podem ser agendados a qualquer hora ou dia da semana;

4.2.2. Os backups podem ser realizados continuamente (todas as gravações das câmeras selecionadas são arquivadas automaticamente. O arquivamento é executado 24 horas por dia, 7 dias por semana);

4.2.3. Os backups podem ser executados por demanda;

4.2.4. O módulo deve fornecer um nível desejado de redundância de arquivamento de vídeo;

4.2.5. O módulo deve suportar armazenamento local e armazenamentos de rede conectados via iSCSI e SMB (CIFS).

4.3. Detecção de movimento, independente do modelo da câmera, seja pelo servidor ou pela câmera, ou simultaneamente:

4.3.1. Plataforma Aberta: API / SDK, para suportar integração com hardware ou aplicativos de terceiros;

4.3.2. Integração nativa de dispositivos compatíveis com os fóruns de compatibilidade Onvif e/ou PSIA;

4.3.3. Instalação em Sistema Operacional de 64 bits projetado para execução em computadores equipados com os sistemas Microsoft® Windows® Server 2008 R2 SP1, 2012 R2 ou 2016, Windows 7 SP1, 8 ou 10;

4.3.4. Integração de dispositivos de controle de acesso, sem a necessidade de trocar a interface principal do usuário, isto é, sem a necessidade de utilização da interface de outro fabricante.

4.4. Ajuste da sensibilidade da detecção de movimento suportando múltiplas zonas em cada câmera, sendo que:

4.4.1. Cada zona deve ser endereçável exclusivamente e ser capaz de ter reações específicas programadas com base no alarme desta;

4.4.2. Cada zona deve ter configurações de sensibilidade individuais para contraste e tamanho do (s) objeto (s) em movimento;

4.4.3. Cada zona terá a opção de ser armada / desarmada individualmente;

4.4.4. Cada zona terá a opção de ser enegrecida (máscara de privacidade);

4.4.5. Para cada zona, a taxa de quadros de vídeo e os quadros de memória podem ser ajustados para detecção de movimento;

4.4.6. Deve possuir a capacidade de ativar / desativar as zonas de movimento na visualização ao vivo da câmera;

4.4.7. Deve exibir a zona de Movimento em uma cor distinta se o movimento foi detectado naquela Zona;

4.4.8. Se estiver usando múltiplos fluxos de vídeo, um fluxo específico usado para detecção de movimento pode ser definido.

4.5. Deve permitir, a título de expansão, uma solução de Vídeo Wall integrada com até 16 monitores por servidor (controller) com suporte à exibição de até 196 câmeras simultâneas

(30 fps) se estiver usando o modo multi-stream (usando fluxos de baixa resolução / alta resolução);

4.6. Suportar a exibição de até 40 câmeras Full HD simultâneas (30 fps), se não estiver usando o modo multi-stream;

4.7. Gerenciamento centralizado: O software de administração deve oferecer um acesso único e consolidado para configuração dos servidores de gravação, mesmo em instalações multisites;

4.8. Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário;

4.9. Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando varredura de IP;

4.10. Exportação / importação de dados de configuração do sistema e de usuários;

4.11. Sistema de backup para a operação do sistema confiável e rápida recuperação do sistema;

4.12. Sistema automático de pontos de restauração: Permite a reversão fácil de pontos de configuração previamente definidos e permite o cancelamento de mudanças de configuração indesejados e a restauração de configurações anteriores válidas;

4.13. Personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando / desabilitando partes da interface para evitar o acesso indevido a ações restritas;

4.14. A capacidade de endereçar cada objeto com nomes exclusivos que possam ser alterados a qualquer momento;

4.15. Uma arquitetura distribuída do banco de dados de configuração do sistema. Cada servidor de vídeo pode armazenar uma cópia local do banco de dados de configuração do sistema para adicionar um nível de redundância integrada;

4.16. O sistema exportará sequências de vídeo de várias câmeras para um único arquivo nativo de evidências.

4.17. O sistema deve possuir a capacidade de programação macro.

4.18. O sistema deve ter um recurso de programação de script embutido baseado em linguagens de programação VB / JScript.

4.19. Envio eventos gerados pelas câmeras do sistema e transmitir seu estado para os computadores especificados como traps SNMP, assim que surgirem no sistema, tais como:

4.19.1. Câmera: estado alterado;

4.19.2. Câmera: focada;

4.19.3. Câmera: desfocada;

4.19.4. Câmera: não cega;

4.19.5. Câmera: cega;

4.19.6. Câmera: anexada;

4.19.7. Câmera: desligada;

4.19.8. Capacidade de notificação sonora de alarme.

4.19.9. O sistema deve suportar, se licenciado, uma solução para failover nativo dos servidores de vídeo. O sistema deve ter a capacidade de ser configurado de forma que, se um dos servidores de vídeo falhar, o servidor de failover automaticamente assume a gravação das câmeras do servidor que falhou. Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia.

4.20. OPERAÇÃO

4.20.1. Exibições de Janelas/Layouts: Trabalha com exibições contendo até 12x08 câmeras, Matriz Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, distribuídos em todos os monitores do computador;

4.20.2. PTZ inteligente: controle manual, presets, macros (vá à preset quando evento), patrulhamento com esquemas múltiplos (pattern), comandos para limpador (palheta) e esguicho de água, controle por joystick e teclado/mouse;

4.20.3. Controle de Entradas/Saídas de Alarme: Das câmeras ou dispositivos de I/O, de forma a criar botões/eventos manuais, ou receber sinais de sistemas de intrusão ou controle de acesso;

4.20.4. Áudio multicanal bidirecional: Ouça áudio ao vivo/gravado com reprodução instantânea no PC cliente e transmita voz pelo microfone a alto-falantes remotos;

4.20.5. Gravação de áudio sincronizada a qualquer canal de vídeo;

4.20.6. Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera;

4.20.7. Funcionalidade de geração de evidência através de quadros comentados (storyboard ou bookmark) permitindo maior detalhamento dos trechos de vídeo e alarmes exportados;

4.20.8. Busca, Backup e dados seguros;

4.20.9. Processamento de gravação: Através da busca de movimento acima do vídeo gravado, PTZ digital com suavização de imagem opcional (apenas no software visualizador);

4.20.10. Backup de Evidência: AVI e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros e impressão de relatórios;

4.20.11. Autenticação: contas de usuário do Microsoft Active Directory e nativos;

4.20.12. Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera;

4.20.13. Histórico: Das ações do usuário por tempo, localizações e câmeras, e toda a operação do sistema;

4.20.14. Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS;

4.20.15. Proteção de evidência: O sistema deve permitir a inserção de "bookmarks", impedindo assim que os trechos de vídeo sejam apagados / alterados;

4.20.16. Capacidade de proteger a gravação de cada câmera com uma senha;

4.20.17. A resolução, a taxa de quadros e a taxa de bits de cada câmera podem ser definidas independentemente de outras câmeras no sistema, e a alteração dessas configurações não afetará as configurações de gravação e exibição das outras;

4.20.18. Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia;

4.20.19. Deve ter a capacidade de gravar vídeo em uma quantidade de quadros (frames) inferior ao recebido da câmera (redução da taxa de quadros).

4.21. SERVIDOR DE GRAVAÇÃO DEVERÁ SUPORTAR:

4.21.1. Gravação digital simultânea de vários canais de vídeo e áudio;

4.21.2. Transmissão de áudio bidirecional do microfone do cliente para alto-falantes remotos;

4.21.3. A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado;

4.21.4. O software cliente pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação;

4.21.5. Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, H.264 e H.265;

4.21.6. Tecnologia de gravação: sistema seguro de alta velocidade de imagens JPEG ou fluxos MPEG4, H264 e H.265 incluindo áudio;

4.21.7. Velocidade de gravação: Mais de 30 quadros (frames) por segundo por câmera, limitado apenas pelo hardware e rede;

4.21.8. Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage;

4.21.9. Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail;

4.21.10. Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso;

4.21.11. Pan Tilt Zoom (PTZ) com presets armazenados pelo sistema, sendo o limite, o suportado pela câmera.

4.21.12. Varredura PTZ em dispositivos suportados: visualização ou gravação enquanto se move lentamente a partir de uma posição para outra;

4.21.13. Acione o limpador ou esguicho de água remotamente, nos modelos suportados de PTZ;

4.21.14. Gravação como um serviço do Windows;

4.21.15. Gravação em multi-estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo, inclusive, a redução da taxa de frames automática para atender a demanda de tempo de configuração;

4.21.16. Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera);

4.21.17. Gravação embarcada na câmera (edge storage) em vários fabricantes e em dispositivos ONVIF;

4.21.18. Serviços de conexão remota aos servidores de imagem;

4.21.19. Sistemas de servidores de gravação de 64 bits, em hardware e software;

4.21.20. Assinatura digital no banco de dados garantindo integridade do vídeo;

4.21.21. Monitoramento do sistema e do servidor de imagens com relatório das configurações;

4.21.22. Alta disponibilidade da gravação de vídeo. O sistema deve permitir que em caso de falha na gravação dos vídeos, outro assuma. A redundância poderá ser efetuada em um (ou vários) standby servers exclusivos para essa função;

4.21.23. Cópias em dispositivos (câmeras ou grupo de câmeras) entre diferentes servidores de gravação;

4.21.24. Exportação de vídeo a uma taxa de quadros menor do que a registrada no vídeo gravado (redução da taxa de quadros);

4.21.25. Configuração para gravar em uma taxa de quadros quando não houver movimento e, em seguida, gravar em outra taxa de quadros quando houver movimento.

4.22. O SOFTWARE DE GERENCIAMENTO DO SERVIDOR DE GRAVAÇÃO DEVE SUPORTAR:

4.22.1. Console local de gerenciamento do servidor acessível a partir da área de notificação do Windows;

4.22.2. Iniciação e interrupção do serviço de gravação;

4.22.3. Acesso à configuração;

4.22.4. Acesso ao sistema de ajuda do servidor;

4.22.5. Informação de status do sistema de visualização e de registro;

4.22.6. Instalado em conjunto ao servidor de gravação;

4.22.7. O Software de visualização de gravação deve suportar:

4.22.8. Linha de tempo de atividade com recurso de lupa, possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados;

4.22.9. Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection).

4.22.10. Pesquisa inteligente, detecção de movimento acima do vídeo gravado. A pesquisa inteligente deve poder utilizar os metadados dos eventos gerados pelo dispositivo como ferramenta de busca de imagens.

4.22.11. Geração de provas por meio de relatório impresso, imagem em AVI ou no formato proprietário (com visualizador incluso).

4.22.12. Exportação de vídeo digital com opção de aplicar zoom para visualizar área de interesse, além de minimizar o tamanho do arquivo exportado;

4.22.13. Exportação de "CD de Evidência" contendo dados nativos e o visualizador.

4.22.14. Criptografia e opção de senha de proteção para as gravações e os arquivos exportados com algoritmos AES128 ou AES256;

4.22.15. Tecnologia de criptografia acelerada por hardware certificada - Self-encrypting Drives- para criptografar todos os dados gravados com AES-128 ou AES-256 usando os recursos de hardware dos Drives;

4.22.16. Comunicação/conceito visual do client e server.

4.22.17. Opção para enviar imagens por e-mail.

4.22.18. O servidor de imagens deve suportar:

a) Acesso remoto para o software de visualização e aplicativo para visualização em web browsers, com opção de conexão segura no acesso à câmera (HTTPS)

b) Arquitetura de servidores Master e Slave

c) Autenticação de acesso baseado em contas de usuário Microsoft Active Directory, ou nativo do sistema.

d) Autoriza os privilégios de acesso por contas de usuário ou grupos do Microsoft Active Directory ou nativo do sistema.

e) Controle de acesso aos perfis: Visualização ao vivo, controle PTZ, presets PTZ, controle de saídas, Eventos, ouça o microfone, fale com a caixa de som remota, gravação manual; Reprodução, exportação AVI, exportação JPG, exportação de

banco de dados, sequências, pesquisa inteligente e áudio. Bem como definir as vistas, editar vistas particulares e públicas.

f) Histórico de provas exportadas por usuário e arquivo.

g) Histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras.

h) Instalação em conjunto com o servidor de gravação.

i) Deverá apresentar carta do fabricante junto a proposta comercial declarando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia.

j) Multi-streams para vídeo ao vivo para diferentes clientes.

4.23. O APLICATIVO DE VISUALIZAÇÃO ATRAVÉS DO WEB BROWSER DEVE SUPORTAR:

4.23.1. Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 13 câmeras simultaneamente, advindos do mesmo ou diferentes servidores;

4.23.2. Navegação de vídeo avançadas, incluindo reprodução lenta/rápida, salto a data/hora e pesquisa de movimento no vídeo;

4.23.3. Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista;

4.23.4. Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador;

4.23.5. Importação de mapas estáticos ou ativos para navegação rápida entre câmeras;

4.23.6. Controle do relé de saída de alarme;

4.23.7. Visão geral das sequências com movimento detectado e janela de visualização;

4.23.8. Visão geral de eventos / alertas;

4.23.9. Controle de câmeras PTZ remotamente, usando também posições pré-determinadas;

4.23.10. Controle remoto de PTZ por clique em ponto;

4.23.11. Criar arquivos JPEG gerados a partir de conteúdo gerado pelo software;

4.23.12. Sistema de login usando nomes de usuário e senhas cadastrados no sistema proprietário ou delegado ao Microsoft Active Directory.

4.24. MATRIZ DE VÍDEO

4.24.1. Uma única matriz virtual deve suportar a exibição de até 250 câmeras;

4.24.2. Deve permitir sequência de câmeras tipo FIFO (first-in-first-out);

4.24.3. Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera;

4.24.4. Deve suportar visualizações de câmera personalizadas ilimitadas (grade da câmera + atribuição da câmera):

a) As visualizações podem ser criadas a partir de qualquer servidor ou estação de trabalho e são salvas globalmente no sistema;

b) Uma visão pode ser criada uma vez e enviada para tantas estações de trabalho do cliente quantas forem necessárias.

4.24.5. Deve fornecer uma opção para arrastar e soltar câmeras dentro da mesma matriz para criar exibições personalizadas.

4.24.6. Deve ter uma opção para visualizar uma lista de câmeras.

a) Os usuários devem poder selecionar câmeras de uma lista e arrastar e soltar cada uma delas em uma célula de câmera;

b) A lista de câmeras deve ter indicadores visuais indicando se a câmera possui um alarme atual, se a câmera está gravando ou se a câmera está sendo visualizada no momento;

c) A lista de câmeras deve suportar o agrupamento de câmeras.

4.24.7. Deve ter a capacidade de alterar automaticamente o fluxo de exibição da câmera quando o tamanho da célula da câmera mudar (por exemplo, Layout é alterado de 1x1, 2x2, 3x3, etc.). Tamanhos de célula maiores podem ser configurados para usar fluxos de resolução mais alta, e tamanhos de célula pequena podem usar fluxos de resolução mais baixa (reduzindo, assim, a carga de processamento e o tráfego de rede).

4.24.8. Deve ter a capacidade de alterar o fluxo de exibição para um fluxo de melhor qualidade quando o zoom digital é usado na exibição ao vivo.

4.24.9. Deve ter a capacidade de fornecer uma verificação visual de todo movimento dentro da (s) Zona (s) da câmera.

4.24.10. Deve possuir a capacidade de criar marcadores com meta-texto exclusivo a partir de uma visualização de câmera ao vivo. Marcadores podem ser posto no tempo ou intervalo de data / hora.

4.24.11. Deve ter um botão na célula da câmera para ligar / desligar a Detecção de Movimento facilmente para uma única câmera.

4.24.12. Deve suportar alternar entre o modo LIVE e ARCHIVE da mesma interface gráfica do usuário.

4.24.13. Deve suportar o redimensionamento para poder encaixar outros componentes da interface do usuário do sistema na mesma área de trabalho;

4.24.14. Deve suportar um Modo:

a) Onde apenas câmeras com movimento serão exibidas;

b) Onde o acesso ao Modo de Gravação será desativado;

c) Onde todos os botões da GUI da Matriz de Vídeo estão ocultos, e somente o vídeo ao vivo das câmeras é exibido.

4.25. O SOFTWARE DE VISUALIZAÇÃO DEVE SUPORTAR:

4.25.1. Início da gravação manual de câmeras;

4.25.2. Zoom digital ao vivo evita gravações com o zoom digital;

4.25.3. Visualização de layouts de 1x1 até 12x08 layouts, além de exibições assimétricas;

4.25.4. A capacidade de alterar automaticamente o fluxo de exibição da câmera quando o tamanho da célula da câmera mudar (por exemplo, Layout é alterado de 1x1, 2x2, 3x3, etc.). Tamanhos de célula maiores podem ser configurados para usar fluxos de resolução mais alta, e tamanhos de célula pequena podem usar fluxos de resolução mais baixa (reduzindo, assim, a carga de processamento e o tráfego de rede);

4.25.5. Vários monitores num mesmo computador;

4.25.6. Função Sequencial que permite um quadrante especificado mostre de tempos em tempos um número selecionado de câmeras;

4.25.7. Transmissão de áudio do microfone para uma ou todas as caixas de som remotas associadas a dispositivos IP;

4.25.8. Disparo de presets diretamente do menu da câmera;

4.25.9. Disparo do limpador ou esguicho de água usando os comandos no menu;

4.25.10. Alertas audíveis ativados por detecção de movimento ou a ocorrência de eventos;

4.25.11. Busca inteligente permite pesquisar rapidamente movimento em áreas selecionadas das imagens gravadas;

4.25.12. Alternar entre o modo LIVE e ARCHIVE da mesma interface gráfica do usuário;

4.25.13. Gráfico mostra cronologia de sequências gravadas por intervalos de tempo ajustáveis para determinar com facilidade quando as imagens foram gravadas;

4.25.14. A Linha de Tempo deverá suportar a reprodução de até 32 câmeras simultâneas, sem degradação do desempenho, sincronizadas ou não;

4.25.15. O zoom digital é ativado por padrão para câmeras fixas em exibição ao vivo e por câmeras fixas e PTZ no modo de reprodução;

4.25.16. Recursos para imprimir imagens;

4.25.17. Exportação de "CD de Evidência" contendo dados nativos e o software de visualização para uso por parte das autoridades;

4.25.18. Exportação de AVI inclui automaticamente o áudio;

4.25.19. Criptografia e opção de senha de proteção para as gravações exportadas e arquivos de exportação para o formato de banco de dados;

4.25.20. Atribuição de saídas, presets PTZ, eventos e vistas como ações do joystick e botões do teclado;

4.25.21. Qualidade do vídeo otimizada quando a tela é maximizada;

4.25.22. Exibição dos controles de PTZ com a opção de controle de "joystick virtual" através da operação do mouse;

4.25.23. Processamento das imagens no momento da visualização; (via cliente de monitoramento) seja feito através de dispositivo de hardware com aceleração gráfica, não via CPU;

4.25.24. Deve suportar múltiplos monitores físicos conectados à mesma estação de trabalho;

4.25.25. Deve permitir a adição de legendas ao vídeo ao vivo que pode ser opcionalmente armazenado como uma marca d'água no arquivo;

4.25.26. Mapas multicamadas nos formatos BMP, JPEG, PNG;

4.25.27. Deve suportar mapas no formato CAD e/ou GIS e/ou PDF e/ou JPEG.

4.25.28. Federação e Monitoramento Centralizado – Funcionalidades;

4.25.29. O VMS deve possuir verdadeira solução de Monitoramento Central, onde câmeras de múltiplos locais independentes poderão ser visualizadas em conjunto a partir de uma estação de monitoramento central e deve suportar:

a) A capacidade de reproduzir vídeos gravados localizados nos Sites Remotos;

b) Câmeras de gravação localmente nos servidores do Centro de Monitoramento;

c) Receber eventos de alarme dos locais remotos;

d) Baixar a configuração do site remoto automaticamente;

e) Uma funcionalidade de administrador global, em que as alterações de configuração nos sites locais podem ser feitas a partir de uma única estação de trabalho no Centro de Monitoramento;

f) Oferecer suporte à visualização de eventos de análise de vídeo nos sites remotos;

g) Atualizações automáticas ou manuais da configuração do sistema remoto;

h) Ser capaz de funcionar como um Proxy de Vídeo;

i) Ser capaz de suportar fluxos de vídeo mediante solicitação.

4.26. O SISTEMA DEVERÁ SUPORTAR AS SEGUINTES OPÇÕES DE INTEGRAÇÃO:

4.26.1. Compatível com software de integração de vídeo-vigilância com sistemas ATM ou POS (registro de fluxo de produtos/ pessoas para a gestão de prevenção de perdas e fraudes);

4.26.2. Compatível com software supervisório de alarmes e estado de dispositivos para grandes instalações.

4.26.3. SDK para integração do vídeo em outros produtos usando a API para exibir imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período de tempo, e buscar por movimento.

4.26.4. Criação, importação e uso de páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização.

4.26.5. Integração nativa a todos os dispositivos listados nos fóruns de compatibilidade Onvif e/ou PSIA.

4.26.6. Integração com sistemas de controle de acesso, alarmes, portões, sistemas de gestão, ótica usando, no mínimo, os eventos de I/O, eventos internos, eventos TCP/IP ou por WEBService, e permitir que os dispositivos de controle de acesso possam ser vinculados às câmeras do VMS para verificação rápida de eventos utilizando o vídeo;

4.26.7. A gestão e monitoramento numa única interface, os eventos gerados pelo sistema de controle de acesso, tais como:

a) Acesso permitido;

b) Acesso bloqueado;

c) Porta aberta;

d) Porta forçada etc.;

4.26.8. Cada um dos eventos citados no item anterior, deve permitir a adição de marcadores a trechos do vídeo correspondente ao evento ocorrido, permitindo a pesquisa por esses marcadores e consequentemente a visualização do vídeo da(s) câmera(s) associadas à área controlada;

4.26.9. Que o usuário, ao realizar a sua identificação (via cartão de acesso, senha, biometria, etc.) para passar por uma barreira física controlada (catraca, cancela, porta, etc.) de uma área, seja possível exibição da foto e informações detalhadas do usuário que estiver realizando o acesso;

4.26.10. A capacidade de procurar eventos correspondentes a um determinado usuário e rastrear cada acesso realizado por ele;

4.26.11. A capacidade de exibir uma lista de todos os dispositivos ACS e seus estados;

4.26.12. O envio de comandos para dispositivos do controle de acesso para abrir uma porta, por exemplo;

4.26.13. Procurar eventos de determinados dispositivos, como uma catraca, por exemplo;

4.26.14. Procurar todos os eventos associados, dentro do campo de visão de uma câmera;

4.26.15. A capacidade de reproduzir o arquivo de vídeo correspondente a um evento gerado pelo controle de acesso;

4.26.16. A configuração flexível da interface do usuário (mova o painel de informações detalhadas, selecione as colunas exibidas etc.).

4.26.17. Ser completamente integrado com soluções de vídeo analítico, onde as configurações desses sejam realizadas na interface do VMS, não sendo necessária a alternância entre aplicações para tal. Os analíticos devem ser, no mínimo, os que seguem:

a) Reconhecimento facial;

b) Leitura de placas veiculares;

c) Leitura de containers;

d) Objetos abandonados/removidos;

e) Cruzamento de linha;

f) Contagem de objetos/pessoas;

g) Aglomeração de pessoas;

h) Cerca virtual/intrusão de área;

i) Tempo de espera;

j) Ociosidade;

k) Detecção de fumaça;

l) Detecção de capacete.

4.27. O SISTEMA DEVERÁ SUPORTAR AS SEGUINTES OPÇÕES SEGURANÇA:

4.27.1. Certificados digitais instalados em câmeras para verificação de dispositivos confiáveis;

4.27.2. Conexão segura (criptografada e verificação de origem) entre a câmera e o servidor de vídeo. O controle da câmera, incluindo sinais de PTZ, vídeo, áudio e comandos I/O, devem ser transferidos e criptografados (por meio de encapsulamento HTTPS);

4.27.3. Estabelecer sessões por HTTPS (autorização segura (por SSL / TLS) com certificado confiável instalado na câmera) para proteger os dados do usuário;

4.27.4. Conexões HTTPS seguras entre os servidores de vídeo e as instâncias do thin client (web e móvel);

4.27.5. Encapsulamento HTTPS ao recuperar vídeo do armazenamento de borda da câmera;

4.27.6. Assinatura digital do vídeo exportado para comprovar a autenticidade do vídeo. A assinatura digital deve ser feita usando certificados digitais compatíveis com "PKCS # 7 assinatura de dados assinados".

4.28. LICENCIAMENTO

4.28.1. Contemplar até 20 servidores de gravação, ilimitados softwares clients, webclients, mobile Server, mobile clients e softwares de matriz virtual.

4.28.2. Cada licença de câmera deve:

4.28.3. Ser necessária para que cada câmera seja visualizada e armazenada no sistema, seja diretamente (câmera IP) ou por canal de vídeo a ser usado de um codificador (encoder) ou DVR

4.28.4. Abranger a instalação de até 20 servidores e a designação como Master ou Slave;

4.28.5. Garantir de serem instalados e utilizados o software cliente em qualquer número de computadores, de forma gratuita;

4.28.6. Não ter limite de validade;

4.28.7. Garantir o Acordo de Manutenção do Produto (PMA):

a) Expansão do Sistema;

b) Garantir a aquisição e uso de forma gratuita de todas as atualizações dos produtos desde que o suporte da licença esteja valido;

c) A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras;

d) O número de servidores de gravação deve permitir ampliar a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto;

e) O número de câmeras pode ser ampliado independentemente da quantidade de servidores de gravação e/ou estações de operação do sistema;

f) O número de clientes de operação e de dispositivos móveis poderão ser ampliados a qualquer momento sem necessidade de licenciamento adicional.

4.29. LICENÇA DE USO DE ANALÍTICO FACIAL

4.29.1. Deve ser do mesmo fabricante da solução de vídeo monitoramento proposta, ou completamente integrada, permitindo inclusive, configurações, busca, e edição das listas de pessoas cadastradas no banco de dados pela mesma interface do VMS, não sedo necessário a alternância entre duas ou mais plataformas;

4.29.2. Deve suportar detecção, captura e reconhecimento de face das pessoas em tempo real;

4.29.3. Deve ser capaz de detectar e capturar simultaneamente múltiplas faces da mesma visão da câmera (assumindo a resolução da câmera e os requisitos de pixel da face sejam atendidos);

4.29.4. Não deve exigir o uso de nenhuma câmera proprietária (totalmente independente de câmera), desde que os requisitos mínimos sejam atendidos;

4.29.5. Deve selecionar automaticamente o quadro de vídeo otimizado para localização de face;

4.29.6. Deve registrar e arquivar na imagem facial, data, hora e câmera do banco de dados;

4.29.7. Deve fornecer capacidade para ajustar parâmetros e limiares de reconhecimento;

4.29.8. Deve ser capaz de registrar um evento / alarme se programado para uma pessoa reconhecida;

4.29.9. Deve possuir a capacidade de clicar no rosto de uma pessoa a partir da GUI e exibir o vídeo associado à imagem facial capturada;

4.29.10. Deve possuir o recurso de exibir na GUI a taxa de qualidade de reconhecimento das faces (%) e o nome de cada pessoa reconhecida;

4.29.11. Deve ser capaz de desconsiderar as taxas de reconhecimento do índice de baixa precisão;

4.29.12. Deve ter capacidade de bloquear o acesso do operador humano;

4.29.13. Deve ter capacidade de localizar e capturar faces de múltiplos canais de vídeo em tempo real;

4.29.14. Deve ter a capacidade de ser gerenciado remotamente;

4.29.15. Deve ter um nível de precisão de 90% e acima (se as diretrizes para a configuração correta da câmera/software tiverem sido seguidas);

4.29.16. Deve poder criar vários perfis de cadastros no banco de dados permitindo, no mínimo:

a) Várias fotos dessa pessoa;

b) Nome, nome do meio e sobrenome;

c) Um campo de comentários opcional;

d) A opção de ser adicionado a uma "lista negra".

4.29.17. Deve ser capaz de reconhecer o desgaste individual da cabeça, se tal desgaste da cabeça não obstruir uma visão clara dos olhos dos indivíduos.

4.29.18. Deve ser capaz de reconhecer uma pessoa usando óculos graduados, mesmo que em sua foto registrada eles não estejam usando óculos (supondo que seus óculos não ofusquem e sejam claros);

4.29.19. Deve poder alarmar e / ou realizar reações complexas com base em rostos reconhecidos;

4.29.20. Caso a solução ofertada necessite de licenciamento por face no banco, a mesma deverá vir licenciada para, no mínimo 30.000 faces.

4.30. PESQUISA

4.30.1. Deve ter a capacidade de procurar uma pessoa com base na câmera pela qual passou;

4.30.2. Deve ser capaz de procurar uma pessoa com base na hora/data;

4.30.3. Deve ser capaz de procurar uma pessoa com base no nome e sobrenome da pessoa;

4.30.4. Deve ser capaz de procurar uma pessoa com base em uma foto tirada anteriormente da pessoa;

4.30.5. Deve ser capaz de, ao clicar na imagem de uma pessoa reconhecida, independente desta estar cadastrada, buscar todas as imagens associadas ao reconhecimento dessa pessoa (câmeras por onde está passou e fora reconhecida);

4.30.6. Todos os resultados da pesquisa devem ser associados a uma foto da pessoa e opcionalmente com uma sequência de vídeo da pessoa que passou.

4.31. INTEGRAÇÃO

4.31.1. Deve ter a capacidade de se integrar com outros dispositivos, tais como dispositivos de contato seco, controle de acesso e etc;

4.31.2. Deve ter a capacidade de integrar e trocar dados em tempo real com bancos de dados externos;

4.31.3. Deve fornecer como SDK, o que permitirá que sistemas de terceiros recebam todos os eventos do VMS de reconhecimento facial;

4.31.4. Deve possuir a capacidade de importar faces para o banco de dados do sistema, quando as imagens faciais atenderem aos requisitos mínimos de importação;

4.31.5. As imagens podem ser importadas uma por uma ou em lote.

4.32. LICENÇA DE USO DE ANALÍTICO LPR

4.32.1. Deve ser do mesmo fabricante da solução de vídeo monitoramento proposta, ou completamente integrada, permitindo inclusive, configurações, busca, emissão de relatórios e edição das listas de veículos cadastrados nos bancos de dados, pela mesma interface do VMS, não sedo necessário a alternância entre duas ou mais plataformas;

4.32.2. A aplicação deve funcionar 24 horas por dia, sete dias por semana sem supervisão humana;

4.32.3. Deve simultaneamente detectar, capturar e comparar placas de veículos em tempo real;

4.32.4. Deve usar mecanismos de rede neural para capturar as placas na imagem e suportar um algoritmo de reconhecimento baseado em modelo e não depender apenas de reconhecimentos individuais de caracteres;

4.32.5. O processo de localização, captura e reconhecimento das placas deve ser baseado em software e não exigir o uso de sensores adicionais;

4.32.6. Deve ser capaz de capturar múltiplas faixas de tráfego com uma câmera (se a câmera / resolução usada permitir);

4.32.7. Não deve exigir o uso de nenhuma câmera proprietária (totalmente independente de câmera) desde que atendidos os requisitos mínimos;

4.32.8. Deve possuir ferramentas que compensem a distorção da câmera e posição (angulação) incorreta da placa capturada do veículo;

4.32.9. Deve fornecer três modos para armazenar as imagens capturadas pelo reconhecimento da placa no banco de dados: foto de cena inteira, apenas o veículo ou apenas a imagem da placa;

4.32.10. Deve automaticamente determinar o melhor quadro da imagem com a placa do veículo no fluxo de vídeo;

4.32.11. Deve ser capaz de armazenar toda uma sequência de vídeo associada ao resultado do reconhecimento da placa, nas seguintes modalidades:

a) Gravação constante;

b) Gravar todo o veículo passando.

4.32.12. Deve fornecer capacidade para ajustar parâmetros e limites de reconhecimento;

4.32.13. Deve fornecer um índice de qualidade das placas capturadas e poderá fazer a filtragem automática dos resultados de reconhecimento, desconsiderando as taxas de baixo limiar de precisão - definidas pelo administrador;

4.32.14. Deve ser capaz de usar estatísticas internas para ajustar os algoritmos de reconhecimento para melhorar a taxa de reconhecimento da câmera definida;

4.32.15. Deve apoiar o reconhecimento de placas de todos os estados do Brasil e Mercosul e ainda da maioria das placas internacionais podendo determinar o país de origem de cada placa;

4.32.16. Deve oferecer uma opção de baixa velocidade para veículos que viajam em até 40km/h;

4.32.17. Deverá ser capaz de referenciar um banco de dados central ou vários bancos de dados remotos paralelamente para corresponder as placas capturadas em tempo real aos bancos de dados. Conexões de baixa largura de banda para bancos de dados não devem impedir o funcionamento do sistema;

4.32.18. Deve ser possível registrar e arquivar em um banco de dados a imagem do vídeo, data, hora, número da placa, País/Estado da placa e direção do deslocamento em relação à câmera, aproximando ou partindo;

4.32.19. Deverá ter capacidade de gerenciar e reconhecer placas de veículos em múltiplos canais de vídeo em tempo real;

4.32.20. Deve ter a capacidade de ser gerenciado remotamente;

4.32.21. Deve estar acessível com os clientes de PC padrão para visualização remota;

4.32.22. Deve fornecer capacidade para editar ou bloquear as edições de placas de veículos reconhecidas pelo operador humano, de acordo os direitos do usuário;

4.32.23. Deve suportar listas de observação internas de placas registradas (branco, preto, informativo);

4.32.24. Deve apoiar a automação das reações do sistema no caso de placas reconhecidas que correspondam a listas de observação internas ou bancos de dados externos;

4.32.25. Deve poder alarmar e/ou executar eventos complexos com base em cadeias de matrículas de valores predeterminados;

4.32.26. Deve suportar a entonação sonora das placas reconhecidas;

4.32.27. Poderá registrar um evento / alarme quando nenhuma placa for reconhecida ou a placa estiver faltando;

4.32.28. Deve suportar unidades mph e km/h para medição de velocidade;

4.32.29. Deve fornecer interface gráfica flexível do operador para resolver diferentes tarefas;

4.32.30. Deve possuir uma ferramenta de relatório para a geração rápida de relatórios do (s) veículo (s) capturado (s) (inclui quadro e informações sobre as placas de veículos reconhecidas);

4.32.31. Deve apresentar precisão de, no mínimo, 95% (noventa e cinco por cento) se as diretrizes para a correta configuração da câmera / software foram seguidas.

4.33. PESQUISA

4.33.1. Deve ter a capacidade de vários métodos de Pesquisa por placa capturada, data e/ou hora e associar os resultados da pesquisa às imagens/vídeos das placas;

4.33.2. Deve poder usar entradas curinga durante a busca por caracteres desconhecidos;

4.33.3. A pesquisa poderá ser feita por qualquer sequência de caracteres conhecida;

4.33.4. O resultado da pesquisa por parte do nome deverá trazer todos os veículos que satisfizerem os critérios de pesquisa;

4.33.5. A pesquisa poderá ser realizada pela câmera que realizou o reconhecimento da placa;

4.33.6. A pesquisa poderá ser realizada com base nos comentários do usuário previamente adicionados para um resultado específico;

4.33.7. A pesquisa poderá ser realizada em placas com caracteres não reconhecidos;

4.33.8. A pesquisa poderá ser realizada em veículos que violaram a velocidade pré-determinada.

4.34. Integração

4.34.1. Deve suportar a capacidade de se integrar com outros dispositivos, como contatos secos ou códigos Wiegand;

4.34.2. Deve ter um mecanismo de scripts interno usado para programar lógica de comportamento de sistema customizada de complexidade variável;

4.34.3. Deve ter a capacidade de integrar e trocar dados em tempo real com bancos de dados externos;

4.34.4. Deve fornecer uma API para aplicativos de terceiros que desejam integrar-se ao sistema;

4.34.5. A API deve suportar o envio de eventos, quadros únicos de vídeo e sequências de vídeo;

4.34.6. Deve ser do mesmo fabricante do VMS, ou completamente integrado, e ser configurado e gerenciado na mesma interface.

5. SOFTWARE - SOFTWARE DE CONTROLE DE ACESSO

5.1.1. Responsável por permitir o registro e o armazenamento on-line real-time das informações de acesso, bem como o processamento das informações e a emissão de relatórios;

5.1.2. O sistema deverá operar como "serviço do Windows" para que o servidor não precise ficar com um usuário conectado para que o sistema funcione;

5.1.3. Deverá possuir as seguintes capacidades:

a) Função de administrar a rede de equipamentos e controlar até 200 (duzentos) equipamentos coletores de impressão digital, cartões, catracas e cancelas, configurando-os, e recebendo informações on-line através da rede Ethernet;

b) Transferência de informações: exportar em formato texto qualquer tabela do banco de dados através do próprio aplicativo;

c) Permitir o cadastro e/ou alterações de usuários, considerando as informações de impressão digital, código de matrícula, nome, foto e CPF, entre outras. Deve checar a existência de cadastro prévio da pessoa através do nome, CPF e impressão digital;

d) Permitir o cadastro de fotos, as quais devem estar armazenadas fora do banco de dados, em formato de arquivo. O acesso a estas fotos pelo sistema, quando estiver sendo executado de uma CPU diferente da que está armazenando as fotos, deve ser feito de forma que não exista compartilhamento de pastas na rede;

e) Permitir cadastrar múltiplas empresas: tais como empresas terceirizadas e permite cadastrar subdivisões hierárquicas de cada empresa, com no mínimo 2 níveis;

f) Cadastro de feriados: permitir cadastrar feriados que abrangem todo o dia, parte do dia e ponto facultativo;

g) Relatórios: Permitir que todos os relatórios do sistema tenham a opção de visualização na tela e exportação para arquivo no formato texto, csv e HTML;

h) Segurança: possuir acesso restrito a usuários cadastrados. Permitir dentro do sistema aos administradores controlar o acesso a cada função do sistema, atribuindo permissões aos usuários ou grupos de usuários cadastrados;

i) Segurança por área: permitir, para cada subdivisão de cada empresa, a restrição de acesso apenas a usuários autorizados, não permitindo que membros administradores de outras áreas bloqueiam acesso de pessoas que não são de sua subordinação;

j) Auditoria na utilização do sistema: armazenar o nome da máquina e usuário registrado na rede no momento que o sistema é executado, junto às informações de quem está utilizando o sistema;

k) Registro de ocorrências: registrar automaticamente condições excepcionais que ocorrem durante sua execução com respectivas mensagens de erro;

5.1.4. Bloquear a identificação pessoal pela data ou horário: negar o acesso fora dos horários cadastrados para a pessoa identificada;

5.1.5. Limitar a identificação pessoal por equipamento, por um usuário: permite que um usuário só possa efetuar a identificação no(s) equipamento(s) atribuídos a ele;

5.1.6. Tipo de equipamento: identifica o modo de utilização de cada equipamento: se acesso, se cadastro ou se o equipamento permite visitantes;

5.1.7. Deve ser capaz de armazenar o cadastro e as informações de acesso de 30.000 alunos e prestadores, não restringe número de visitantes;

5.1.8. Capacidade de cadastro de traços biométricos da solução e de 250.000 (duzentos e cinquenta) amostras biométricas com TFA (Taxa de falso aceite), máxima de 1:1.000.000 e TFR (Taxa de falsa rejeição) inferior a 0,5%. A solução permite o cadastro de mais de uma amostra por pessoa, a limitação do cadastro interativo em 1 (uma) amostra por pessoa, e o cadastro de novas amostras automaticamente;

5.1.9. Tempo de identificação biométrica (busca 1:N) e de no máximo 1,5 segundos no banco de impressões com 1.000.000 (um milhão) amostras cadastradas. Este limite e respeitado tanto para identificação positiva (aceite), quanto para negativa (rejeição);

5.1.10. Comunicação dos Coletores com o Software

5.1.11. Toda transmissão de pacotes entre o equipamento servidor e coletores biométricos ou de cartões, utiliza criptografia padrão AES 128 bits com chave criptográfica configurável;

5.1.12. Permite a comunicação on-line, via TCP/IP, com pelo menos 2 (dois) computadores servidores pré-configurados para a pesquisa de informações, execução de registros e tomada de ações. Caso o equipamento servidor principal não esteja disponível, é feita a tentativa de comunicação com o segundo servidor;

5.1.13. Permite replicação;

5.1.14. Possui a funcionalidade de verificação e envio de pacote para o equipamento servidor no momento em que informações são geradas, evitando que o servidor fique emitindo comandos para checar se o coletor possui algum dado ou evento (polling);

5.1.15. Permite configuração remota, através do software de controle de acesso especificado nesta especificação técnica;

5.1.16. O tempo de identificação, busca 1:N, der no máximo 1,5 segundos tanto para o reconhecimento quanto para o não reconhecimento;

5.1.17. Transmite automaticamente as coletas em off-line assim que a comunicação com um dos computadores servidores for restabelecida.

5.2. SEGURANÇA E ACESSIBILIDADE

5.2.1. O sistema deverá possuir interface gráfica por meio de programa aplicativo a ser executado no ambiente cliente;

5.2.2. Os textos das interfaces do sistema com o usuário e os dados a serem registrados pelo usuário final no sistema devem estar de acordo com a ortografia da língua portuguesa, conforme legislação brasileira vigente e de acordo com o Vocabulário Ortográfico da Língua Portuguesa, da Academia Brasileira de Letras;

5.2.3. Todo usuário deve possuir um código de usuário e uma senha (criptografada);

5.2.4. Todas as alterações realizadas por um usuário devem ser possíveis de auditoria no sistema, contendo a estação através da qual o usuário fez a operação, a data e hora e um registro da informação alterada/inserida/removida antes e depois da alteração;

5.2.5. Deve ser registrado e mantido o histórico de todas as alterações efetuadas em qualquer campo, em qualquer tempo (mesmo alterações retroativas), identificando quem e quando as realizou.

5.3. COLETA DE DADOS

5.3.1. Todos os registros de acesso, no banco de dados, devem possuir um hash de proteção criado através de criptografia AES com 128 bits ou superior;

5.3.2. Os registros dos acessos que alimentam o sistema, devem ser realizados a partir de qualquer um dos itens abaixo ou a todos concomitantemente:

a) De forma on-line e real-time, dos coletores de dados acoplados a bloqueios (catracas, portas, cancelas, torniquetes, etc.);

b) Automaticamente quando o sistema reestabelecer a comunicação com os coletores que operaram em modo off-line (autônomos) durante algum período;

c) Digitação posterior feita diretamente no sistema (por um administrador);

d) Importação de arquivos texto de qualquer origem (por um administrador).

5.4. SENHAS E PERFIS DE USUÁRIOS / ADMINISTRADORES

5.4.1. O sistema de controle de acesso deve permitir ao administrador/usuário o acesso ao seu próprio perfil, identificado através de senha, sendo possível definir, para cada perfil:

a) Funções que podem ser acessadas;

b) Empresas e Departamentos que podem ser manipulados;

c) Coletores de dados que podem ser manipulados;

d) Relatórios a serem acessados;

e) O sistema permite aos administradores e usuários consultar, incluir, modificar e excluir informações, de acordo com as permissões previamente estabelecidas.

5.5. RELATÓRIOS

5.5.1. O sistema, no que diz respeito ao controle de acesso, permite a exibição de todos os relatórios em tela e a geração de relatórios em arquivo texto, HTML, ou impressos com diferentes critérios de ordenação, possuindo, as seguintes facilidades de exibição e impressão de relatórios:

a) Relação de funcionários presentes;

b) Acesso de pessoas;

c) Tempo de permanência em um determinado local;

d) Espelho de acesso de uma determinada pessoa, com opção para incluir as tentativas de acesso não liberadas;

e) Consulta aos registros de um determinado período. Opção para seleção de órgãos, empresas (prestadoras de serviço), locais de acesso e categoria da pessoa;

f) Relatório de exceção: relaciona as ocorrências de bloqueio de acesso acusadas pelo sistema;

g) Relatório de quem está presente ou ausente, dado um determinado período;

h) Consulta do histórico de visitantes em um determinado período.

5.6. FACILIDADES DE PROCESSAMENTO

5.6.1. O sistema deve possuir as seguintes facilidades de processamento:

a) Consultar todas as informações cadastrais e as regras aplicadas ao servidor;

b) Visualizar meses anteriores ao atual;

c) Informar observações;

d) Geração automática de marcações de acordo com critérios definidos pelo usuário;

e) Processamento por lotes de servidores, selecionados e/ou editados;

f) Processamento em rede com acessos simultâneos;

g) Inclusão de novos campos no cadastro de servidores, sem que seja necessária programação pelo administrador do sistema;

h) Pesquisa de servidores por qualquer parte do nome, CPF, matrícula, departamento, categoria e subcategoria.

5.7. INTEGRAÇÃO COM OUTROS SISTEMAS

5.7.1. O sistema deve permitir que as informações possam ser integradas automaticamente com outras bases de dados através de triggers, views, programas de vinculação ou procedures do Banco de Dados, sem intervenção manual;

5.7.2. Vinculação dos dados entre os sistemas será realizada pelo CPF.

5.8. CRITÉRIOS DE VALIDAÇÃO DE ACESSO

5.8.1. O sistema utiliza os seguintes critérios de validação de acesso:

a) Código - Se existente no Banco de Dados;

b) Situação - Se o código está liberado;

c) Validade - Se dentro do período de validade;

d) Local - Se a pessoa pode ter acesso a uma determinada área;

e) Horário - Se a pessoa pode ter acesso naquele local naquele momento;

f) Diferenciação entre as faixas horárias de acesso e de ponto;

g) Situação Funcional - Se a pessoa está ativa na empresa (não está de férias, licença, etc.):

h) A situação funcional permite o bloqueio ou liberação de acesso, acesso a refeitórios, registro de frequência;

i) Senha - Acesso condicionado à verificação do código de acesso;

j) Antidupla - Bloqueia dois acessos consecutivos de mesma natureza no mesmo local, evitando o "empréstimo" da impressão digital / crachá.

5.9. PORTARIAS

5.9.1. O sistema de controle de acesso deve incluir tratamento especial para as portarias.

5.9.2. Nas estações de trabalho localizadas nas portarias deve ser realizado o registro e a baixa dos visitantes e registro da movimentação de materiais.

5.9.3. O sistema deve possuir as seguintes funções:

a) Registro dos dados do visitante: Nome, Empresa, Documento, Motivo da Visita, Telefone;

b) Pesquisa na base de dados de visitantes, por parte do nome, pelo documento ou pela impressão digital, para evitar a repetição da digitação de informações dos visitantes mais frequentes;

c) Verificação se o visitante possui restrição de acesso (persona non grata);

d) Possibilitar captura de imagem e documento e imprimir crachá ou etiqueta para os visitantes;

e) Baixa do crachá na saída, permitindo sua reutilização por outro visitante (quando for necessária a utilização do crachá em função das características biométricas da impressão digital);

f) Consulta dos visitantes que ainda não saíram das instalações visitadas;

g) Edição do cadastro de um visitante (últimas visitas, alteração do cadastro);

h) Verificação se a visita foi pré-agendada no sistema, aumentando o nível de segurança da empresa e agilizando o processo de registro do visitante;

i) Movimentação de Materiais na Portaria;

j) Registro da entrada e saída de material e pertences das pessoas que passam pela portaria;

k) Registro de ocorrências anormais.

5.10. MONITORAMENTO

5.10.1. O sistema de controle de acesso deve permitir o monitoramento de operações controladas, permitindo o monitoramento a partir de uma ou mais estações de trabalho simultaneamente mantendo as seguintes características:

a) Exibição em tempo real de todas as tentativas de entrada e saída nos bloqueios, indicando o sucesso da operação;

b) Sinalização de tentativa de arrombamento ou de presença indevida, através de sensores de porta aberta;

c) Exibição em tempo real das fotos do pessoal reconhecido;

d) Exibição em tempo real do status da rede de bloqueios e de coletores de dados;

e) Exibição em tempo real de indicação de pânico.

6. SERVIÇO DE INSTALAÇÃO DE SOFTWARE.

6.1.1. Instalação, configuração e atualização de todos os módulos do software;

6.1.2. Deverá ser instalado e configurado todas as máquinas que terão acesso ao VMS;

6.1.3. Deverá ser instalado e configurado o servidor que deverá rodar o VMS;

6.1.4. Deverão ser configurados as funcionalidades solicitadas pela CONTRATANTE na reunião de planejamento e kick-off, abordando todos os pontos de segurança.

7. TREINAMENTO DA SOLUÇÃO – SOFTWARE.

7.1.1. A CONTRATADA deverá executar treinamentos específicos dos softwares e equipamentos adquiridos de acordo com as seguintes condições:

7.1.2. Carga horária mínima de 20h (vinte horas), com dedicação diária de até 04h (quatro horas);

7.1.3. O idioma a ser adotado deverá ser português Brasil;

7.1.4. Os treinamentos deverão ser ministrados por profissionais certificados;

7.1.5. O treinamento deverá ocorrer nas dependências da CONTRATANTE, após a instalação dos componentes adquiridos.

8. CARACTERÍSTICAS GERAIS DO SUPORTE E GARANTIA

8.1. Esse suporte deverá ser realizado por um período de 12 (doze) meses após a implantação da solução e, durante esse período, a CONTRATADA deverá manter equipe especializada remota para atender as solicitações de suporte e manutenção corretiva e preventiva da CONTRATANTE. Por atividades de suporte, entende-se que a CONTRATADA deverá realizar os seguintes serviços:

8.1.1. Atualização de pacotes de correção dos sistemas: Atividades funcionais e técnicas para atualizar a plataforma com atualizações de cada sistema criadas pela CONTRATADA em ambiente de homologação e produção, conforme necessidade de negócio e de segurança da CONTRATANTE, sempre referentes a módulos e funcionalidades previamente disponíveis e em uso em cada sistema;

8.1.2. Manutenções preventivas: Atividades técnicas pró ativas de checagem no ambiente de produção de cada sistema que visem garantir um melhor funcionamento do sistema, seus aspectos de integridade, disponibilidade e segurança;

8.1.3. Manutenções corretivas: Correção técnica e funcional de eventuais bugs que possam aparecer no ambiente de produção nos sistemas associados aos módulos implantados e definidos no escopo deste documento. Por "bugs" ou "erros" entende-se comportamentos divergentes do esperado quanto ao funcionamento padrão já em uso nos módulos e funcionalidades previamente disponíveis e em uso em cada sistema. Mudanças de processos ou de funcionalidades já em uso não serão consideradas "bugs", logo, não fazem parte do escopo de Manutenções Corretivas.

8.1.4. Manutenções adaptativas: ajustes técnicos e funcionais nos sistemas para deixá-los adequados a mudanças legais e que estejam em concordância com o escopo da administração da CONTRATANTE.

8.1.5. Acompanhamento de atividades de infraestrutura: Acompanhamento remoto de ações técnicas que poderão ser realizadas pela equipe técnica da CONTRATADA para recuperação em caso de desastres, restauração sob demanda de backups previamente realizados, gestão da segurança de acesso e apoio na gestão da disponibilidade dos ambientes de homologação e produção dos sistemas implantados pelo projeto.

8.2. O registro de chamado para acionamento de solicitações de suporte, deverá ser feito pela CONTRATANTE em ferramenta informatizada disponibilizada pela CONTRATADA, que deve estimar o tempo a ser gasto e a data de entrega, informar a CONTRATANTE que deve autorizar o atendimento.

8.3. O horário de atendimento para atividades de suporte deverá ser de segunda à sexta-feira, em dias úteis, das 08h00min às 18h00min.

8.4. A CONTRATADA deverá manter equipe suficiente e capacitada para prestar os serviços de suporte acordo com o tamanho e complexidade da operação da CONTRATANTE e que garanta o atendimento do Nível de Serviço esperado para essas atividades.

8.5. Para controlar prazos de atendimento às solicitações de suporte, devemos assumir a classificação de cada chamado (ou solicitações de suporte) em 4 (quatro) categorias relacionadas ao impacto de negócio associado a cada solicitação:

8.5.1. Alta: O incidente que causou o chamado tem impacto direto em um processo de negócio com viés totalmente financeiro e/ou legal e não existem maneiras de contornar o problema para que o usuário possa continuar a executar o processo de negócio na ferramenta;

8.5.2. Média: O incidente que causou o chamado tem impacto direto em um processo de negócio com um possível impacto financeiro e/ou legal associado, porém, existem maneiras de se contornar o problema para que o usuário possa continuar a executar o processo de negócio na ferramenta;

8.5.3. Baixa: O incidente que causou o chamado tem impacto direto em um processo de negócio, mas não endereça impacto financeiro e/ou legal, porém, existem maneiras de se contornar o problema para que o usuário possa continuar a executar o processo de negócio na ferramenta;

8.5.4. Mínima: O incidente que causou o chamado não está associado a um impacto financeiro e não impacta diretamente um processo de negócio. O usuário pode continuar a utilização da ferramenta sem maiores riscos associados.

8.6. A classificação de cada chamado será realizada inicialmente pela CONTRATADA assim que receber a solicitação da CONTRATANTE, de acordo com os detalhes expostos pelos usuários que abrirem a solicitação. Caso a CONTRATANTE classifique a solicitação de forma diferente, as partes devem discutir seus pontos-de-vista e chegarem a um consenso quanto ao grau de criticidade do chamado.

8.7. A solução (ou entrega do chamado, considerando o envio da solução ao cliente e não as atividades de validação por parte do cliente para encerramento do chamado) deve ser provida pela CONTRATADA conforme segue:

ANS por chamado/incidente aberto			
Severidade	**Tempo de resposta**	**Tempo de solução**	**Metas de atendimento**
Alta	Em até 1 hora	8 horas úteis	90% dos chamados dessa severidade devem ser atendidos dentro conforme essa regra
Média	Em até 3 horas	Em até 15 dias	85% dos chamados dessa severidade devem ser atendidos dentro conforme essa regra
Baixa	Em até 8 horas	Em até 21 dias	80% dos chamados dessa severidade devem ser atendidos dentro conforme essa regra
Mínima	Em até 16 horas	Em até 30 dias	80% dos chamados dessa severidade devem ser atendidos dentro conforme essa regra

8.8. Esses valores devem ser seguidos como base sempre que o incidente não envolver o acionamento de uma terceira parte, como o Fabricante da solução. Nesses casos, é obrigação da CONTRATADA avisar previamente a CONTRATANTE deste cenário para que os usuários estejam cientes do envolvimento de outros na resolução de cada solicitação.

8.9. Para os equipamentos gerenciamento e gravação, exige-se como atividades mínimas de suporte técnico:

8.9.1. Limpeza física dos equipamentos;

8.9.2. Configuração inicial de equipamento;

8.9.3. Configuração e verificação do correto funcionamento do failover;

8.9.4. Configuração de NTP, local e fuso horário;

8.9.5. Verificação de temperatura, situação das fontes, ventoinhas, discos etc.;

8.9.6. Verificação do adequado funcionamento de todos os serviços do gerenciador (por exemplo, script manager, system locator, NTP);

8.9.7. Realização de backup;

8.9.8. Verificação da integridade da base de dados;

8.9.9. Verificação da sincronização dos demais dispositivos com o gerenciador;

8.9.10. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer.

8.9.11. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial.

8.9.12. Configuração e verificação do correto funcionamento de gravação redundante;

8.9.13. Configuração de NTP, local e fuso horário;

8.9.14. Verificação de temperatura, situação das fontes, ventoinhas, discos (RAID, SMART e CF Card) etc.;

8.9.15. Verificação do adequado funcionamento de todos os serviços do gravador;

8.9.16. Verificação da ocorrência de perda de pacotes nos streams de vídeo;

8.9.17. Verificação da integridade da base de dados, da ocorrência de gravações em duplicidade, da existência de vídeos sem referência e outras ocorrências que impedem o bom funcionamento do equipamento;

8.9.18. Verificação e correção da distribuição de gravação dentro de um mesmo pool;

8.9.19. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer;

8.9.20. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial;

8.9.21. Montagem e desmontagem de pools de gravação, colocação e remoção de dispositivos.

8.10. Para os equipamentos da sala de monitoramento, exige-se como atividades mínimas de suporte técnico:

8.10.1. Limpeza física dos equipamentos;

8.10.2. Verificação de temperatura, situação das fontes, ventoinhas, discos etc.;

8.10.3. Verificação do adequado funcionamento de todos os serviços dos dispositivos;

8.10.4. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer;

8.10.5. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial.

8.11. Para os equipamentos Câmeras IP diversas, exige-se como atividades mínimas de suporte técnico:

8.11.1. Limpeza física de todos os equipamentos e aplicação de composto hidrofóbico nos dispositivos externos sempre que necessário;

8.11.2. Configuração inicial de câmeras para funcionamento no sistema;

8.11.3. Identificação e correção de problemas de alimentação de câmeras;

8.11.4. Identificação e resolução de problemas de software (incluídos SO, web server etc.) de câmeras;

8.11.5. Identificação de problemas físicos nas câmeras e apresentação de relatório apontando o problema e causa provável;

8.11.6. Apresentação de changelogs e aplicação de patches ou atualizações de firmware para câmeras;

8.11.7. Instalação e/ou remoção simples de câmera com base, incluída a identificação com adesivo no equipamento e acessórios para a adequada proteção do dispositivo contra água e poeira, limitadas.

8.12. Para os equipamentos de controle de acesso, exige-se como atividades mínimas de suporte técnico:

8.12.1. Limpeza física de todos os equipamentos;

8.12.2. Reparos de peças que sofrem desgastes naturais pelo uso contínuo;

8.12.3. Manutenção preventiva para reaperto e ajuste de peças móveis;

8.12.4. Lubrificação de partes rotativas.

8.13. Para os equipamentos de CFTV, exige-se como atividades mínimas de suporte técnico:

8.13.1. Configuração inicial de equipamento;

8.13.2. Verificação de temperatura, situação das fontes, ventoinhas, discos etc.;

8.13.3. Verificação do adequado funcionamento de todos os serviços do gerenciador (por exemplo, script manager, system locator, NTP);

8.13.4. Realização de backup;

8.13.5. Verificação da integridade da base de dados;

8.13.6. Verificação da sincronização dos demais dispositivos com o gerenciador;

8.13.7. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer.

8.13.8. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial.

8.13.9. Verificação e correção da distribuição de gravação dentro de um mesmo pool;

8.13.10. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer;

8.13.11. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial.

8.14. Para o software de controle de acesso, exige-se como atividades mínimas de suporte técnico:

8.14.1. Configuração inicial de equipamento;

8.14.2. Verificação de temperatura, situação das fontes, ventoinhas, discos etc.;

8.14.3. Verificação do adequado funcionamento de todos os serviços do gerenciador (por exemplo, script manager, system locator, NTP);

8.14.4. Realização de backup;

8.14.5. Verificação da integridade da base de dados;

8.14.6. Verificação da sincronização dos demais dispositivos com o gerenciador;

8.14.7. Identificação e correção de problemas de software e hardware já ocorridos ou na iminência de ocorrer;

8.14.8. Apresentação de changelogs e aplicação de patches ou atualizações de firmware em caráter emergencial.

8.15. Para controladoras e leitores de acesso, exige-se como atividades mínimas de suporte técnico:

8.15.1. Limpeza física dos equipamentos;

8.15.2. Verificação de temperatura, situação das fontes, ventoinhas, discos etc.;

8.15.3. Verificação do adequado funcionamento de todos os serviços dos dispositivos;

8.15.4. Configuração inicial dos equipamentos.

8.16. As câmeras de vídeo removidas para manutenção devem ser repostas imediatamente por câmeras reservas da CONTRATADA, e para os demais equipamentos, quando o período de reparo ultrapassar 48 (quarenta e oito) horas, a CONTRATADA deverá, obrigatoriamente, instalar equipamento tecnicamente similar ou superior de sua propriedade.

8.17. Os bens ou serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no edital, no contrato e no que foi estabelecido no Acordo de Nível de Serviço, devendo ser substituídos/refeitos no prazo de 12 (doze) horas quando não houver fornecimento de peças ou no prazo de 48 (quarenta e oito) horas quando houver substituição de peças, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação de penalidades.

8.18. Prazo de execução dos serviços de, no máximo, 12 (doze) horas, contadas a partir da abertura da ordem de serviço, quando não houver necessidade de substituição de peças e de, no máximo, 48 (quarenta e oito) horas, quando necessária a substituição e/ou fornecimento de peça ou equipamento, contadas da abertura da ordem de serviço.

8.19. Toda e qualquer substituição de peças ou componentes deverá ser autorizada e acompanhada por funcionário designado pelo SESC, e deverá ser por peças/componentes novos e de características iguais ou superiores ao daquele que for retirado.

8.20. Prazo de garantia dos serviços é de, no mínimo, 90 (noventa) dias, e das peças/componentes será de, no mínimo, de 6 (seis) meses, contados a partir do recebimento definitivo do objeto pelo gestor, prevalecendo o prazo de garantia fixado pelo fabricante ou fornecedor, caso seja maior.

9. RESPONSÁVEL PELA ESPECIFICAÇÃO TÉCNICA

Saule Tassara Bortolani
Líder da Seção de Infraestrutura e Suporte de TI

Tiago Silva Santos
Diretor de Transformação Digital e Inovação

Goiânia, 05 de julho de 2023.