ANEXO V

Caderno de Especificações e Encargos

ANEXO H

CADERNO DE ESPECIFICAÇÕES E ENCARGOS

CADERNO DE ESPECIFICAÇÕES E ENCARGOS

1. Dados do profissional responsável

Nome do Responsável Técnico:	Fábio Banda Roland
Título:	Engenheiro Eletricista
Endereço:	Av. Inconfidência, 650, sala 510
Cidade:	Canoas – RS
Telefone:	(51) 3785-4683
E-mail:	fabio.roland@rolandgroup.com.br
CREA-RS:	185070
Número de ART do Presente Projeto:	11282863

2. Objetivo

2.1. Estabelecer as especificações mínimas dos componentes da solução e as diretrizes gerais para a execução de serviços referentes a Implantação de Sistema de CFTV (CIRCUITO FECHADO DE TV) e Controle de Acesso, nos edifícios Sede e Assis Brasil do Tribunal Regional Eleitoral do Rio Grande do Sul.

3. Especificações Mínimas dos Componentes da Solução

3.1. Condições Gerais

3.1.1. A solução deverá ser entregue completamente licenciada na modalidade perpétua, incluindo hardware, softwares e licenças de operação necessárias para a interconexão e integração de todas as suas partes.

3.1.1.1. Devem ser fornecidas, inclusive, as licenças de acesso de cliente (CAL) para todos os equipamentos, se aplicável.

3.1.2. Todas as funcionalidades exigidas no projeto básico e seus anexos deverão estar disponíveis e licenciadas, sem que seja necessário a aquisição de produtos ou licenciamentos adicionais.

3.2. Servidores da Solução

3.2.1. Servidor de Gerenciamento de Vídeo

3.2.1.1. Possuir dois processadores Xeon E5-2620v4 ou superior;

3.2.1.2. O servidor deve ocupar espaço máximo de 3U em rack de 19”

3.2.1.3. Possuir duas conexões SFP+ 10G com gbics homologadas para o sistema;

3.2.1.4. Memória RAM: 32 GB DDR4 ECC REG em dual channel;

3.2.1.5. Possuir dispositivo de armazenamento sólido, destinado ao armazenamento do sistema operacional e inicialização do servidor (boot), com:

3.2.1.5.1. No mínimo 240GB (duzentos e quarenta gigabytes) de armazenamento líquido;

3.2.1.5.2. Nível de proteção RAID 1 ou equivalente.
3.2.1.6. Possuir área de armazenamento em disco mecânico de 70TB líquidos com proteção RAID5 ou equivalente e capacidade hot-plug;
3.2.1.7. Principais características dos discos de armazenamento:
3.2.1.7.1. Possuir interface, de no mínimo, SATA de 6 Gb/s;
3.2.1.7.2. Possuir memória cache de 256 MB;
3.2.1.7.3. Ser desenvolvido para operar em 24/7;
3.2.1.7.4. Possuir MTBF de 1 milhão de horas;
3.2.1.8. Fonte de alimentação:
3.2.1.8.1. Duas fontes de alimentação redundantes hot-plug (1 + 1);
3.2.1.8.2. Cada fonte deve ter capacida para alimentar o servidor em sua capacidade máxima;
3.2.1.9. Deve ser entregue com sistema operacional compatível com a solução.
3.2.1.10. Deve ser entregue com trilhos deslizantes e cesta organizadora de cabos para instalação em rack padrão 19" com furação quadrada;
3.2.1.11. Possuir leds indicativos de equipamento ligado e de uso do disco rígido;
3.2.1.12. Deve possuir, no mínimo, 3 (três) portas USB 3.0 ou superior;
3.2.1.13. Controladora de 8 (oito) canais com suporte a RAID 0, 1, 5, 6,10, 50 e 60;
3.2.1.14. Deve possuir ao menos 1x PCI-E 3.0 x16, 2x PCI-E 3.0 x8;
3.2.1.15. Deverá ser fornecido com 2(Dois) cabos de energia padrão IEC C13/IEC C14, com pelo menos 2,5m(dois vírgula cinco metros) de comprimento e com amperagem compatível com o consumo do servidor;
3.2.1.16. Deve acompanhar kit de instalação.
3.2.1.17. Deve possuir estrutura de conexão óptica conforme dispõe o item 3.2.3.

3.2.1.18. Marca(s) de referência: Dell, HP e Lenovo

3.2.2. Servidor de Controle de Acesso

3.2.2.1. Possuir processador Xeon E-2124G ou superior;
3.2.2.2. Possuir duas conexões SFP+ 10G e Gibics homologadas para o sistema;
3.2.2.3. Possuir gabinete rack 1U com fonte single de 260W ou superior;
3.2.2.4. Possuir memória RAM de, no mínimo, 32 GB DDR4-2133 ECC ou superior;
3.2.2.5. Possuir dispositivo de armazenamento sólido, destinado ao armazenamento do sistema operacional e inicialização do servidor (boot), com:
3.2.2.5.1. Capacidade mínima de 240GB (duzentos e quarenta gigabytes) de armazenamento líquido;
3.2.2.5.2. Nível de proteção minimo RAID 1 ou equivalente.
3.2.2.6. Possuir área de armazenamento em disco mecânico de 1TB líquidos e proteção mínima de RAID 5;
3.2.2.7. Deve ser entregue com sistema operacional compatível com a solução.
3.2.2.8. Deve ser entregue com trilhos deslizantes e cesta organizadora de cabos para instalação em rack padrão 19" com furação quadrada;
3.2.2.9. Deverá ser fornecido com cabo de energia padrão IEC C13/IEC C14, com pelo menos 2,5m(dois vírgula cinco metros) de comprimento e com amperagem compatível com o consumo do servidor;
3.2.2.10. Deve acompanhar kit de instalação.
3.2.2.11. Deve possuir estrutura de conexão óptica conforme dispõe o item 3.2.3.

3.2.2.12. Marca(s) de referência: Dell, HP e Lenovo.

3.2.3. Interconexão lógica com a switch do Tribunal

3.2.3.1. Cada servidor deve possuir duas conexões lógicas (principal e redundante) por cordão óptico Om4 com o switch modelo HP 10500 existente no Datacenter.

3.2.3.2. Cada servidor deve possuir dois módulos Gbic SFP+ apropriados para a conexão do cordão óptico.

3.2.3.3. O cordão óptico multímodo OM4 LC-LC deverá:

3.2.3.3.1. Possuir dispositivo que impeça a inversão dos pares;

3.2.3.3.2. Possuir 10m de comprimento;

3.2.3.3.3. Atender às especificações da norma ISO/IEC 11801.

3.2.3.3.4. Atender às especificações da norma ANSI/TIA-568-C.3.

3.2.3.3.5. Atender às especificações da norma IEC 60793-2-10(A1_3b).

3.2.3.3.6. Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br, para os conectores e cordão.

3.2.3.3.7. Composto por fibras multimodo com núcleo de 50/125µm de diâmetro;

3.2.3.3.8. Ser do tipo COA-MM-DP-LSZH-20, tipo tight e duplex.

3.2.3.3.9. Revestimento externo em material retardante a chama e com baixa emissão de fumaça, LSZH.

3.2.3.3.10. As duas extremidades devem vir devidamente conectorizadas e testadas de fábrica.

3.2.3.3.11. Polimento UPC:

3.2.3.3.11.1. - PI: 0,1dB típico, 0,25dB máx. (IEC 61300-3-45);

3.2.3.3.11.2. - PR: 30dB mín. (IEC 61300-3-6).

3.2.3.3.12. Marcas de referência: Systimax, Panduit e Siemon.

3.3. Estrutura Lógica

3.3.1. Switches PoE 24P

3.3.1.1. **Características básicas**

3.3.1.1.1. Apropriado para ser instalado em rack padrão EIA (19”) e possuir kits completos para instalação.

3.3.1.1.2. Possuir altura máxima de 1 RU.

3.3.1.1.3. Possir, no mínimo, 24 (vinte e quatro) portas 10/100/1000 BaseT full-duplex ativas simultaneamente, autosense com conectores RJ-45 diretamente conectada ao chassi, sem conversores externos, com MDI/MDIX automático.

3.3.1.1.4. Possuir mínimo de 4 (quatro) Slots SFP (Small Form-factor Pluggable), não populadas, para uplink 1000 base X.

3.3.1.1.5. Possuir suporte as normas IEEE 802.3af e 802.3at em todas as portas.

3.3.1.1.6. Implementar os padrões Ethernet: IEEE 802.3 (Ethernet), 802.3u (FastEthernet) e 802.3z, 802.3ab (Gigabit Ethernet), 802.3ae, IEEE 802.3x (Flow Control), IEEE 802.1AB (LLDP) e LLDP-MED.

3.3.1.1.7. Todas as interfaces devem ser 100% Non-Blocking.

3.3.1.1.8. Possuir porta console RS-232 com conectores DB9 ou RJ-45 ou USB.

3.3.1.1.9. Possuir fonte de alimentação primária interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência

60hz.

3.3.1.1.10. Possuir potência adequada para os requisitos da solução.

3.3.1.1.11. Suportar alocação dinâmica de energia (Power Over Ethernet), onde possa disponibilizar apenas o consumo necessário do dispositivo conectado.

3.3.1.2. Capacidades

3.3.1.2.1. Possuir capacidade de encaminhamento de no mínimo 41 (quarenta e um) Mpps.

3.3.1.2.2. Possuir capacidade encaminhamento de tráfego de no mínimo 56 (cinquenta e seis) Gbps, ou seja, wirespeed.

3.3.1.2.3. Implementar tabela de endereçamento para, no mínimo, 16000 (dezesseis mil) endereços MAC.

3.3.1.2.4. Implementar no mínimo 256 (duzentos e cinquenta e seis) VLANs estáticas - IEEE 802.1Q.

3.3.1.2.5. Suportar rotas estáticas em IPv4.

3.3.1.2.6. Suportar rotas estáticas em IPv6.

3.3.1.2.7. Suportar no mínimo 8 rotas em IPv4 e 4 rotas em IPv6.

3.3.1.2.8. Implementar IEEE 802.3ad, com no mínimo 16 (dezesseis) LAGs com 08 (oito) portas por LAG, inclusive entre portas de switches distintos da pilha.

3.3.1.2.9. Implementar IGMP v1, v2, v3 e snooping.

3.3.1.2.10. Suportar no mínimo 256 endereços MAC estáticos.

3.3.1.2.11. Implementar spanning tree, RSTP e MSTP.

3.3.1.2.12. Implementar STP BPDU Protection (BPDU Guard).

3.3.1.2.13. Implementar DHCP Snooping, DHCP client e DHCP Relay.

3.3.1.2.14. Implementar mecanismo de configuração automática de VLANs - uma VLAN configurada em um switch poderá ser replicada automaticamente para outro switch na mesma LAN.

3.3.1.2.15. Implementar Jumbo Frame 9K.

3.3.1.2.16. Implementar MVRP segundo o padrão IEEE 802.1Q.

3.3.1.2.17. Implementar as seguintes RFCs relativas ao IPv6: 1886, 2292, 2373, 2374, 2460, 2462, 2461, 2463, 2466, 2452, 2454, 2464, 2553, 2893, 3493, 3513, 3056, 3542, 3587, 4007 e 4193.

3.3.1.3. **Empilhamento**

3.3.1.3.1. Permitir empilhar, no mínimo, 02 (duas) unidades.

3.3.1.3.2. Permitir o gerenciamento do switch e da pilha de switches através de endereço IP único.

3.3.1.3.3. Possuir 02 (duas) conexões para empilhamento (stack), com desempenho mínimo de 5 (cinco) Gbps por porta.

3.3.1.3.4. Suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha.

3.3.1.3.5. Fornecido com todos os componentes necessários para realizar seu empilhamento com outra unidade, incluindo cabo para redundância do empilhamento (por pilha de switches).

3.3.1.4. Qualidade de serviço

3.3.1.4.1. Implementar IEEE 802.1p.

3.3.1.4.2. Implementar Rate Limiting por porta.

3.3.1.4.3. Implementar classificação de tráfego: por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS.
3.3.1.4.4. Possuir a capacidade de associar um dispositivo autenticado por 802.1x a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço.
3.3.1.4.5. Implementar gerenciamento de banda de entrada (ingress) e saida (egress).
3.3.1.4.6. Possuir a capacidade de associar um dispositivo autenticado por endereço MAC a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço.
3.3.1.4.7. Implementar a remarcação do campo ToS/DSCP.
3.3.1.4.8. Possuir no mínimo 08 (oito) filas de prioridade por porta;
3.3.1.4.9. Possuir algoritmo de enfileiramento: Strict Priority (SP) e Weighted Round Robin (WRR).
3.3.1.4.10. Suportar Auto QoS para gerenciamento do switch e telefones IP.
3.3.1.4.11. Implementar QoS Tri color marker, tráfego simples e duplo, com análise de banda reservada, banda excedida e burst size.
3.3.1.4.12. Implementar controle fluxo para broadcast, multicast e fluxo desconhecido permitindo fixar o limite por porta.
3.3.1.4.13. Suportar End to End Head-Of-Line Blocking Protection (E2E-HOL).
3.3.1.4.14. Implementar as seguintes RFCs: 896, 1122, 2474, 2475, 2597, 3168, 3246, 3635, 2697 e 2698.

3.3.1.5. Segurança

3.3.1.5.1. Permitir o controle de acesso a rede baseado no endereço MAC.
3.3.1.5.2. Ser possível configurar explicitamente os endereços MACs que podem ser aprendidos em uma porta do switch.
3.3.1.5.3. Possibilitar informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos dinamicamente, devendo permitir a configuração do valor mínimo para 1 (um) endereço MAC.
3.3.1.5.4. Implementar envio de trap SNMP quando ocorrer uma violação de filtro de MAC das situações acima.
3.3.1.5.5. Implementar IEEE 802.1X Port-Based Network Access Control.
3.3.1.5.6. Suportar no mínimo 3 autenticações por porta.
3.3.1.5.7. Implementar autenticação de dispositivos através de endereço MAC, realizando a validação do endereço MAC em servidor Radius.
3.3.1.5.8. Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS.
3.3.1.5.9. Implementar no mínimo 1000 ACLs.
3.3.1.5.10. Implementar recurso para possibilitar que uma interface executando o protocolo Spanning Tree seja colocada no estado down quando a mesma receber um BPDU.
3.3.1.5.11. Implementar funcionalidade que bloqueie a operação de servidores DHCP inválidos (DHCP Spoof).
3.3.1.5.12. Implementar funcionalidade de Arp Spoof protection.
3.3.1.5.13. Implementar recurso de DHCP Server.
3.3.1.5.14. Oferecer detecção e proteção dinâmica para ataques ARP.
3.3.1.5.15. Oferecer STP Root Guard.

3.3.1.6. Gerenciamento

3.3.1.6.1. Implementar SSH V2.
3.3.1.6.2. Implementar SNMP v1, v2c e v3.
3.3.1.6.3. Implementar NTP ou SNTP.
3.3.1.6.4. Implementar Syslog Permitindo configurar no mínimo 04 (quatro) servidores de syslog distintos.
3.3.1.6.5. Implementar Radius e TACACS+.
3.3.1.6.6. Implementar Telnet.
3.3.1.6.7. Implementar TFTP ou FTP.
3.3.1.6.8. Implementar configuração via CLI e WEB.
3.3.1.6.9. Implementar Sflow ou Netflow v5 ou Netflow v9.
3.3.1.6.10. Implementar RMON, 04 (quatro) grupos, sem utilização de probe externa.
3.3.1.6.11. Implementar gerenciamento por HTTP ou HTTPS através de acesso direto ao equipamento por web browser padrão.
3.3.1.6.12. Suportar, no mínimo, 02 (duas) Imagens do sistema operacional e 2 (dois) arquivos de configuração.
3.3.1.6.13. Acompanhar kit de instalação.

3.3.1.7. Marcas de referência: Alcatel.

3.3.2. Patch Panel

3.3.2.1. Ser projetado para ambiente interno.
3.3.2.2. Atender as normas de CAT.6.
3.3.2.3. Apresentar largura de 19", conforme requisitos da norma EIA/ECA-310E.
3.3.2.4. Possuir porta etiquetas em acrilico para identificação das portas.
3.3.2.5. Possuir guia traseiro que permite a fixação individual dos cabos.
3.3.2.6. Possuir 24 posições RJ45 fêmea fixado a circuito impresso.
3.3.2.7. Incluir 24 conectores RJ45 fêmea.
3.3.2.8. Possuir estrutura em aço SAE 1020.
3.3.2.9. Possuir painel frontal em termoplástico de alto impacto e não propagante a chama.
3.3.2.10. Suportar diâmetros do condutor de 26 a 22 AWG.
3.3.2.11. Acompanhar kit de instalação.

3.3.3. Cabeamento UTP

3.3.3.1. Cabo UTP CAT6

3.3.3.1.1. Atender as especificações da norma ABNT NBR 14565.
3.3.3.1.2. Atender as especificações da norma ABNT NBR 14703.
3.3.3.1.3. Atender as especificações da norma ABNT NBR 14705.
3.3.3.1.4. Atender as especificações da norma ISSO/IEC 11801.
3.3.3.1.5. Atender as especificações da norma ANSI/TIA-568-C.2.
3.3.3.1.6. Atender as especificações da norma IEC 60332-3, IEC 61156-5.
3.3.3.1.7. Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br.
3.3.3.1.8. Possuir classe de flamabilidade CM. Esta informação deverá estar impressa na capa do cabo.
3.3.3.1.9. Ser composto por condutores de cobre nú, possuir 23 AWG de

diâmetro nominal isolados em polietileno termoplástico de alta densidade.

3.3.3.1.10. Deve possuir um elemento central (crossfiler) garantindo a geometria e performance do cabo. O cross filler mantém a equidistância dos pares e reduz a perda de performance nas curvaturas.

3.3.3.1.11. Atender ao padrão de cores Azul/Branco, Laranja/Branco, Verde/Branco, Marrom/Branco, quanto à isolação dos pares.

3.3.3.1.12. Possuir gravação sequencial métrica decrescente na capa do cabo (XXXX a 0m).

3.3.3.1.13. Atender à Diretiva RoHS 3 (UE) 2015/863.

3.3.3.2. Marcas de referência: Nexans e Furukawa.

3.3.3.3. Cabo UTP CAT5 para elevador

3.3.3.3.1. Ser do tipo flexível para conexão de câmeras do sistema instaladas nos elevadores.

3.3.3.3.2. Ser do tipo UTP e categoria 5e ou superior.

3.3.3.3.3. Possuir capa externa em material termoplástico.

3.3.3.3.4. Possuir blindagem para interferências eletromagnéticas.

3.3.3.3.5. Possuir capa externa retardante a chama.

3.3.3.3.6. Possuir padrão de transmissão ANSI/TIA-568C.2.

3.3.3.3.7. Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br.

3.3.3.3.8. Possuir gravação sequencial métrica decrescente na capa do cabo (XXXX a 0m).

3.3.3.3.9. Marca de referência: Furukawa.

3.3.4. Conector RJ45

3.3.4.1. RJ45 CAT6 Macho – conectorização para cabos CAT6

3.3.4.1.1. Atender às especificações da norma ABNT NBR 14565.

3.3.4.1.2. Atender às especificações da norma ANSI/TIA-568-C.2.

3.3.4.1.3. Produzido em material termoplástico de alto impacto não propagante à chama (UL 94 V-0).

3.3.4.1.4. Cor transparente.

3.3.4.1.5. Adequado para cabos de fios sólidos ou flexível.

3.3.4.1.6. Suportar condutores com diâmetro de 22 a 26 AWG.

3.3.4.1.7. Suportar temperatura de operação de -10ºC a +60ºC.

3.3.4.1.8. Atender à diretiva RoHS Compliant.

3.3.4.1.9. Marcas de referência: Nexans e Furukawa.

3.4. Câmeras

3.4.1. Câmera fisheye

3.4.1.1. Possuir formato tipo Dome Fixa com sensor de imagem em estado sólido de 1/3” ou maior.

3.4.1.2. Possuir lente fixa, entre 1.0 a 2.0 mm, que proporcione visualização de imagem em 180°, com correção de IR, filtro de corte de infravermelho removível automaticamente.

3.4.1.3. Deve fornecer fluxo de vídeo no formato 360° (visão geral), 180° (panorama) e formato quatro visualizações simultâneas (quad view).
3.4.1.4. Possuir funcionalidade de PTZ digital com posições pré-definidas e ronda eletrônica.
3.4.1.5. Ser capaz de fornecer fluxos H.264.
3.4.1.6. Permitir a transmissão em resolução 1792 x 1792 pixels, com taxa de quadros de pelo menos 15 fps.
3.4.1.7. Possuir tecnologia de protocolo de compactação inteligente em H.264 (H.264+, H.264 Plus, ou similar).
3.4.1.8. Possibilitar compensação automática para tomada de imagem contra luz de fundo.
3.4.1.9. Possuir Wide Dynamic Range.
3.4.1.10. Possuir tempo do obturador entre 1/10000s a 1/2s.
3.4.1.11. Possuir capacidade de armazenamento local através de SD/MicroSD card, compact Flash ou USB memory card.
3.4.1.12. Possuir dispositivo de armazenamento local com capacidade de no mínimo 64Gb.
3.4.1.13. Possuir sensibilidade mínima igual ou inferior a no modo colorido a 0,4 lux e no modo PB a 0,15 lux.
3.4.1.14. Ser fornecida com capacidade embarcada para rotacionar digitalmente a imagem no sensor em 180°;
3.4.1.15. Ser equipada com funcionalidade integrada de eventos, que podem ser desencadeados por: detecção de movimento, evento agendado, violação da câmera, aplicações incorporadas de terceiros, acionamento manual.
3.4.1.16. Responder a estes eventos através de: Notificações usando TCP, HTTP, HTTPS ou email; Envio de imagens por FTP, HTTP, HTTPS, compartilhamento de rede ou email; Envio de vídeo clipe por FTP, HTTP, HTTPS, compartilhamento de rede ou email; Envio de mensagem de trap SNMP; Gravação para armazenamento anexado à rede; clipe de audio; gravação para armazenamento local; controle da funcionalidade PTZ.
3.4.1.17. Possuir largura de banda configurável em H.264.
3.4.1.18. Fornecer níveis de compressão configuráveis.
3.4.1.19. Possuir arquitetura aberta para integração com outros sistemas.
3.4.1.20. Possuir porta para conexão em rede TCP/IP com conector RJ-45 100BASE-T.
3.4.1.21. Ser fornecida com caixa com grau de proteção IP66, grau de resistência a impacto IK10.
3.4.1.22. A caixa de proteção e seus acessórios devem ser do mesmo fabricante da câmera ou homologados pela mesma garantindo a qualidade da solução.
3.4.1.23. Possuir suporte para fixação do mesmo fabricante da caixa de proteção.
3.4.1.24. Possuir os protocolos: RTP, RTSP, UDP, TCP, IPv4, IPv6, DHCP, HTTP, IGMP, SNMP, SMTP.
3.4.1.25. Possuir os protocolos de segurança HTTPS e SSL/TLS.
3.4.1.26. Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais.
3.4.1.27. Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no web site do mesmo.
3.4.1.28. Possuir dispositivo para restauração aos padrões de fábrica.
3.4.1.29. Incluir kit de instalação.

3.4.1.30. Marcas de referência: Axis M3057-PLVE, Panasonic WV-X4571L e Bosch FLEXIDOME IP panoramic 5000 MP.

3.4.2. Câmera Dome

3.4.2.1. Possuir sensor de imagem em estado sólido de 1/3" ou maior.
3.4.2.2. Possuir lente entre 2.0 e 3.0 mm e proporcionar ângulo de visualização apropriado.
3.4.2.3. Permitir a transmissão em resolução 1920x1080 pixels à 30 quadros por segundo com compressão de vídeo em H.264 e Motion JPEG (MJPEG).
3.4.2.4. Possuir sensibilidade mínima igual ou inferior com o iluminador infravermelho desligado: modo colorido a 0,25 lux e no modo P&B a 0,06 lux.
3.4.2.5. Possuir Wide Dynamic Range (WDR).
3.4.2.6. Possuir tempo do obturador entre 1/12.000s a 1/12s.
3.4.2.7. Possuir formato tipo Domo Fixa e permitir os seguintes ajustes manuais de ângulo de instalação: panorâmico, vertical e rotação.
3.4.2.8. Possuir capacidade de armazenamento local através de SD/MicroSD card, compact Flash ou USB memory card.
3.4.2.9. Possuir dispositivo de armazenamento local com capacidade de no mínimo 64Gb.
3.4.2.10. Ser equipada com funcionalidade integrada de eventos, que podem ser desencadeados por: detecção de movimento, evento agendado, violação da câmera, acionamento manual.
3.4.2.11. Responder a estes eventos através de: Notificações usando TCP, HTTP, HTTPS ou email; Envio de imagens por FTP, HTTP, HTTPS, compartilhamento de rede ou email.
3.4.2.12. Possuir largura de banda configurável em H.264 e fornecer níveis de compressão configuráveis.
3.4.2.13. Possuir capacidade de análise de vídeo embarcado através da simples adição de licença e software.
3.4.2.14. Possuir arquitetura aberta para integração com outros sistemas.
3.4.2.15. Possuir porta para conexão em rede TCP/IP com conector RJ-45 100BASE-TX.
3.4.2.16. Possuir os protocolos: RTP, RTSP, UDP, TCP, IPv4, IPv6, DHCP, HTTP, IGMP, SNMP, SMTP.
3.4.2.17. Suportar qualidade de serviço (QoS) para ser capaz de priorizar o tráfego.
3.4.2.18. Possuir os protocolos de segurança HTTPS e SSL/TLS.
3.4.2.19. Permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no web site do mesmo.
3.4.2.20. Possuir capacidade embarcada para a configuração de máscaras de privacidade na própria câmera.
3.4.2.21. A caixa de proteção e seus acessórios devem ser do mesmo fabricante da câmera ou homologados pela mesma.
3.4.2.22. Permitir alimentação PoE conforme padrão IEEE 802.3af sem uso de equipamentos adicionais.
3.4.2.23. Incluir kit de instalação.

3.4.2.24. Marcas de referência: Axis M3105-L, Panasonic WV-V2530L1 e Bosch NII-50022-A3.

3.4.3. Cartão de Memória para câmeras

3.4.3.1. Cartão SD/MicroSD card, compact Flash ou USB memory card, com capacidade de no mínimo 64Gb compatível com as câmeras.

3.4.4. Suportes de Câmera fisheye

3.4.4.1. Suporte de parede

3.4.4.1.1. Possuir prolongamento de 1,5 metros de comprimento, frabricado em aço tubular galvanizado a fogo.

3.4.4.1.2. Possibilitar fixação de canto em parede.

3.4.4.1.3. Possuir pintura eletrostática.

3.4.4.1.4. Acompanhar kit de fixação em parede.

3.4.4.2. Suporte de poste

3.4.4.2.1. Possuir corpo em metal tubular para passagem interna do cabeamento.

3.4.4.2.2. Possuir pintura eletrostática.

3.4.4.2.3. Acompanhar kit de fixação.

3.5. Conjunto de Controladoras

3.5.1. Características básicas

3.5.1.1. Cada controladora de catraca deve armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deve também suportar até 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

3.5.1.2. O armazenamento das transações em seu buffer deve ser transferido para o Servidor sempre que o software do Sistema estiver em operação com a rede disponível (on-line) – tecnologia de “pushing”.

3.5.1.3. Cada controladora deve ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

3.5.1.4. Cada controladora deve possuir servidor web interno “web server”, protegido por usuário e senha, onde se pode verificar informações relativas ao funcionamento da mesma, bem como atualizar versões de seu software embutido.

3.5.1.5. Cada controladora deve manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

3.5.1.6. As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente.

3.5.1.7. A controladora deve possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo (esta fonte deve ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deve ser de no

mínimo 12VCC, 7Ah. A bateria de backup deve prover 12VCC a 1A (max) para até duas fechaduras. A fonte de alimentação deve prover carga suficiente para baterias de backup de até 12,7Ah.

3.5.1.8. A Controladora deve ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

3.5.1.9. As controladoras a serem instaladas no *shaft* de cada andar no edifício Assis Brasil deverão ser apropriadas para fecho do tipo eletromecânico.

3.5.1.10. Deve acompanhar a placa o carregador flutuante de bateria, buzzer, eletroímã para portas de vidro e corta-fogo e trava eletromecânica para as portas dos shaft no Edifício Assis Brasil, acionador de emergência rearmável, placa de instrução de Saída de Emergência, leitor de cartões, botão de abertura para saída, bem como kit de instalção (eletroduto ou eletrocalha, buchas e parafusos para fixação); versões de controladoras de acesso com alimentação via PoE (Power over Ethernet).

3.5.1.11. Todos as controladoras de acesso fornecidas deverão ser padronizadas ("standard"), ou seja, sua construção e aplicabilidades deverão ser originais de fábrica, e não customizadas para este edital.

3.5.2. Detecção de Energia

3.5.2.1. As controladoras de campo deverão possuir circuito e função de detecção de falha no fornecimento de energia, bem como estado de bateria com baixa carga e corte de bateria (hardware e software deverão monitorar corrente contínua e alternada). Caso haja um o período de corte de energia, cada controladora afetada deve enviar um sinal para a Central de Gerenciamento e Monitoramento de Acesso e Segurança, para avisar sobre a falha. O mesmo deve ocorrer quando as baterias de backup tiverem atingido um nível baixo de carga. Quando na ocorrência de falha no fornecimento de energia e no caso das baterias de backup estiverem com carga baixa e tensão abaixo de 10,5 VCC, as controladoras afetadas deverão liberar suas respectivas portas e reportar seu status à Central de Gerenciamento e Monitoramento de Acesso e Segurança. Esta liberação não se aplica para a controladora do Datacenter e salas de lógicas de TI.

3.5.2.2. Todos os eventos de detecção de falha de fornecimento de energia deverão ser registrados no Sistema e deverão incluir data, hora, unidade que falhou e seu status.

3.5.3. Atualização de Firmware

3.5.3.1. A controladora deve possuir servidor web interno ("web server") com interface gráfica amigável e protegido com login de usuário e senha, para atualização do firmware via rede Ethernet, facilitando a manutenção e atualização do sistema de controle de acesso.

3.5.4. RTC

3.5.4.1. A controladora deve possuir RTC (Real Time Clock) em seu hardware padrão, garantindo que mesmo em caso de queda de energia ou falha de bateria, a controladora não perca referência de data e horário.

3.5.5. Controladora para Catraca

3.5.5.1. Possuir três entradas para leitoras (uma leitora de entrada, uma de saída e uma da urna coletora), duas entradas para botão de requisição de saída, uma entrada

para tamper, duas entradas para confirmação de giro e duas saídas de relé comandadas (para liberação do giro de entrada ou de saída).

3.5.5.2. As controladoras deverão ser montadas dentro das catracas, de tamanho suficiente para permitir uma fácil montagem e cablagem de todos os dispositivos das mesmas, bem como espaço para a bateria de backup.

3.5.5.3. Alimentação 14,5 VDC.

3.5.5.4. A controladora deve ser instalada dentro da estrutura da respectiva catraca.

3.5.5.5. Ser compatível com os demais itens do sistema.

3.5.5.6. Marcas de referência: Acess-e, Lenel e Bosch.

3.5.6. Controladora para Porta

3.5.6.1. Possuir duas entradas para leitoras (uma leitora de entrada e uma de saída), uma entrada para botão de requisição de saída, uma entrada para tamper, uma entrada para sensor de status de porta/fechadura, um entradas para integração com sistema de incêndio ou emergência e uma saída de relé comandadas (para uma fechadura);

3.5.6.2. Alimentação 14,5 VDC.

3.5.6.3. Deve acompanhar gabinete para a instalação da controladora e bateria de backup.

3.5.6.4. Deve possuir ou acompanhar buzzer.

3.5.6.5. A controladora deve possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo. A fonte deve prover carga suficiente para baterias de backup de até 12,7Ah.

3.5.6.6. Marcas de referência: Acess-e e Bosch.

3.5.7. Fechadura – mecanismo de travamento

3.5.7.1. As fechaduras a serem fornecidas são do tipo eletroímã ou eletromecânica próprias para instalação em portas de vidro, metálicas ou madeira, sendo que a mesma deve conseguir aliar características de fácil instalação, moderno design e construção robusta. Estas fechaduras deverão funcionar alimentadas em 12V, sendo que estando energizadas mantém as portas travadas, destravando-se por ocasião da desenergização garantindo a sua liberação em casos de incêndio ou pânico.

3.5.7.2. As fechaduras quando energizadas devem possuir força de atração de 272 kgf para portas em madeira ou corta-fogo com consumo de até 300mA e 136kgf para portas de vidro com consumo de até 500 mA.

3.5.7.2.1. Todas as fechaduras deverão ser fornecidas com os devidos suportes para aplicação nas portas do projeto.

3.5.7.2.2. Na sala do datacenter deverá ser utilizada a fechadura existente e devem ser integrados (aproveitados) os mecanismos de autenticação já instalados (biometria e senha).

3.5.7.2.3. As portas de madeira das salas de lógica da TI utilizar fechadura eletromecânica.

3.5.8. Leitor de Proximidade

3.5.8.1. Padrão – proximidade mifare 13,56 MHz.

3.5.8.2. Comunicação: wiegand 34 bits.

3.5.8.3. Alcance: mínimo de 5 cm.

3.5.8.4. O leitor deverá ser apropriado para montagem sobreposta, com alta resistência mecânica, e ter no frontal indicação através de LED com vermelho indicando "acesso negado" e verde indicando "acesso permitido".

3.5.8.5. Marcas de referência: Acess-e e Acura.

3.5.9. Bateria

3.5.9.1. Ser selada de no mínimo 12VCC, 7Ah. A bateria de backup deve possuir capacidade para prover 12VCC a 1A (max) para até duas fechaduras.

3.5.10. Gabinete

3.5.10.1. Ser de sobrepor.
3.5.10.2. Possuir construção em metal com pintura.
3.5.10.3. Possuir fechadura e chave.
3.5.10.4. Possuir contra-chapa para a controladora.
3.5.10.5. Suportar em seu interior, controladora, bateria selada, fonte de alimentação e buzzer.
3.5.10.6. Acompanhar kit de fixação do gabinete e componentes a serem nela instalados.

3.6. Antena RFID

3.6.1. Possuir grau de proteção IP66.
3.6.2. Possuir alcânce de até 5 metros.
3.6.3. Possuir fonte de alimentação.
3.6.4. Possuir transformador.
3.6.5. Possuir saídas de comunicação: wiegand (26/34 bits), Abatrack (10/14 dig), RS 232 e Ethernet TCP/IP.
3.6.6. Possuir entrada de contato seco para trigger.
3.6.7. Possuir potência de saída RF.
3.6.8. Possuir relógio interno com sincronização via SNTP.
3.6.9. Possuir configuração através de HTML.
3.6.10. Acompanhar kit de fixação (suporte e parafusos).

3.6.11. Marcas de referência: Acura e Solid Invent.

3.7. **Urna coletora de cartão**

3.7.1. Possuir corpo em aço inox.
3.7.2. Possuir abertura para depósito manual de cartões com o protetor/porta crachá.
3.7.3. Possuir dispositivo antipesca.
3.7.4. Deverá ser fornecida com fonte de alimentação, sensores, solenóides, cabo do leitor e demais acessórios, para garantir seu perfeito funcionamento.
3.7.5. Cada urna coletora deverá acompanhar leitor de proximidade, bem como suporte de fixação em parede.
3.7.6. Ser apropriada para os cartões do sistema.
3.7.7. Permitir a deposição de cartão do sistema com protetor e alça plástica com prendedor tipo jacaré.
3.7.8. Incluir totem quando necessário.
3.7.9. Incluir leitor de cartões compatível com a solução.
3.7.10. Acompanhar kit de instalação.

3.7.10.1. Marcas de referência: Volpac, Magnetic e Digicom.

3.8. **Sensor de Movimento**

3.8.1. Ser de material plástico e na cor branca.
3.8.2. Ser alimentado por 12 VCC (alimentação fornecida pela E/S da câmera).
3.8.3. Ter conectores 4P 2.5 STR.
3.8.4. Ter um período de aquecimento inferior a 40s.
3.8.5. Ter condições de operação -20°C a 50°C.
3.8.6. Ter montagem em parede.
3.8.7. Ter altura de montagem variando de 1,5 a 2,4m.
3.8.8. Ter método de detecção por Infravermelho passivo.
3.8.9. Operar a uma distância máxima de 12 x 12 m.
3.8.10. Ter ângulo de abertura de 85°.
3.8.11. Ter ajuste de sensibilidade selecionável.
3.8.12. Ter LED indicador de alarme ligado/desligado.
3.8.13. Ter chave de violação NC (Normalmente fechado).
3.8.14. Ter saída para alarme NC (Normalmente fechado).
3.8.15. Ter conformidade RoHS (Diretiva EU 2011/65/EU) WEEE (2012/19/EU) EMC (2004/108/EC) LVD (2006/95/EC).

3.8.16. Marcas de referência: Paradox, Axis e DSC.

3.9. Estações de trabalho

3.9.1. Estação de Monitoramento tipo 1

3.9.1.1. Possuir processador intel CORE I7-8700K, com 06 (seis) núcleos, com 12 (doze) threads e frequência 3,7 GHz.
3.9.1.2. Possuir placa mãe com chipset h310 ou B360M, 4 (quatro) slots de memória e conector pci express x16 3.0.
3.9.1.3. Placa de vídeo off board.
3.9.1.3.1. Possuir memória tipo GDDR5x de 8Gb.
3.9.1.3.2. Possuir Interface de memória 256-bit.
3.9.1.3.3. Possuir no mínimo três saídas HDMI com resolução FullHD cada.
3.9.1.4. Possuir memória DDR4 de 16GB.
3.9.1.5. Possuir HD/SSHD híbrido de 1 Tb, 7200 rpm.
3.9.1.6. Possuir gabinete com suporte de (modelo/referência Carbide 300r):
3.9.1.6.1. Placas de vídeo de até 450mm.
3.9.1.6.2. Fonte de até 240mm.
3.9.1.6.3. Placa mãe ATX.
3.9.1.7. Possuir fonte com (modelo referência CORSAIR TXM Séries TX750M 80 Plus Gold):
3.9.1.7.1. Potência de 650 a 750W reais.
3.9.1.7.2. Selo de qualidade 80 plus.
3.9.1.8. Mínimo 4 (quatro) portas USB (destas, no mínimo, duas 3.0).
3.9.1.9. Possuir mouse interface USB.
3.9.1.10. Possuir Teclado interface USB, com todos os caracteres da língua portuguesa, inclinação ajustável, regulação de altura e inclinação do teclado.
3.9.1.11. As estações devem possuir sistema operacional apropriado para a solução, instalado com licença e direito a atualizações.
3.9.1.12. O equipamento deverá ser entregue com Manual do Usuário contendo todas

as informações do produto, com instruções para instalação, configuração e operação em português, bem como, deverá ser entregue todos os cabos, conectores e acessórios necessários para o funcionamento do computador.

3.9.1.13. Marcas de referência: Dell, HP e Lenovo.

3.9.2. Estação de Monitoramento tipo 2

3.9.2.1. Processador i7-7700 3,6Ghz.
3.9.2.2. Placa de vídeo off board:
3.9.2.2.1. Possuir memória de 1 GB, GDDR5, 128-bit;
3.9.2.2.2. Possuir no mínimo uma saída com resolução FullHD.
3.9.2.3. Possuir memória RAM 8GB DDR4 2133 Dual Channel.
3.9.2.4. Possuir HD 1TB.
3.9.2.5. Incluir conjunto teclado e mouse.
3.9.2.6. Incluir fonte de alimentação bivolt.
3.9.2.7. Incluir sistema operacional apropriado para a solução.
3.9.2.8. Deverá ser entregue todos os cabos, conectores e acessórios necessários para o funcionamento do computador.

3.9.2.9. Marcas de referência: Dell, HP e Lenovo.

3.9.3. Monitor 42”

3.9.3.1. Monitor profissional LFD (Large Format Display).
3.9.3.2. Possuir resolução de imagem mínima de 1920 x 1080p a 60 Hz.
3.9.3.3. Possuir brilho de 350 cd/m².
3.9.3.4. Possuir proporção de contraste (típica) de 1300:1.
3.9.3.5. Possuir proporção da imagem de 16:9.
3.9.3.6. Possuir tempo de resposta (típico) mínimo de 12 ms.
3.9.3.7. Possuir tratamento da superfície antiofuscante.
3.9.3.8. Possuir ângulo de visão mínima de 178°/178° (horizontal/vertical).
3.9.3.9. Possuir conexões de saída: HDMI e USB.
3.9.3.10. Ser projetado para operação em 24/7.
3.9.3.11. Possuir alimentação bi volt (110/220V).
3.9.3.12. Acompanhar cabo de força.
3.9.3.13. Acompanhar cabo HDMI de dez metros de comprimento.
3.9.3.14. Acompanhar suporte biarticulado que permite, no mínimo, inclinação de 15º e rotação de 90º.

3.9.3.15. Marcas de referência: LG e Samsung.

3.9.4. Monitor 21”

3.9.4.1. Possuir tela LED Full HD (1920 x 1080).
3.9.4.2. Possuir saída HDMI e VGA.
3.9.4.3. Ser bivolt (110V e 220V).
3.9.4.4. Acompanhar cabo de força.
3.9.4.5. Acompanhar cabo HDMI de cinco metros.

3.9.4.6. Marcas de referência: LG, Philips e AOC.

3.9.5. Estação de cadastramento

3.9.5.1. Processador i7-7700 3,6Ghz.
3.9.5.2. Memória RAM 8GB DDR4 2133 Dual Channel.
3.9.5.3. HD 1TB.
3.9.5.4. Deve ser fornecido com um conjunto teclado e mouse.
3.9.5.5. Deverá acompanhar monitor 21" FullHD.
3.9.5.6. Acompanhar cabos de conexão.
3.9.5.7. Possuir sistema operacional compatível para a solução.
3.9.5.8. Ser compatível com os demais requisitos da solução.
3.9.5.9. Deverá ser entregue todos os cabos, conectores e acessórios necessários para o funcionamento do computador.

3.9.5.10. Marcas de referência: Dell, HP e Lenovo.

3.9.6. Webcam

3.9.6.1. Possuir resolução mínima de 720p, conexão USB 2.0 ou superior e suporte para fixação em mesa/balcão com altura compatível para cadastro de pessoas.

3.9.7. **Leitor de proximidade USB.**

3.9.7.1. Padrão – USB 2.0.
3.9.7.2. Comunicação: wiegand 34 bits.
3.9.7.3. Alcance: mínimo de 5 cm.
3.9.7.4. Compatível com o sistema a ser instalado.

3.9.7.5. Marcas de referência: Acura e Acess-e.

3.10. Impressora de cartões

3.10.1. Possibilitar impressão por sublimação direta no cartão/Termotransferência em resina.
3.10.2. Possibilitar impressão de margem a margem, de frente e verso.
3.10.3. Possuir resolução personalizável 300 x 600 ppp e resolução 300 x 1200 ppp.
3.10.4. Possuir 32 MB de memória RAM.
3.10.5. Possuir desempenho mínimo de impressão:
3.10.5.1. Colorida (YMCKO): 150 cartões/hora;
3.10.5.2. Monocromática: 600 cartões/hora.
3.10.6. Possuir desempenho mínimo de impressão de frente e verso Colorida (YMCKO-K): 120 cartões/hora.
3.10.7. Possibilitar a impressão em cartões de PVC, cartões de PVC composto, cartões de PET, cartões de ABS, cartões envernizados especiais e nos formatos: ISO CR80 - ISO 7810 (86 x 54 x 0,9 mm).
3.10.8. Possuir interfaces USB 1.0 (compatível com 1.1, 2.0 e 3.0), cabo incluído, ethernet TCP-IP 10BaseT, 100BaseT;
3.10.9. Apresentar notificações gráficas da impressora, alertas de limpeza, alertas de fita vazia/nível baixo e alertas de cartões.
3.10.10. Incluir todos os acessórios necessários como mídias de instalação e cabos.
3.10.11. Incluir kit de limpeza com 10 cartões de limpeza compatíveis de limpeza compatíveis com o modelo da impressora.
3.10.12. Incluir software de edição de leiaute e impressão de cartões compatível com o modelo da impressora.
3.10.13. Incluir três conjuntos de suprimento (ribbons) YMCKO com capacidade para 250 impressões compatível com o modelo da impressora.

3.10.14. Marcas de referência: Evolis Primacy.

3.11. Credencial de liberação de acesso

3.11.1. Cartão

3.11.1.1. Possuir construção em PVC.
3.11.1.2. Possuir as tecnologias UHF e HF (passivo).
3.11.1.3. Ser do tipo ISO.
3.11.1.4. Possuir frequência de operação de 860 - 960 MHz e 13,56 MHz.
3.11.1.5. Permitir impressão nas duas faces.
3.11.1.6. Possuir encapsulamento em PVC branco brilhante.
3.11.1.7. Possuir dimensões aproximadas de 86 x 54 x 0,9 mm.
3.11.1.8. Possuir grau de proteção IP67.
3.11.1.9. Ser compatível com as demais equipamentos do sistema.

3.11.1.10. Marca de referência: Acura.

3.11.2. Mecanismo de porte

3.11.2.1. 800 (oitocentos) cordões personalizados no padrão do TRE-RS, sendo:
3.11.2.1.1. 600 (seiscentos) cordões na cor azul com impressão da sigla "TRE-RS" na cor branca;
3.11.2.1.2. 200 (duzentos) cordões na cor verde com impressão da sigla "TRE-RS" na cor branca.
3.11.2.2. 1000 (mil) protetores/porta crachá em plástico rígido transparente com configuração para uso somente na posição vertical e abertura para prendedor tipo jacaré.
3.11.2.3. 800 (oitocentos) dispositivos de cordão extensor retrátil personalizados (roller clip), sendo:
3.11.2.3.1. 700 (setecentos) unidades na cor azul, com etiqueta resinada epoxi personalizada com fundo branco e os dizeres "TRE-RS" na cor azul;
3.11.2.3.2. 200 (duzentas) unidades na cor verde, com etiqueta resinada epoxi personalizada com fundo branco e os dizeres "TRE-RS" na cor verde.
3.11.2.4. 200 (duzentas) presilhas para crachá com alça plástica transparente de fácil remoção (fechamento por pressão) com prendedor tipo jacaré em uma extremidade.

3.12. Catracas

3.12.1. Pivotante

3.12.1.1. Catraca pedestal de 3 braços (equidistantes), bidirecional, com braço que cai.
3.12.1.2. Deverá possuir corpo em aço inox escovado.
3.12.1.3. Deverá acompanhar urna coletora embutida, com dispositivo anti pesca, apropriada para os cartões do sistema (permitir a deposição de cartão do sistema com protetor e alça plástica com prendedor tipo jacaré).
3.12.1.4. Deverá possuir pictograma superior;
3.12.1.5. Possuir dimensões compatíveis com o local de instalação.
3.12.1.6. Deverá possuir MTBF (tempo médio entre falhas): mínimo 60.000 horas.
3.12.1.7. Deverá possuir MCB (número de ciclos entre falhas): mínimo 1.000.000 de ciclos.

3.12.1.8. Deverá ser fornecida completa com fonte de alimentação, sensores, solenoides, bem como qualquer acessório para garantir o funcionamento da catraca.

3.12.1.9. Marcas de referência: Digicom, Wolpac, Dorma e Kaba.

3.12.2. PNE

3.12.2.1. Deverá possuir 1 braço em aço inox polido montado em ângulo de passagem com abertura de 90º e 84,5cm.

3.12.2.2. Deverá possuir mecanismo silencioso e suave.

3.12.2.3. Deverá possuir pedestal em aço carbono SAE1020 com pintura em epóxi pó eletrostática texturizada de alta resistência, revestido em aço carbono SAE1020 ou aço inox AISI304.

3.12.2.4. Deverá possuir cabeça em aço inox AISI304 ou aço carbono SAE 1020 com pintura em epóxi pó eletrostática texturizada de alta resistência, com design moderno e linhas arredondadas e acabamento com chapa de aço inox, com dobradiça e chave.

3.12.2.5. Possuir instalação de 2 leitores de proximidade nas laterais externamente ou 1 leitor frontal interno sob a tampa;

3.12.2.6. Possuir urna coletora de cartões integrada apropriada para os cartões do sistema (permitir a deposição de cartão do sistema com protetor e alça plástica com prendedor tipo jacaré).

3.12.2.7. Permitir incorporar display de cristal líquido;

3.12.2.8. Possuir pictograma superior, com matriz de 39 leds de consumo reduzido, que evita aquecimento, aplicado para a indicação de entrada e saída autorizada e acesso negado, indicação de local para devolução do crachá do visitante.

3.12.2.9. Possuir no mínimo 1 sensor ótico utilizado para a identificação de rotação dos braços e mais 1 com as mesmas características quando o equipamento tiver urna coletora.

3.12.2.10. Permitir que o giro da catraca seja controlado por 1 solenóide.

3.12.2.11. Possuir dimensões compatíveis com o local de instalação.

3.12.2.12. Marcas de referência: Digicom, Wolpac, Dorma e Kaba.

3.13. Eletrocalhas, eletrodutos, canaletas e miscelâneas

3.13.1. Eletrocalha perfilada

3.13.1.1. As eletrocalhas deverão ser do tipo leve perfurada tipo “U”, 50x50x300m em chapa CH 24 incluindo todos os acessórios (tampas, emendas, junções, suportes, buchas, parafusos, etc...) necessários a instalação, atendendo as normas ABNT-NBR 7008 e NBR 7013.

3.13.2. Eletroduto metálico

3.13.2.1. Ser construídos em aço galvanizado a fogo, atendendo a NBR-5624, do tipo classe leve, com espessura de parede mínima de 0,65mm, nos diâmetros de 3/4” ou 1”, acompanhados e fixados com abraçadeiras tipo cunha com chaveta próprias para eletrodutos, com diâmetro compatível com o eletroduto.

3.13.2.2. Acompanhar os acessórios de fixação como buchas, arruelas, abraçadeiras, etc.

3.13.3. Canaleta em alumínio

3.13.3.1. Perfil discreto em alumínio extrudado, com encaixe rápido, dimensões máximas de 14mmx53mm.
3.13.3.2. Apropriada para a instalação dos conjuntos de controladora de portas.
3.13.3.3. Deve acompanhar acessório de fixação.

3.13.4. Conjunto de Miscelâneas para Infraestrutura

3.13.4.1. Conjunto de materiais necessários para as adaptações da infraestrutura. Caixas de passagem, derivação, porta equipamentos, curvas, luvas, tampões, adaptadores, acessórios de fixação e conexões de uso geral.

4. Licenças de Softwares

4.1. Software de Gerenciamento de Vídeo

4.1.1. Licença de Software de Gerenciamento de Vídeo por unidade de Servidor Instalado.
4.1.2. Solução de software a nível profissional altamente escalável.
4.1.3. Funcionalidades do Software:
4.1.3.1. O Software deverá oferecer uma completa solução de vigilância de vídeo, escalável de uma até milhares de câmeras e que poderão ser adicionadas individualmente.
4.1.3.2. O VMS deverá gerenciar ilimitadas câmeras, servidores e clientes remotos. Este limite de capacidade deve ser dado pelo hardware e não pelo software.
4.1.3.3. O software deverá possibilitar o resgate de imagens através de *streams* de vídeo previamente configurados.
4.1.3.4. O Software deverá incluir os seguintes aplicativos / funções:
4.1.3.4.1. Núcleo do sistema;
4.1.3.4.2. Arquivo;
4.1.3.4.3. Vídeo Gateway;
4.1.3.4.4. Watchdog;
4.1.3.4.5. Ferramentas de configuração;
4.1.3.4.6. Visualização ao vivo;
4.1.3.4.7. Player de vídeos gravados;
4.1.3.4.8. Editor de macros;
4.1.3.4.9. Visualizador de relatórios;
4.1.3.4.10. Aplicações de software cliente:
4.1.3.4.10.1. Visualização ao vivo;
4.1.3.4.10.2. Player de vídeos gravados;
4.1.3.4.10.3. Visualização ao vivo em plataforma móvel;
4.1.3.5. Todos os streams de vídeos fornecidos por câmeras analógicas ou câmeras IP deve permitir codificar em formatos de compressão MJPEG, MPEG-4, JPEG2000, H.265 e/ou H.264, e gravados simultaneamente em tempo real.
4.1.3.6. O VMS deverá servir de interface para servidores compostos por dispositivos IP e/ou codificadores de vídeo analógicos e digitais; daqui em diante referido como servidores de vídeo digital (Digital Video Server – DVS).
4.1.3.7. A taxa de bits, taxa de quadros e resolução de cada câmera deverá poder ser alterada sem afetar a configuração de gravação e visualização das outras câmeras do sistema.
4.1.3.8. O sistema deverá ser baseado em uma arquitetura aberta que deverá permitir o uso de Storages não proprietários, provendo um sistema de armazenamento sem limite de capacidade e deverá permitir upgrade gradual da capacidade.
4.1.3.9. O sistema deverá ser capaz de usar múltiplas mesas controladoras de CFTV

para manusear a operação das câmeras, incluindo câmeras de diversos fabricantes / marcas, e suas funcionalidades PTZ, independente do fabricante / marca da mesa controladora.

4.1.3.10. O sistema deverá suportar ao menos os seguintes fabricantes de câmeras IP: ACTi, Arecont Vision, Avigilon, Axis, Basler, Bosch, Brickcom, Canon, Cisco, Dahua, Dynacolor, Flir, Hanwha Techwin, Hikvision, Messoa, Merit Lilin, Mobotix, Panasonic, Pelco, Samsung, Sony, UDP Technology e Vivotek.

4.1.3.11. O VMS deverá suportar as mais recentes revisões dos padrões ONVIF/PSIA.

4.1.3.12. O sistema deverá suportar integrações com outras plataformas (sistemas de controle de acesso, intrusão e incêndio), permitindo o recebimento de eventos e interação entre as soluções;.

4.1.3.13. O sistema deverá suportar ao menos os seguintes protocolos de câmeras PTZ: Pelco, Panasonic, Samsung, Sony, Sensormatic, Dynacolor, Kalatel, American Dynamics, Lilin, Everfocus, Sanyo, Videotec.

4.1.3.14. O sistema deverá permitir aos usuários ativar todos os controles da visualização ao vivo usando um teclado padrão de PC.

4.1.3.15. O sistema deverá ser constituído de módulos - Server Software Modules (SSM) - e software cliente - Client Software Application (CSA).

4.1.3.16. SSM e CSA deverão ser capazes de trabalhar em redes separadas.

4.1.3.17. O sistema deverá permitir o usuário a configurar o fuso horário para cada câmera conectada a um DVS e para cada SSM. Para a busca de imagens gravadas, os usuários deverão ter a possibilidade de pesquisar por vídeo com as seguintes opções:

4.1.3.17.1. Hora local da câmera;

4.1.3.17.2. Hora local do SSM;

4.1.3.17.3. Hora local da estação de trabalho do usuário;

4.1.3.17.4. Outro fuso horário;

4.1.3.18. Para prevenir a exclusão, modificação ou a adição de quadros no vídeo gravado, uma assinatura digital deverá ser implementada para proteger a integridade dos vídeos arquivados. Uma vez arquivados no servidor, a assinatura digital deverá ser aplicada, e caso um único pixel seja alterado, o sistema deverá notificar o usuário que aquele vídeo foi violado.

4.1.3.19. O sistema deverá suportar mecanismo de failover para se proteger de uma acidental perda de dados. O sistema de failover deverá agir como um hot standby, pronto para assumir as funções do(s) servidor(es) de vídeo primário. A função de failover deverá acontecer em menos de 1 minuto, sem a necessidade de nenhuma intervenção do usuário.

4.1.3.20. O sistema deverá suportar atualização de versão sem ser necessária à desinstalação da versão anterior.

4.1.4. MÓDULOS DE SOFTWARE DE SERVIDOR (SERVER SOFTWARE MODULES – SSM):

4.1.4.1. O SSM deverá ser constituído de Núcleo do sistema, Arquivo, Gateway de vídeo, Watchdog, Ferramenta de Configuração, Visualização ao vivo, Reprodutor de Arquivo, Cliente Mobile, Cliente Web, Editor de Macro, Visualizador de Relatórios;

4.1.4.2. O SSM deverá ter a capacidade de ser instalado em vários PCs em arquitetura distribuída em um ambiente LAN ou WAN. O SSM não deverá limitar o número de PCs que podem estar interligados para formar o sistema.

4.1.4.3. Núcleo do sistema deverá:

4.1.4.3.1. Manter um catálogo de configurações para todos os CSA, SSM e DVS no sistema;
4.1.4.3.2. Possibilitar o CSA a criar conexões entre diferentes DVS dinamicamente em toda a rede;
4.1.4.3.3. Prover a capacidade de visualizar todos os DVS em uma rede, mesmo se o DVS estiver associado a diferentes servidores de arquivo;
4.1.4.3.4. Caso a câmera perca o sinal de vídeo, detectar esta perda e alertar o administrador do sistema;
4.1.4.3.5. Receber todos os eventos de entrada (detecção de movimento, alarme, relê, etc.) no sistema e tomar a ação apropriada baseada em uma relação evento / ação definida pelo usuário;
4.1.4.3.6. Receber todos os eventos do controle de acesso ofertado neste certame, de tal forma que o software seja capaz de receber e tratar eventos dentro de sua própria interface, sem que haja necessidade de monitorá-los no controle de acesso. O VMS deverá receber no mínimo os seguintes eventos:
4.1.4.3.6.1. Entrada e saída válidas;
4.1.4.3.6.2. Entrada e saída inválidas;
4.1.4.3.6.3. Evento de porta aberta;
4.1.4.3.6.4. Evento de botoeira;
4.1.4.3.6.5. Ativação de sensor dentro da placa de alarme;
4.1.4.3.7. O núcleo deverá criar um alerta sonoro para eventos e atividades de usuários;
4.1.4.3.8. O núcleo deverá efetuar gerenciamento de banda dinâmico;
4.1.4.3.9. O núcleo deverá autenticar usuários e dar-lhes acesso ao sistema baseado nos direitos de acesso pré-definidos;
4.1.4.3.10. O núcleo deverá receber e armazenar em log os seguintes eventos:
4.1.4.3.10.1. Alarmes e eventos:
4.1.4.3.10.1.1. Ativo;
4.1.4.3.10.1.2. Encaminhado;
4.1.4.3.10.1.3. Standby.
4.1.4.3.10.1.4. Aplicações e eventos:
4.1.4.3.10.1.5. Perda de aplicação;
4.1.4.3.10.2. Eventos de arquivo:
4.1.4.3.10.2.1. Arquivo parado;
4.1.4.3.10.2.2. Backup iniciado;
4.1.4.3.10.2.3. Backup realizado;
4.1.4.3.10.2.4. Backup falhou.
4.1.4.3.10.3. Eventos de câmeras:
4.1.4.3.10.3.1. Gravação auto-iniciada;
4.1.4.3.10.3.2. Gravação auto-encerrada;
4.1.4.3.10.3.3. Movimento iniciado;
4.1.4.3.10.3.4. Movimento parado;
4.1.4.3.10.3.5. Perda de sinal;
4.1.4.3.10.3.6. Sinal recuperado;
4.1.4.3.10.3.7. Usuário iniciou a gravação;
4.1.4.3.10.3.8. Usuário parou a gravação;
4.1.4.3.10.3.9. Evento de entrada digital;
4.1.4.3.10.3.10. Saída digital abrindo;
4.1.4.3.10.3.11. Saída digital fechando.

4.1.4.3.10.4. Eventos de macro:
4.1.4.3.10.4.1. Erro de macro;
4.1.4.3.10.4.2. Macro iniciada;
4.1.4.3.10.4.3. Macro parada.
4.1.4.3.10.5. Eventos de controle de acesso:
4.1.4.3.10.5.1. Entrada e saída válidas;
4.1.4.3.10.5.2. Entrada e saída inválidas;
4.1.4.3.10.5.3. Evento de porta aberta;
4.1.4.3.10.5.4. Evento de botoeira;
4.1.4.3.10.5.5. Ativação de sensor dentro da placa de alarme.
4.1.4.3.10.6. Eventos DVS:
4.1.4.3.10.6.1. Perda de sinal;
4.1.4.3.10.6.2. Sinal recuperado;
4.1.4.3.10.6.3. Unidade encontrada;
4.1.4.3.10.6.4. Unidade perdida.
4.1.4.3.10.7. Eventos de usuário:
4.1.4.3.10.7.1. Logon de usuário;
4.1.4.3.10.7.2. Logoff de usuário;
4.1.4.3.11. O núcleo deverá ter a capacidade de executar qualquer uma das seguintes ações em resposta a qualquer um dos eventos listados acima:
4.1.4.3.11.1. Ações de arquivo:
4.1.4.3.11.1.1. Iniciar gravação;
4.1.4.3.11.1.2. Parar gravação;
4.1.4.3.11.1.3. Alterar qualidade de gravação.
4.1.4.3.11.2. Ações de monitoramento:
4.1.4.3.11.2.1. Visualizar a câmera em um monitor;
4.1.4.3.11.2.2. Visualizar a câmera em uma janela independente no Visualizador ao vivo;
4.1.4.3.11.2.3. Visualizar um mapa no Visualizador ao vivo.
4.1.4.3.11.3. Ações de notificações de usuários:
4.1.4.3.11.3.1. Enviar uma mensagem;
4.1.4.3.11.3.2. Enviar um som de alerta;
4.1.4.3.11.3.3. Enviar um e-mail;
4.1.4.3.11.3.4. Acionar um alarme;
4.1.4.3.11.4. Ações de saída de relê:
4.1.4.3.11.4.1. Definir a saída de relê para o inverso do estado padrão;
4.1.4.3.11.4.2. Definir a saída de relê para o estado padrão;
4.1.4.3.11.4.3. Definir a saída de relê como ligada;
4.1.4.3.11.4.4. Definir a saída de relê como desligada.
4.1.4.3.11.5. Ações de controle de dispositivo:
4.1.4.3.11.5.1. Enviar uma string para a porta serial.
4.1.4.3.11.6. Ações de macro:
4.1.4.3.11.6.1. Executar uma macro.
4.1.4.4. O núcleo deverá prover funcionalidade de armazenar vídeo e áudio baseado em eventos como:
4.1.4.4.1. Detecção de movimento digital;
4.1.4.4.2. Entrada digital ativada;
4.1.4.4.3. Macros;
4.1.4.5. O núcleo deverá permitir múltiplas agendas de gravação relacionadas a uma única câmera, cada agenda deverá poder ser criada com os seguintes parâmetros:

4.1.4.5.1. Configurações de qualidade de vídeo:
4.1.4.5.1.1. Modo de gravação (contínua, alarme/manual, desabilitada);
4.1.4.5.1.2. Configurações de data e hora (diário, semanal, contínua).
4.1.4.6. O núcleo deverá ter a habilidade de alterar dinamicamente a configuração de qualidade de vídeo nos eventos citados acima.
4.1.4.7. O núcleo deverá suportar gerenciamento de alarmes avançados:
4.1.4.7.1. Associar alarmes e procedimentos para usuários ou grupos específicos;
4.1.4.7.2. Permitir que usuários coloquem alarmes em fila, e visualize o histórico de alarmes;
4.1.4.7.3. Exibir em uma estação de trabalho alarmes compostos de stream de vídeo ao vivo, stream de vídeo gravado, ou conjunto de imagens estáticas. Combinações de todos esses itens deverão poder ser configuradas para cada alarme;
4.1.4.7.4. Configurar múltiplas câmeras para exibir em um alarme;
4.1.4.8. Arquivo:
4.1.4.8.1. O sistema de arquivo deverá ter a capacidade de agendar backups de vídeo gravados, com a base de dados de eventos associada;
4.1.4.8.2. O sistema de arquivo deverá ter a capacidade de down-sample para armazenamento do vídeo;
4.1.4.8.3. O Sistema de Arquivo deverá ser capaz de manter uma cópia redundante dos dados associados ao vídeo, como eventos e alarmes;
4.1.4.8.4. O Sistema de Arquivo deverá usar um stream de vídeo multicast do DVS e não devem requerer uma conexão adicional com nenhum outro DVS;
4.1.4.8.5. O Sistema de Arquivo deverá utilizar o stream ao vivo de vídeo do DVS para gravação;
4.1.4.8.6. O Sistema de Arquivo deverá utilizar as capacidades de redirecionamento do stream de rede DVS e balanceamento de carga;
4.1.4.9. Watchdog:
4.1.4.9.1. O watchdog deverá monitorar a operação de todos os serviços do SSM e reiniciá-los em caso de mau funcionamento. Como último recurso, caso o watchdog não consiga reinicializar os serviços, deverá reiniciar o Computador.
4.1.4.10. Ferramenta de Configuração:
4.1.4.10.1. A ferramenta de configuração permitir que o administrador ou usuários com permissões de acesso apropriadas alterem as configurações do sistema. Deverá ter as capacidades mínimas abaixo:
4.1.4.10.1.1. Deverá fornecer administração descentralizada do sistema completo, de qualquer lugar da rede;
4.1.4.10.1.2. O Layout das Câmeras deverá estar disponível para todos os usuários salvos no Servidor Principal e disponíveis para todos os Aplicativos de visualização ao Vivo/Player de Sistema de Arquivos conectados a este Servidor Principal;
4.1.4.10.1.3. Deverá permitir a alteração da qualidade de vídeo, largura de banda e taxa de frames na câmera (stream) para ambos os vídeos ao vivo e gravados;
4.1.4.10.1.4. Deverá fornecer a capacidade de definir acessos e privilégios por grupo de usuário, bem como usuário individual por meio de um menu no CSA;

4.1.4.10.1.5. Deverá fornecer ajuste da configuração de brilho, contraste e cor para cada câmera num mesmo DVS;
4.1.4.10.1.6. Deverá fornecer a ativação de gravação de áudio nas unidades de DVS que suportam áudio;
4.1.4.10.1.7. Deverá fornecer a alteração dos parâmetros de áudio, porta serial e configuração de I/O para unidades individuais de DVS;
4.1.4.10.1.8. Deverá fornecer a capacidade de renomear todas as unidades de DVS baseada na topologia do sistema e adicionar informações descritivas adicionais para cada DVS;
4.1.4.10.1.9. Deverá fornecer a capacidade de reagrupar câmeras específicas e restringir ou ativar permissões de acesso a este grupo numa base por usuário;
4.1.4.10.1.10. Deverá permitir o ajuste de modos de gravação para cada câmera de forma individual baseado na detecção de movimento, entrada de alarme, agendamento ou contínua;
4.1.4.10.1.11. Deverá fornecer um tutorial para criação de macros complexas para ativação de um evento. O tutorial deverá permitir que o usuário selecione de uma variedade de comandos comuns e complexos:
4.1.4.10.1.12. Abrir porta serial;
4.1.4.10.1.13. Sobrescrever com qualidade de gravação manual;
4.1.4.10.1.14. Sobrescrever com qualidade de gravação por detecção de movimento;
4.1.4.10.1.15. Gravar a câmera visualizada;
4.1.4.10.1.16. Qualidade de gravação como configuração padrão;
4.1.4.10.1.17. Executar uma macro;
4.1.4.10.1.18. Executar um padrão de visualização;
4.1.4.10.1.19. Executar um script com conteúdo;
4.1.4.10.1.20. Enviar uma mensagem;
4.1.4.10.1.21. Enviar um alerta de som;
4.1.4.10.1.22. Enviar um e-mail;
4.1.4.10.1.23. Enviar uma ação customizada;
4.1.4.10.1.24. Enviar um evento customizado;
4.1.4.10.1.25. Ajustar a interface de call-back;
4.1.4.10.1.26. Ajustar a saída de relé para seu estado padrão;
4.1.4.10.1.27. Ajustar a patrulha padrão;
4.1.4.10.1.28. Iniciar o backup;
4.1.4.10.1.29. Iniciar a gravação;
4.1.4.10.1.30. Parar a gravação;
4.1.4.10.1.31. Visualizar um mapa;
4.1.4.10.1.32. Deverá suportar a criação de agendamentos, onde os seguintes parâmetros poderão ser associados:
4.1.4.10.1.32.1. Gravação;
4.1.4.10.1.32.2. Brilho, Contraste e Cor;
4.1.4.10.1.32.3. Entradas de relés;
4.1.4.10.1.32.4. Logon de usuário;
4.1.4.10.1.32.5. Macros;
4.1.4.10.1.32.6. Alarmes.
4.1.4.10.1.33. Deverá permitir a criação de ilimitados agendamentos de gravação e associar qualquer câmera a qualquer agendamento;
4.1.4.10.1.34. Deverá fornecer ferramentas para definir ações automáticas a

serem tomadas em resposta a eventos internos/externos;

4.1.4.10.1.35. Quando uma nova unidade é adicionada ao sistema, deverá ser designado um nome de preset;

4.1.4.10.1.36. Os usuários deverão ter a capacidade configurar o retorno à posição inicial depois de um tempo predeterminado de inatividade nas câmeras PTZ;

4.1.4.10.1.37. Os usuários deverão ter a capacidade de configurar diferentes tipos de vídeo análise na interface da câmera, com a possibilidade de calibrar cada recurso de vídeo análise de acordo com o tamanho do objeto, velocidade de movimento e contraste com o segundo plano;

4.1.4.10.2. Visualização ao vivo;

4.1.4.10.2.1. Deverá permitir o monitoramento ao vivo de 1 a 64 streams de vídeo simultaneamente num único monitor, e trabalhar com multi-monitores;

4.1.4.10.2.2. Deverá permitir que os operadores escolham padrões de visualização pré-definidos;

4.1.4.10.2.3. Deverá exibir todas as câmeras associadas ao sistema;

4.1.4.10.2.4. Deverá exibir todas as sequências de câmeras criadas no sistema;

4.1.4.10.2.5. Deverá permitir que os operadores controlem as sequências de câmeras (Pause/Play, pular para frente, pular para trás), sem afetar a capacidade de outros operadores visualizarem e controlarem a mesma sequência;

4.1.4.10.2.6. Deverá permitir que o operador crie uma imagem sem emenda a partir de diferentes câmeras com visão mesclada. O posicionamento de câmeras, rotação, tamanho e ângulo deverão ser configurados pelo operador na interface de Visualização sem a necessidade de executar ferramentas e aplicações adicionais;

4.1.4.10.2.7. Os streams de vídeo deverão poder ser associados a mosaicos que não estejam atualmente visíveis no padrão exibido atualmente;

4.1.4.10.2.8. Deverá suportar funcionalidade de Mapa, onde mapas digitais são utilizados para representar a localização física de câmeras e outros dispositivos por todo o sistema de segurança. Os mapas deverão suportar hyperlinks com a finalidade de criar uma hierarquia entre os mapas interligados. A funcionalidade de mapa deverá permitir a importação de mapas de qualquer aplicativo gráfico suportando imagens em formato BMP, JPEG e/ou GIF;

4.1.4.10.2.9. O operador deverá ser capaz de clicar num ícone de câmera de um mapa para visualização ao vivo desta imagem;

4.1.4.10.2.10. O operador deverá ser capaz de clicar num ícone dentro de um mapa para iniciar um preset de câmera ou acionar um I/O;

4.1.4.10.2.11. Deverá suportar a funcionalidade de procedimentos, onde estes poderão ser desencadeados para aparecer durante um determinado evento e poderão ser utilizados para fornecer instruções detalhadas ao operador, assim como as ações que ele deverá tomar;

4.1.4.10.2.12. Deverá suportar zoom digital em streams de vídeo ao vivo;

4.1.4.10.2.13. Deverá alternar automaticamente entre os streams de baixa e alta resolução de acordo com o tamanho da câmera na tela;

4.1.4.10.2.14. Deverá permitir que o usuário envie um stream de vídeo para um Cliente de dispositivo móvel;

4.1.4.10.2.15. Deverá permitir comunicação com áudio com as unidades DVS. O operador deverá ter a opção de utilizar o modo full duplex (para atuar como um sistema de intercomunicação IP) ou para áudio unidirecional. O áudio deverá ser arquivado no mesmo banco de dados que o vídeo das câmeras;

4.1.4.10.2.16. O operador deverá navegar facilmente entre esta e demais aplicações CSA (caso tenha as permissões de acesso), através de funcionalidades de apontar e clicar;

4.1.4.10.2.17. O operador deverá ser capaz de iniciar/parar a gravação em qualquer câmera do sistema, através da gravação manual, clicando em um único botão;

4.1.4.10.2.18. O operador deverá ser capaz de ativar ou desativar a visualização de todos os eventos do sistema conforme sua ocorrência;

4.1.4.10.2.19. O sistema deverá permitir que os operadores visualizem um replay instantâneo do vídeo de qualquer câmera gravada. O operador deverá ser capaz de definir o quanto ele deseja recuar a imagem (não deverá haver limite). Ele deverá ser capaz de controlar o Playback com:

4.1.4.10.2.19.1. Pause;

4.1.4.10.2.19.2. Travar a velocidade;

4.1.4.10.2.19.3. Avançar o Playback em: 1x, 2x, 4x, 8x;

4.1.4.10.2.19.4. Recuar o Playback em: -1x, -2x, -4x, -8x;

4.1.4.10.2.19.5. Reduzir o avanço do Playback em: Quadro a quadro;

4.1.4.10.2.19.6. Reduzir o recuo do Playback em: -Quadro a -quadro.

4.1.4.10.2.20. A função de Replay Instantâneo deve reproduzir o vídeo no momento do alarme quando ativado em um mosaico exibindo um alarme. Com uma representação gráfica em linha do tempo, o usuário deverá ser capaz de controlar que momento ele está buscando;

4.1.4.10.2.21. Os usuários deverão ser capazes de tirar snapshots de imagens ao vivo no Visualizador, e salvá-las ou imprimi-las;

4.1.4.10.2.22. O operador deverá ser capaz de escolher e acionar uma ação de uma lista de ações;

4.1.4.10.2.23. O usuário deverá ser capaz de visualizar a mesma câmera múltiplas vezes em diferentes mosaicos;

4.1.4.10.2.24. Os usuários deverão ser capazes de exibir um layout de streams de vídeo com um monitor de PC sem qualquer componente gráfico de vídeo. Os delimitadores entre os mosaicos deverão possuir largura de 2 pixels;

4.1.4.11. Reprodutor de Arquivo;

4.1.4.11.1. O Reprodutor de arquivo deverá permitir a reprodução de arquivo de vídeo e áudio. Deverá seguir as seguintes especificações mínimas:

4.1.4.11.1.1. Deverá suportar a reprodução de áudio e vídeo de qualquer intervalo de tempo;

4.1.4.11.1.2. Deverá suportar a exibição de 64 vídeos gravados simultaneamente;

4.1.4.11.1.3. Deverá permitir que os operadores escolham um número de câmeras possíveis para exibição em mosaico;

4.1.4.11.1.4. Deverá permitir que o operador selecione a reprodução síncrona de todos os streams de vídeo selecionados, permitindo que os operadores visualizem os eventos de múltiplos ângulos ou através

de vários campos da câmera, ou reprodução assíncrona;

4.1.4.11.1.5. Deverá permitir que o operador visualize a mesma câmera simultaneamente em múltiplos mosaicos, em diferentes intervalos de tempo.

4.1.4.11.2. Deverá permitir que o operador controle a reprodução com:

4.1.4.11.2.1. Pause;

4.1.4.11.2.2. Travar a velocidade;

4.1.4.11.2.3. Avançar o Playback em: 1x, 2x, 4x, 8x;

4.1.4.11.2.4. Recuar o Playback em: -1x, -2x, -4x, -8x;

4.1.4.11.2.5. Reduzir o avanço do Playback em: Quadro a quadro;

4.1.4.11.2.6. Reduzir o recuo do Playback em: -Quadro a quadro;

4.1.4.11.3. Deverá exibir uma única linha do tempo, ou opcionalmente uma linha do tempo para cada stream de vídeo selecionado, com o qual o operador poderá navegar através da sequência de vídeo simplesmente apontando e clicando em qualquer ponto da linha do tempo;

4.1.4.11.4. Deverá exibir a unidade de disco na qual um arquivo está localizado, como resultado de uma consulta de pesquisa realizada pela Aplicação Cliente;

4.1.4.11.5. Deverá fornecer ferramenta para pesquisa de vídeo e áudio associado em eventos definidos pelo usuário ou parâmetros de movimento;

4.1.4.11.6. Deverá permitir que os operadores carreguem arquivos de vídeo previamente exportados de seus computadores ou rede;

4.1.4.11.7. Deverá permitir que os operadores validem se uma sequência de vídeo digitalmente assinada foi ou não adulterada;

4.1.4.11.8. Deverá suportar zoom digital em streams de vídeo reproduzidos;

4.1.4.11.9. Deverá fornecer exportação de imagem estática em formato JPEG e BMP com data e hora estampada na imagem;

4.1.4.11.10. Deverá fornecer ferramentas para exportar sequências de vídeo e um player de vídeo proprietário, de forma que os arquivos possam ser reproduzidos em computadores que não tenham o CSA previamente instalado;

4.1.4.11.11. Deverá fornecer ferramentas para exportar sequências de vídeo em formatos padrões de vídeo, como AVI e ASF;

4.1.4.11.11.1.1. O operador deverá navegar facilmente entre esta e outras aplicações CSA (caso ele possua permissões de acesso) com a função de apontar e clicar;

4.1.5. CLIENT SOFTWARE APPLICATIONS (CSA)

4.1.5.1. CSA deverá ser composto por uma aplicação Visualização ao vivo, Reprodutor de vídeos gravados, Cliente Web e uma aplicação Visualizador Mobile.

4.1.5.2. O CSA deverá executar os seguintes aplicativos simultaneamente sem interferir com qualquer das operações SSM (gravação, alarmes, etc.):

4.1.5.2.1. Exibição em tempo real das câmeras em uma estação de trabalho;

4.1.5.2.2. Reprodução de vídeos arquivos em uma estação de trabalho;

4.1.5.2.3. Recuperação de vídeo arquivado;

4.1.5.2.4. Repetição imediata de vídeo em tempo real de uma estação de trabalho;

4.1.5.2.5. Reprodução instantânea em tempo real de vídeo no monitor;

4.1.5.2.6. Uso de mapas;

4.1.5.2.7. Configuração dos parâmetros de sistema;
4.1.5.2.8. Execução de macro do sistema;
4.1.5.2.9. Visualização e gerenciamento de alarmes em uma estação de trabalho;
4.1.5.2.10. Criar e imprimir snapshots de transmissões de vídeo em tempo real;
4.1.5.2.11. Criar e imprimir snapshots de arquivos de transmissões de vídeo;
4.1.5.2.12. Criar detectores de análise de vídeo em tempo real;

4.1.5.3. Todas as aplicações deverão suportar qualquer forma de conectividade de rede IP, incluindo LAN;

4.1.5.4. Todas as aplicações deverão suportar Multicast (UDP) e Unicast (TCP ou UDP) de streaming de vídeo;

4.1.5.5. Todas as aplicações deverão adaptar-se automaticamente para a topologia de rede e usar o melhor método para receber o streaming de vídeo;

4.1.5.6. Todas as aplicações deverão providenciar um mecanismo de autenticação que verifica a validade do usuário. Onde, o administrador pode definir permissões de acesso específico para cada usuário do sistema e inclui:

4.1.5.6.1. Administrador ou usuário básico:
4.1.5.6.1.1. Administrador deverá possuir todas as permissões de acesso;
4.1.5.6.1.2. Cada usuário deverá poder ter diferentes regras de acesso;
4.1.5.6.1.3. Ter ou não acesso a determinados locais;
4.1.5.6.1.4. Deverá poder ter ou não acesso a tipos de aplicações;
4.1.5.6.1.5. Listas de privilégios;
4.1.5.6.1.6. Aplicações:
4.1.5.6.1.7. Visualização em tempo real;
4.1.5.6.1.8. Leitor de arquivos;
4.1.5.6.1.9. Visualizações em tempo real via WEB;
4.1.5.6.1.10. Leitor de arquivos via WEB;

4.1.5.6.2. Usuários avançados:
4.1.5.6.2.1. Configuração de Locais;
4.1.5.6.2.2. Configuração de câmeras;
4.1.5.6.2.3. Configuração de Gravação;
4.1.5.6.2.4. Configuração de Visualização;
4.1.5.6.2.5. Configuração de máscara de movimento;

4.1.5.6.3. Eliminação:
4.1.5.6.3.1. Criação, eliminação e configuração de monitores;
4.1.5.6.3.2. Criação, eliminação e configuração de áudio;
4.1.5.6.3.3. Criação, eliminação e configuração de portas serial;
4.1.5.6.3.4. Criação, eliminação e configuração de PTZ;
4.1.5.6.3.5. Configuração e eliminação de Pinos de entrada;
4.1.5.6.3.6. Configuração e eliminação de Pinos de saída;
4.1.5.6.3.7. Criação, eliminação e configuração de horários e coberturas;
4.1.5.6.3.8. Criação, eliminação e configuração de eventos e ações definidas pelo usuário;
4.1.5.6.3.9. Criação, configuração e eliminação de Alarmes;
4.1.5.6.3.10. Criação, configuração e eliminação de Macros;
4.1.5.6.3.11. Criação, configuração e eliminação de sequências câmeras;
4.1.5.6.3.12. Criação, configuração e eliminação de grupo de visualização em tempo real;
4.1.5.6.3.13. Criação, configuração e eliminação de grupos de câmeras;
4.1.5.6.3.14. Configuração e eliminação de visualizador de layouts;
4.1.5.6.3.15. Operador de backup;

4.1.5.6.4. Privilégios de Leitura de arquivos:
4.1.5.6.4.1. Exportar arquivo de vídeos;
4.1.5.6.5. Privilégios de visualização em tempo real:
4.1.5.6.5.1. Mudar as entidades exibidas;
4.1.5.6.5.2. Editar/salvar o layout de configuração;
4.1.5.6.5.3. Áudio (escuta/conversa);
4.1.5.6.5.4. Acesso ao Zoom Digital;
4.1.5.6.5.5. Repetição instantânea;
4.1.5.6.5.6. Controle de sequência de câmeras;
4.1.5.6.5.7. Executar Macros;
4.1.5.6.6. Outros privilégios:
4.1.5.6.6.1. Gravação Manual;
4.1.5.6.6.2. Visualização de câmera ligada em um monitor analógico;
4.1.5.6.6.3. Envio de mensagens;
4.1.5.6.6.4. Envio de sons;
4.1.5.6.6.5. Envio de e-mails;
4.1.5.6.6.6. Execução de ações customizadas;
4.1.5.6.6.7. Salvar e imprimir Snapshots;
4.1.5.6.6.8. Prioridade de PTZ (para controle de câmera);
4.1.5.6.6.9. Bloqueio de câmera;
4.1.5.6.6.10. Gravação local;
4.1.5.6.7. Os grupos de usuários deverão ser autorizados a designar sub-administradores que terão a autoridade sobre um subconjunto de usuários;
4.1.5.6.8. Cada estação de trabalho com o CSA deverá ser capaz de usar um teclado de CCTV ou PC que deverá poder controlar todo o conjunto de câmeras em todo o sistema, mesmo que o sistema seja constituído por câmeras motorizadas produzidas por diferentes fabricantes;
4.1.5.6.9. Toda aplicação CSA deverá permitir que múltiplas instâncias sejam executadas simultaneamente, por um ou vários usuários. O número de instâncias das aplicações de visualização em tempo real, leitor de arquivos, visualização em tempo real via WEB e Visualização em tempo real via Mobile só deverá ser limitado pelo número de licenças de aplicativos disponíveis.
4.1.5.6.10. Quailquer módulo diverso a serer inserido, deverá ser previamente omologado com o software de gerenciamento da solução.

4.1.6. Marcas de referência: Axxon, Lenel e Tyco.

4.2. Software de Gerenciamento de Controle de Acesso

4.2.1. Funcionalidades do Software

4.2.1.1. Interface Gráfica

4.2.1.1.1. O software de gerenciamento do Sistema de Controle de Acesso deve possuir interface Web amigável e robusta, a fim de facilitar a operação e manutenção do sistema em casos de atualização e operação, não necessitando a instalação do software em outras máquinas além do servidor.
4.2.1.1.2. O software de gerenciamento deve permitir, para suas principais funções, integração com diferentes navegadores Web, obrigatoriamente Firefox, a fim de melhorar a experiência dos usuários de software.

4.2.1.1.3. Módulos opcionais como de Cadastramento e Gerenciamento de Visitantes poderão ser do tipo Aplicativo.

4.2.1.2. Portas de Comunicação

4.2.1.2.1. A comunicação entre software e controladora deve ser Ethernet nativa (10/100Mbps), permitindo escalabilidade de um até centenas de portas, em incremento de controladoras uma a uma. Nestes circuitos, não serão aceitos sistemas com arquitetura que compreenda redes ou sub-redes seriais como RS-232, RS-422, RS-485 ou outras, ou concentradores TCP/IP e redes seriais entre estes e módulos, de forma a não prejudicarem a performance e velocidade de transmissão de dados no sistema, bem como prejudicarem sua escalabilidade, flexibilidade e manutenção.

4.2.1.2.2. O Sistema deve permitir a utilização da infraestrutura de rede Ethernet já existente, bem como a adição de uma nova rede de dados, para monitorar e controlar o acesso local ou o acesso remoto de filiais (outras localidades), de uma mesma central de segurança, via VPN em LAN ou WAN.

4.2.1.2.3. O sistema deve permitir que uma controladora não afete o funcionamento de outra, como no caso de redes em "daisy-chain" ou "looping", a fim de aumentar drasticamente a confiabilidade do sistema, assim como garantir a rápida e simples manutenção do mesmo.

4.2.1.2.4. instalação das controladoras na rede Ethernet deve ser simples e rápida, sem que seja necessária a configuração de jumpers de endereçamento nas mesmas. O sistema deve ser inteligente o suficiente para auto detectar o endereço IP padrão ("default") de cada controladora, e automaticamente, adicioná-la no banco de dados do sistema, permitindo a mudança manual de endereço IP, via software, para adequação dos dispositivos à rede existente.

4.2.1.2.5. Deverão ser usadas diferentes portas TCP (Transfer Control Protocol) para comunicação e recepção de eventos, para garantia de entrega de pacote de eventos (eventos como acesso de entrada válida, acesso de saída válida, etc.).

4.2.1.3. Integração com permissões de Usuários

4.2.1.3.1. O sistema deve permitir integração com MSAD (Microsoft Active Directory) para gerenciamento das permissões de login do usuário, facilitando a criação e gerenciamento de logins e permissões de acesso ao sistema de controle de acesso.

4.2.1.4. Configurações Horárias

4.2.1.4.1. O sistema deve permitir o cadastramento de até 99 (noventa e nove) configurações horárias, sendo que as configurações horárias são as permissões de horário no dia.

4.2.1.4.2. Cada configuração Horária deve definir de um até três intervalos em um mesmo dia, onde uma credencial terá acesso a determinados locais/controladoras.

4.2.1.5. Zonas Horárias

4.2.1.5.1. O sistema deve permitir o cadastramento de até 99 (noventa e nove) zonas horárias, sendo que estas são as permissões semanais de acesso em determinados locais ou controladoras atreladas as configurações horárias.

4.2.1.6. Níveis de Acesso

4.2.1.6.1. O sistema deve permitir o cadastramento de até 999 (novecentos e noventa e nove) níveis de acesso, sendo que estes níveis são as permissões

de acessos aos locais/controladoras, atrelados às zonas horárias.

4.2.1.7. Níveis de Acesso Customizado por Usuário

4.2.1.7.1. O sistema deve permitir a alteração de um nível de acesso dentro do cadastro de usuário, customizando o nível de acesso para este usuário específico.

4.2.1.8. Feriados

4.2.1.8.1. O sistema deve permitir o cadastramento de até 50 (cinquenta) datas distintas de Feriados, sendo que estes possuem configurações horárias específicas e prioritárias, que sobrepõe as configurações horárias correntes.

4.2.1.9. Acesso Temporário

4.2.1.9.1. O sistema deve permitir o agendamento por data e horário, para a troca das permissões / nível de acesso dos usuários, individualmente e por lote. Para realizar o agendamento, o sistema deverá possuir diversos filtros, dentre eles, empresa, departamento, cargo, etc. a fim de agilizar o processo de agendamento.

4.2.1.9.2. O sistema deve permitir que a qualquer momento o agendamento seja cancelado e as credenciais voltem para seu nível de acesso anterior.

4.2.1.9.3. Ao final do período agendado, o sistema deve retornar automaticamente as permissões de acesso cadastradas anteriormente.

4.2.1.10. Cartão Provisório

4.2.1.10.1. O sistema deve permitir o cadastramento de cartões provisórios para os usuários normais (colaboradores), com validade definida, caso estes esqueçam seus cartões permanentes, que serão temporariamente desativados automaticamente. Ao se retornar o cartão provisório, o cartão permanente será novamente ativado.

4.2.1.10.2. O sistema deve manter as permissões de acesso do cartão provisório no cartão permanente.

4.2.1.11. Cartão de Emergência

4.2.1.11.1. O sistema deve possuir a opção de cadastramento de cartões de emergências, sendo que estes cartões acionarão a liberação das controladoras e suas fechaduras pré-definidas, da rota de incêndio.

4.2.1.12. Informações e Permissões do Usuário

4.2.1.12.1. O sistema deve permitir que se configure uma data para expiração da credencial do colaborador, ou isentar este usuário da expiração.

4.2.1.12.2. O sistema deve permitir a armazenagem de 1 (uma) fotografia do usuário funcionário e até 5 (cinco) fotografias do usuário visitante, relacionada à sua credencial, permitindo a importação de uma foto ou tirá-la no momento do cadastro.

4.2.1.12.3. O sistema deve permitir a personalização das permissões de acesso (nível de acesso) da credencial do usuário.

4.2.1.12.4. O sistema deve permitir o cadastramento de pelo menos 05 campos de informação personalizados.

4.2.1.12.5. No cadastro de usuário, deve ser possível cadastrar os dados pessoais do usuário cadastrado, como placa do veículo, modelo, cor, além de documentos do usuário.

4.2.1.12.6. Deve ser possível configurar por usuário uma senha de quatro dígitos quando solicitada a integração por teclado de acesso. Deve ser possível agendar um período para o usuário utilizar apenas credencial, na leitora, e outro período com credencial mais a senha de quatro dígitos, para elevar o nível de segurança em determinado horário.

4.2.1.12.7. Quando da utilização do sistema integrado a leitores biométricos (de terceiros), cada usuário deve ter a possibilidade de ter cadastrado pelo menos dois registros biométricos, um cartão de proximidade e uma senha numérica, além de se selecionar o modo de autenticação individualmente por usuário (Digital & Senha, Digital ou Senha, Digital & Cartão & Senha, etc.).

4.2.1.12.8. O sistema deve permitir o cancelamento individual da regra de *antipassback*, por usuário.

4.2.1.12.9. O sistema deve possuir pelo menos 10 grupos de dupla autenticação, além de possuir um grupo mestre capaz de se autenticar com qualquer grupo, a fim de aumentar a segurança em áreas que requerem controle mais rigoroso. Em dupla autenticação, somente usuários do mesmo grupo podem realizar a abertura da porta controlada.

4.2.1.12.10. Quando utilizado integração com pontos de alarme, todas as credenciais do sistema devem possuir opção de habilitar/desabilitar permissão de armar/desarmar alarme, aumentando a comodidade/segurança da operação.

4.2.1.13. Dupla Autenticação

4.2.1.13.1. O sistema deve possuir a opção de Dupla Autenticação para acessar em alguns locais. A dupla autenticação é dividida por grupos previamente cadastrados, dividindo as credenciais por estes grupos. Cada credencial poderá acessar um local somente acompanhado por outa credencial do mesmo grupo.

4.2.1.13.2. O sistema deve possuir a opção de grupos Mestres (“Masters”), onde o usuário poderá acessar os locais determinados com Dupla-Autenticação, acompanhados por qualquer credencial independente do grupo.

4.2.1.14. Eventos

4.2.1.14.1. O sistema deve possibilitar quais eventos dispararão e quais não dispararão sinalização na janela de planta gráfica (quadro sinótico).

4.2.1.14.2. Deve ser possível escolher diferentes cores para diferentes eventos que deverão ser apresentados na lista de transações on-line ou na lista de transações de alarme, a fim de facilitar a identificação das diferentes transações.

4.2.1.14.3. Deve também ser possível selecionar quais eventos enviarão e-mails para até cinco usuários diferentes, em decorrência de seus disparos.

4.2.1.15. Livro de ocorrência

4.2.1.15.1. O sistema deve possuir a opção de se registrar manualmente as ocorrências dos eventos no sistema, sendo que estes registros digitados deverão ser salvos no Banco de Dados para posterior auditoria.

4.2.1.15.2. O relatório deve ter sua saída de impressão em arquivo PDF (portable document file) e .xls (planilha Excel).

4.2.1.16. Tratamento de ocorrências de Alarme

4.2.1.16.1. O sistema deve possuir as seguintes funcionalidades:

4.2.1.16.2. Indicação na janela de navegador contendo planta de pavimento (quadro sinótico) com a sinalização dinâmica da porta ou sensor em disparo (alarmes de porta deixada aberta, porta forçada, violação de sensores, cartão desconhecido, antipassback, cartão expirado, falha de alimentação elétrica, bateria baixa, queda de controladora, etc.).

4.2.1.16.3. Lista específica de transações de alarme (esta lista deve filtrar e apresentar apenas alarmes), em tempo real, de onde se pode obter de forma

imediata, através de menu flutuante, imagem de vídeo em tempo real ou imagem gravada do momento do alarme (no caso de utilização do módulo de integração de CFTV), ou foto do usuário (caso o alarme esteja relacionado à uma credencial específica).

4.2.1.16.4. Nesta mesma lista, e através do mesmo menu flutuante, o operador poderá reconhecer o alarme, abrindo uma janela específica contendo os dados detalhados da porta, barreira ou sensor violado, bem como campo específico para a digitação de texto, justificando o tratamento e fechamento de ocorrência, para posterior pesquisa e auditoria.

4.2.1.16.5. O usuário também poderá reconhecer e tratar os alarmes diretamente da planta de pavimento (quadro sinótico), ao se clicar sobre o ícone dinâmico da porta ou sensor de alarme representado nesta planta, abrindo o menu flutuante.

4.2.1.16.6. Permite a utilização de tabelas com filtros dinâmicos para busca de alarmes, eventos e quaisquer outras transações efetuadas no sistema.

4.2.1.17. Planta de Pavimento

4.2.1.17.1. O sistema deve possuir a opção de inclusão de plantas dos pavimentos e de ícones animados para facilitar a visualização dos eventos de alarmes.

4.2.1.17.2. Deve se apresentar na forma de janela on-line individual ou aba de navegador Web.

4.2.1.17.3. Deve permitir a importação e adição de inúmeras imagens de plantas de pavimento individuais, em arquivo JPEG ou BMP.

4.2.1.17.4. Deve permitir que se adicionem ícones individuais para portas e sensores de alarme, que piscarão (ícones dinâmicos) para sinalização em caso de alarme.

4.2.1.17.5. Deve permitir o rápido acionamento de diversas aplicações, através de menu flutuante, ao se clicar sobre o ícone apresentado na planta gráfica, tais como pulsar abrir porta, configurar parâmetros de controladora, reconhecer alarme, etc.

4.2.1.18. Monitoramento em tempo real

4.2.1.18.1. O sistema deve permitir a visualização do local dos eventos através de ícone animado em um mapa gráfico (planta de pavimento), diretamente na tela de seu computador em tempo real, reduzindo falsos alarmes e otimizando seu tempo de resposta para as diversas ocorrências.

4.2.1.19. Agendamento de Visitantes

4.2.1.19.1. O sistema deve possuir um módulo para o pré-registro de visitantes, sendo este totalmente integrado ao módulo de Gerenciamento dos visitantes. Este módulo deve possuir interface Web amigável, robusta e protegido por senha, a fim de facilitar a operação e manutenção do sistema em casos de atualização/operação, não necessitando a instalação do software em outras máquinas além do servidor.

4.2.1.19.2. O software de agendamento deve permitir, para suas principais funções, integração com diferentes navegadores Web, a fim de melhorar a experiência dos usuários de software.

4.2.1.19.3. O sistema deve efetuar um pré-cadastro do visitante, sendo este associado a pessoa que irá visitar, informando o nome completo, n° do documento, data e hora prevista de chegada e de saída, agilizando o processo de liberação dos visitantes nas recepções \ portarias

4.2.1.19.4. Todas as informações do pré-registro devem ser totalmente sincronizadas com o banco de dados de visitante e do sistema de controle

de acesso. O sistema de pré-registro deve possuir um banco de dados dedicado.

4.2.1.20. Antipassback

4.2.1.20.1. Em seu módulo básico, o sistema deve possuir a função de Antipassback (anti-dupla na entrada e na saída): para evitar que um cartão usado para entrada/saída seja reutilizado, impedindo que mais de uma pessoa tenha acesso a um mesmo local usando o mesmo cartão. O Antipassback impede que este cartão passe duas vezes, em sequência, pela mesma leitora. Para alguns cartões, deve existir a opção para a liberação do Antipassback; isto é; para estes cartões o acesso será livre, sendo que eles poderão passar várias vezes na leitora de Entrada e/ou de Saída.

4.2.1.20.2. O sistema deve possuir a opção (modular) para a função de Antipassback GLOBAL: este previne que um mesmo cartão seja usado por mais de uma pessoa, mais de uma vez, em um grupo de controladoras / área de acesso programável.

4.2.1.20.3. O sistema deve possuir a opção de Rotas de Antipassback GLOBAL: este previne que um usuário tenha acesso (entrada ou saída) em determinadas controladoras sem que antes tenham sidos acessadas outras controladoras em uma sequência previamente programável.

4.2.1.20.4. Deve ser possível a seleção de até noventa e nove diferentes grupos de controladoras para a função de Antipassback Global.

4.2.1.20.5. As funções de Antipassback, Antipassback GLOBAL e Rotas de Antipassback GLOBAL, deverão permanecer funcionando de forma integral sem a necessidade do Servidor de Controle de Acesso estar on-line, ou seja, independentemente do PC Servidor e software de Controle de Acesso, no caso dos servidores estarem desligados ou fora da rede.

4.2.1.21. Relatórios

4.2.1.21.1. O Sistema deve permitir a visualização de todos os tipos de eventos, bem como disponibilizar a função de procura de eventos. Também deve permitir a geração de relatórios dentro de períodos de tempo determinados pelo operador. Deve permitir uma grande gama de filtros de relatórios, compreendendo todas as funções e transações do Sistema. Filtros por data e hora de início, data e hora de fim, número de cartão, nome de empresa, grupo de acesso, acessos válidos de entrada ou saída, zonas de alarme ativadas, bateria baixa, falha de alimentação elétrica, pulsar abrir porta, filtro de relatório por porta ou barreira específica, ou seja, TODAS as transações do sistema deverão poder ser filtradas para relatório específico.

4.2.1.21.2. Os relatórios deverão ser apresentados, previamente à sua impressão, na tela do computador, de forma que ainda se possa trabalhar sub-filtros de tabela dinâmica. Nesta tabela dinâmica poder-se-á buscar, por exemplo, a imagem de vídeo (módulo de integração de CFTV) de acesso de um determinado usuário de cartão, em uma controladora que tiver uma câmera analógica ou câmera IP relacionada à mesma.

4.2.1.21.3. O relatório deve ter sua saída de impressão em arquivo PDF (portable document file), .xls (planilha Excel) ou .ods.

4.2.1.21.4. Deve ainda possuir um relatório individual para listar, de maneira instantânea, todos os usuários de cartão presentes em um determinado edifício, inclusive mostrando em que sala do prédio o usuário se encontra (para que esta função funcione eficientemente, leitoras de entrada e de saída em cada barreira deverão ser instaladas).

4.2.1.21.5. Deve possuir um módulo de relatório de auditoria, que permite auditar todas as operações e configurações realizadas no software, por usuário, por máquina, por endereço IP, com data e hora. Pode-se, por exemplo, emitir-se um relatório sobre qual usuário do sistema mudou o nível de acesso (nível X para nível Y) de um usuário de cartão (com nome deste usuário).

4.2.1.21.6. Deve permitir que informações ou dados coletados no banco de dados e mostrados através de relatório possam ser exportados para softwares de ponto (ou outros), através de arquivo .xls ou .ods.

4.2.1.21.7. O relatório de transações deverá permitir integração com o sistema de CFTV, permitindo a visualização das imagens gravadas dos eventos de acesso. As imagens não devem ficar armazenadas no controle de acesso, a integração deverá ser realizada diretamente com o sistema de CFTV, a fim de poupar espaço em disco.

4.2.1.22. Controle de Frequência Gerencial

4.2.1.22.1. O sistema deve permitir a implantação de um módulo de frequência gerencial, que emita relatórios com as transações gerenciais de frequências, apurar alguns eventos tais como: atraso, hora excedente, ausência.

4.2.1.23. Parâmetros do sistema

4.2.1.23.1. O sistema deve possuir, no mínimo, 5 (cinco) diferentes de usuários do sistema, permitindo a configuração de acesso a todos os menus presentes no software.

4.2.1.23.2. Administrador do Sistema – o administrador do sistema poderá programar, monitorar e emitir relatórios através do software central. Também poderá adicionar novos usuários para o software e atribuir níveis de acesso a eles.

4.2.1.23.3. Permissão de uso do sistema – O Sistema deve permitir diferentes níveis de permissão para diferentes grupos de usuários.

4.2.1.23.4. O sistema deve registrar toda entrada (log) de usuários no Sistema e possuir um relatório de auditoria para que as operações no software possam ser auditadas. Cada usuário autorizado deve digitar seu nome de usuário e sua senha individual.

4.2.1.23.5. Deve ser possível o download de comandos e parâmetros às controladoras, através da rede Ethernet, tais como: pulsar para abrir porta, pulsar para entrar ou sair por barreira (o pulso deve comandar o sentido de giro de catracas, por exemplo), envio de datas e horários, cartões, níveis de acesso, etc.

4.2.1.23.6. Deve ser possível o upload de informações contidas nas controladoras, através da rede Ethernet, tais como cartões, níveis de acesso, parâmetros de porta, etc.

4.2.1.23.7. Deve ser possível o rastreamento de cartões e transações.

4.2.1.23.8. O sistema deve possuir uma janela de transações on-line, onde deverão ser apresentadas todas as transações ocorridas nas controladoras e no sistema, em tempo real. As transações poderão ter cores específicas, para sua fácil identificação. Ainda deve ser possível se obter de forma imediata, através de menu flutuante e do módulo de integração de CFTV, imagem de vídeo em tempo real ou imagem gravada do momento do alarme, bem como uma comparação de vídeo de entrada e saída (imagem gravada no momento de entrada × vídeo em tempo real da saída), ou foto do usuário do cartão (caso o alarme esteja relacionado a um cartão específico).

4.2.1.23.9. O sistema deverá possuir um painel indicativo de conexão com as controladoras, a fim de identificar se as controladoras estão online ou off-line no sistema, permitindo a criação de filtros a fim de facilitar a busca para empreendimentos com muitas controladoras.

4.2.1.23.10. O sistema deverá permitir visualizar a última transação da credencial, a fim de identificar qual foi a última barreira acessada pelo colaborador/visitante.

4.2.1.24. Exportar

4.2.1.24.1. O Sistema deve permitir a exportação de dados de usuário/relatórios em formato, .ods, .xls ou .pdf (portable document file). Os dados deverão conter data, horário, número de cartão, controladora e tipo de transação, para inclusive servir de base para softwares de ponto, exportando as transações em TXT para que possam ser usadas futuramente para controle de frequência.

4.2.1.25. Licenciamento

4.2.1.25.1. O sistema deve possuir a opção de liberação dos módulos através de contra chave, a qual deverá permitir ativação online ou offline, podendo ser expandidas a qualquer momento, fornecendo uma solução totalmente segura, com uma operação extremamente simples, garantindo a escalabilidade do sistema.

4.2.1.26. Envio de E-mails

4.2.1.26.1. O sistema deve possuir a opção de enviar e-mails de todos os eventos de transação do sistema de controle de acesso para uma ou mais contas. Não serão permitidas integrações externas, a configuração deverá ser feita diretamente na plataforma de controle de acesso, a fim de tornar a operação menos propícia a falhas.

4.2.1.27. Idioma

4.2.1.27.1. O sistema deve contemplar o idioma Português do Brasil.

4.2.1.28. Integração com Sistemas de CFTV

4.2.1.28.1. O sistema deve possuir o módulo para a integração com o Sistema de CFTV para permitir a observação de múltiplos vídeos em tempo real dentro da interface gráfica do Sistema, provenientes de câmeras analógicas ou câmeras IP (simultaneamente, se for o caso, através de sistema híbrido). Permite que se recupere, em até dois cliques, sobre qualquer evento de acesso ou de alarme, o vídeo gravado deste evento ou o vídeo correspondente em tempo real, desde que haja uma câmera previamente relacionada para a controladora/barreira correspondente, na programação.

4.2.1.28.2. O Software de Controle de Acesso deverá permitir a inclusão de servidores de vídeo e correspondentes câmeras.

4.2.1.29. Integração entre vídeo e controle de acesso e alarmes na lista de Transações

4.2.1.29.1. Cada controladora deverá permitir, no mínimo, duas câmeras relacionadas, uma vinculada à leitora de entrada, e uma vinculada à leitora de saída ou botoeira de saída. Essa vinculação deverá ser realizada pelo software de controle de acesso;

4.2.1.29.2. A câmera vinculada à leitora de entrada de uma controladora também deverá estar relacionada aos alarmes provenientes das entradas de sensores, ou dos eventos desta controladora, tais como sensor de status de porta, sensor de tamper, entrada de integração com sistema de incêndio, etc.;

4.2.1.29.3. O sistema deverá permitir a chamada de vídeo ao vivo ao se clicar sobre o evento na Lista de Transações, onde se chama um pop-up de janela do navegador web;

4.2.1.29.4. O sistema deverá permitir a chamada de vídeo gravado ao se clicar sobre o evento na Lista de Transações, onde se chama um pop-up de janela do navegador web (desde que esse vídeo gravado se encontre ainda armazenado no storage de vídeo do sistema de CFTV, e não tenha sido descartado ou reciclado). Este consiste em um clipe de vídeo que se apresenta pausado (para evitar consumo indevido de banda de transmissão de dados na rede Ethernet), e que pode ser ativado para que se visualize a gravação, clipe este relativo ao evento de acesso ou alarme proveniente da leitora e controladora relacionada. A precisão deste clipe é de suma importância para poder-se rapidamente relacionar, por exemplo, o acesso de um usuário com sua imagem no exato instante em que apresenta sua credencial. Para tanto, o servidor de controle de acesso e o(s) servidor(es) de vídeo vigilância deverá(ão) estar perfeitamente sincronizado(s) em tempo (sincronização NTP – Network Time Protocol);

4.2.1.29.5. O sistema deverá permitir a chamada simultânea, em um mesmo pop-up de janela do navegador web, do vídeo ao vivo na leitora de saída ao lado da imagem gravada no último acesso de entrada pela leitora de entrada (desde que esse vídeo gravado se encontre ainda armazenado no storage de vídeo do sistema de vídeo vigilância, e não tenha sido descartado ou reciclado), a fim de se poder comparar, instantaneamente, o usuário que utilizou um cartão para o acesso de entrada, e o mesmo cartão para acesso de saída;

4.2.1.29.6. Deverá ser possível a visualização de vídeo ao vivo ou clipe gravado (desde que esse vídeo gravado se encontre ainda armazenado no storage de vídeo do sistema de vídeo vigilância, e não tenha sido descartado ou reciclado) proveniente, no mínimo, dos seguintes eventos:

4.2.1.29.6.1. Acesso de Entrada Válido (câmera relacionada à leitora de entrada de uma controladora);

4.2.1.29.6.2. Acesso de Saída Válido (câmera relacionada à leitora de saída de uma controladora);

4.2.1.29.6.3. Acesso de Saída Válido (câmera relacionada à botoeira de requisição de saída de uma controladora);

4.2.1.29.6.4. Pulso por software para abertura de barreira – entrada ou saída por porta, catraca, etc.;

4.2.1.29.6.5. Alarme de Porta Forçada (câmera relacionada à leitora de entrada de uma controladora);

4.2.1.29.6.6. Alarme de Porta Deixada Aberta (câmera relacionada à leitora de entrada de uma controladora);

4.2.1.29.6.7. Alarme de Porta Deixada Aberta (sonoro do tipo buzzer que deve ser alocado dentro do ambiente seguro, em caixa controladora com chave). O sinal sonoro ficará ligado até que a porta seja fechada;

4.2.1.29.6.8. Alarme de Cartão Desconhecido – tentativa de utilização de cartão não cadastrado no sistema (câmera relacionada à leitora de entrada de uma controladora);

4.2.1.29.6.9. Alarme de Zona de Horário Incorreta – tentativa de utilização de cartão fora de seu nível de acesso (câmera relacionada à leitora de entrada de uma controladora);

4.2.1.29.6.10. Alarme de corte de energia da controladora;
4.2.1.29.6.11. Alarme de bateria baixa da controladora;
4.2.1.29.6.12. E todos os eventos ou alarmes originados por uma controladora de acesso;
4.2.1.29.6.13. O sistema deverá permitir a implantação de faixas horárias em que não será feito o controle, como manter a porta aberta durante horário de expediente (por controladora de interesse).

4.2.1.30. Integração entre vídeo e acesso e alarmes no Mapa Sinótico

4.2.1.30.1. O mapa sinótico do sistema de controle de acesso deverá permitir a inclusão de ícones das câmeras vinculadas, a fim de se chamar o vídeo ao vivo da câmera desejada com um duplo clique do botão esquerdo do mouse sobre o ícone da câmera correspondente. Assim, quando se faz presente uma camada de mapa sinótico, onde um ícone de porta ou sensor de alarme esteja ativado (piscando), ou até desativado, pode-se trazer o vídeo ao vivo clicando-se sobre o ícone de câmera mais próxima.

4.2.1.31. Integração entre vídeo e acesso e alarmes em Relatórios de Transações

4.2.1.31.1. Quando se faz uso dos relatórios de transações do sistema, deverá ser possível recuperar o vídeo gravado da câmera vinculada à leitora de entrada de uma controladora (desde que esse vídeo gravado se encontre ainda armazenado no storage de vídeo do sistema de vídeo vigilância, e não tenha sido descartado ou reciclado), de qualquer transação que possa ser filtrada no sistema (no mínimo as seguintes transações: acesso de entrada válida, acesso de saída válida, zona de horário incorreta, cartão desconhecido, porta forçada, porta deixada aberta, alarme de tamper, problema na leitora de entrada, problema na leitora de saída, bateria baixa, corte de energia, zona de alarme ativada, pulsar para abrir barreira, etc.).

4.2.1.32. Integração de CFTV via Metadados

4.2.1.32.1. O sistema deve possuir um servidor de Metadados (XML), para permitir a integração via Metadados com sistemas de circuito fechado de TV de terceiros, de modo que todas as transações provenientes das Controladoras de Acesso sejam enviadas ao Sistema de CFTV, podendo ser escritas sobre imagens de uma ou mais câmeras selecionadas, bem como criando regras e ações específicas para determinadas transações, tais como apresentação de mensagens customizadas sobre as imagens de câmeras, acionamento de presets, envio de SMS, envio de email, popup de câmeras, popup de E-map, acionamento de relés, envio de frames de imagens para FTP, acionamento de mensagem sonora e envio de notificação para central de monitoramento.

4.2.1.33. Integração com Alarme de Incêndio

4.2.1.33.1. Deve possuir função de integração com sistemas de incêndio de terceiros, através de uma entrada digital no hardware da controladora. A controladora, ao receber, nesta entrada digital, sinal proveniente de um módulo da rede da central de incêndio de terceiros, comunica-se peer-to-peer (ponto a ponto) com outras controladoras de seu grupo, através da rede Ethernet, desativando a função de segurança das controladoras e liberando todas as fechaduras e/ou barreiras agrupadas, até que o operador as rearme novamente, pelo sistema.

4.2.1.33.2. A Integração com o módulo de alarme de incêndio, deve permanecer funcionando de forma integral sem a necessidade do Aplicativo de Controle de Acesso estar on-line, ou seja, independentemente do PC

Servidor e aplicativo de Controle de Acesso, no caso dos servidores estarem desligados ou fora da rede.

4.2.1.33.3. De modo a facilitar a integração com o sistema de alarme de incêndio, o sistema de controle de acesso deverá permitir que o operador crie diferentes rotas de incêndio, sendo controlada cada uma delas por um único contato seco, diminuindo os gastos com infraestrutura e cabeamento.

4.2.1.34. Gerenciamento de Visitantes

4.2.1.34.1. O sistema deve possuir um módulo para o gerenciamento de visitantes, totalmente integrado ao software de controle de acesso.

4.2.1.34.2. O sistema deve permitir:

4.2.1.34.2.1. Cadastrar os visitantes com até 5 fotos (Ex: foto do visitante, documento frente e verso, foto do veículo, foto de Nota Fiscal, etc);

4.2.1.34.2.2. Cadastrar os dados de endereço, empresa, contato de emergência dos visitantes, placa do veículo e motivo da visita;

4.2.1.34.2.3. Permitir o acesso de diferentes níveis de acesso a diferentes visitantes;

4.2.1.34.2.4. Gerenciar e rastrear rapidamente os visitantes;

4.2.1.34.2.5. Cadastrar os ativos que acompanham o visitante (cadastro de bens);

4.2.1.34.2.6. Criar diferentes de níveis de permissão para os operadores do software (cada operador poderá conceder determinados níveis de acesso a visitantes enquanto que outros níveis de acesso lhe serão negados);

4.2.1.34.2.7. Cadastrar \ Liberar os Cartões Provisórios dos colaboradores;

4.2.1.34.3. Possuir a opção de integração com o módulo de Agendamento de Visitantes;

4.2.1.34.4. Possuir o módulo de impressão de crachás com os dados do visitante;

4.2.1.34.5. Possuir relatório Gerenciais e do Histórico dos visitantes;

4.2.1.34.6. Possuir o histórico dos dados dos visitantes, para que quando o mesmo retorne; através do número do documento ou nome informado anteriormente, o sistema busque as informações para que não haja um retrabalho de digitação nas portarias \ recepções;

4.2.1.34.7. Possuir a função de Baixa Automática de Cartões de Visitantes: ao se depositar um cartão de visitantes em uma urna coletora de cartões, o cartão deve ser automaticamente apagado da controladora em questão, bem como de todas as controladoras que pertençam ao mesmo grupo de baixa (programável), ou através da rotina de expiração com dia e hora de validade.

4.2.1.34.8. A Baixa Automática dos Cartões de Visitantes, deve permanecer funcionando de forma integral sem a necessidade do Aplicativo de Controle de Acesso estar on-line, ou seja, independentemente do PC Servidor e aplicativo de Controle de Acesso, no caso dos servidores estarem desligados ou fora da rede.

4.2.2. Marcas de referência: Axxon, Lenel e Tyco.

5. Descrição dos serviços

5.1. A presente descrição trata dos serviços de instalação de infraestrutura e cabeamento estruturado para interligação dos sistemas de CFTV e Controle de Acesso, contemplando a instalação, configuração e ativação dos equipamentos alocados no Data Center e salas de

lógica, onde estarão alocados os switches.

5.2. A obra deverá ser executada em duas fases, conforme cronograma contido no Projeto Básico. A Fase 1, consiste na implantação dos sistemas no Edifício Sede, localizado na Rua Duque de Caxias n. 350 e a Fase 2 no Edifício Assis Brasil, localizado na Rua Sete de Setembro n. 730, incluindo o remanejamento da Central de Monitoramento do Edifício Sede para o Edifício Assis Brasil. Cabe ressaltar a necessidade de realização de configuração e de testes no circuito de fibra óptica que fará a interligação entre os dois edifícios do TRE-RS.

5.3. **Instalação, Configuração e Ativação do Sistema**

5.3.1. A instalação do sistema deverá iniciar com a construção de toda a infraestrutura (eletrodutos, eletrocalhas, etc.) para acomodação de todo o cabeamento lógico. Após construção da infraestrutura a empresa executora deverá de forma concomitantemente executar a passagem dos cabeamentos e instalação dos equipamentos (câmeras, controladoras, servidor, entre outros).

5.3.2. A contratada deverá fornecer relatório de certificação dos cabos de rede extraído de equipamento scanner profissional, bem como relatórios de certificação dos equipamentos instalados.

5.3.3. Após instalação física dos equipamentos a empresa executora deverá testar todos os equipamentos antes de suas ativações. É recomendado que todos os equipamentos devam ser configurados “in-loco”.

5.3.4. Após ativação do sistema a empresa executora deverá iniciar a etapa de treinamento imediata aos operadores do sistema.

5.4. Instalação de Câmera Interna

5.4.1. Instalação de Câmera Interna devidamente fixada com parafusos e buchas (com contrachapa adequada na forração).

5.4.2. A empresa executora deverá construir infraestrutura adequada, conforme a necessidade de cada ponto, através de prolongamento ou derivação da infraestrutura existente, mantendo o padrão instalado.

5.4.3. Cada câmera deverá acompanhar kit de instalação com buchas e parafusos, suporte quando necessário e caixa para acomodação de rabicho quando estes ficarem aparentes.

5.4.4. As câmeras deverão ser posicionadas e ajustadas conforme o ambiente de modo a cobrir a maior área de imagem ou local específico de interesse, que deve ser definido em conjunto com a contratante.

5.4.5. As novas câmeras deverão ser instaladas priorizando os locais externos, elevadores e de maior movimento. Câmeras existentes nestes ambientes deverão ser realocadas para outros ambientes (Seguir diagrama dos Anexos VII e VIII).

5.4.6. As câmeras que substituirão outras câmeras deverão ser posicionadas nos locais de origem das substituídas ou, quando solicitado pelo TRE-RS, em locais novos, após verificada a viabilidade técnica e de funcionamento.

5.4.7. Todas as câmeras deverão receber limpeza e eventual ajuste se necessário após instalação. As câmeras existentes deverão receber manutenção atendendo aos seguintes itens:

5.4.7.1. Verificar imagens de modo a identificar possíveis falhas: foco, interferência, resolução, contraste, cores e enquadramento;

5.4.7.2. Realizar limpeza das lentes e do exterior das câmeras.

5.4.8. Verificar a tensão de alimentação elétrica, aterramentos e fixação, visando sua proteção e longevidade.

5.5. Instalação de Câmera Externa

5.5.1. Instalação de Câmera Externa com necessidade de utilização de andaime ou sexto aéreo. A câmera deverá ser devidamente fixada com parafusos e buchas ou suporte de fixação conforme necessidade. Deverá ser posicionada de acordo com o ambiente e de forma que priorize a maior cobertura de imagem ou ponto específico de interesse.

5.5.2. A empresa executora deverá construir infraestrutura adequada, conforme a necessidade de cada ponto, através de prolongamento ou derivação da infraestrutura existente, mantendo o padrão instalado.

5.5.3. Em particular, a câmera externa Fisheye 1, do edifício Sede, deverá receber alimentação elétrica e de dados através de cabeamento percorrendo o mesmo caminho da câmera speed dome a ser substituída pela mesma, descendo externamente pelo prédio até o 3° pavimento onde será fixada e posicionada com suporte prolongador.

5.5.4. Nas câmeras externas do prédio Sede também deve ser revisada a impermeabilização contra umidade.

5.6. Instalação de Conjunto de Controladora de Porta

5.6.1. Instalação de placa controladora para portas com equipamentos, tais como: caixa de sobrepor com contra chapa, bateria selada, fonte de alimentação integrada (mínimo de 2A em 12 VCC) e supervisionada, carregador flutuante de bateria, buzzer, eletroímã para portas de vidro e corta-fogo e trava eletromecânica para as portas dos shaft no Edifício Assis Brasil, acionador de emergência rearmável, placa de instrução de Saída de Emergência, leitor de cartões, botão de abertura para saída, bem como kit de instalação (eletroduto ou eletrocalha, buchas e parafusos para fixação); versões de controladoras de acesso com alimentação via PoE (Power over Ethernet). Todas estas controladoras deverão funcionar na mesma rede TCP/IP, simultaneamente, conforme a alternativa de solução mais rápida e prática para ampliação do sistema.

5.6.2. Para cada controladora de porta deverá acompanhar kit de instalação de equipamentos, tais como: caixa de sobrepor com contra chapa para a controladora, bateria selada, fonte de alimentação e buzzer, eletroímã (trava eletromecânica para as portas dos *shaft* no Edifício Assis Brasil), acionador de emergência rearmável, placa de instrução de Saída de Emergência, leitor de cartões, botão de abertura para saída, bem como buchas e parafusos para fixação.

5.6.3. Todos os dados e regras de negócio deverão permanecer na memória da controladora de forma definitiva, e em caso de queda de energia, não poderão se perder. O equipamento deve trabalhar de forma autônoma ou em rede, provendo o acesso a quem cotidianamente utiliza-se do sistema.

5.6.4. Cablagem e Observações Relacionadas

5.6.4.1. Para conexão das controladoras à rede Ethernet TCP/IP, devem ser seguidas as regras e normas de cabeamento estruturado. No prédio Sede deve ser instalado cabo do *switch* instalado no 1º pavimento até o respectivo ponto de instalação da controladora, no edifício Assis Brasil o cabo deve ser instalado a partir do *switch* do respectivo andar até a controladora, salvo os equipamentos acima do 15º pavimento que devem ser conectados no *switch* do 15º pavimento.

5.6.4.2. Para conexões entre as controladoras e as leitoras.

5.6.4.2.1. É recomendado cabo tipo Belden 18 AWG.

5.6.4.2.2. Para conexões entre as controladoras e as fechaduras, devem ser considerados no mínimo os seguintes parâmetros: tensão e corrente de consumo da fechadura, tipo de fechadura (falha-aberta ou falha-fechada),

distância entre controladora e fechadura, número de fechaduras conectadas.

5.6.5. A empresa executora deverá construir infraestrutura adequada, conforme a necessidade de cada ponto, através de prolongamento ou derivação da infraestrutura existente, mantendo o padrão instalado.

5.6.6. As placas controladoras e alimentação redundante devem ser instaladas em gabinetes de proteção, preferencialmente sobre a porta (na forração) a ser controlada.

5.6.7. Os leitores de proximidade e botoeiras devem ser instalados diretamente sobre as paredes (de alvenaria, alumínio ou divisórias).

5.6.8. As conexões entre a placa controladora e seus periféricos (fecho eletromagnético, leitores de proximidade e botoeira) devem estar protegidas (por eletrodutos ou canaletas) que impeçam violações, devendo respeitar o *desing* do ambiente em que serão instalados.

5.6.9. Devem ser feitos os ajustes nas fechaduras das portas para permitir a operação conforme requisitos de controle do sistema.

5.6.10. O contratante disponibilizará ponto de elétrica 110V e de lógica próximo às portas, sobre o forro (onde houver) para as conexões.

5.6.11. Os acabamentos devem respeitar o padrão do ambiente de instalação de cada porta.

5.7. Instalação de Leitor UHF

5.7.1. Instalação de Leitor UHF em parede. Deverá acompanhar suporte de fixação com bucha e parafusos.

5.7.2. A empresa executora deverá construir infraestrutura adequada, conforme a necessidade de cada ponto, através de prolongamento ou derivação da infraestrutura existente, mantendo o padrão instalado.

5.7.3. O direcionamento da cobertura deve ser para o ponto de interesse indicado pelo contratante.

5.7.4. Configurar a sirene/buzzer para indicar a passagem de cartão não autorizado, bem como alerta na central de monitoramento. O sinal sonoro deve ser de 5 segundos para que o funcionário seja alertado para solicitar a devolução do cartão se a antena estiver localizada em área de saída.

5.8. Instalação de Urna Coletora

5.8.1. Instalação de Urna Coletora acompanhada de leitor de proximidade, bem como suporte de fixação em parede ou piso, conforme necessidade, parafusos e buchas.

5.8.2. A empresa executora deverá construir infraestrutura adequada, conforme a necessidade de cada ponto, através de prolongamento ou derivação da infraestrutura existente, mantendo o padrão instalado.

5.8.3. Cada urna coletora terá instalado na mesma rota de saída um leitor de proximidade RFID, bem como suporte de fixação em parede. Deverão ser instaladas antes da porta de saída, não podendo estar dentro da área de cobertura do leitor de UHF. O visitante deverá depositar o cartão na urna coletora antes de sair, caso o procedimento não seja executado, ao passar na área de cobertura do leitor UHF, uma sirene/buzzer deverá ser acionado durante 5 segundos para que um funcionário solicite a devolução do cartão.

5.9. Instalação de catracas

5.9.1. Cada catraca deverá acompanhar os seguintes materiais: placa controladora, urna coletora, leitor de proximidade RFID para urna coletora, acionador de emergência rearmável e catraca, bem como chumbadores para fixação.

5.9.2. Na instalação devem ser respeitados os detalhes das plantas constantes no Anexo VI.
5.9.3. Os acabamentos devem respeitar o padrão do ambiente em que serão instaladas.
5.9.4. As catracas existentes deverão ser removidas para a instalação das novas.

5.10. Instalação da impressora de cartões

5.10.1. Os serviços incluem a instalação dos drives da impressora, bem como os ajustes para permitir a impressão a partir da solução instalada.

5.10.2. O sistema deve permitir a impressão do crachá a partir do sistema de cadastramento com a seleção dos campos de impressão conforme o grupo definido (servidor, estagiário, terceirizado, visitante).

5.11. Instalação das conexões lógicas e certificações de pontos

5.11.1. No edifício Sede, a contratada deverá revisar todos os pontos de conexão lógica do sistema existente a partir dos switches, substituindo todos os cabos e RJ-45 (Cat 5e) por novos com a devida crimpagem. As demais conexões necessárias devem ser construídas com cabo e conectores Cat6 já especificados.

5.11.2. As conexões das câmeras dos elevadores devem ser obrigatoriamente substituídas por cabo apropriado para elevador.

5.11.3. A substituição da conexão lógica nos elevadores deve ser agendada com a empresa responsável pela manutenção dos elevadores.

5.11.4. No edifício Sede realizar as crimpagens nos pacth painel do sistema das conexões lógicas entre os equipamentos do sistema, identificando devidamente as conexões.

5.11.5. Todos os pontos de lógica devem ser certificados.

5.11.6. A certificação deve ser na capacidade máxima do cabo (10G ou 1G).

5.11.7. No edifício Sede esta certificação deve incluir as conexões entre os switches.

5.11.8. Após a instalação e configuração dos equipamentos, os mesmos devem estar ativos em modo operacional para uso do TRE-RS, sendo que os softwares instalados deverão ser disponibilizados em sua melhor configuração tecnológica (última versão e upgrade de firmware).

5.12. Instalação dos servidores do sistema

5.12.1. Cada servidor deverá ser instalado fisicamente em rack 19", sobrepostos um sobre o outro, com a devida fixação individual por porca gaiola, instalação de seus equipamentos e acessórios, bem como a conexão dos cabos fornecidos seguindo as boas práticas de mercado. Realizar o start-up do equipamento executando as atualizações de softwares, patches, drivers e firmwares para suas mais recentes versões suportadas. Realizar a ativação e configurar o acesso de gerenciamento remoto do equipamento. Realizar testes de verificação no término da instalação. Antes da execução do serviço, a empresa contratada deve preparar um planejamento das tarefas a serem executadas e submeter à aprovação prévia da contratante, em prazo mínimo de 3 (três) dias úteis antes da data prevista de início do serviço. No planejamento deverá ser priorizada a manutenção das principais atividades e serviços de TI mantidos pela contratante. A execução deverá ser realizada, na medida do possível, no horário comercial. O planejamento do serviço deverá listar todas as atividades a serem desenvolvidas em cada dia programado e deve considerar ainda a possibilidade de eventuais paradas de serviço não programadas, sendo que nesse caso caberá à contratada colaborar junto com a contratante para o restabelecimento imediato do serviço. A contratada deve ser responsável pela execução e qualidade do serviço, indicando o responsável técnico pela realização do hands-on, assim como aquele que realizará a instalação do equipamento. A Contratada deverá entregar

documentação detalhando configurações, esquema de conexões e procedimentos realizados.
A instalação inclui a conexão lógica (cordão óptico) com os switches do contratante. Também deve, junto com a equipe de TI do contratante, ser procedida a configuração de VLAN específica da solução na rede do contratante (interconexão a partir do Datacenter com o switch do sistema no 1º andar do edifício Sede e pontos de lógica nos switches de cada pavimento no prédio Assis Brasil).

5.13. Instalação dos switches (Edifício Sede)

5.13.1. Dois switches, existentes no edifício Sede, deverão ser substituídos pelos novos, com a organização dos cabos de manobra. A contratada deve proceder à desconexão e remoção dos switches a serem substituídos, afixação dos novos switches na mesma posição, conexão às redes elétrica e lógica do local e ativação dos componentes. Deve, também, proceder à verificação das condições básicas de funcionamento, estabelecendo o estado operacional da rede local.

5.14. Instalação de infraestrutura

5.14.1. Condulete

5.14.1.1. Os conduletes ou caixa de terminação metálica para infraestrutura de eletrodutos deverão ser instalados a cada lance de 6 metros de eletroduto, incluindo curvas, subidas e descidas e desvios.

5.14.1.2. Os eletrodutos deverão ser conectados aos conduletes através de conectores retos de alumínio 3/4" ou 1" sem rosca fornecidos com parafusos e arruelas. Deverão estar incluídos na proposta todos os acessórios de fixação bem como as respectivas tampas de proteção.

5.14.2. Conexões

5.14.2.1. As emendas dos eletrodutos só serão permitidas com o emprego de conexões apropriadas, tais como luvas ou outras pecas que assegurem a regularidade da superfície interna, bem como a continuidade elétrica.

5.14.2.2. Deverão ser utilizadas graxas especiais nas roscas, a fim de facilitar as conexões e evitar a corrosão, sem que fique prejudicada a continuidade elétrica.

5.14.3. Caixas de Passagem

5.14.3.1. Deverão ser empregadas caixas de passagem nos seguintes casos:

5.14.3.1.1. Em todos os pontos de entrada ou saída dos eletrodutos, exceto na transição de linhas abertas através de dutos.

5.14.3.1.2. Em todos os pontos de emenda ou derivação dos condutores.

5.14.3.1.3. Em todos os pontos de confluência e derivações dos eletrodutos.

5.14.3.1.4. Em todos os pontos de instalações de dispositivos ou equipamentos.

5.15. Instalação e configuração das estações de monitoramento e cadastramento

5.15.1. Instalação das estações em locais próprios (mesa ou escrivaninha existente) nos locais indicados.

5.15.2. Efetuar a montagem dos componentes e acessórios para o seu perfeito funcionamento.

5.15.3. Configuração do sistema operacional e softwares, bem como a licença da solução.

5.16. Configuração de leiaute de cartões para impressão

5.16.1. Realizar a configuração de leiautes (cinco) de impressão de crachás para terceirizados e visitantes a partir do software disponibilizado.
5.16.2. Os cartões terão formatação similar aos atualmente utilizados com indicação dos campos obrigatórios pelo Gestor do contrato.
5.16.3. O crachá dos servidores deve ter na frente fundo variando da cor branca ao azul marinho e conter o brasão da república, inscrição TRE-RS, foto do servidor, designação (principal nome destacado), nome completo e cargo e, no verso (fundo branco), título de eleitor, matrícula e código de barras respectivo.
5.16.4. O crachá dos terceirizados deve conter na frente o brasão da república, inscrição TRE-RS, foto do profissional, designação (principal nome destacado), nome completo e empresa contratada e, no verso, número do registro no cadastro e código de barras respectivo.
5.16.5. O Crachá dos visitantes deve conter na frente o brasão da república, inscrição TRE-RS, indicação "Visitante", tarja colorida (vermelho, laranja ou, azul).

5.17. Treinamento

5.17.1. Prever o mínimo de 12 (doze) horas/aula, distribuído nos seguintes módulos:
5.17.1.1. Módulo 1 - 04 (quatro) turmas de operadores de estações de cadastramento - tipo HandsOn - 01 (uma) hora de treinamento para cada turma.
5.17.1.2. Módulo 2 - 01 (uma) turma de operadores de estação de monitoramento e responsáveis para impressão de crachás - tipo HandsOn - 02 (duas) horas de treinamento.
5.17.1.3. Módulo 3 - 01 (uma) turma de administradores do sistema e equipe técnica de TI com 06 (seis) horas de treinamento.
5.17.2. O treinamento deve abranger, no mínimo, os seguintes tópicos:
5.17.2.1. Para administradores do sistema - aspectos de arquitetura, instalação, configuração, operação, restore do banco de dados, cadastramento de perfis, personalização (customização/parametrização) do sistema, emissão de relatórios, manutenção, necessária.
5.17.2.2. Para operadores das estações de monitoramento e responsáveis pela impressão dos cartões - confecção, impressão de cartões, operação de todas as funcionalidades relativas a credenciamento de pessoas e emissão de relatórios. Deve abranger também as principais funcionalidades do sistema, incluídndo alteração da planta, lotação de servidores e parametrização de itinerários de liberação de acesso.
5.17.2.3. Para operadores de estações de cadastramento - o cadastramento de visitantes, consulta ao cadastro de visitantes já existentes, consulta aos credenciamentos dos servidores, estagiários, prestadores de serviços e terceirizados.
5.17.3. Cada turma terá até 8 participantes.
5.17.4. Para todos os treinamentos, devem ser entregues materiais didáticos impressos (dois conjuntos por módulo de treinamento) para acopanhamento e disponibilizados em mídia, em português.
5.17.5. A contratada deverá agendar com o gestor do contrato a data de início do treinamento e a distribuição da carga horária, com antecedência mínima de 5 dias.
5.17.6. Para todos os treinamentos, devem ser entregues materiais didáticos impressos (dois conjuntos por módulo de treinamento) e disponibilizados em mídia, em português.
5.17.7. Autorizar filmagem do treinamento para posterior consulta dos participantes.
5.17.8. O treinamento ocorrerá na cidade de Porto Alegre, RS, nas dependências do

contratante, em endereço a ser definido pelo Gestor do contrato e preparado pela contratada.

5.18. Documentação para Entrega do Sistema

5.18.1. Projeto "As Built" da solução instalada, abrangendo todos os dispositivos, e configurações integrantes do sistema, incluindo:

5.18.1.1. Diagrama lógico da solução indicando as conexões com as devidas identificações.

5.18.1.2. Mapeamento dos IP da rede e equipamentos da solução, com a respectiva senha (se aplicável).

5.18.1.3. Manual do administrador do sistema.

5.18.1.4. Guia de referência do sistema em duas vias.

5.18.1.5. Manual do usuário, com seções próprias a cada perfil de usuário (administrador, operador de estação de monitoramento, operador de cadastramento) em duas vias.

5.18.1.6. Guia de consulta rápida para operador de estação de cadastramento e operador de estação de monitoramento em quatro vias.

5.18.1.7. Guia de consulta rápida para o administrador do sistema.

5.18.1.8. Catalogação das rotinas configuradas, processadas e mapeadas na solução.

5.18.1.9. Entrega de manual(is) e/ou documentação técnica de cada equipamento fornecido, em mídia impressa e/ou digital, preferencialmente em português.

5.18.1.10. Entrega de todos os comprovantes das licenças de uso definitivo incluindo os números de registro, códigos e/ou chaves necessários para instalação dos softwares.

5.18.1.11. Entrega de manual(is) e/ou documentação de cada software fornecido, para o usuário final (utilização do software) e para a equipe de suporte técnico (instalação, configuração, atualização, backup e outros), em mídia impressa e/ou digital, preferencialmente em português.

5.18.1.12. ART de execução "As-Built" da respectiva fase, devidamente quitada e assinada pelo responsável técnico da obra.

5.19. Garantia e Manutenção Preventiva e Corretiva do Sistema

5.19.1. Os serviços de manutenção e assistência técnica deverão ser prestados na modalidade on-site (para os casos em que houver necessidade de intervenção física no equipamento, inclusive para troca de peças), nas dependências TRE-RS.

5.19.2. A cada 06 (seis) meses a contar do recebimento definitivo, independentemente de acionamento de suporte, a contratada deve realizar obrigatoriamente visita de manutenção preventiva quando deve ser revista a integridade da solução e corrigidos bugs do sistema, bem como implementadas as atualizações disponibilizadas.

5.19.3. A contratada poderá realizar visitas de manutenção preventiva em períodos reduzidos mediante agendamento com o gestor do contrato quando entender necessário.

5.19.4. O suporte técnico, local (on-site), compreende o atendimento de incidentes, esclarecimento de dúvidas, a manutenção preventiva e corretiva dos equipamentos em garantia e a manutenção corretiva e evolutiva do software de controle de acesso e sistema de CFTV.

5.19.5. A solução de controle de acesso e sistema de CFTV deverão ter garantia de 48 (quarenta e oito) meses em relação aos equipamentos e softwares fornecidos pela contratada.

5.19.6. Durante todo o período de garantia, a contratada deve prestar suporte técnico, por mão de obra qualificada, com reposição de equipamentos, peças, acessórios e para os serviços solicitados, sem ônus adicional ao contratante;

5.19.7. A contratada deve oferecer garantia 5X7, on-site, para os equipamentos e funcionalidades da solução.

5.19.8. Acordo de nível de serviço:

5.19.8.1. A classificação de uma solicitação de suporte a um incidente deverá estar de acordo com o estabelecido na tabela a seguir:

Nível	Urgência de Atendimento	Tipo de incidente
1	Alta	- parada total do sistema - parada total da solução em software - parada do cadastramento de todas as posições de uma planta (edifício)
2	Média	- controle em porta inoperante - parada do credenciamento - câmera fora do ar
3	Baixa	- parada de uma estação de cadastramento ou monitoramento (quando houver mais de uma no acesso) - interrupção de uma funcionalidade específica da solução em software

5.19.8.2. Para a solução de problemas, após o chamado, a contratada deverá respeitar os prazos máximos descritos a seguir:

Nível	Urgência	Atendimento/Solução	Prazo Máximo
1	Alta	Início do atendimento	1 dia útil
		Solução do incidente sem troca de peça	1 dia útil
		Solução do incidente com troca de peça	2 dias úteis
2	Média	Início do atendimento	1 dia útil
		Solução do incidente sem troca de peça	2 dias úteis

		Solução do incidente com troca de peça	3 dias úteis
3	Baixa	Início do atendimento	2 dias úteis
		Solução do incidente sem troca de peça	3 dias úteis
		Solução do incidente com troca de peça	4 dias úteis

5.19.8.3. Em caso de necessidade de troca de equipamentos e não tendo equipamento novo disponível, a contratada deverá disponibilizar equipamento com funcionalidades equivalente nos prazos acima estabelecidos e proceder a troca por novo no prazo máximo de 45 (quarenta e cinco dias).

5.19.8.4. Os chamados poderão ser abertos através de telefone ou aplicativo web.

5.19.8.5. Os prazos máximos contam da abertura do chamado.

5.19.8.6. Durante a garantia, o contratante deverá ter direito ao:

5.19.8.6.1. Acesso às atualizações regulares de software disponíveis.

5.19.8.6.2. Acesso às últimas correções de bugs e erros de segurança.

5.20. Desinstalação de sistema atualmente instalado

5.20.1. O TRE-RS possui atualmente um sistema com tecnologia instalado no edifício Sede, sendo responsabilidade da contratada a desativação deste sistema.

5.20.2. Em virtude da impossibilidade da interrupção de sua operacionalidade, na medida do possível, os equipamentos existentes permanecerão trabalhando em paralelo com o novo sistema ate a execução dos testes finais de recebimento.

5.20.3. Apos este período, a contratada deverá executar a desativação, a remoção e embalagem de todo material do sistema antigo (câmeras, matrizes de vídeo, monitores, DVRs, cabeamento, eletrodutos, suportes, etc.) bem como sua entrega a contratante.

5.21. Croquis de instalação

5.21.1. Layout dos Pontos de Monitoramento.

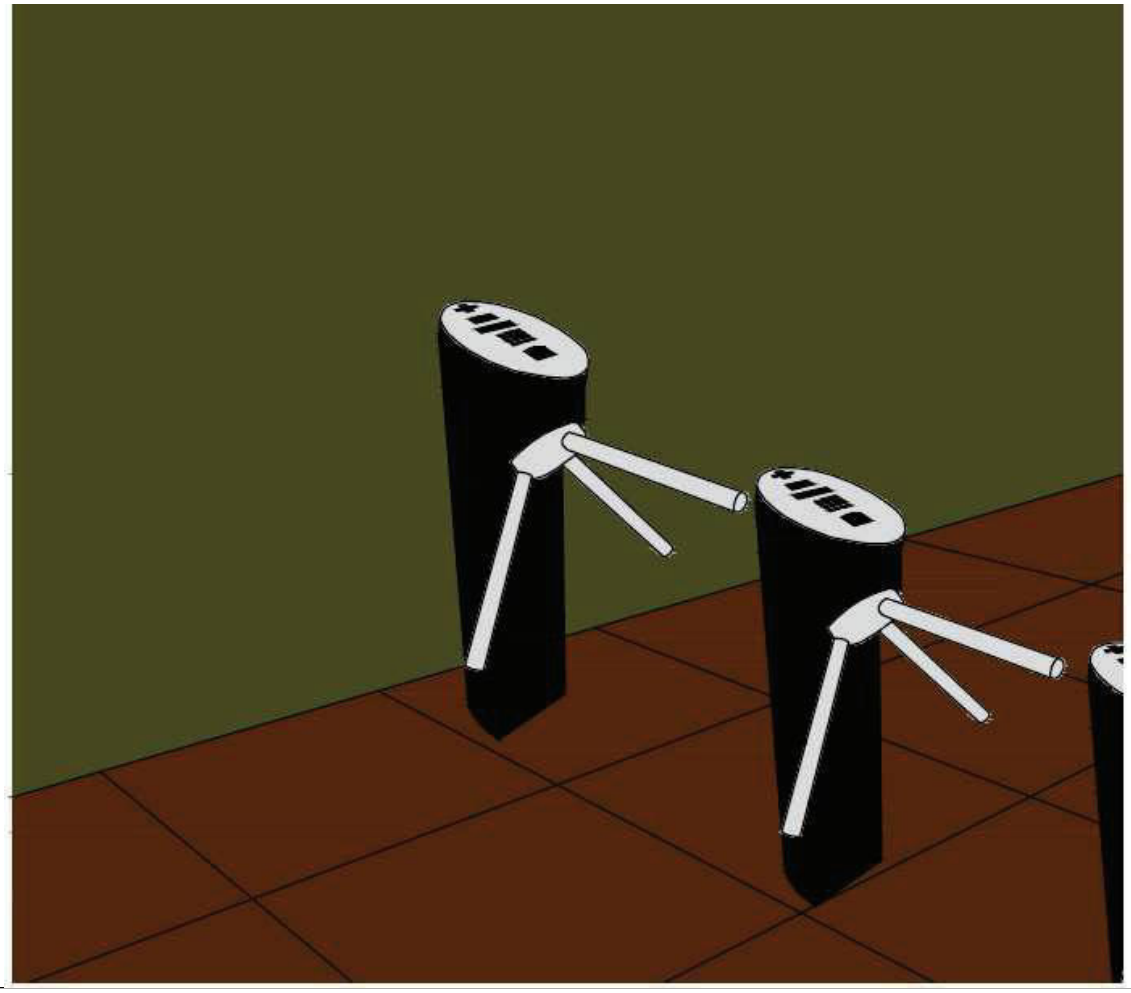
5.21.2. Layout das Catracas.

5.21.3. Layout das Controladoras de Portas.

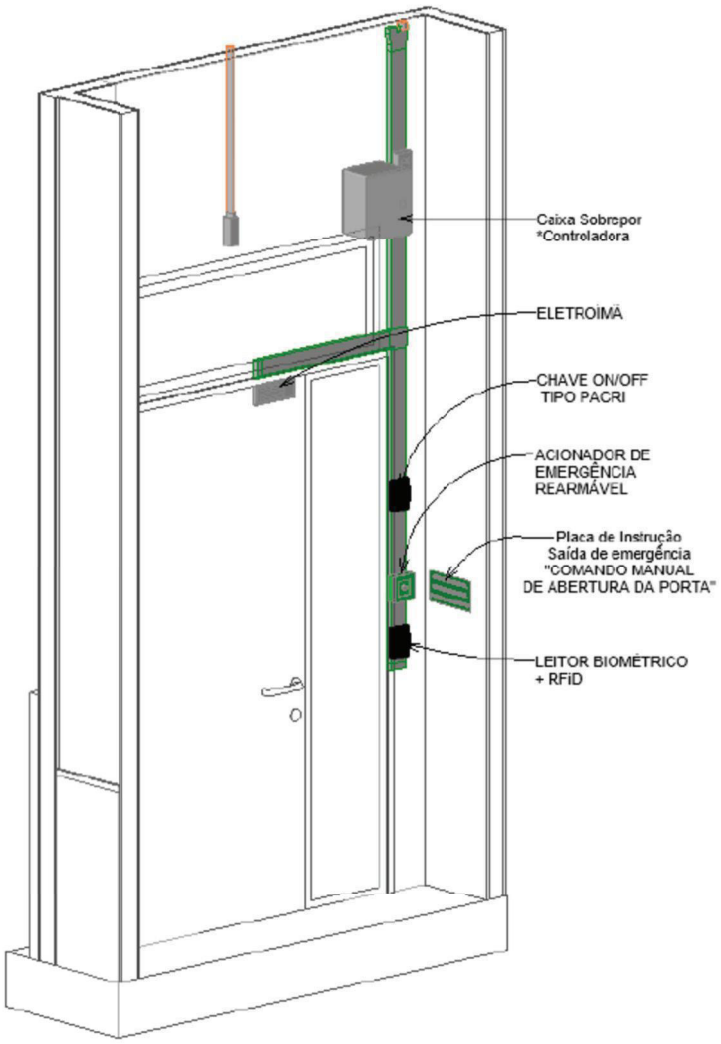
5.21.4. Layout da Central de Monitoramento.

5.21.5. Layout do Rack no Data Center.

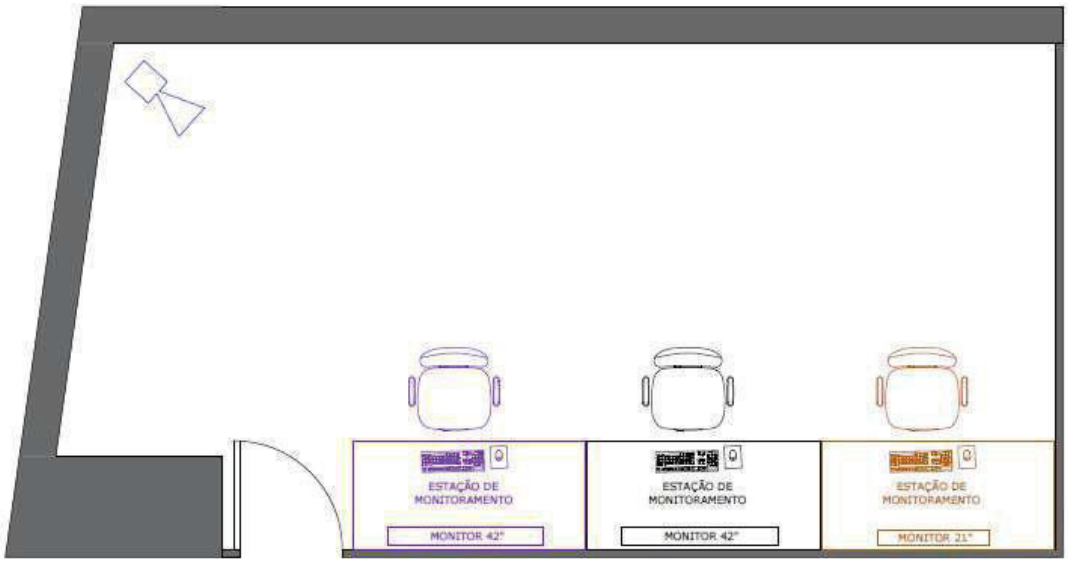
Layout dos Pontos de Monitoramento



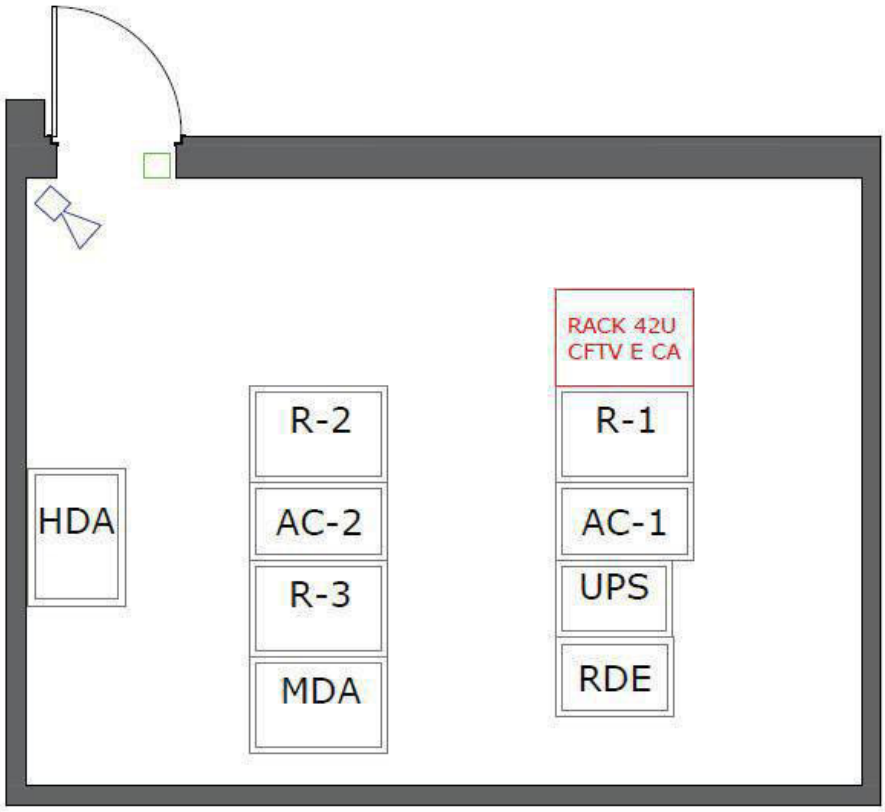
Layout das Catracas



Layout das Controladoras de Portas



Layout da Central de Monitoramento



Layout do Rack no Data Center

6. Administração da obra

6.1. A empresa contratada deverá manter uma equipe administrativa na obra contendo no mínimo:

6.1.1. Técnico em Eletrônica/Eletrotécnica: A contratada deverá manter na obra em regime integral um profissional habilitado.

6.1.2. Técnico em Segurança do Trabalho: A contratada deverá manter na obra em regime integral um profissional habilitado.

6.1.3. Responsável Técnico pela instalação: A contratada deverá manter na obra em regime de tempo parcial, conforme necessidade.

7. Normas e padrões de referência

7.1. Todo e qualquer serviço executado será avaliado segundo o estabelecido neste memorial descritivo e nas normas e padrões de referência abaixo especificados.

7.2. Normas Nacionais

7.2.1. ABNT–NBR14565: Procedimentos Básicos para Elaboração de Projetos de Cabeamento e Telecomunicações para Rede Interna Estruturada.

7.2.2. ABNT–NBR5410: Instalações Elétricas de Baixa Tensão.

7.2.3. ABNT–NBR5419: Proteção de Edificações Contra Descargas Atmosféricas.

7.2.4. Prática Telebrás nº 565-001-800: Sinalização de obras.

7.2.5. Prática Telebrás nº 235-130-704: Especificação de postes de concreto seção circular e duplo T.

7.2.6. Prática Telebrás nº 235-130-600: Suplemento procedimentos de projeto linhas de postes.

7.2.7. Recomendações dos fabricantes quanto a instalação de seus equipamentos.

7.3. Normas e Padrões Internacionais

7.3.1. IEEE 802: IEEE Standard for Local and Metropolitan Area Networks.

7.3.2. ANSI/TIA/EIA-568-B: Commercial Building Telecommunications.

7.3.3. ANSI/TIA/EIA-569-A: Commercial Building Standard.

7.3.4. ANSI/TIA/EIA-607: Commercial Building Grounding and Bonding.

7.3.5. ANSI/TIA/EIA-606: Administration Standard for the Cabling Standard.

7.3.6. Telecommunications Pathways and Spaces. Requirements for Telecommunications.

7.3.7. Telecommunications Infrastructure of Commercial Buildings.

8. Equipamentos de segurança

8.1. É de inteira responsabilidade da empresa executora a observação e adoção dos equipamentos de segurança que se fizerem necessários, conforme Normas Regulamentadoras (NR-6, NR-10 e NR-35), visando não permitir a ocorrência de danos físicos e materiais, não só com relação aos seus funcionários, como também, com relação a terceiros.

8.2. Também é de inteira responsabilidade da empresa executora a Sinalização de Segurança, tendo como objetivos:

8.2.1. Advertir quanto a risco de queda;

8.2.2. Alertar quanto a obrigação de uso do de EPI, específico para a atividade executada, com a devida sinalização e advertência próximas ao posto de trabalho;

8.2.3. Anexar cartazes indicando as saídas com setas;

8.2.4. Advertir contra perigo de área;

8.2.5. Usar fita zebrada para demarcação de área.

9. Avaliação técnica

9.1. O TRE-RS avaliará os hardwares e softwares que constituem a solução para verificação

de desempenho, qualidade e conformidade com as especificações técnicas do Projeto Básico.

10. Alteração de projeto executivo

10.1. O executor da obra, antes do início dos serviços, deverá analisar a viabilidade do projeto e discutir previamente com o responsável técnico do projeto executivo, os possíveis impedimentos e consequentes alterações do projeto. Estas alterações deverão ser também aprovadas pelo proprietário da obra.

10.2. Caso as alterações sejam permitidas, o executor deverá fornecer ao projetista o projeto "as-built" da obra para que as alterações sejam atualizadas no projeto.

11. Limpeza final da obra

11.1. Limpeza de todas as peças, devendo ser removida toda a poeira e quaisquer vestígios de tinta e argamassa.

11.2. Limpeza dos pisos entregando o mesmo em condições de utilização.

11.3. Remoção de todo entulho proveniente da obra para local fora do canteiro de obras, durante a execução, bem como no final da obra.

12. Memória de cálculo dos quantitativos a serem fornecidos, instalados, configurados

12.1. Edifício Sede

Nr O	Descrição	Referência	Referência de medida	Quantidade
01	Servidor de gerenciamento de vídeo		cj	01
	Conexão ótica com módulos Gbic		cj	02
	Acessórios de instalação		kit	01
02	Servidor de Controle de acesso - gerenciamento		cj	01
	Conexão ótica com módulos Gbic		cj	02
	Acessórios de instalação		kit	01
	Conexão ótica com módulos Gbic		cj	02
	Acessórios de instalação		kit	01
04	Switches PoE 24P		unid	02
	Patch panel 24P, com RJ-45 fêmea		unid	02
	Acessórios de instalação		kit	02
05	Patch cord		unid	42

06	Cabo UTP Cat6		m	1.240
	Cabo UTP Cat5e (ou superior) para elevador		m	245
	RJ-45 macho		unid	50
	Calha		m	12
	Acessórios de fixação e derivação calha		cj	1
	Eletroduto		m	35
	Acessórios de fixação e derivação eletroduto		cj	1
07	Certificações		unid	43
08	Câmeras fisheye		unid	2
	Suporte parede		unid	1
	Suporte poste		unid	1
	Acessórios de fixação		kit	2
09	Câmeras Dome		unid	14
	Acessórios de fixação		kit	14
10	Controladora datacenter – placa, leitor cartões, bateria, kit de instalação		cj	1
11	Controladora porta corta fogo – placa, gabinete, dois leitores de cartões, botão de saída, fecho eletromagnético		cj	1
	Conexões, eletrodutos e kit de instalação		cj	1
12	Antena RFID, com kit de fixação		cj	3
13	Urna coletora de cartões, com kit de fixação		cj	2
14	Estação de monitoramento		cj	2
15	Estações de cadastramento		cj	4
	Leitor de cartões de mesa (USB)		unid	4
	Webcam USB		unid	4

16	Impressora de cartões		unid	1
	Software de edição de leiaute de cartões		unid	1
	Ribbon		kit	3
	Cartão adesivo de limpeza		unid	10
17	Cartão		unid	1000
	Cordão personalizado com clip roller		unid	800
	Porta cartão		unid	1000
	Presilha plástica e prendedor tipo jacaré para porta cartão		unid	200
18	Licença software servidor – CFTV		unid	1
19	Licença software servidor – controle de acesso		unid	1
20	Licença software servidor – banco de dados		unid	1
21	Licença software para cliente – CFTV		unid	3
22	Licença software para cliente – controle de acesso		unid	6
23	Licença software – equipamento CFTV		unid	28
24	Licença software – equipamento controle de acesso		unid	7
25	Instalação de câmera externa		unid	2
26	Instalação/revisão de câmera interna		unid	26
27	Instalação de conjunto de controladora de porta		unid	2
28	Instalação de urna coletora de cartões		unid	2
29	Instalação de antena RFID		unid	3
30	Instalação de estação monitoramento		unid	2
31	Instalação de cadastramento		unid	4
32	Instalação de switch		unid	2

33	Instalação de servidor		unid	3
34	Interconexão com o sistema de incêndio		unid	1
35	Configuração do sistema		unid	1
25	Garantia		mês	48

12.2. Edifício Assis Brasil

Nr O	Descrição	Referência	Referência de medida	Quantidade
01	Cabo UTP Cat6		m	2320
	Cabo UTP Cat5e (ou superior) para elevador		m	300
	RJ-45 macho		unid	126
	Acessórios de fixação e derivação calha		cj	1
	Eletroduto		m	200
	Acessórios de fixação e derivação eletroduto		cj	1
02	Certificações		unid	126
03	Câmeras fisheye		unid	4
	Acessórios de fixação		kit	4
04	Câmeras Dome		unid	52
	Sensores de movimento		unid	3
	Acessórios de fixação		kit	52
05	Controladora porta corta fogo – placa, gabinete, dois leitores de cartões, botão de saída, fecho eletromagnético		cj	3
	Controladora porta madeira – placa, gabinete, dois leitores de cartões, botão de saída, fecho eletromagnético		cj	1
	Controladora porta vidro – placa, gabinete, dois leitores de cartões, botão de saída, fecho eletromagnético		cj	33

	Controladora porta madeira – placa, gabinete, dois leitores de cartões, botão de saída, fecho eletromecânico		cj	14
	Conexões, eletrodutos e kit de instalação		cj	51
06	Antena RFID, com kit de fixação		cj	2
07	Catraca Pivotante		cj	3
08	Catraca PNE		cj	1
09	Urna coletora de cartões, com kit de fixação		cj	2
10	Estação de monitoramento tipo 1 – placa três monitores		cj	2
11	Monitor 42” com cabo HDMI e suporte articulado		unid	4
	Suporte articulado		unid	4
	Cabo HDMI 10 m		unid	4
12	Estação de monitoramento tipo 2 – placa um monitor		cj	1
	Monitor 21 “		unid	1
13	Estações de cadastramento		cj	5
	Leitor de cartões de mesa (USB)		unid	5
	Webcam USB		unid	5
14	Licença software para cliente - cftv		unid	3
15	Licença software para cliente – controle de acesso		unid	5
16	Licença software – equipamento CFTV		unid	56
17	Licença software – equipamento controle de acesso		unid	59
18	Serviço de Interconexão com o sistema de incêndio		unid	1
19	Garantia		meses	48

Porto Alegre, 26 de maio de 2021.

FÁBIO BANDA ROLAND

Engenheiro Eletricista

CREA: RS 185070