MEMORIAL DESCRITIVO

EQUIPAMENTOS DE T.I.

1. INTRODUÇÃO

1.1. INFRAESTRUTURA LÓGICA

O cabeamento estruturado deverá ser realizado com fibra óptica e UTP CAT6 ou CAT6A blindada, identificados e acondicionados em eletrocalhas aramadas, devidamente organizados em dispositivos com arquitetura de alta densidade, disponíveis nos racks de distribuição.

- Painéis de Telecom para entrada de links externos;
- Eletrocalhas Aramadas;
- Cabeamento em fibra óptica e UTP CAT6/6A;
- Rack do core de rede e distribuição em cada pavimento.

1.2. AUTOMAÇÃO PREDIAL E SEGURANÇA ELETRÔNICA

Toda a edificação deverá ser monitorada 24/7 através de um circuito de CFTV sobre IP. O acesso aos ambientes deverá ser restrito através de um sistema integrado de controle de acesso digital. Além disso, deverá ser utilizada uma central de alarme para detecção de incêndio. A temperatura, umidade, iluminação, água e energia elétrica de cada ambiente deverão ser monitoradas através de sensores específicos. Todos esses sistemas poderão ser gerenciados através de um único sistema integrado de automação predial quando necessário, atendendo aos sistemas indicados abaixo:

- Circuito de CFTV;
- Controle de Acesso;
- Central de Alarme com sistema de detecção de incêndio;
- Sensores para monitoramento da infraestrutura;
- Supervisório integrado de automação predial, quando desejado.

1.3. SEGURANÇA

É importante ressaltar que a integridade e segurança da informação deverão ser essenciais dentro de um ambiente no qual convergirão e se compartilharão informações estratégicas e confidenciais.

A implementação da arquitetura centralizada de processamento e armazenamento de dados também deverá permitir eliminar o contato físico entre o usuário e sua máquina, a qual se encontrará em um ambiente isolado e seguro.

Neste caso, o gestor de TI poderá, via software, configurar e gerenciar a rede integrada com vários níveis de segurança e restringir o acesso às portas USB, em função do perfil do usuário, eliminando o risco de cópia ou intrusão indevida de dados ou aplicativos:

- Eliminação do contato físico entre o usuário e a máquina;
- Acomodação dos equipamentos de TI em ambiente controlado e seguro;
- Rede integrada com níveis de segurança gerenciáveis;
- Restrição na conexão de equipamentos e no acesso às portas USB em função do perfil do usuário.

1.4. PERFORMANCE

A velocidade na análise das situações de crise e na tomada de decisões é essencial para garantir a eficiência das operações e ou ações gerenciadas por entidades internas ao Centro Integrado. Considerando a diversidade, quantidade e complexidade dos aplicativos e sistemas utilizados, assim como o nível requisitado de desempenho e rendimento dos ambientes e dos operadores, deverão ser utilizados equipamentos e tecnologia que permitirão um rápido processamento de dados e de vídeo, inclusive para aplicações gráficas de alta complexidade que exigirão uma visualização multiscreen.

Para as posições mais críticas nos ambientes, deverão ser utilizadas estações de trabalho virtualizadas de alta performance, com aceleração 3D e capacidade de trabalhar com múltiplos monitores de alta resolução. A estação de trabalho virtualizada que deverá ser acessada remotamente através de protocolo de comunicação seguro, com criptografia nativa, de baixa latência e baixo consumo de banda de rede.

Os operadores precisarão, também, ter acesso, em tempo real, a todas as informações, para poder fazer uma análise rápida e correta de qualquer situação e, assim tomar decisões adequadas.

Portanto, toda a tecnologia que sustentará a operação deverá atender aos requisitos técnicos mínimos para garantir a capacidade de processamento de dados e de visualização gráfica, assim como a velocidade de transmissão e de disponibilização da informação.

Sistemas de vídeo de alta performance do tipo vídeo wall deverão ser utilizados para visualização simultânea de várias fontes de informações, via IP ou através de coleta analógica de sinais.

1.5. DISPONIBILIDADE

Uma operação em regime contínuo 24x7 exigirá que toda a solução implementada garanta a disponibilidade máxima do ambiente para reduzir o tempo de downtime e de interrupção da operação.

A arquitetura centralizada de processamento e de armazenamento permitirá acomodar todos os equipamentos críticos na Sala Técnica com uma infraestrutura totalmente redundante.

Da mesma forma, toda a arquitetura de TI implementada assim como a infraestrutura técnica e operacional deverá oferecer uma redundância e contingência dos principais sistemas para garantir a continuidade das operações em caso de falha do sistema primário.

1.6. CONFIABILIDADE

A confiabilidade da infraestrutura e dos equipamentos instalados deverá ser primordial para garantir a atividade contínua e eficiente tanto do operador quanto do ambiente.

Os equipamentos de tecnologia deverão ser de fabricantes primeira linha, considerando itens como garantia de qualidade e robustez, não sendo aceitas soluções baseadas em computadores de propósito geral.

1.7. PERENIDADE

A vida útil tecnológica e operacional de ambientes internos ao Centro Integrado deverá ser, em média, de 5 (cinco) anos. Considerando o nível alto de investimento que representa este tipo de solução, deverá ser imperativo que os equipamentos estejam configurados e dimensionados para sustentar a demanda de processamento de dados e processamento gráfico e garantir a compatibilidade com futuras versões dos aplicativos e sistemas.

Da mesma forma, a infraestrutura de redes deverá estar pronta para atender aos futuros requisitos de maior consumo e velocidade de banda.

Todos os equipamentos de tecnologia e infraestrutura deverão ser projetados para funcionar com alto desempenho em regime contínuo 24x7.

1.8. IMAGEM

Os ambientes de gestão, por possuírem vídeo wall, têm como vocação, além da função de gestão, ser a vitrine tecnológica da organização.

Desta forma, tornar-se-ão uma ferramenta de marketing poderosa para demonstrar aos seus clientes e parceiros a capacidade de inovação, o controle e a eficiência das operações, assim como a seriedade e a confiabilidade na Organização.

Para tal, deverão possuir:

- Projeto Arquitetônico diferenciado;
- Design moderno e arrojado do mobiliário técnico;

- Customização dos consoles em conformidade com a identidade visual da organização;
- Impacto visual dos sistemas de display e vídeo.

2. TECNOLOGIA DA INFORMAÇÃO

Os ambientes que comporão o Centro Integrado deverão ser ambientes críticos para os quais convergirão os dados e os informes que posteriormente deverão ser processados e transformados em informações e em conhecimento que, aliados às informações operacionais existentes, formarão a inteligência necessária ao gerenciamento das operações e permitirão, ainda, o acionamento e o controle dos recursos e ações que irão prever, neutralizar ou impedir a ocorrência de riscos ou minimizar seus efeitos.

Por se tratar de ambientes de apoio a processos de decisões estratégicas, o Centro Integrado deverá, imprescindivelmente, atender aos seguintes quesitos:

- Infraestrutura de TIC baseada em uma plataforma centralizada e segura, que permita entregar os recursos corretos para as equipes de TIC, de maneira ágil, sem impactar a operação;
- Segurança física e lógica da informação e da infraestrutura de TIC;
- Alta disponibilidade do ambiente computacional para funcionamento contínuo 24x7;
- Permitir a compatibilidade e a interoperabilidade dos sistemas de informação, incluindo sistemas legados;
- Maximizar os benefícios e mitigar interrupções inesperadas geradas por um conjunto finito de recursos da atual infraestrutura.

Além de ser um ambiente de missão crítica, com controles, procedimentos e atividades específicos e acesso controlado, deverá, ainda, prever um alto grau de modularidade, permitindo que sua configuração possa ser readequada, no que se refere ao layout físico e a sua infraestrutura de TIC com o intuito de melhor atender as necessidades da operação, quando estas sofrerem alterações, recebendo ou excluindo serviços, escalando sua capacidade e até mesmo permitindo a integração com infraestruturas hibridas para acesso a dados abertos e outras agências.

Pontos que deverão ser levados em consideração para a construção de um ambiente de alta criticidade e segurança:

2.1. SEGURANÇA

É importante ressaltar que a integridade e segurança da informação são essenciais dentro de um ambiente no qual convergem e se compartilham informações estratégicas e confidenciais.

A implementação da arquitetura centralizada de processamento e armazenamento de dados deve permitir também eliminar o contato físico entre o usuário e sua máquina, que se encontra num ambiente isolado e seguro.

Esta arquitetura deve ser instalada em uma Sala técnica para garantir proteção contra as principais ameaças físicas para evitar o roubo de informações ou eventual vandalismo, furto de partes e peças, e outros danos aos equipamentos.

2.2. PERFORMANCE

Considerando a diversidade, quantidade e complexidade dos aplicativos e sistemas utilizados assim como o nível requisitado de desempenho e rendimento do ambiente e dos operadores, devem ser utilizados equipamentos e tecnologia que permitam um rápido processamento de dados.

A velocidade na análise das situações de crise e na tomada de decisões é essencial para garantir a eficiência das operações.

Para as posições mais críticas, normalmente são utilizadas soluções baseadas em equipamentos de alta performance, com alta capacidade de processamento de dados e gráficos e acesso remoto às Estações de Trabalho sem limite de distância, através da tecnologia de extensão digital de comando sobre IP (USB, Áudio, Multivídeo), através de protocolos de comunicação seguros e de alta performance e baixo consumo de banda de rede, permitindo entregar em tempo real aos operadores, acesso as suas workstations e, quando necessário, acesso a portas USB, Áudio e Multivídeo.

2.3. REDE SEGURA E DE ALTA VELOCIDADE

Toda a tecnologia que sustenta essa operação deve atender aos requisitos técnicos mínimos para garantir a capacidade de processamento de dados e visualização gráfica, assim como a velocidade de transmissão e disponibilização da informação.

2.4. SOLUÇÃO DE VÍDEO COLABORATIVA – VIDEO WALL DE ÚLTIMA GERAÇÃO

Soluções de visualização colaborativa que permitam integrar diversas fontes e formatos de dados, integrar diferentes plataformas de informação e ainda permitir a colaboração em tempo real de todos os envolvidos em situações de crise e que sejam capazes de permitir a construção da "consciência situacional".

2.5. DISPONIBILIDADE

Uma operação em regime contínuo 24 horas por 7 dias exige que toda a solução implementada garanta a disponibilidade máxima do ambiente para reduzir ou eliminar o tempo de downtime.

Em caso de falhas técnicas, a solução deve permitir uma manutenção rápida e fácil dos equipamentos, não prejudicando assim o desempenho dos operadores.

Da mesma forma, a infraestrutura técnica e operacional, deverá oferecer uma redundância e contingência dos principais sistemas para garantir a continuidade das operações em caso de falha do sistema primário.

2.6. GERENCIAMENTO

Profunda capacidade de gerenciamento de toda a infraestrutura, desde a camada física até os elementos virtualizados em uma única ferramenta de gestão que deverá proporcionar a capacidade de análise da saúde da infraestrutura de TIC e a predição de cenários de eventuais necessidades de capacidade de carga de trabalho.

2.7. CONFIABILIDADE

A confiabilidade da infraestrutura é primordial para garantir a atividade contínua e eficiente tanto do operador quanto do ambiente.

Para que tal nível de excelência e segurança seja alcançado, é necessário atender às especificações mínimas quanto as soluções de TIC necessárias para a operação dos ambientes que comporão o Centro Integrado.

3. SERVIÇOS

- Treinamento dos sistemas implementados;
- Comissionamento dos equipamentos fornecidos no projeto.

4. GARANTIAS

- Garantia de equipamentos – 12 meses a partir do termo de entrega da obra;
- Garantia de equipamentos de TI – 12 meses a partir do termo de entrega da obra;
- Garantia Estendida, pelo período de 60 meses.

5. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – CABEAMENTO LÓGICO

5.1. CABEAMENTO LÓGICO

5.1.1. MÃO-DE-OBRA:

Segue descrição dos serviços orçados a serem executados para a implementação da infraestrutura lógica e de cabeamento estruturado, garantindo plena aderência aos requisitos de missão crítica, disponibilidade, desempenho e segurança da informação.

Fornecimento e a execução dos serviços de infraestrutura lógica, incluindo instalação de eletrocalhas, passagem e organização de cabos, montagem de racks, conectorização, certificação e comissionamento de toda a rede de dados (física) utilizando cabeamento estruturado em fibra óptica, cabos UTP CAT6 e CAT6A blindado.

INFRAESTRUTURA FÍSICA

- Instalação de eletrocalhas aramadas nos trajetos horizontais e verticais conforme projeto executivo;
- Fixação adequada nos elementos estruturais (lajes, aredes, shafts) com distanciamento conforme normas técnicas;
- Organização e fixação dos cabos sobre eletrocalhas com uso de abraçadeiras e divisores, mantendo segregação adequada entre dados e energia elétrica;
- Instalação de racks fechados na Sala Técnica e racks abertos ou fechados nos pontos de distribuição por pavimento.

CABEAMENTO

Cabeamento Metálico:

- Lançamento de cabos UTP CAT6 e CAT6A blindados, em atendimento às exigências de desempenho (10Gbps para CAT6A);
- Cada ponto de rede contará com dois cabos UTP, com identificação física nas extremidades (patch panel e faceplate);
- Fixação e organização dos cabos em racks com uso de organizadores verticais e horizontais; - Conectorização dos cabos nos patchs panels e keystones, com certificação através de testador de rede (Fluke DSX ou similar).

Cabeamento Óptico:

- Lançamento de fibras ópticas multimodo OM3 entre os racks de telecom e a Sala Técnica, conforme topologia definida no projeto; - Uso de caixas de emenda, bandejas de acomodação e conectores SC ou LC, conforme especificado;
- Certificação de todos os enlaces ópticos com OTDR e Power Meter, com emissão de relatório.

MONTAGEM E ORGANIZAÇÃO DE RACKS

- Instalação dos equipamentos ativos e passivos de rede nos racks (patch panels, witches, organizadores, PDU);
- Conexão dos patchs cords e organização estética e funcional do cabeamento interno;
- Ligação elétrica e aterramento de todos os racks conforme normas de segurança e projeto elétrico; - Toda a infraestrutura deverá ser devidamente identificada com etiquetas permanentes: cabos, pontos, portas de switch, patch panels e racks;
- Fornecimento de mapa lógico e planta baixa com a distribuição dos pontos de rede e fibras;
- Testes de continuidade, desempenho, perda e certificação dos enlaces metálicos CAT6/CAT6A);
- Certificação dos enlaces ópticos com OTDR;
- Emissão de laudos técnicos e relatórios com resultados por ponto, conforme normas técnicas aplicáveis (ANSI/TIA/EIA...)

MÃO DE OBRA ENVOLVIDA

- Engenheiro de telecomunicações (responsável técnico);
- Técnico em cabeamento estruturado;
- Instaladores de infraestrutura (eletrocalhas, dutos, etc.);
- Especialista em fibra óptica (fusões, certificação);
- Auxiliares de instalação.

EQUIPAMENTOS E FERRAMENTAS

- Equipamentos de medição e certificação (Fluke DSX, OTDR, Power Meter);
- Guinchos, escadas, alicates de crimpagem, ferramentas de corte e conectorização;
- EPIs para trabalho em altura e ambiente elétrico;
- Ferramentas para montagem e fixação de racks e eletrocalhas.

Todo o serviço deverá ser executado de acordo com o projeto executivo fornecido, em conformidade com as melhores práticas da indústria de TIC.

5.1.2 [RCK01] - Racks Fechados 600 mm x 1100 mm x 42U's

- Estrutura em perfis de alta resistência (aço ou alumínio), com conexão angular rígida, garantindo precisão e robustez;
- Fechamentos laterais/ traseiro em chapa de aço 1.0mm;
- Portas em aço 1.0mm ou aço/vidro temperado 6.0mm, ângulo de abertura de 180 graus;
- 2 planos de montagem com perfis verticais 19" em chapa de aço eletrozincada 1,5mm;
- Capacidade de cargas
- 1500Kg conforme testes realizados.

5.1.3. [RCK02] - Racks Fechados 800 mm x 1100 mm x 42U's

- Estrutura em perfis de alta resistência (aço ou alumínio), com conexão angular rígida, garantindo precisão e robustez;
- Fechamentos laterais/ traseiro em chapa de aço 1.0mm;
- Portas em aço 1.0mm ou aço/vidro temperado 6.0mm, ângulo de abertura de 180 graus;
- 2 planos de montagem com perfis verticais 19" em chapa de aço eletrozincada 1,5mm;
- Organizador frontal vertical em ambas as laterais internas, L=100mm
- Capacidade de Cargas
- 1500kg conforme testes realizados.

5.1.4. [RCK03] - Rack Aberto 2kVA – 2 Postes

- Estrutura em chapa de aço de 1 a 3mm de espessura;
- Fingers em ABS preto;
- Base sólida (espessura 3mm) garante robustez à estrutura 19" (espessura 2mm) e possui ainda abertura central para entrada de cabos do solo ou piso elevado. Na parte superior, teto com curvatura para descida de cordões ópticos;
- Estrutura projetada e construída em chapa de aço de 1.5 a 3mm de espessura, modular e flexível, podendo ser facilmente montada em campo.
- Capacidade de Carga: 500kg de equipamentos distribuídos uniformemente por toda a extensão dos perfis 19" (rack chumbado ao piso).

5.1.5. [RCK04] - Rack Aberto 3kva – 2 Postes

- Estrutura em chapa de aço de 1 a 3mm de espessura;
- Fingers em ABS preto;
- Base sólida (espessura 3mm) garante robustez à estrutura 19" (espessura 2mm) e possui ainda abertura central para entrada de cabos do solo ou piso elevado. Na parte superior, teto com curvatura para descida de cordões ópticos;
- Estrutura projetada e construída em chapa de aço de 1.5 a 3mm de espessura, modular e flexível, podendo ser facilmente montada em campo.

- Capacidade de Carga: 500kg de equipamentos distribuídos uniformemente por toda a extensão dos perfis 19” (rack chumbado ao piso).

Os racks seguirão as especificações acima, sendo localizados, preferencialmente, nas Salas Técnicas, para atender a infraestrutura de TI e Comunicação.

5.1.6. [RCK05] - RACK DE PAREDE – DESMONTÁVEL 450MM X 8U (E-208)

- Altura interna útil: 355,60mm
- Largura externa: 550 mm.
- Profundidade externa máxima: 450 mm.
- Capacidade de carga: no mínimo 100kg.
- Estrutura soldada em aço SAE 1020 com esp. 0,75/0,9mm.
- Laterais em aço SAE 1020 removíveis com aletas de ventilação e fecho rápido;
- Porta frontal embutida, com visor em acrílico transparente de 2,0mm de esp. com fecho e chave;
- Pintura eletrostática epóxi em pó, com acabamento microtexturizado;
- Plano de Fixação móvel;

5.1.7. MONTAGEM RACKS E CABEAMENTO ESTRUTURADO

Deverá ser implantada uma rede estruturada que deverá ser baseada na disposição que integre os serviços de dados e voz, que poderão ser facilmente redirecionados no sentido de prover um caminho de transmissão entre quaisquer pontos desta rede.

Todas as técnicas de instalações, o material empregado e a documentação, deverão seguir e serem certificados em conformidade com as Normas NBR 14565, ANSI/EIA/TIA 568-B, ANSI/EIA/TIA 569A, ANSI/EIA/TIA 606, ANSI/EIA/TIA 607 e outras normas aplicáveis.

Os materiais de cabeamento deverão ser de um único fabricante e possuir certificados de fabricação ISO-9001.

As soluções deverão ser compostas por:

- Cabeamento Metálico UTP:
- Cabo UTP Cat6 ou 6A (dependendo do local) LSZH;
- Patch panel descarregado;
- Guia de cabos horizontal;
- Ponto de consolidação;
- Conector fêmea Cat6 ou 6A;
- Patch Cord UTP Cat 6 ou 6A, conforme projeto executivo. Cabeamento Óptico
- (solução MPO):
- DIO Modular;
- DIO Cassete 12F OM3 MPO;
- Cabo Óptico Pré Conectorizado 12F OM3 MM, conforme projeto;
- Cordão Duplex MM LC-UPC, conforme projeto;

- Painel de Fechamento.

Todos os acessórios de organização e identificação, tais como porta-etiqueta, organizadores horizontais e verticais e velcros deverão ser instalados conforme recomendação da norma EIA/TIA 568-B.

Deverá ser fornecido cabeamento lógico estruturado conforme descrição abaixo:

TIPO	AMBIENTE
UTP CAT 6	01 ponto por posição de trabalho – todas as salas pertencentes a este escopo; 02 pontos por mesa de reunião – todas as salas pertencentes a este escopo. 02 pontos por mesa de console de rádio - sala de comando e controle
UTP CAT 6A	02 pontos para cada Video Wall; 01 ponto para Access Point Wi-Fi (Considerar 4 por pavimento instalado no entre-forro).
UTP CAT 6A	96 pontos para cada rack de Servidor – Sala Técnica 24 pontos para cada rack de Telecom – Sala Técnica 24 pontos para cada rack de CFTV – Sala Técnica
OM3 MM	2 pares para cada rack de Servidor – Sala Técnica

Deverá ser realizado o fornecimento e instalação de backbone atendendo os seguintes pontos:

TIPO	QUANTIDADE	DE	PARA
UTP CAT 6A	24	Sala Técnica Pav. Térreo	Shaft Pav. Superior

6. EQUIPAMENTOS TI

[TI01] - ESTAÇÃO DE TRABALHO MFF (MICRO FORM FACTOR)

Aquisição de estações de trabalho para as posições de trabalho dos usuários. O hardware envolvido deve ser homologado para a utilização dos sistemas operacionais Windows 11.

As características deverão ser as seguintes:

Gabinete:

- Os gabinetes deverão ser compatíveis com o padrão VESA de instalação dos equipamentos;
- Deverá ter trava para segurança física de padrão Kensington;
- Deve permitir de acesso à suporte e troca de peças sem a necessidade ferramentas;

Processamento:

- Deve ter processador compatível com X86 (x64);
- O processador deverá possuir ao menos 6 cores de performance;
- Os processadores deverão ter frequência de mínimo de 1.6 GHz por core de performance com turbo clock de no mínimo 3.0 GHz;
- Deverá ter um mínimo de 8 MB de cache.

Memória:

- Deverá ser fornecido com memória RAM de 8GB DDR4;
- A velocidade de trabalho das memórias deverá ser de 2666 MHz ou superior, expansível até 32GB.

Armazenamento:

- Deverá fornecer armazenamento do tipo All-Flash;
- O disco deverá ter no mínimo 240 GB;
- Os discos devem ser do tipo NVMe ou SSD.

Conectividade de Rede:

- Deverá ter placa de rede com interface de rede Gigabit Ethernet (10/100/1000 Mbps) para garantir alta velocidade de conectividade.

Portas USB, Áudio e Vídeo:

- O equipamento deve contar com um mínimo de duas portas USB 3.0, permitindo a conexão de periféricos de alta velocidade, como discos externos, impressoras e scanners;
- O equipamento deve possuir pelo menos duas portas USB 2.0 para a conexão de periféricos de menor demanda de dados, como mouses e teclados;
- A estação de trabalho deve ser equipada com pelo menos duas portas de saída de vídeo, suportando monitores duplos. As opções podem incluir DisplayPort (DP) ou HDMI. As saídas de vídeo devem ser compatíveis com adaptadores para outros padrões, como VGA ou DVI, para assegurar a compatibilidade com diferentes tipos de monitores existentes na infraestrutura corporativa;
- O dispositivo deve possuir um conector combo de áudio (3,5 mm) para entrada/saída, suportando fones de ouvido, microfones, ou alto-falantes externos.

Energia:

- Deverá ser fornecido com fontes de alimentação fornecidas pelo mesmo fabricante do equipamento;

Suporte e Garantia:

- Deverá ser fornecido com período de Garantia de 12 meses (5 anos) de garantia on-site com resposta no próximo dia útil.
- Deverá ter Suporte 24/7 com acesso a atualizações de software e firmware durante o período de garantia.

Certificações e Conformidades:

- Deverá ser compatível com as principais normas internacionais de qualidade e segurança, como ISO/IEC 27001.
- Deverá ter as seguintes Certificações Ambientais: RoHS (Restriction of Hazardous Substances); WEEE (Waste Electrical and Electronic Equipment); REACH (Registration, Evaluation, Authorization and Restriction of Chemicals); ENERGY STAR;

Periféricos:

Deverá acompanhar os periféricos com a seguinte configuração:

- **Teclado**: Teclado padrão ABNT, com fio, do tipo alfanumérico estendido, com teclado numérico integrado, obedecendo aos padrões de disposição de teclas ABNT NBR 10346 e NBR 10347; deve possuir tecla dedicada para ativação do menu Iniciar (Start) do Windows; deve permitir ajuste de inclinação (pés retráteis ou mecanismo equivalente); deve ser plug and play, sem necessidade de

instalação de drivers adicionais para funcionamento básico no Windows, e compatível com utilização em modo legado no boot (funcionamento na BIOS/UEFI); deve possuir teclas com aspecto quadrado ou retangular, não sendo aceito outro formato; deve sinalizar as funções Caps Lock, Num Lock e Scroll Lock por indicadores visuais no teclado e/ou por mensagem específica na tela do computador; a impressão/legenda das teclas deve ser permanente e de alta durabilidade, não devendo apresentar desgaste por abrasão ou uso prolongado, sendo aceitas tecnologias como gravação a laser, dupla injeção (double-shot) ou equivalente; durante o período de garantia, teclados que apresentarem desgaste de impressão por uso normal deverão ser substituídos sem custos para a contratante; deve possuir cor preta ou cinza, compatível com o padrão estético dos equipamentos desktops fornecidos; Interface de conexão: USB (com cabo integrado), compatível com Windows 11, com funcionamento plug and play e suporte a uso em BIOS/UEFI.

- **Mouse:** Mouse do tipo óptico, com fio, para uso em computador; conexão por interface USB (cabo integrado); deve ser plug and play, sem necessidade de instalação de drivers adicionais para funcionamento básico no Windows; deve possuir sensor óptico por LED ou laser; resolução mínima de 1000 DPI; deve possuir no mínimo 3 botões, sendo: esquerdo, direito e botão scroll para rolagem vertical tipo wheel mouse, com clique; a roda de rolagem deve possuir rolagem por etapas (“steps”); deve possuir taxa de polling mínima de 125 Hz; deve possuir comprimento mínimo do cabo de 1,5 m; deve possuir formato ergonômico para uso ambidestro; deve possuir tamanho normal para operação por adultos, não sendo aceito mini mouse; deve ser compatível com Windows 11; cor preta ou cinza, preferencialmente compatível com o padrão dos equipamentos desktops fornecidos; durante o período de garantia, mouses que apresentarem defeito de fabricação ou falhas de funcionamento em condições normais de uso deverão ser substituídos sem custos para a contratante.
- **Webcam:** Webcam (câmera de vídeo para computador), não-PTZ (sem movimentação motorizada); Resolução mínima de vídeo (chamada): 4K (3840×2160) com taxa mínima de 30 fps; Resolução mínima de gravação: 4K (3840×2160) com taxa mínima de 30 fps; Resolução desejável: 4K a 60 fps (quando suportado); 4K deve estar disponível em modo UVC (sem depender de driver/software do fabricante). Microfone integrado: Sim, microfone embutido, preferencialmente com redução de ruído e captação adequada para uso individual (aprox. até 1 metro); Conectividade: USB 3.0 / USB 3.1 ou superior (preferencialmente USB-C, aceitando USB-A via cabo/adaptador quando aplicável); deve ser compatível com Windows 11 e com aplicativos de videoconferência (Microsoft Teams, Zoom, Google Meet e similares); Campo de visão (FOV): mínimo 70° e máximo 90° (uso individual); Foco: autofocus (obrigatório); Baixa luminosidade: correção/ajuste automático para baixa iluminação (desejável); Montagem: clipe/suporte para monitor/notebook e rosca padrão para tripé (desejável); Privacidade: tampa/obturador físico de privacidade (desejável); Indicadores: LED de funcionamento/uso da câmera; Itens inclusos: webcam; cabo USB compatível (integrado ou incluso); manual (PT-BR); durante o período de garantia, webcams que apresentarem defeito de fabricação ou falhas de funcionamento em condições normais de uso deverão ser substituídos sem custos para a

contratante; cor preta ou cinza, preferencialmente compatível com o padrão dos equipamentos desktops fornecidos.

[TI02] – LAPTOPS DE TRABALHO

Aquisição laptops de trabalho de acordo com as especificações, além de serviço de instalação, treinamento, suporte técnico e garantia do fabricante, com as especificações técnicas que seguem:

Gabinete:

- Deverá ter trava para segurança física de padrão Kensington;
- Deverá ter trackpoint ou touch-pad com dois botões;
- Deverá ser fornecido com Sistema Operacional Windows 11 Pro 64 bits;
- Deverá contar com bateria de íon de lítio de no mínimo 3 células;
- O peso do equipamento deverá ser inferior a 2 kg;
- Deverá ser fornecido com fonte bivolt e cabo de alimentação de tomada em padrão brasileiro;

Processamento:

- Deve ter processador compatível com X86 (x64);
- O processador deverá possuir ao menos 4 cores de performance.;
- Os processadores deverão ter frequência de mínimo de 1.6 GHz por core de performance com turbo clock de no mínimo 3.0 GHz;
- Deverá ter um mínimo de 8 MB de cache.

Memória:

- Deverá ser fornecido com memória RAM de 8GB DDR4;
- A velocidade de trabalho das memórias deverá ser de 2666 MHz ou superior, com expansibilidade de até 32GB.

Armazenamento:

- Deverá fornecer armazenamento do tipo All-Flash.
- O disco deverá ter no mínimo 240 GB;
- Os discos devem ser do tipo NVMe ou SSD.

Tela:

- Deverá contar com tela LED de 15 polegadas;
- Deverá ter resolução mínima Full HD (1920x1080)
- A configuração deverá suporte placa de vídeo Integrada Intel ou AMD com varredura de 60 Hz.

Conectividade e Recursos:

- Deverá ter placa de rede com interface de rede Gigabit Ethernet (10/100/1000Mbps) para garantir alta velocidade de conectividade;
- Deverá fornecer conectividade dos equipamentos com conectividade Wi-Fi mínima de versionamento 802.11ac ou superior;
- Deverá fornecer conectividade Bluetooth versão 5.0;
- Deverá prover portas de conectividade nas seguintes quantidades mínimas: 2

- (duas) USB 3.2 Gen 1, 1 (uma) USB 2.0, 1 (um) HDMI 1.4, 1 (uma) porta RJ-45 (Ethernet), 1 (um) Conector de áudio combinado;
- Deverá fornecer câmera de resolução HD de 720p com microfone integrado;
- Deverá ter alto-falantes estéreo.

Suporte e Garantia:

- Deverá ter Suporte 24/7 com acesso a atualizações de software e firmware durante o período de garantia.

Certificações e Conformidades:

- Deverá ser compatível com as principais normas internacionais de qualidade e segurança, como ISO/IEC 27001.
- Deverá ter as seguintes Certificações Ambientais: RoHS (Restriction of Hazardous Substances); WEEE (Waste Electrical and Electronic Equipment); REACH (Registration, Evaluation, Authorization and Restriction of Chemicals); ENERGY STAR;
- **Mouse:** Mouse do tipo óptico, sem fio (wireless), com receptor USB (nano transceptor); tecnologia wireless 2,4 GHz, de alta confiabilidade; alcance de operação sem fio mínimo de 8 metros, em ambiente típico de escritório (sem barreiras significativas); receptor USB de encaixe (nano receiver); plug and play, sem necessidade de instalação de drivers adicionais para funcionamento básico no Windows; sensor óptico por LED ou laser; resolução mínima de 1000 DPI; no mínimo 3 botões (esquerdo, direito e botão scroll para rolagem vertical tipo wheel mouse, com clique); botão liga/desliga; alimentação por bateria interna recarregável, com recarga via USB no próprio mouse (preferencialmente USB-C, aceitando micro-USB), acompanhado de cabo de recarga compatível incluso; indicador de bateria fraca e/ou indicador de carregamento por LED no dispositivo ou via software do fabricante; formato ergonômico para uso ambidestro; tamanho normal para operação por adultos, não sendo aceito mini mouse; compatível com Windows 11; cor preta ou cinza, compatível com o padrão dos equipamentos desktops fornecidos; durante o período de garantia, **mouses** que apresentarem desgaste de impressão por uso normal deverão ser substituídos sem custos para a contratante
-

[TI03] – MONITOR LED DE 24”

Especificações técnicas mínimas:

- Painel LCD (visor de cristal líquido) e 4k ultra HD;
- Área de visualização: 24 polegadas;
- Número de Cores: 16,7 milhões;
- Resolução nativa mínima: 2560x1440;
- Tempo de resposta máximo: 5ms;
- Brilho mínimo 250 cd/m²;
- Contraste mínimo 1000:1;
- OSD (On Screen Display): Menu Digital na Tela;
- Portas de Entrada digital: HDMI ou Display Port;

- Fonte externa ou interna;
- Ângulo de Visão: +/- 178°/178° (H/V) Típico;
- Pixel Pitch máximo: 0,2745 x 0,2745 mm.

[TI04] – MONITOR LED DE 34”

Especificações técnicas mínimas:

- Painel LCD curvo Ultrawide (visor de cristal líquido);
- Área de visualização: 34 polegadas ultrawide;
- Número de Cores: 16,7 milhões;
- Resolução nativa mínima: 3440x1440;
- Tempo de resposta máximo: 5ms;
- Brilho mínimo 250 cd/m²;
- Contraste mínimo 1000:1;
- OSD (On Screen Display): Menu Digital na Tela;
- Portas de Entrada digital: HDMI ou Display Port;
- Fonte externa ou interna;
- Ângulo de Visão: +/- 178°/178° (H/V) Típico;
- Pixel Pitch máximo: 0,2745 x 0,2745 mm;

[TI05] – MONITOR LED DE 27”

Especificações técnicas mínimas:

- Painel LCD (visor de cristal líquido) e 4k ultra QHD;
- Área de visualização: 27 polegadas;
- Número de Cores: 16,7 milhões;
- Resolução nativa mínima: 3840x2160;
- Tempo de resposta máximo: 5ms;
- Brilho mínimo 250 cd/m²;
- Contraste mínimo 1000:1;
- OSD (On Screen Display): Menu Digital na Tela;
- Portas de Entrada digital: HDMI ou Display Port;
- Fonte externa ou interna;
- Ângulo de Visão: +/- 178°/178° (H/V) Típico;
- Pixel Pitch máximo: 0,2745 x 0,2745 mm.

[TI06] – TELA INTERATIVA DE 75”

- Tecnologia: Painel LCD (visor de cristal líquido).
- Área de visualização: 75 polegadas.
- Número de cores: mínimo 16,7 milhões.
- Resolução nativa: mínimo 3840 × 2160 (UHD 4K).
- Brilho: mínimo 500 cd/m².
- Contraste: mínimo 1.000:1.
- Ângulo de visão: mínimo +/- 178°/178° (H/V) típico.
- Tela antirreflexiva (anti-glare).
- OSD (On Screen Display): menu digital na tela.
- A tela deve ser nativamente interativa (touch screen), sem uso de molduras/adaptações externas, devendo ser montada em chassi único (solução integrada de fábrica).
- Conectividade de rede IP:
- Porta RJ45 (Ethernet); e
- Acesso sem fio via Wi-Fi.
- O monitor deve possuir sistema próprio de gerenciamento de conteúdo, com acesso disponibilizado aos notebooks dos usuários.
- O sistema de gerenciamento de conteúdo deve ser compatível com:
- Windows 11; e
- macOS 10 (conforme tua exigência original).
- Deve acompanhar software de lousa digital, permitindo no mínimo:
- escrever/anotar sobre a superfície;
- ajustar espessura do traço/pincel;
- alterar cor da caneta;
- função apagar/borracha;
- inserir objetos prontos (ex.: formas geométricas).
- O software deve ser fornecido com licença completa e perpétua de uso (conforme você pediu).
- Entradas digitais: HDMI ou DisplayPort (aceita-se qualquer uma ou ambas, conforme item específico) , e USB 3.0 Tipo-C.
- Portas USB para conteúdo: mínimo 2 (duas) portas USB 2.0.
- Fonte de alimentação: interna ou externa.
- Deve ser fornecido com controle remoto.
- Base de apoio sobre rodas, compatível com o monitor interativo, com sistema de inclinação (tilt) ajustável de 0° a 90°, permitindo posicionamento na vertical (0°) até horizontal (90°), com travamento mecânico em, no mínimo, 0°, 45° e 90°, e com rodízios com freio.

[TI07] SMART TV 55”: (TV 55);

- Televisores Smartv UHD 4K Led 55”:
    - **Especificações técnicas mínimas:**

      Controle por voz compatível com assistentes virtuais.

      Sistema operacional integrado: Interface intuitiva com acesso rápido a aplicativos e streaming.

      HDMI: 3 entradas (com suporte para áudio de alta qualidade).

      USB: 2 portas para reprodução e gravação.

      Bluetooth e Wi-Fi: Conexão sem fio para áudio e internet.

      Saída óptica e LAN: Para integração com sistemas externos.

      Modo de economia de energia inteligente: Ajuste automático de brilho.

[TI08] SMART 75”: (TV 75)

- Televisores Smartv UHD 4K Led 75”:
    - **Especificações técnicas mínimas:**

      Controle por voz compatível com assistentes virtuais.

      Sistema operacional integrado: Interface intuitiva com acesso rápido a aplicativos e streaming.

      HDMI: 3 entradas (com suporte para áudio de alta qualidade).

      USB: 2 portas para reprodução e gravação.

      Bluetooth e Wi-Fi: Conexão sem fio para áudio e internet.

      Saída óptica e LAN: Para integração com sistemas externos.

      Modo de economia de energia inteligente: Ajuste automático de brilho.

[TI09] SMART TV 85” (TV 85)

- Televisores Smartv UHD 4K Led 85”:
    - **Especificações técnicas mínimas:**

      Controle por voz compatível com assistentes virtuais.

      Sistema operacional integrado: Interface intuitiva com acesso rápido a aplicativos e streaming.

      HDMI: 3 entradas (com suporte para áudio de alta qualidade).

      USB: 2 portas para reprodução e gravação.

      Bluetooth e Wi-Fi: Conexão sem fio para áudio e internet.

      Saída óptica e LAN: Para integração com sistemas externos.

      Modo de economia de energia inteligente: Ajuste automático de brilho.

7. SISTEMA DE TELECOMUNICAÇÕES, LÓGICA – NOBREAK – UPS [61-64]

Deverá ser compatível com o anteprojeto elétrico

6.1. Mão-de-obra e materiais para instalação

Apresentamos os serviços e materiais necessários para a instalação completa de 02 (dois) sistemas de UPS (No-break) trifásicos, redundantes entre si, com dimensionamento e autonomia exigida para operação crítica. A instalação será realizada em Sala UPS dedicada, climatizada e com infraestrutura redundante prevendo:

- Instalação de eletrocalhas metálicas e conduítes de energia entre a Sala UPS e os quadros de distribuição (QGBT, QDLs, etc);
- Instalação de painéis elétricos para entrada e saída das UPS, com dispositivos de proteção e seccionamento;
- Instalação de sistema de aterramento específico para os UPS e banco de baterias, com medições de resistência ôhmica conforme NBR 5410;
- Instalação de sistema de climatização redundante na Sala UPS,
- Desembalagem, movimentação e fixação das UPS e dos bancos de baterias no local definitivo; - Interligação elétrica entre as UPS, painéis, bancos de baterias e sistema de carga;
- Configuração dos parâmetros das UPS, operação em paralelo redundante, teste funcional dos modos Normal, Emergência, Recarga e Bypass;

Comissionamento e Testes:

- Execução de testes com banco de carga resistivo para verificação da performance e autonomia exigida (mínimo 7 minutos a 120kW);
- Registro de todos os parâmetros de operação (tensão, corrente, frequência, potência, tempo de backup etc.);
- Emissão de relatório técnico completo com os resultados dos testes e medições.

Materiais e insumos necessários

- Gabinetes metálicos para baterias com ventilação e proteção;
- Eletrocalhas metálicas, perfilados e conduítes para passagem de cabos de força e sinal;
- Cabos elétricos dimensionados conforme potência: cabos de cobre isolação 0,6/1kV (alimentação e saída);
- Conectores, terminais, barramentos e kits de fixação;
- Etiquetas de identificação permanente de cabos, painéis e componentes;
- EPIs e ferramentas específicas para trabalho com sistemas energizados.
- Instalação deve seguir o padrão estabelecido nas Normas existentes.

MÃO DE OBRA ENVOLVIDA

- Engenheiro eletricista responsável técnico;
- Técnico em sistemas de energia ininterrupta;
- Eletricistas e instaladores industriais;

- Técnicos em ar-condicionado (para climatização da Sala UPS);
- Equipe de testes e comissionamento (com banco de carga);

Todos os serviços deverão ser realizados com base em projeto executivo e supervisionados por responsável técnico registrado no CAU/CREA.

A instalação deverá considerar acessibilidade para manutenção, segurança de operação e confiabilidade contínua do sistema.

6.1.2. [UPS01] Sistema de energia ininterrupta UPS (Nobreak)

Deverão ser fornecidos e instalados 02 (dois) equipamentos UPS´s, redundantes entre si, trifásico, 380 V, 60Hz, com dimensionamento para alimentar as seguintes cargas Críticas e Operacionais:

- Sala POP – Racks (E-205) – 3kW/Rack
- Sala Técnica 1 – Rack para ativos de rede dos postos de trabalho (E-201) – 2kW/Rack
- Sala Técnica – Racks para TIC (E-202/E206) – 5kW/Rack
- Sistemas de Segurança (CFTV, Controle de Acesso, BMS/Supervisório e DCIM)
- Estrutura audiovisual do Auditório
- Estrutura audiovisual da Sala de Crise
- Video Wall, monitores e telas digitais
- Demais postos de trabalho e salas de reunião.

Características técnicas do equipamento de UPS:

Modos de Operação:

O UPS irá operar obrigatoriamente como um sistema On-Line Dupla/Conversão nos seguintes modos:

- NORMAL: A carga crítica ficará continuamente alimentada pelos inversores do UPS. Os retificadores/carregadores transforma a energia AC da rede em DC para alimentar os inversores e carregar simultaneamente as baterias.
- EMERGÊNCIA: Quando a energia AC da rede falhar, a carga crítica ficará alimentada pelos inversores que, sem nenhum chaveamento, obtém energia das baterias. Não haverá interrupção de energia para a carga crítica quando houver falha ou retorno da energia AC da rede.
- RECARGA: Uma vez restaurado a energia AC da rede, os retificadores/carregadores passam a alimentar os inversores e simultaneamente carregam as baterias. Isto é uma função automática e não irá causar nenhuma interrupção para a carga crítica.
- BYPASS: Se o UPS for desligado para manutenção ou reparo, a chave estática irá transferir a carga para a fonte de by-pass sem interrupção para a carga crítica.

Retificador:

- Tensão nominal de alimentação: 380/400/415 Vac;
- Frequência nominal da tensão de alimentação: 60Hz;
- Número de fases do ramal alimentador: 3F + N + T;
- Fator de Potência de Entrada: ≥ 0,99 plena carga;
- Tecnologia: IGBT.

Inversor:

- Tensão nominal de saída: 380 Vac;
- Número de fases da tensão de saída: 3F + N + T;
- Frequência nominal de saída: 60 Hz;

Chave Estática (interna ao UPS)

- Tensão nominal de entrada da chave estática: 380 Vac;
- Potência nominal: 120 kVA;
- Número de fases: 3F+N+T;
- Frequência nominal da fonte alternativa: 60 Hz.

Instrumentos de Medição

- Tensão de entrada: Sim;
- Tensão de saída do retificador: Sim;
- Corrente de saída do retificador: Sim;
- Tensão de saída do inversor: Sim;
- Corrente de saída do inversor: Sim;
- Frequência de saída: Sim;
- Tempo de funcionamento da bateria: Sim;
- Potência de saída do UPS (kVA / kW): Sim;
- Frequência do By-pass: Sim.

Sinalização

- Inversor operando: Sim;
- Carga alimentada pelo inversor: Sim;
- Carga alimentada pela chave estática: Sim;
- Carga alimentada pela chave de by-pass: Sim;
- Carga alimentada pela bateria (remoto): Sim.

[UPS02] Sistema de BATERIAS para energia ininterrupta UPS (Nobreak)

As UPS e suas respectivas baterias deverão ser instaladas Sala UPS com climatização apropriada e redundante. O sistema de distribuição da rede elétrica a partir das UPS deverá ser responsável por todas as cargas críticas do Centro.

Os equipamentos deverão ser devidamente testados com bancos de carga resistivos e as baterias estarem em condições de suportar toda a carga do sistema por um período de 7 minutos de maneira redundante, ou seja, cada UPS deve dispor dessa autonomia.

Características técnicas:

- Tipo de elemento de bateria: Selada, chumbo ácida, regulada a Válvula (VRLA);
- Autonomia: 07 min @ 120 kW;
- Tipo de montagem: Gabinete fechado externo a UPS.

8. EQUIPAMENTOS DE REDE

[RDE01] - SWITCHES PARA REDE

Aquisição de switches de acesso, de acordo com as especificações, além de serviço de instalação, treinamento, suporte técnico e garantia de 12 meses.

Especificações técnicas:

- Deverá possuir no mínimo 48 portas Switch Gigabit Ethernet 10/100/1000BaseT;
- Deverá possuir nativamente 2 portas SFP/SFP+ para instalação de transceivers ópticos 1/10 Gigabit Ethernet. As portas SFP/SFP+ deverão vir fixas no chassi dos equipamentos;
- Deverá fornecer nas 48 portas Gbe alimentação compatível com padrão PoE+;
- Deverá suportar as tecnologias SFP e SFP+;
- Deverá possuir capacidade de vazão de ao menos 170 Gbps;
- Deverá possuir capacidade de encaminhamento de no mínimo 120 Mpps;
- Deverá ser fornecido com todas as portas ativas/licenciadas e com pelo menos 2 (dois) transceivers de 10GBase-SR, por equipamento. Os transceivers fornecidos deverão ser do mesmo fabricante ou homologados pelo fabricante (indicando a matriz de compatibilidade);
- Deverá ser entregue cordões ópticos para prover a interligação dos itens contratados nesse Termo de Referência;
- Deverá possuir buffer de pacotes de ao menos 1,5 MB;
- Deverá possuir tabela para no mínimo 12k endereços MAC;
- Deverá suportar no mínimo 512 VLAN´s simultâneas, permitir o registro dinâmico de VLAN's de acordo com o padrão 802.1q, além de oferecer suporte a VLANs baseadas em MAC;
- Deverá implementar agregação de links em modo estático e dinâmico (LACP).;
- Deverá suportar os protocolos RIPv1, RIPv2;
- Deverá implementar 802.1s - MSTP, STP BPDU Protection e BPDU Guard;
- Deverá Implementar IGMP Snooping de acordo com a RFC 2236, além de oferecer suporte aos serviços DHCP Snooping, DHCP client, DHCP Relay e DHCP protection;
- Deverá possuir no mínimo 24 interfaces de roteamento IP (VLAN Interface);
- Deverá implementar autenticação 802.1x de múltiplos usuários por porta;

- Deverá implementar controle de Acesso (ACL) baseado em endereço IPv4, IPv6 e MAC de origem e destino, porta protocolo e VLAN;
- Deverá permitir autenticação em servidores RADIUS e TACACS+ sem a necessidade de instalação de produto terceiro no chassis;
- Deverá implementar associação automática de VLAN, qualidade de serviço de acordo com usuário autenticado;
- Deverá implementar accounting RADIUS e autenticação de endereço MAC em servidor Radius. Deverá permitir também a atribuição de VLAN conforme o perfil do dispositivo cadastrado no servidor Radius;
- Deverá suportar protocolos SNMPv3, SSL e SSHv2;
- Os switches deverão possuir módulos de empilhamento de 10 Gb ou fornecer portas frontais para empilhamento, de no mínimo 2 portas de 10 Gb;
- Implementar TFTP, FTP, LLDP, LLDP-MED e Sflow;
- Deverá implementar STP BPDU Protection (BPDU Guard);
- Deverá implementar Jumbo frames com tamanho de até 9000 bytes;
- Deverá implementar IEEE 802.3ad Link Aggregation Control Protocol (LACP);
- Deverá implementar IEEE 802.1s - MSTP;
- Deverá implementar IEEE 802.3x Flow Control;
- Deverá implementar roteamento estático;
- Deverá implementar RFC 1812 IPv4 Routing;
- Deverá implementar IGMP Snooping v1, v2 e v3;
- Deverá suportar roteamento dinâmico.

[RDE02] - SWITCHES DE AGREGAÇÃO (CORE)

Aquisição de Switches de Agregação, de acordo com as especificações, além de serviço de instalação, treinamento, suporte técnico e garantia de 12 meses.

Especificações técnicas:

- Deverá possuir no mínimo 48 portas Switch 10 Gigabit;
- Deverá suportar a tecnologia SFP+;
- Deverá possuir capacidade de vazão de ao menos 840 Gbps;
- Deverá possuir capacidade de encaminhamento de no mínimo 720 Mpps;
- Deverá ser entregue cordões ópticos para prover a interligação dos itens contratados nesse Termo de Referência;
- Deverá possuir buffer de pacotes de ao menos 12 MB;
- Deverá possuir tabela para no mínimo 272k endereços MAC;
- Deverá suportar no mínimo 480 VLAN´s L3 e 4000 VLAN’s L2 simultâneas, permitir o registro dinâmico de VLAN's de acordo com o padrão 802.1q, além de oferecer suporte a VLANs baseadas em MAC;

- Deverá implementar agregação de links em modo estático e dinâmico (LACP).;
- Deverá permitir autenticação em servidores RADIUS e TACACS+;
- Deverá implementar associação automática de VLAN, qualidade de serviço de acordo com usuário autenticado;
- Deverá implementar accounting RADIUS e autenticação de endereço MAC em servidor Radius. Deverá permitir também a atribuição de VLAN conforme o perfil do dispositivo cadastrado no servidor Radius;
- Deverá suportar roteamento dinâmico em protocolo público.

[RDE03] – PONTOS DE ACESSO WIRELESS

Especificações técnicas:

- Deverão ofereçam suporte a padrões Wi-Fi de alta velocidade, como 802.11ac Wave 2 e 802.11ax (Wi-Fi 6), fornecendo velocidades de até 3,5 Gbps.
- Deverá possuir múltiplas portas Ethernet Gigabit, permitindo a conexão com uma variedade de dispositivos de rede, incluindo switches, roteadores e firewalls.
- Deverá incluir recursos avançados de gerenciamento e segurança, como autenticação de usuário baseada em certificado digital, filtragem de conteúdo e controle de acesso baseado em função, para garantir a integridade e a confidencialidade dos dados da rede.
- Deverá possuir design compacto e discreto, adequado para instalação em tetos, paredes ou prateleiras, permitindo uma instalação fácil e flexível em qualquer ambiente, contendo os elementos de montagem para sua fixação;
- Deverá oferecer gerenciamento de rede baseado em nuvem, permitindo o Monitoramento remoto e a configuração simplificada de múltiplos pontos de acesso em várias localizações.
- Deverá possuir ao menos 3 antenas de forma que sejam capazes de transmitir e receber sinais nas polarizações vertical e horizontal, aumentando a flexibilidade e a robustez da comunicação sem fio;
- O sistema de conectividade entre os equipamentos deverá permitir movimentação de clientes entre os pontos de acesso de forma transparente a partir de controle integrado, permitindo que os dispositivos móveis se conectem automaticamente ao ponto de acesso mais próximo à medida que se movem pela área de cobertura sem fio;
- Cada access point deverá suportar até 512 dispositivos simultâneos conectados à rede sem fio, permitindo que múltiplos usuários acessem a internet ou aplicativos de rede de forma simultânea e sem interrupções;
- O equipamento deverá ter ajustes que permitam que o administrador da rede ajuste a potência de saída e a direção do sinal para otimizar a cobertura e minimizar as interferências em ambientes com muitos obstáculos ou alta densidade de usuários;
- Deverá ser compatível com tecnologia MESH estendendo a cobertura sem fio em áreas que não podem ser alcançadas por um único ponto de acesso;

- A infraestrutura de pontos de acesso deverá suportar a configuração de múltiplos SSIDs (identificadores de rede sem fio) e VLANs (redes virtuais), permitindo a segmentação da rede sem fio para diferentes usuários, grupos ou aplicativos, e a otimização da cobertura e da largura de banda para cada segmento da rede;
- Deverá ser compatível com os protocolos de rede: IPv4, IPv6, DHCP, VLAN, SNMP v1/v2c/v3, SSH, TACACS+, RADIUS, LLDP, 802.1X, LACP, IGMP, PIM-SM, PIM-SSM, OSPF, RIP, BGP, GRE, VRRP, HSRP;
- Deverá ser compatível com os padrões de rede sem fio: IEEE 802.11a/b/g/n/ac/ax, WMM (Wi-Fi Multimedia), WMM-PS (Wi-Fi Multimedia Power Save), WPA/WPA2-PSK, WPA/WPA2-Enterprise, WPA3-Personal, WPA3 Enterprise, 802.11r, 802.11k, 802.11v, 802.11w, 802.11u, 802.11e, 802.11i;
- Deverá ser compatível com tecnologia de antena adaptativa, transmissão e recepção MIMO (Multiple-Input Multiple-Output), MU-MIMO (Multi-User Multiple Input Multiple-Output), OFDMA (Orthogonal Frequency Division Multiple Access), BSS Coloring, Wi-Fi CERTIFIED 6;
- Deverão ser compatíveis com a controladora de acesso da cisco.

[RDE04] Firewalls

Gabinete:

- Deverá ocupar, no máximo, 2U de altura para instalação e uso em rack de 19” padrão de mercado;
- Deverá possuir, no mínimo, duas fontes de energia redundantes instaladas e configuradas;
- Deverá ser possuir licença de sistema operacional Windows 11 de 64 bits Professional em português do Brasil
- Para todos os equipamentos deverá ser fornecido bandeja ou suporte para montagem em rack;
- Assinaturas fornecidas pelos provedores da solução para IPS, Antivírus e os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- Os equipamentos que compõem a solução devem estar homologados pela Anatel.

Conectividade:

- Possuir ao menos 18 interfaces 1 GE RJ45;
- Possuir ao menos 8 interfaces 1 GE SFP com transceivers inclusos;
- Possuir ao menos 4 interfaces 10 GE SFP+ com transceivers inclusos;

Características de Firewall:

- Throughput de, no mínimo, 3 Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas concorrentemente;
- Throughput de, no mínimo, 12 Gbps de VPN IPSec;

- Estar licenciado para, ou suportar sem o uso de licença, 2000 túneis de VPN IPSEC Site-to-Site simultâneos;
- Suporte a, no mínimo, 300 mil novas conexões por segundo;
- Suportar no mínimo 3 Gbps de throughput de Inspeção SSL;
- Suportar a criação de no mínimo 10 instâncias virtuais;
- Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo; • Deverá permitir o funcionamento em modo transparente tipo “bridge”;
- Deverá suportar PBR – Policy Based Routing;
- Deverá possuir controle de acesso à Internet por endereço IP de origem e destino;
- Deverá possuir controle de acesso à Internet por subrede;
- Deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;
- Deverá suportar controles por zonas de segurança;
- Deverá suportar controles de políticas por porta e protocolo;
- Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;
- Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado.
- Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;
- Deve ser possível realizar um espelhamento do tráfego de-criptografado.
- Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;
- A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.
- Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall
- Suporte a objetos e regras multicast;
- Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego.

- Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos.
- Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução.
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

Características de Funcionalidades NGFW:

- A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);
- Os hardwares e os softwares que compõem a solução devem ser do mesmo fabricante;
- As funcionalidades de NGFW devem ser ofertadas no mesmo appliance, não sendo permitido a composição de equipamentos separados para cada uma das funções;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações com ou sem identificação de porta TCP ou protocolo/endpoint;

Controle de Aplicações:

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- Reconhecer pelo menos 2000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, dap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para eles;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para eles;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc);
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;
- Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da

aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet;

- Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP;

Prevenção de ameaças:

- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra-ataques de negação de serviços;
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Detectar e bloquear a origem de portscans;
- Bloquear ataques efetuados por worms conhecidos;
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- Identificar e bloquear comunicação com botnets;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de call-back;
- A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;
- Deve ser possível filtrar assinaturas com base no identificador CVE;
- Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador;
- As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;
- Deve incluir proteção contra-ataques de negação de serviços;
- Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

Filtro de URLs:

- Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

- Deve possuir a função de exclusão de URLs do bloqueio;
- Permitir a customização de página de bloqueio;
- Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário.
- Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego.
- Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website.
- Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado.
- Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;
- Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo.
- Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;

Identificação de usuários:

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

Filtro de dados:

- Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

Características de VPN:

- Suportar VPN IPSec Site-to-Site;
- A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Gerenciamento e Suporte:

- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- Deverá suportar tags de VLAN (802.1Q);
- Deverá possuir suporte a agregação de links via 802.3ad LACP;
- Deverá possuir ferramenta de diagnóstico do tipo tcp dump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;
- Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

- Deverá possuir integração com tokens para autenticação de duplo fator;
- Deverá suportar single-sign-on;
- Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;
- Deverá suportar roteamento estático para IPv4 e IPv6;
- Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP, RIP);
- Deverá suportar ECMP;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia, tais como: H.323 e SIP;
- Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deverá possuir mecanismo de anti-spoofing;
- Deverá permitir criação de regras definidas pelo usuário;
- Deverá suportar sFlow ou Netflow;
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- Deverá permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer via espelhamento;
- Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster, eventos de segurança e estatísticas das verificações de saúde da camada SD-WAN;
- Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais;
- Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;
- Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- Deverá suportar ambientes multi-cloud;

- Deverá possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;

Centralizador de Logs e Relatórios para os Equipamentos Firewall:

- A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução de NGFW, e ter como objetivo a centralização de logs e geração de relatórios para a solução;
- Poderá ser entregue em formato de appliance físico ou appliance virtual;
- Deverá estar devidamente licenciada para:
- Suportar a coleta de, no mínimo, 5 GB de logs diários;
- Permitir espaço de armazenamento de, no mínimo, 4 TB;
- Caso a solução seja entregue como appliance virtual, este deve suportar:
- Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;
- Não deverá existir limite para o número de vCPUs no appliance virtual;
- Não deverá existir limite para a expansão da memória RAM no appliance virtual;
- Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
- Caso a solução seja entregue como appliance físico, este deve suportar:
    - Pelo menos duas interfaces 1GE padrão RJ45;
    - Suportar a configuração de RAID 0 e 1 para os discos internos;
    - Possuir fonte de alimentação interna, redundante e hot-swap;
- Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
- Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
- Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;
- Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
- Deve suporta a visualização de logs e geração de relatórios;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- Deve possuir mecanismos de remoção automática para logs antigos;

- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
- Deve permitir exportar os logs no formato CSV;
- Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
- A solução deve ter relatórios predefinidos;
- Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
- Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real; • Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- Permitir o envio por e-mail relatórios automaticamente;
- Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- Deve permitir o uso de filtros nos relatórios;
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- Permitir especificar o idioma dos relatórios criados;
- Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Deve permitir visualizar em tempo real os logs recebidos;
- Deve permitir o encaminhamento de log no formato syslog;
- Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
- Deve permitir gerar alertas de eventos a partir de logs recebidos;
- Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;

Suporte e Garantia:

- Deverá ter Suporte 24/7 com acesso a atualizações de software e firmware durante o período de garantia.

[RDE05] Servidores Para Suporte à Operação;

Gabinete:

- Deverá ocupar, no máximo, 2U de altura para instalação e uso em rack de 19" padrão de mercado;
- Deverá possuir, no mínimo, duas fontes de energia redundantes instaladas e configuradas;
- Deverá possuir, pelo menos, duas portas USB 2.0;
- Deverá ser possuir licença de sistema operacional Windows Server 2022 ou superior, no modelo Datacenter;

Processador:

- Deverá possuir 2 (dois) processadores de arquitetura de servidor com tecnologia x86; com no mínimo 8 (oito) núcleos de processamento, clock frequência mínima de 1.8 GHz e turbo clock de no mínimo 3.0GHz, ou apresentar processador similar ou superior à estas configurações;
- Deverá ter no mínimo 15MB de memória cache;
- Deverá suportar memórias de até 4500 MT/s;

Memória:

- Deverá possuir, no mínimo instalado de 64GB de memória RAM tipo DDR5 ECC
- Deverá suportar expansão para no mínimo 512GB;
- As memórias deverão ter frequência de trabalho de no mínimo 4500 MHz;

Armazenamento:

- Deverá possuir no mínimo 2 discos rígidos instalados com a seguinte configuração:
    - 2 Discos rígido de 4 TB NL SAS ou SATA;
    - Configuração em RAID1 •
- Deverá suportar até 4 discos instalados internamente no servidor;

Conectividade e Recursos:

- Deverá possuir, no mínimo, duas portas de rede Gigabit Ethernet 10/100/1000, instaladas fisicamente;
- Deverá possuir, no mínimo, duas portas de rede 10 Gbps SFP+;
- Deverá possuir recursos para acesso remoto OOB (out-of-band);

Suporte e Garantia:

- Deverá ser fornecido com período de Garantia de 60 meses (5 anos) de garantia on-site com resposta no próximo dia útil.
- Deverá ter Suporte 24/7 com acesso a atualizações de software e firmware durante o período de garantia.

9. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – CFTV

9.1 MÃO-DE-OBRA E MATERIAIS PARA INSTALAÇÃO

MATERIAIS

- Patch panels CAT6 – 19”
- Ponto de rede para cada câmera
- Cabos UTP CAT6 para interligação
- Patch cords CAT6 para interconexão
- Conectores RJ45
- Eletrocalhas, dutos, conduítes e acessórios de fixação
- Suportes e caixas de passagem para câmeras Serviços
- Levantamento técnico e marcação dos pontos de instalação
- Montagem e fixação dos suportes das câmeras
- Passagem de cabeamento estruturado para CFTV (UTP CAT6)
- Crimpagem e identificação dos pontos
- Instalação física das câmeras (interna e externa)
- Interligação das câmeras aos switches PoE
- Instalação e configuração dos switches PoE em racks
- Instalação de servidor NVR e configuração do software VMS
- Configuração das câmeras IP com todos os parâmetros técnicos exigidos
- Criação de zonas privativas e cercas virtuais
- Testes de visualização, gravação, detecção de movimento e cruzamento de linha • Documentação técnica e certificação dos cabos
- Todos os materiais deverão ser homologados pela Anatel quando aplicável
- As câmeras deverão possuir certificações CE, FCC ou UL
- O sistema deverá ser entregue operando com todas as funcionalidades exigidas Todos os serviços deverão seguir as boas práticas de instalação, respeitando normas técnicas e de segurança, garantindo a durabilidade e confiabilidade do sistema.

9.2 CÂMERAS DE REDE TIPO DOME E BULLET

[CFTV01] – CÂMERA DE REDE TIPO BULLET DE 2.0 MEGAPIXELS

A câmera IP para uso interno deverá possuir as seguintes características:

- Câmera do tipo bullet, com dispositivo de captura de 1/2.9" ou maior, CMOS de 2MP com varredura progressiva;
- Possuir resolução mínima de 2.0 Megapixels;
- Iluminação mínima de 0.15Lux (F1.8) no modo colorido e 0 Lux no modo Preto C Branco com IR ligado;
- Possuir lente fixa de 2.8mm;
- Função Day/Night real com filtro ICR;
- Deverá possuir iluminação IR para 15 metros;
- Possuir compensação da luz de fundo;
- A câmera deve possuir função de aprimoramento de contraste através de WDR;
- Permitir a criação de áreas poligonais para detecção de movimento;
- A câmera deve permitir a criação de zonas privativas na área de imagem;
- Possuir controle automático de ganho;
- Possuir Balanço do Branco manual e automático;
- Possuir variação de obturador eletrônico entre mínimo e máximo;
- A câmera deve possuir análise de vídeo embarcada para detecção de cruzamento de linha (cerca virtual);
- Possuir interface de rede, conexão através de RJ45 (10/100BASE-T);
- Possuir as compressões de vídeo MJPEG, H.264 e H.265;
- Possuir as seguintes resoluções de vídeo variando entre 1920 x 1080 e 1280 X 720;
- Permitir a taxa de atualização de 30fps em todas as resoluções, utilizando os codecs H.264 ou H.265;
- Possuir os seguintes métodos de controle de taxa de bits: CBR ou VBR;
- Suportar os métodos de endereçamento IPv4 e IPv6;
- Permitir a gravação de imagens em cartão de memória micro-SD;
- A linguagem da interface de usuário deve estar no idioma português;
- Deve ser compatível com os seguintes navegadores: Internet Explorer, Firefox, Google Chrome;
- Ser resistente a entrada de água e poeira com certificação IP67;
- Alimentação 12VDC e PoE (IEEE 802.3af, Classe3);
- Temperatura de operação de -30ºC a +55ºC;
- A câmera deve possuir as certificações internacionais FCC ou UL, ou CE;
- O fabricante deve possuir empresa de assistência técnica autorizada no Brasil.

[CFTV02] – CÂMERA DE REDE TIPO DOME EXTERNA DE 2.0 MEGAPIXELS

A câmera IP para uso externo deverá possuir as seguintes características:

- Câmera do tipo dome, com dispositivo de captura de 1/2.9" ou maior, CMOS de
- 2MP com varredura progressiva;
- Possuir resolução mínima de 2.0 Megapixels;
- Iluminação mínima de 0.15Lux (F1.8) no modo colorido e 0 Lux no modo Preto C Branco com IR ligado;
- Possuir lente fixa de 2.8mm;
- Função Day/Night real com filtro ICR;
- Deverá possuir iluminação IR para 20 metros;
- Possuir compensação da luz de fundo;
- A câmera deve possuir função de aprimoramento de contraste através de WDR;
- Permitir a criação de áreas poligonais para detecção de movimento;
- A câmera deve permitir a criação de zonas privativas na área de imagem;
- Possuir controle automático de ganho;
- Possuir Balanço do Branco manual e automático;
- Possuir variação de obturador eletrônico entre mínimo e máximo;
- A câmera deve possuir análise de vídeo embarcada para detecção de cruzamento de linha (cerca virtual);
- Possuir interface de rede, conexão através de RJ45 (10/100BASE-T);
- Possuir as compressões de vídeo MJPEG, H.264 e H.265;
- Possuir as seguintes resoluções de vídeo variando entre 1920 x 1080 e 1280 X 720;
- Permitir a taxa de atualização de 30fps em todas as resoluções, utilizando os codecs H.264 ou H.265;
- Possuir os seguintes métodos de controle de taxa de bits: CBR ou VBR;
- Permitir a criação e configuração de 2 (dois) perfis independentes de fluxos de vídeo;
- Suportar os métodos de endereçamento IPv4 e IPv6;
- Permitir a gravação de imagens em cartão de memória micro-SD;
- A linguagem da interface de usuário deve estar no idioma português;
- Deve ser compatível com os seguintes navegadores: Internet Explorer, Firefox, Google Chrome;
- Ser resistente a entrada de água e poeira com certificação IP67;
- Alimentação 12VDC e PoE (IEEE 802.3af, Classe3);
- Temperatura de operação de -30ºC a +55ºC;
- A câmera deve possuir as certificações internacionais FCC ou UL, ou CE;
- O fabricante deve possuir empresa de assistência técnica autorizada no Brasil.

[CFTV03] – STORAGE PARA NVR 32 CANAIS

Requisitos gerais:

- Deverá ser um equipamento desenvolvido especificamente para a função de processamento de câmeras de segurança IP em rede (não deverão ser aceitos equipamentos adaptados ou desenvolvidos para outras finalidades);
- Deverá possuir gabinete tipo rack padrão 19" (dezenove polegadas) com altura máxima de 2U (Rack Unit), entregue com trilhos e quaisquer outros componentes necessários para instalação em rack padrão 19" (dezenove polegadas);
- O equipamento cotado deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;

Características técnicas:

- Deverá possuir pelo menos 1 (um) processador X86, com frequência baseada em processador de pelo menos 3.6 GHz, frequência turbo máx. de pelo menos 4.6 GHz, no mínimo 6 núcleos, no mínimo 10 threads, cache de pelo menos 12 MB, TDP de no máximo 80 W, e pelo menos 16 linhas PCI Express;
- Processador deve possuir capacidade integrada de processamento gráfico com performance de pelo menos 1 GHz e memória gráfica de pelo menos 112 GB.
- Possuir, pelo menos, memória instalada de 16GB DDR4 SDRAM, dispostas em 2 (dois) pentes de 8 GB expansível a pelo menos 128 GB;
- Os canais de memória deverão ser preenchidos obedecendo as regras de máxima desempenho para o sistema conforme recomendação do fabricante do servidor;
- Possuir 04 slots DIMM, suporte para módulos de memória DDR4 até pelo menos 2666MHz;
- Possuir pelo menos 8 (oito) conectores SATA 6 Gb / s interfaces integradas;
- Deve possuir no mínimo 1 x conector M.2 e suporte a SSD PCIe x4 / x2) (M2A) não sendo aceitos adaptadores (ex.: PCI) para tal funcionalidade por reduzir a taxa de comunicação efetiva;
- Deverá possuir 1 (uma) unidade de estado sólido (SSD) com capacidade de, no mínimo, 240 GB SSD M.2 onde deverá ser instalado o sistema operacional e o(s) aplicativo(s);
- Deve possuir interface gráfica de vídeo integrada com no mínimo 3 (três) saídas de vídeo; sendo 1(uma) porta D-Sub, suportando uma resolução máxima de pelo menos 1920x1200 a 60 Hz; 1 (uma) porta DVI-D, com resolução máxima de pelo menos 1920x1200 a 60 Hz e 1 (um) DisplayPort, suportando uma resolução máxima de pelo menos 4096x2304 a 60 Hz;
- Deve possuir pelo menos uma porta USB 3.1 Gen 2 e pelo menos 4 portas USB 3.1 Gen 1 ou superior;
- Deve possuir pelo menos 2 (duas) Interfaces de rede RJ-45 Gigabit Ethernet Controlador Integrado
- Deverá possuir pelo menos 8 (oito) discos rígido HDD 3,5 polegadas apropriados para sistemas de segurança e vigilância de, no mínimo, 8 TB, cache de pelo menos 192 MB, pronto para operação 24x7, interface SATA 6 Gb/s taxa de transferência sustentada de pico de pelo menos 200 MB/s, potência média de trabalho de no máximo 9 W preparado para operar no mínimo 8600 horas por ano, mantendo alta AFR de <1%, os discos rígidos. Deverão ser designados para carga de trabalho de videovigilância e operação de gravação em tempo integral;

- Não deverão ser aceitos equipamentos com discos rígidos de uso comum para computadores, não fabricados e com características especificas para videomonitoramento, conforme informação do fabricante dos HDDs;
- Os HDDs dos equipamentos já deverão estar devidamente instalados e configurados no modo de agrupamento RAID 5;
- Deve possuir discos e baias adequados para permitir a funcionalidade de troca a quente dos discos;
- Deve permitir a configuração de arranjos de disco em agrupamento pelo menos nas modalidades RAID 0, RAID 1, RAID 5 e RAID 10;
- O equipamento deverá suportar armazenamento bruto de pelo menos 192TB;
- Ventilação apropriada à configuração, com fontes de alimentação redundantes de, no mínimo, 750 W reais cada, bivolt;
- Deverá possuir faixa de tensão de entrada de 100 a 240V (automático) à 60Hz, com fonte interna ao equipamento (não deverão ser aceitos equipamentos que operem em tensão de entrada em 12Vdc ou 24Vdc);
- O equipamento deverá possuir ventiladores internos originais do equipamento, necessários para a perfeita refrigeração do sistema interno do servidor na sua configuração máxima;
- Deverá suportar pelo menos 10 (dez) baias do tipo hot-swappable de 3,5" e pelo menos 2 (duas) baia de 2,5"
- A temperatura de operação deverá ser de pelo menos 0°~60°C;
- Deve possuir pelo menos 1 (um) slot PCI Express x16, executando x16 (PCIEX16); 1 (um) PCI Express x16, executando x8 (PCIEX8), 2 (dois) slots PCI Express x1
- Equipamento não deverá ser aceito caso sejam utilizados discos em gabinetes externos ao servidor;
- Deverá possuir sistema operacional Windows Enterprise 10 IoT ou superior, já gravado e totalmente compatível com o equipamento;
- O sistema operacional deverá possuir os recursos (e os eventuais softwares adicionais se necessários) para implementar:
- funcionalidade para bloqueio ao instalar novos app’s;
- criptografia dos discos;
- boot seguro;
- suportar geração de consulta de integridade de dispositivos gerenciados;
- autenticação de múltiplos fatores ao fazer logon no servidor;
- controle de atualização do Windows de forma remota e com horário agendado em modo avançado;
- modo leitura de pastas e arquivos somente, sem permitir escrita, modificação, ou deletar arquivos;
- sistema operacional deverá sempre carregar aplicativos padrão autorizados ao logon, controlado pelo administrador de rede;
- Considerar o fornecimento de um switch Poe 8 portas.

A CONTRATADA deverá fornecer a respectiva licença de uso definitiva do software de sistema operacional.

O fabricante deverá possuir página de suporte técnico na Internet com disponibilidade das últimas versões de drivers, firmwares.

Garantia de total de 1 (um) ano on-site, disponibilizada pelo fabricante.

Os equipamentos deverão, comprovadamente, estar em fase normal de produção/fabricação, no portfólio de produtos do(s) fabricante(s), não sendo aceitos equipamentos descontinuados pelo(s) fabricante(s).

Equipamentos e com previsão de continuidade de fabricação de no mínimo um ano. Caso seja descontinuado no período mencionado deverá ser substituído.

Sistema e Integração

O sistema deve suportar:

- Gerenciamento de armazenamento de vídeo;
- Deve ser capaz de armazenar conteúdo em vídeo que não são críticos em diferentes topologias e arquitetura de armazenamento;
- Deve suportar a detecção de movimento, independente do modelo da câmera; seja pelo servidor ou pela câmera; ou simultaneamente;
- Plataforma Aberta: Deve fornecer API / SDK de forma gratuita e suportar integração com hardware ou aplicativos de terceiros.
- Instalação em Windows 64 bits
- Deve permitir exibição do alerta gerado pelos dispositivos, através do processamento dos metadados recebido das câmeras / encoders, mostrando os quadros (overlay) nos formatos e cores gerados pelos dispositivos. Tudo isto deve ser permitido através do dispositivo integrado via ONVIF.
- Deve permitir a integração de sistemas de controle de acesso de forma bidirecional sem a necessidade de interfaces físicas para tal.
- Deve permitir que alarmes do sistema de acesso sejam vistos na interface do usuário do Sistema de Vídeo assim como o vídeo e os alarmes dele sejam vistos na interface do Sistema de Acesso.
- Deve possibilitar total compatibilidade com, no mínimo, duas versões anteriores do sistema;

[CFTV07] Software de Gerenciamento e interface para aplicativo de smartphone

- Gerenciamento centralizado: O software de administração deve oferecer um acesso único e consolidado para configuração dos servidores de gravação;
- Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário;
- Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando métodos como a Universal Plug and Play, Broadcast e varredura por faixa de IP;

- Opção de configuração em massa: Altera as configurações em vários dispositivos ao mesmo tempo com poucos cliques; independentemente de estarem no mesmo site ou em sites remotos;
- Comportamento da aplicação adaptável: Guia usuários novatos, enquanto usuários experientes podem otimizar o sistema para seu uso eficiente;
- Importação de dados de configuração off-line: Permite a edição off-line de dados de configuração, incluindo câmeras e as definições de dispositivos;
- Sistema automático de pontos de restauração: um ponto de restauração é criado a cada vez que uma mudança de configuração é feita. Permite a reversão fácil de pontos de configuração previamente definidos e permite o cancelamento de mudanças de configuração indesejados e a restauração de configurações anteriores válidas;
- Deve permitir a personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando / desabilitando partes da interface para evitar o acesso indevido a ações restritas;
- Ser nativamente compatível com Microsoft Active Directory para gestão de usuários e perfis de acesso do Windows e permitir autenticação de usuário única (SSO) ;
- Trabalhar com banco de dados centralizado de fabricantes reconhecidos de mercado como SQL Server, Oracle ou MySQL ;
- Deve permitir acesso remoto para o software de visualização e aplicativo para visualização em web browsers, com opção de conexão segura no acesso à câmera (HTTPS);
- Ter servidor de Web embutido para download de softwares e plug-ins;
- Ter histórico de provas exportadas por usuário e arquivo;
- Ter histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras;
- Pode ser instalado em conjunto com o servidor de gravação;
- Fornecer streams múltiplos de vídeo ao vivo para diferentes clientes.

Serviço de Gestão de Eventos e Alarmes

Deve fornecer uma caixa de diálogo de configuração no estilo Microsoft Outlook, na qual eventos predefinidos e personalizados são usados nas regras para acionar ações.

Deve ter as seguintes categorias de eventos:

- Hardware: dispositivos de hardware físico conectados ao sistema;
- Dispositivos: certas funções e estados de dispositivos disponíveis através de dispositivos de hardware conectados;
- Externo: relacionado às integrações do VMS;
- Servidor de gravação: funções de arquivamento e banco de dados;
- Análise: a partir de aplicativos e sistemas de análise integrados;
- Definido pelo usuário: Eventos configurados de forma personalizada, permitindo que os usuários disparem.

Perfis de horário.

- Ter gerenciamento de evento / alarme de ponto único: gerenciamento central de todos os alarmes internos do sistema e alarmes externos de segurança.
- Ter suporte à associação de alarmes a mapas.
- Deve possuir um Gerenciador de Alarmes que permita:
- Lista de alarmes com amplos recursos de classificação e filtragem;
- Visualização instantânea de vídeo gravado de câmeras primárias e relacionadas, no momento do incidente;
- Imagem em miniatura da câmera principal, no momento do incidente;
- A opção de desativação de alarme deve permitir que os usuários suprimam alarmes de um determinado dispositivo por um período especificado;
- Relatórios de tratamento de alarmes, fornecendo informações sobre a entrada e o desempenho do tratamento de alarmes.

Serviço de Gravação e gerenciamento das gravações

O sistema deve suportar:

- A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado.
- O software client pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação.
- Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, MPEG4, MPEG4 ASP, H.264 e MxPEG, H.265.
- Detecta automaticamente os modelos de câmeras durante a instalação.
- Número ilimitado de câmeras instaladas.
- Tecnologia de gravação: banco de dados seguro de alta velocidade de imagens JPEG ou fluxos MPEG4 e H264.
- Velocidade de gravação: Mais de 30 frames por segundo por câmera, limitado apenas pelo hardware e rede.
- A qualidade da gravação depende inteiramente da câmera e do encoder: não há limitação de software.
- Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage.
- Exportação de vídeo configurável por hora ou diária, com passagem automática opcional para unidade de rede de maior capacidade de armazenamento, com imagens disponíveis para reprodução de forma transparente para o operador.
- Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail.
- Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso.
- Ativação de presets e patterns quando acontecem determinados eventos.

- Programação para ativação do pattern em períodos diferentes: isto é, diferente para dia e noite / semana etc.
- Em eventos pré-definidos comandos são enviados automaticamente para exibir vídeo ao vivo em computadores remotos.
- O servidor de gravação é executado como um serviço do Windows.
- Gravação em multi estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo até a redução da taxa de frames automática para atender a demanda de tempo de configuração.
- Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera).

Software De Visualização De Gravação (Operação)

O sistema deve suportar:

- Visualização ao vivo e reprodução: Clients desde dispositivos móveis a computadores com suporte para visualizar até 100 câmeras de vários servidores ao mesmo tempo.
- Exibições de Janelas/Layouts: Trabalha com exibições contendo até 10x10 câmeras, Hot spot, Matriz, Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, mapas HTML, distribuídos em todos os monitores do computador.
- Matriz Virtual: exibições de controle de câmara ao vivo em computadores remotos para visualização distribuída.
- Controle de Entradas/ Saídas de Alarme: Das câmeras ou dispositivos de I/O, de forma a criar botões/eventos manuais, ou receber sinais de sistemas de intrusão ou controle de acesso.
- Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera por um tempo predefinido.
- Dupla autenticação, exigindo com que o usuário tenha autenticação de um usuário supervisor para conseguir se autenticar no software, protegendo o sistema de acessos indevidos.

Busca, backup e dados seguros

O sistema deve suportar:

- Backup de Evidência: JPEG, AVI, WAV e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros, notas de usuários e impressão de relatórios.
- Autenticação: contas de usuário do Microsoft Active Directory e nativos.
- Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera.
- Histórico: Todas as ações do usuário por tempo, localizações e câmeras, e toda a operação do sistema.

- Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS.
- Visualização de até 16 câmeras com tempo sincronizado durante a reprodução.
- Linha de tempo de atividade com recurso de lupa; possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados;
- Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection).
- Provas podem ser geradas com relatório impresso, imagem em JPEG, AVI ou no formato proprietário (com visualizador incluso), ou ainda pode exportar vídeo em formato MKV padrão.
- Exportação de vídeo digital com zoom para visualizar área de interesse, e para minimizar o tamanho do arquivo exportado.
- Criptografia e opção de senha de proteção para as gravações e os arquivos exportados.
- Capacidade de adicionar comentários às provas exportadas, também criptografadas.
- Possuir interface proprietária, desenvolvida pelo mesmo fabricante e com mesmo código fonte do servidor de gerenciamento e gravação.
- Possuir mesma comunicação/ conceito visual do server side.
- Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento/ banco de dados SQL Server.
- Opção para enviar imagens por e-mail.

Aplicativo de visualização através do Web Browser

O sistema deve suportar:

- Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 16 câmeras simultaneamente, advindos do mesmo ou diferentes servidores.
- Navegação de vídeo avançadas, incluindo reprodução lenta/rápida, salto a data/hora e pesquisa de movimento no vídeo.
- Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista.
- Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador.
- Importação de mapas estáticos ou ativos para navegação rápida entre câmeras.
- Controle do relé de saída de alarme.
- Visão geral das sequências com movimento detectado e janela de visualização.
- Visão geral de eventos / alertas.
- Controle remoto de zoom sinalando um retângulo.
- Criar arquivos AVI ou criar imagens JPEG geradas a partir de conteúdo gerado pelo software, seja estas imagens advindas de vídeo ou não;
- Imprimir relatórios de incidentes com os comentários livres e pertinentes ao usuário.

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

Matriz de Vídeo

O sistema deve suportar:

- Matriz virtual mostrando o vídeo ao vivo diretamente de no mínimo 04 câmeras por cada tela individual a serem acionadas remotamente por comandos remotos e manuais;
- Sequência de câmeras tipo FIFO (first-in-first-out);
- Vários eventos podem controlar um monitor de matriz e eventos únicos pode controlar vários monitores.
- Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera.

[CFTV06] Cliente Celular

O sistema deve suportar:

- Aplicativos gratuitos para dispositivos baseados em sistema operacional Android (Google), iOS (Apple) e Windows Phone 8;
- Permitir a visualização de múltiplas imagens simultaneamente.
- Busca e reprodução de vídeo gravado.
- Toque na tela do dispositivo para zoom digital e diferentes modos de visualização da imagem.
- Salvar ou compartilhar uma foto do vídeo exibido ao vivo.
- Permitir a utilização da câmera de vídeo do dispositivo móvel como um gerador de imagens para o sistema principal.

Opções de Integração

O sistema deve ser:

- Compatível com software de integração de videovigilância com sistemas ATM ou POS (registro de fluxo de produtos/ pessoas para a gestão de prevenção de perdas e fraudes);
- Compatível com software supervisório de alarmes e estado de dispositivos para grandes instalações.
- Integrado com sistemas de controle de acesso, alarmes, portões, sistemas de gestão, ótica usando os eventos de I/O, eventos internos, eventos TCP/IP ou por OPC DA.
- Ter SDK gratuito para integração do vídeo em outros produtos usando a API para exibir imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período, e buscar por movimento.
- Criar, importação e usar páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização.

Licenciamento

Deve estar composto por:

- Licença de Sistema
- Obrigatório para a instalação do produto
- Deve abranger a instalação de um número ilimitado de servidores usando a mesma licença do software de código e a designação de servidores.
- A licença contempla um número ilimitado de servidores de gravação, softwares clientes, clientes web e aplicativos móveis.
- Não tem validade e ser de propriedade do contratante.
- Todos os softwares clientes não deverão ser licenciados e podem ser instalados e utilizados em qualquer número de computadores, de forma gratuita.
- Acordo de Manutenção do Produto: Esta licença garante a aquisição e uso de forma gratuita de todas as atualizações dos produtos. Deverá ser adquirida para 3 anos.

Expansão do Sistema

- A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras.
- O número de servidores de gravação deve permitir ser ampliado a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto.
- O número de câmeras pode ser ampliado independentemente da quantidade de servidores de gravação e/ou estações de operação do sistema.
- O número de clientes de operação e de dispositivos móveis, poderá ser ampliado a qualquer momento sem necessidade de licenciamento adicional.

[CFTV04] – NVR

Equipamento utilizado em sistemas de videomonitoramento IP para gravar, armazenar, gerenciar e visualizar imagens de até 32 câmeras de rede (IP) simultaneamente.

Abaixo estão descritas as principais características técnicas e funções desse tipo de equipamento:

- Suporta até 32 câmeras IP simultâneas, com visualização em tempo real e gravação.
- Permite configurar gravação 24h, por horário ou por eventos (movimento, alarme etc.).
- Acesso às imagens em tempo real.
- Busca e reprodução de gravações por data/hora, evento ou marcações.
- Administração de todas as câmeras conectadas: configurações, atualizações, posicionamento etc.
- Criação de múltiplos usuários com diferentes permissões (admin, operador, visitante).

[CFTV05] – SWITCH POE 24 PORTAS

Equipamento de rede que desempenha funções essenciais de comutação de dados e também fornece alimentação elétrica a dispositivos compatíveis (como câmeras IP e etc.) através do mesmo cabo Ethernet (Cat5e, Cat6 etc.).

- 24 portas RJ45 (10/100/1000 Mbps – padrão Gigabit Ethernet).
- Compatível com padrões IEEE 802.3af (PoE) e 802.3at (PoE+).
- Capacidade de fornecer até 15,4 W por porta (PoE) ou 30 W por porta (PoE+).
- Potência total estimada entre 250 W e 400 W,
- Throughput elevado, geralmente de 48 Gbps a 56 Gbps.
- Tabela MAC com capacidade de armazenar milhares de endereços.
- Latência baixa para aplicações em tempo real.
- Switch gerenciável (Managed):
    - Interface via Web, CLI, SNMP ou Telnet.
    - VLANs, QoS, Spanning Tree, RSTP/MSTP, LACP, port mirroring, ACLs.
    - Monitoramento de tráfego e consumo PoE por porta.

Recursos de segurança:

- Controle de acesso por MAC/IP.
- Proteção contra tempestades de broadcast e loops de rede.
- Isolamento de portas.

Construção e instalação:

- Montável em rack 19” (1U ou 2U).
- Ventilação ativa (com cooler) ou passiva. • Fonte interna AC (geralmente 100~240V, 50/60 Hz).
- Transmissão de dados em rede local (LAN) – comuta pacotes de dados entre dispositivos conectados.
- Fornecimento de energia via cabo de rede – elimina a necessidade de fontes ou tomadas próximas dos dispositivos PoE.
- Gerenciamento de rede – em modelos gerenciáveis, permite controle avançado de tráfego e segurança.
- Priorização de tráfego (QoS) – essencial para voz sobre IP e vídeo.
- Segmentação de rede com VLANs – para maior segurança e organização da rede.

10. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA - EQUIPAMENTOS DE REDE RÁDIO

10.1 CONSOLE DE DESPACHO E SOFTWARE DE GERENCIAMENTO.

[RR01] Console de Despacho

Os consoles de despacho IP são equipamentos responsáveis por permitir a interação entre os despachantes (central de operações) e as equipes de campo que fazem uso, através das repetidoras, dos rádios móveis e rádios portáteis por rádio frequência analógica e/ou digital, também integrando com a telefonia através dos ramais SIP oriundos de Central Telefônica Digital, garantindo as funcionalidades presentes nas comunicações de forma rápida e segura. Para isto

deve utilizar-se dos mais modernos recursos em hardware e software garantindo a funcionalidade do sistema.

O sistema de console de despacho deverá ser completamente compatível com os equipamentos em operação bem como os softwares utilizados no serviço de despacho do rádio, com o objetivo de permitir o escalonamento / crescimento do sistema atual sem perda de recursos e/ou funcionalidades, integrando as centrais regionalizadas e permitindo a qualquer tempo a centralização ou descentralização dos serviços através da rede TCP/IP;

O subsistema de consoles de despacho deverá alocar o número de operadores de despacho, para atender as demandas, a fim de permitir o controle das diversas redes operacionais, de forma a criar uma rede de comunicação, combinando funcionalidade, flexibilidade e confiabilidade;

CARACTERÍSTICAS GERAIS DO CONSOLE DE DESPACHO:

Os consoles de despacho IP deverão apresentar no mínimo, mas não se limitando, os seguintes recursos:

- Interface gráfica amigável, intuitiva e de fácil operação com textos em português, permitindo a criação e alteração de grupos, chamadas seletivas, chamadas de grupo, disponibilização de acionamento do PTT por ícone e através de botão específico integrado na mesma tela a fim de facilitar a operação do despachante;
- Operação da interface gráfica de usuário deve ser multi touch permitindo acionar controles em mais de um ponto da tela simultaneamente, sem uso de periféricos (teclado e mouse);
- A tela Multi touch de interface gráfica deverá ter:
    - Tamanho 24” ou maior - padrão widescreen 16:9;
    - Resolução da tela: 1920 x 1080 - 60Hz;
- Capacidade de processamento mínimo 8Gb RAM da máquina;
- Possibilidade de integrar o sistema de telefonia;
- Possibilidade de buscar gravações das últimas conversas/chamadas recebidas e realizadas.
- Devem disponibilizar, pelo menos, duas saídas de áudio, com controle de volume individuais. A seleção do canal direciona a monitoração de áudio para o alto falante selecionado, sendo que os canais não selecionados podem ser monitorados pelo alto-falante secundário. Devem possuir capacidade de integrar-se com central telefônica com protocolo SIP
- Funcionalidades:
    - Chamada seletiva;

- Chamada em grupo;
- Criação de grupos conforme necessidade;
- Broadcast;
- Visualização das últimas chamadas do grupo, no mínimo as 5 últimas;
- Permitir troca de mensagens entre console e terminais com as tecnologias que disponibilizam este recurso;
- Interligação temporária entre estações (bridge entre canais de diferentes tecnologias);
- Seleção múltipla de canais, permitindo ao operador acionar simultaneamente várias estações;
- Deverá permitir silenciar todo o áudio de entrada exceto o grupo selecionado, se necessário;
- Atendimento telefônico, através de softphone, integrado na mesma tela agilizando a integração das comunicações;
- Permitir a realização da comunicação entre consoles (intercom);

Deverá permitir acesso a URL pré-determinado pelo administrador do sistema, a fim de permitir o uso de páginas web diretamente na tela da console de despacho.

O subsistema de console deverá permitir operação com sinalização padrão DMR em modo digital, permitindo despachar, monitorar, gravar, supervisionar e gerenciar as redes de voz do sistema de radiocomunicação, possibilitando controlar todos os canais de rádio.

Todos os equipamentos fornecidos deverão ser compatíveis com o sistema de radiocomunicação que utiliza protocolo de comunicação DMR em modo digital.

Mapa e Georreferenciamento (GPS/AVL):

O console de despacho deverá permitir a interação em mesma tela ou em tela adicional a verificação de mapa, esta funcionalidade deve estar contemplada para a possibilidade de integração com o posicionamento geográfico dos terminais de rádio;

O referido recurso deverá permitir a construção de “cercas limitadoras” no intuito de registrar e gerenciar as possíveis ocorrências, emitindo alarme no console de despacho;

Deverá permitir a gravação do histórico do GPS, possibilitando extrair os relatórios das rotas percorridas pelos terminais de rádio com licença de GPS.

- Sinalização:
  - Indicação visual de chamada presente no canal;
  - Indicação de canal ocupado, caso outro console, em paralelo, esteja em estado de transmissão;

A ação de transmissão do operador sobre o canal selecionado deve indicar através de medidor na tela, o nível de voz correspondente do operador;

O console deverá apresentar na tela, informações de todas as operações em andamento com no mínimo, mas não se limitando a:

- Estação recebendo;
- Transmissão individual;
- Transmissão simultânea;
- Operação agrupada;
- Chamada não respondida (pendente);
- Estação selecionada;
- Estação monitorada;
- Estação fora do sistema.

Áudio

O hardware deverá possuir 02 (dois) alto-falantes integrados ao equipamento;

O console de despacho deverá possibilitar atendimento simultâneo de chamada telefônica e a chamada de rádio, desviando a comunicação ao pressionar o PTT para o rádio e ao soltar voltar o microfone para a chamada telefônica;

Comandos, acionamentos e controles

Todos os comandos deverão ser possíveis de serem realizados através de ícones no próprio dashboard, sempre da forma mais rápida;

- Controle independente dos volumes do monitorado e selecionado;

Toda a operação/configuração deverá ser possível sem a necessidade de utilização de periféricos como mouse, ou teclado, e deverá permitir ao despachante operar no modo “hands free” ou “mãos livres”;

Periféricos

Cada Console de Despacho deve possuir 01(um) pedal de PTT (footswitch) robusto, com corpo fundido em alumínio, grau de proteção mínimo IP65, com no mínimo 01 contato, cabo de interconexão à console, isolação preta e comprimento mínimo de 2,5m.

Cada Console de Despacho deve possuir 04 (quatro) headset de uso individual para cada operador, com design confortável, do tipo cabeça, monoauricular (que atenda aos requisitos estabelecidos na NR 17 – Ergonomia – Anexo II), com tecnologia de cancelamento de ruído, atenuador de limite acústico de 118dB, com dispositivo de conexão tipo rápida;

Cada Console de Despacho deve possuir 01 (um) Adaptador Quick Disconnect USB para conexão com o Headset.

Sistema de Gravação

- Deverá permitir a gravação de áudio do sistema de radiocomunicação.
- Deverá possuir busca de gravações por filtros como data, hora e usuário;
- Deverá permitir exportar o áudio em arquivos: .MP3;
- Deverá gerar relatórios das gravações em extensões como: .doc, .xls, .pdf;
- Deverá permitir a visualização da taxa de ocupação da rede de rádio por estações e por ID dos terminais;
- Deverá apresentar em formato de gráfico as comunicações para permitir o gerenciamento das estações em tempo real;
- Deverá permitir o monitoramento do áudio em tempo real;
- Deverá permitir o acesso web através de protocolo seguro HTTPS para consultas e downloads dos arquivos de voz e dados com no mínimo 2 (dois) usuários simultâneos para cada localidade;
- Deverá possuir login e senha para registro de usuários e LOG de controle de acesso e tarefas executadas.
- Deverá permitir gravar as comunicações com conexão direta via IP na Repetidora atualmente utilizada pela Corporação, e via Gateway de Interoperabilidade com rádios de diferentes tecnologias: Analógico, DMR, P25, NXDN ou Tetra, mantendo todas as características de Identificação (ID) e coordenada geográfica dos terminais.

LICENÇAS E SOFTWARES

O fornecedor será o único responsável por entregar o subsistema de consoles de despacho com todas as licenças e softwares necessários para o completo e perfeito funcionamento dele.

[RR02] Gateway de Interoperabilidade

O Gateway de Interoperabilidade deverá possuir as seguintes características:

- Deverá realizar a comunicação/via IP acessando os rádios analógico ou digital, a fim de controlar as funções de transmissão e recepção e troca de canal;
- Deverá permitir no mínimo controlar dois rádios de diferentes tecnologias: Analógico, DMR, P25, NXDN ou Tetra. Permitindo operar simultaneamente, garantindo interoperabilidade entre protocolos em nível de voz com identificação ID;
- Deverá permitir acesso via web para configuração e gerenciamento do equipamento;

- Possuir indicadores luminosos (display LCD) na parte frontal para informações e indicar o status operacional da unidade. Além das características citadas, deverá possuir as seguintes características:
- Conector RJ45 para conexão via rede IP;
- Suporte para Rack 19” integrado;
- Alimentação AC por fonte externa com entrada 127~220V @60Hz;

[RR03] Software de Gestão e Monitoramento do Sistema

- Acesso ao estado do sistema (monitoramento dos serviços que o compõem);
- Acesso à todas as configurações do sistema (redes de rádio, usuários, segurança, entre outros);
- Deverá permitir a criação de lista de bloqueio de terminais;
- Deverá permitir bloqueio e desbloqueio dos terminais;
- Acesso às gravações de voz e dados do sistema;
- Acesso às informações de localização em tempo real;
- Criação de cercas, marcos e regras de alarmes. Configurando pelo software de gestão e replicando para o sistema de console de despacho;
- Gravação do histórico do GPS simulando a rota percorrida pelos terminais;
- Acesso às definições e visualização de dashboards;
- Widgets para acompanhamento em tempo real (comunicações das estações em tempo real; linha do tempo de comunicações e eventos de dados; listas de gravações, usuários e terminais; distribuições de chamadas por estação, terminal ou usuário);
- Dashboards públicos ou privados;
- Filtros avançados e flexíveis para encontrar informações em qualquer nível de granularidade;
- Deverá permitir gerenciamento dos terminais através de registro de inventário dos rádios;
- Acesso às definições e emissões de relatórios;
- Definições públicas ou individualizadas;
- Definição de períodos fixos ou dinâmicos;
- Filtros avançados e flexíveis para encontrar informações em qualquer nível de granularidade;
- Configuração de escala de plantonistas pelo software de gestão mostrando a escala na tela da console de despacho.

[RR05] ANTENA DE COMUNICAÇÃO E RÁDIO PORTÁTIL

Antena de Comunicação VHF/UHF

- Tipo: Antena colinear vertical de alto ganho
- Faixa: 136–174 MHz (VHF) / 400–470 MHz (UHF)
- Ganho mínimo: 3 a 6 dBi
- Impedância: 50 Ω
- VSWR ≤ 1.5:1
- Polarização: Vertical
- Conector: tipo N fêmea
- Construção em alumínio anodizado e fibra de vidro
- Montagem em mastro (diâmetro 40–50 mm)
- Resistência a ventos de até 160 km/h
- Homologação ANATEL e certificação IP66

[RR06] Rádio Transceptor Portátil (VHF/UHF)

Características Gerais

- Equipamento tipo transceptor portátil digital e analógico, com tecnologia TDMA DMR (Digital Mobile Radio), conforme ETSI TS 102 361.
- Compatível com operações em VHF (136–174 MHz) ou UHF (400–470 MHz) conforme modelo.
- Modos de operação: Analógico (FM) e Digital (DMR Tier II).
- Potência de transmissão ajustável: 1 W (baixa) e 5 W (alta).
- Criptografia digital AES de 256 bits e autenticação por hardware.
- Canalização: 12,5 kHz (narrowband) e 25 kHz (wideband).
- Função de varredura (scan) e seleção rápida de canal (quick access).
- Compatível com chamadas individuais, de grupo e de emergência.
- Indicação sonora e visual de canal ocupado.

Construção e Robustez

- Estrutura em policarbonato de alta resistência.
- Grau de proteção mínimo: IP67 (proteção contra poeira e imersão temporária).
- Conformidade com normas MIL-STD-810 C/D/E/F/G (resistência a vibração, queda e umidade).

- Peso máximo: < 380 g com bateria e antena.
- Dimensões aproximadas: 130 × 55 × 35 mm.

Alimentação e Bateria

- Bateria de íon-lítio recarregável, mínima 2200 mAh, 7,4 V.
- Autonomia mínima: 12 h (digital) e 9 h (analógico).
- Carregador rápido bivolt (100–240 V AC) incluso.

Interface e Operação

- Display LCD colorido (1,77” ou superior) com retroiluminação.
- Teclado completo (modelo full) ou simplificado (modelo básico).
- 3 botões programáveis.
- Conector para microfone externo e fone de ouvido padrão Motorola multipino.
- Compatibilidade com software de programação via USB ou Bluetooth (CPS).

Funcionalidades Avançadas

- Identificação de chamadas (Caller ID) e mensagens curtas (SMS).
- Registro de eventos e histórico de chamadas.
- Bloqueio remoto e ativação remota via rádio.
- Compatível com repetidores digitais Motorola.
- Atualização de firmware via CPS.

Acessórios Mínimos

- 1 × bateria de íon-lítio;
- 1 × antena;
- 1 × clip de cinto;
- 1 × carregador rápido individual;
- 1 × manual técnico e de operação.

10.2 ENTREGA, INSTALAÇÃO, TREINAMENTO, GARANTIA E ASSISTÊNCIA TÉCNICA

Entrega e Instalação

Os equipamentos deverão ser entregues no endereço indicado pela Defesa Civil, em horário comercial, devidamente acondicionados e acompanhados de notas fiscais e documentação técnica.

Quando aplicável, a contratada deverá realizar a instalação, configuração e testes de funcionamento, inclusive dos conjuntos de antena e mesa de rádio operador.

Garantia

Os equipamentos deverão possuir garantia mínima de 60 (sessenta) meses, contados do recebimento definitivo.

Assistência Técnica

A contratada deverá assegurar assistência técnica autorizada no território nacional, disponibilizando peças de reposição pelo período mínimo de 5 (cinco) anos após o término da garantia.

Treinamento operacional e técnico

Operação assistida 01 (uma) semana. Treinamento operacional e técnico.

11. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA - CONTROLE DE ACESSO

11.1 SISTEMA DE TELECOMUNICAÇÕES, LÓGICA – CONTROLE DE ACESSO

[CA01] LEITOR BIOMÉTRICO FACIAL

Para segurança interna do empreendimento, deverão ser fornecidas e instaladas leitoras de controle de acesso biométrico facial nas portas de ambiente considerados críticos/restritos, além de catracas do acesso, nas seguintes portas:

• Pavimento Térreo: Hall/Foyer, Acesso Secundário.

Obs.: ver posicionamento dos mesmos na planta de pontos

Especificações leitor Biométrico Facial

- Capacidade de usuários (1:N): 10.000 usuários
- Capacidade de memória: 100.000 sem imagem /30.000 com imagem
- Capacidade de cartões: 10.000
- Leitura biométrica: facial
- Operação: Face, cartão e senha
- Iluminação: Led Soft e infravermelho
- Sistema de operação: Linux
- Memoria: 4GB Flash
- RS485: 1 Canal Host ou Slave
- Wiegand: 1 Canal Saída ou Entrada

- Interfaces: rede (1), entrada de alarme (2), saída de alarme (1), saída para fechadura (1), entrada para sensor magnético (1), entrada para botoeira (1)
- Alimentação: 12VDC@2,5A
- Dimensões: 87 x 26 x 168 mm
- Tamanho da tela: 4 polegadas
- Resolução LCD: 800 x 480 pixels

[CA02] Catracas do Tipo SWING GATE

- Estrutura Pintada em epóxi a Pó ou em Aço Inox Escovadas AISI 304 com espessura mínima de 1,5mm, escovado #180 – 220;
- Tampa Superior Customizável;
- Peças Internas em Aço SAE 1020 Bicromatizadas;
- Peças do Mecanismo em Aço Cementado e Temperado com Dureza 48-52 HRc;
- Pontos de Fixação com Reforço Interno;
- Sensores Ópticos;
- Mecanismo Resistente a vibrações e impactos;
- Mecanismo com Capacidade de Carga Suportável de uma Pessoa de 120kgs a 5 Km/h;
- Sistema de Travamento (Entrada e Saída);
- Cofre Coletor de Cartões Smart com Fechadura (Opcional);
- MCBF (Número de ciclos médios entre falhas): 2.700.000;
- MTBF (Tempo médio entre falhas): 4.500 horas (600 ciclos/h);
- MTTR (Tempo médio para reparo): máx. 30 min.
- Umidade relativa: 95% não condensada;
- Temperatura de operação: -10° à 55° C;
- Dimensões: 1400 x 85 x 1100 mm – opção de abertura (1100 ou 600mm)

[CA03] Catraca Tipo Swing Gate PCD

- Estrutura: em aço inox AISI 304 escovado (acabamento #180–220) ou pintura epóxi a pó, com espessura mínima de 1,5 mm.
- Tampa superior customizável.
- Peças internas em aço SAE 1020 bicromatizado.
- Peças do mecanismo em aço cementado e temperado, dureza 48–52 HRc.
- Pontos de fixação com reforço interno para maior estabilidade.
- Sensores ópticos para detecção precisa.
- Mecanismo resistente a vibrações e impactos.
- Capacidade de carga: suporta pessoa de até 120 kg a 5 km/h.
- Sistema de travamento bidirecional (entrada e saída).
- Destravamento automático em caso de falta de energia (fail-safe).
- Cofre coletor de cartões Smart com fechadura (opcional).

- MCBF: 2.700.000 ciclos (média entre falhas).
- MTBF: 4.500 horas (600 ciclos/hora).
- MTTR: máximo 30 minutos.
- Umidade relativa: até 95% não condensada.
- Temperatura de operação: -10°C a 55°C.
- Estrutura: 1400 x 85 x 1100 mm.
- Largura útil mínima: 800 mm (atende cadeiras de rodas).
- Opções de abertura: 1100 mm ou 600 mm.

[CA04] Controladora POE para Porta de 02 portas

- Cada controladora de porta deve armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deve suportar até 70.000 (setenta mil) usuários e 5.000 (cinco mil) visitantes simultâneos. As transações armazenadas no buffer da memória interna, devem ser transferidas para o Servidor sempre que a aplicação do sistema de controle de acesso estiver em operação (com a rede disponível (on-line) – tecnologia de "pushing").
- Cada controladora deve comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.
- Cada controladora deve possuir servidor web interno "web server", protegido por usuário e senha, onde se pode verificar informações relativas ao funcionamento dela, bem como atualizar versões de seu software embutido.
- Cada controladora deve possuir quatro entradas para leitoras (duas leitoras de entrada e duas de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensor de status de porta/fechadura, duas entradas para integração com sistemas de incêndio ou emergência e duas saídas de relé comandadas (para duas fechaduras).
- 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.
- As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente. A controladora deve possuir fonte PoE (power over ethernet) 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), com capacidade máxima de corrente de 1,75A, a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da, 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 Controladora deve ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 32, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

[CA05] Controladora POE para Catraca ou Torniquete

- Cada controladora de porta deve armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deve suportar até 70.000 (setenta mil) usuários e 5.000 (cinco mil) visitantes simultâneos. As transações armazenadas no buffer da memória interna devem ser transferidas para o Servidor sempre que a aplicação do sistema de controle de acesso estiver em operação (com a rede disponível (on-line) – tecnologia de "pushing").
- Cada controladora deve comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.
- Cada controladora deve possuir servidor web interno "web server", protegido por usuário e senha, onde se pode verificar informações relativas ao funcionamento dela, bem como atualizar versões de seu software embutido.
- Cada controladora deve possuir quatro entradas para leitoras (duas leitoras de entrada e duas de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensor de status de porta/fechadura, duas entradas para integração com sistemas de incêndio ou emergência e duas saídas de relé comandadas (para duas fechaduras).
- 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. As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente.
- A controladora deve possuir fonte PoE (power over ethernet) 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), com capacidade máxima de corrente de 1,75A, a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da, 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 Controladora deve ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 32, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

[CA06] Botoeira de emergência verde;

- Botoeira de emergência cor verde
- Dispositivo tipo Call Point

- Tensão de trabalho 12/24VDC
- Contato de resistência: 100mOHMs
- 02 contatos NA/NF
- Tampa acrílica de proteção

[CA07] Fecho magnético (fechadura eletroímã), fonte e botão

- Sistema de eliminação de magnetismo residual;
- Tensão de operação: 12/24 VCC;
- Consumo de corrente: 480mA em 12VCC e 240mA em 24VCC;
- Força de atraque: 272KG;
- Acabamento: Alumínio Anodizado;
- Dimensões: 250 x 26 x 42 (C x L x A) mm;
- Sensor de atracação: SPDT 0,5A / 20 VCC;
- Peso líquido: 2Kg;
- Suporte LZ Botoeira de requisição de saída;
- Contato de saída: NA/NF/COM;
- Consumo Nominal: 3A @ 36 VCC;
- Peso: 0,20 Kg;
- Dimensões: 70 x 114 x 2 (C x L x A) mm;
- Acabamento: Aço Inox Escovado;
- Frase orientativa: português

[CA08] Software para Gerenciamento do Controle De Acesso Interface Gráfica

- 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. O software de gerenciamento deve permitir, para suas principais funções, integração com diferentes navegadores Web, a fim de melhorar a experiência dos usuários de software podendo também estar integrado à IA. Módulos opcionais como de Cadastramento e Gerenciamento de Visitantes poderão ser do tipo Aplicativo.
- Deverão ser previstas câmeras para cadastro junto ao balcão de recepção. Considerar um equipamento NVR 32 canais para armazenamento das imagens de segurança. Considerar um equipamento Switch Poe 24 portas Gigabit.
- Configurações Horárias: 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. Cada configuração horária deve definir de um até três intervalo em um mesmo dia, onde uma credencial terá acesso a determinados locais/controladoras.

- Zonas Horárias: 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.
- Níveis de Acesso: 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.
- Níveis de Acesso Customizado por Usuário: 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.
- Feriados: 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.
- Acesso Temporário: 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 entre outros, a fim de agilizar o processo de agendamento. O sistema deve permitir que a qualquer momento o agendamento seja cancelado e as credenciais voltem para seu nível de acesso anterior. Ao final do período agendado, o sistema deve retornar automaticamente as permissões de acesso cadastradas anteriormente.
- Cartão Provisório: O sistema deve permitir o cadastramento de cartões provisórios para os usuários normais (colaboradores), com validade definida, caso estes esqueçam seus cartões permanentes, que deverão ser temporariamente desativados automaticamente. Ao se retornar o cartão provisório, o cartão permanente deverá ser novamente ativado. O sistema deve manter as permissões de acesso no cartão provisório existentes no cartão permanente.
- Cartão de Emergência: 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.
- Informações e Permissões do Usuário: O sistema deve permitir que se configure uma data para expiração da credencial do colaborador, ou isentar este usuário da expiração. O sistema deve permitir a armazenagem de fotografia do usuário relacionada à sua credencial, permitindo a importação de uma foto ou tirá-la no momento do cadastro. O sistema deve permitir a personalização das permissões de acesso (nível de acesso) da credencial do usuário. O sistema deve permitir o cadastramento de pelo menos 05 campos customizados. Permitir a integração com modulo de gerenciamento de datas de expiração (nestes campos – que podem ser atribuídos a data de validade de exame médico, NR10, ASO e etc.), o modulo checa as validades e muda o acesso do usuário (retirando a permissão de acesso), na data de expiração do mesmo – neste processo o operador é notificado por e-mail, da alteração executada. 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. 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. 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 C Senha, Digital ou Senha, Digital C Cartão C Senha, etc.). O sistema deve permitir o cancelamento individual da regra de antipassback, por usuário. 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. 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.

- Dupla Autenticação: 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. 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.
- Eventos: O sistema deve possibilitar quais eventos dispararão e quais não dispararão sinalização na janela de planta gráfica (quadro sinótico). 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. Deve também ser possível selecionar quais eventos enviarão e-mails para até cinco usuários diferentes, em decorrência de seus disparos. Deve permitir a integração com sistemas de terceiros, para o envio de todos os eventos do sistema.
- Livro de ocorrência: 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. O relatório deve ter sua saída de impressão em arquivo PDF (portable document file) e .xls (planilha Excel).
- Tratamento de ocorrências de Alarme: O sistema deve possuir as seguintes funcionalidades:
    - 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.).
    - 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). 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. 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. Permite a utilização de tabelas com filtros dinâmicos para busca de alarmes, eventos e quaisquer outras transações efetuadas no sistema.

- Planta de Pavimento: O sistema deve possuir a opção de inclusão de plantas dos pavimentos e de ícones animados para facilitar a visualização dos eventos de alarmes. Deve se apresentar na forma de janela on-line individual ou aba de navegador Web. Deve permitir a importação e adição de inúmeras imagens de plantas de pavimento individuais, em arquivo JPEG ou BMP. Deve permitir que se adicionem ícones individuais para portas e sensores de alarme, que piscarão (ícones dinâmicos) para sinalização em caso de alarme. 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.
- Monitoramento em tempo real: O sistema deve permitir a visualização o 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. Integração com Leitores Biométricos O sistema deve permitir o cadastramento e gerenciamento das templates diretamente na plataforma de controle de acesso.
- Integração com LPR: O sistema deve permitir a integração com sistemas de LPR, recebe a informação da placa, verifica o nível de acesso e libera ou nega o acesso.
- Integração com Alarme de Incêndio: 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 peerto-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. A Integração com o módulo de alarme de incêndio, deve permanecer funcionando de forma integral sem a necessidade de o Aplicativo de Controle de Acesso estar on-line, ou seja, independentemente do PC Servidor e aplicativo de Controle de Acesso, no caso de os servidores estarem desligados ou fora da rede. 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.
- Antipassback: 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 à 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 deverá ser livre, sendo que eles poderão passar várias vezes na leitora de Entrada e/ou de Saída. 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. 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. Deve ser possível a seleção de até noventa e nove diferentes grupos de controladoras para a função de Antipassback Global. As funções de Antipassback, Antipassback GLOBAL e Rotas de Antipassback GLOBAL, deverão permanecer funcionando de forma integral sem a necessidade de o Servidor de Controle de Acesso estar on-line, ou seja, independentemente do PC Servidor e software de Controle de Acesso, no caso de os servidores estarem desligados ou fora da rede.

- Relatórios: 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 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. 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. O relatório deve ter sua saída de impressão em arquivo PDF (portable document file) ou .xls (planilha Excel). 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). 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). 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. 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.
- Parâmetros do sistema: O sistema deve possuir até 100 níveis diferentes de usuários do sistema, permitindo a configuração de acesso a todos os menus presentes no software.

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

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. 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.

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

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 à um cartão específico).

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.

O sistema de controle de acesso deverá permitir controle de sites remotos com horários diferenciados (GMT diferentes), além de possibilitar o filtro de transações por site e por controladora.

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

- Exportar: O Sistema deve permitir a exportação de dados de usuário/relatórios em formato .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.
- Licenciamento: 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.
- Envio de E-mails: 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 deverão ser 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.

- Idioma: O sistema deve contemplar o idioma português do Brasil (mínimo).
- Software para Cadastramento de visitantes: O sistema deve possuir um módulo para o gerenciamento de visitantes, totalmente integrado ao software de controle de acesso. O sistema de cadastro deve permitir:
    - Cadastrar os visitantes com até 5 fotos (Ex: foto do visitante, documento frente e verso, foto do veículo, foto de Nota Fiscal, etc.), através webcam ou câmera IP;
    - Cadastrar os dados de endereço, empresa, contato de emergência dos visitantes, placa do veículo e motivo da visita;
    - Permitir o acesso de diferentes níveis de acesso a diferentes visitantes;
    - Gerenciar e rastrear rapidamente os visitantes;
    - Criar diferentes de níveis de permissão para os operadores do software (cada operador poderá conceder determinados níveis de acesso a visitantes enquanto outros níveis de acesso lhe deverão ser negados);
    - Cadastrar \ Liberar os Cartões Provisórios dos colaboradores;
    - Possuir o módulo para gerar e imprimir os crachás com QR Code e os dados do visitante;
    - Possuir relatório Gerenciais e do Histórico dos visitantes;
    - 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;
    - Possuir integração com leitores de reconhecimento facial para cadastro e a rotina de baixa automática;
    - 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.
    - A Baixa Automática dos Cartões de Visitantes, deve permanecer funcionando de forma integral sem a necessidade do Aplicativo de Controle de Acesso estar online, ou seja, independentemente do PC Servidor e aplicativo de Controle de Acesso, no caso de os servidores estarem desligados ou fora da rede.
    - Possuir lista de pessoas não gratas vinculadas ao documento do visitante, permitindo que no momento da visita seja gerado um alerta com as observações de restrição para aquele visitante.
    - Possuir módulo de envio de QRCode por e-mail, tanto para temporários quanto para visitantes.
    - Possuir módulo alerta de empresa/colaborador visitado por e-mail.
    - Permitir criação de ilimitados grupos de webcam/câmeras IP selecionáveis pelo operador no momento de cadastro.

- Permitir liberação de intertravamento de forma remota quando integrado com hardware de terceiros.

12. SOLUÇÃO DE VISUALIZAÇÃO COLABORATIVA – LED WALL

Implementação de solução de sistema visual especializado para monitoramento, gerência e colaboração de imagens, inclusos os serviços de instalação, configuração, ativação, treinamento e garantia.

A solução de visualização deverá ser baseada em painel de LED indoor de pixel pitch fino (LED Wall), constituído por gabinetes/módulos LED montados de forma contínua e sem emendas aparentes (montagem seamless, com fresta zero entre módulos), controlados por processador de imagens dedicado. A solução proposta deverá contemplar todo o hardware e o software necessários ao pleno funcionamento do LED Wall, incluindo licenças, estrutura metálica de sustentação, sistemas de fixação e nivelamento, acabamento perimetral e o cabeamento de vídeo e dados. O acesso para manutenção deverá ser frontal, permitindo a remoção individual de módulos e fontes sem a necessidade de desligar os módulos adjacentes, com estrutura que assegure alinhamento, planicidade e vedação adequada.

O sistema deverá ser composto pelos seguintes painéis:

Painel	Sala	Configuração	Dimensão da tela	Área de LED
WALL01	Comando e Controle	4×4	4,87 × 2,74 m	13,34 m²
WALL02	Crise	2×2	2,44 × 1,37 m	3,34 m²

O conjunto de gabinetes deverá ser tratado como um display lógico único em ambiente gráfico, permitindo o gerenciamento e o monitoramento de todos os módulos por meio de software, de forma local ou remota.

Características Gerais:

Os sistemas visuais especializados para monitoramento, gerência e colaboração de imagens, em vários setores definidos neste edital, deverão funcionar em alta disponibilidade, permitindo a inclusão de novos e variados conteúdos, com impacto direto no aumento da eficiência e performance da contratada.

Todas as funcionalidades devem ser completamente atendidas e habilitadas em sua capacidade igual ou superior. As informações aqui mencionadas devem ser consideradas como minimamente aceitáveis.

Todas as funcionalidades e licenças devem operar de forma completa, em conjunto e integradas em versões de hardware, versões de firmware e versões de software.

Salvo quando explicitamente determinado um período específico de vigência para uma funcionalidade ou licença, estas deverão ser perpétuas.

Toda a vigência de licenças, suporte e garantia da fabricante, deverá contar a partir da data de recebimento da CONTRATANTE, dentro do prazo contratual entre o Recebimento Provisório e Definitivo, cabendo a responsabilidade e ônus à CONTRATADA em caso de a(s) fabricante(s) iniciarem a contagem a partir da emissão da Nota Fiscal da Distribuidora, Fabricante etc.

Todos os equipamentos deverão estar em linha de produção no momento da oferta.

A solução não deve entrar em processo de fim de suporte até o último dia da garantia e do suporte técnico.

Todos os materiais necessários para a instalação e integração da solução, são de responsabilidade da CONTRATADA.

Deve ser fornecida documentação completa e detalhada da implantação, de toda instalação e configurações da solução, topologia, em até 60 (sessenta) dias após a implantação e migração do sistema.

Deverá ser considerado pela CONTRATANTE e estar incluso na solução proposta e entregue, todo e qualquer, equipamento, material, partes e peças, licença e/ou serviço, mesmo que não citados diretamente, mas que sejam necessários para o pleno funcionamento dessa solução no ambiente da CONTRATADA em acordo com características solicitadas.

Os equipamentos deverão ser fornecidos montados, totalmente conectados, ensaiados, configurados e prontos para operação, incluindo os acessórios, materiais de instalação, hardwares e softwares.

Os equipamentos devem ser do mesmo fabricante e homologados por este, incluindo todas as licenças necessárias para seu funcionamento.

O acesso para manutenção deverá ser frontal, sendo os módulos extraíveis individualmente da matriz sem a necessidade de desligar os módulos adjacentes. A estrutura física do painel deverá permitir o alinhamento e empilhamento dos módulos, com vedação que impeça a contaminação interna dos equipamentos.

Especificações técnicas para o Painel modular para uso interno:

- Tecnologia: LED indoor SMD ou COB, em montagem fine pitch;
- Pixel pitch máximo: 1,25 mm (Painel WALL01);
- Brilho mínimo: 600 cd/m² (com ajuste automático de luminosidade);
- Relação de contraste ≥ 5.000:1;
- Taxa de atualização (refresh rate) ≥ 3.840 Hz;
- Profundidade de cor ≥ 14 bits;
- Ângulo de visão ≥ 160° (H/V);
- Uniformidade de cor: ±0.003Cx,Cy, ou melhor;
- Uniformidade de brilho: > 96%, ou melhor;

- Suportar HDR (High Dynamic Range);
- Calibração ponto a ponto (point-by-point) de cor e brilho, realizada de fábrica e ajustável em campo;
- Devem permitir operação em tensão de alimentação automática entre 100 à 240VAC, 50Hz/60Hz;
- Os gabinetes devem possuir chassi em liga de alumínio.
- Os gabinetes devem permitir instalação frontal.
- Os gabinetes devem permitir serviço de manutenção frontal.
- Devem possuir as seguintes certificações regulatórias: CE, CB, FCC, IC, ROHS, TUV ou cTUVus, WEEE e Baixa emissão de luz azul.
- Manutenção frontal, com módulos, fontes e cartões de recepção removíveis pela parte frontal;
- Vida útil (MTBF) ≥ 100.000 horas;
- Redundância de fontes de alimentação e do sistema de recepção de dados;
- O display deve ser capaz de operar em uma temperatura de 10°C a 40°C;
- O display deve atender ou exceder o padrão de proteção IP52 ou superior;
- Consumo médio por metro quadrado de no máximo 200W;
- O fabricante deve possuir suporte técnico estabelecido no Brasil;
- O fabricante deve possuir assistência técnica própria estabelecido no Brasil;
- O material deve ser considerado para fornecimento por metro quadrado [m²];
- Estrutura metálica sob medida, com sistema de nivelamento micrométrico entre gabinetes.

Processamento e distribuição de imagem

O processamento e a distribuição de imagem para o LED Wall deverão ser realizados por processador de imagens dedicado para painéis LED, responsável pelo escalonamento, pela composição de múltiplas fontes e pela formação de tela lógica única, dotado de entradas digitais (HDMI/DisplayPort) e de saídas para os cartões de recepção dos gabinetes. Deverá ser mantida a arquitetura redundante do tipo N+1, de modo que, em caso de falha de um equipamento, outro assuma automaticamente a operação (auto-failover).

Instalação

Para a instalação deverá ser previsto: elaboração do projeto executivo; montagem da estrutura metálica de suporte do LED Wall; instalação e nivelamento micrométrico dos gabinetes LED; conexão dos cartões de recepção e do processador de imagens; execução do acabamento perimetral do painel; calibração point-by-point; testes de uniformidade de cor e brilho; e ensaios de redundância e recuperação automática (failover).

[TI13] Software para Sistema de Colaboração e Gerenciamento do Led Wall;

O sistema de colaboração deverá ser compatível com arquitetura de servidor e com ambiente virtualizado. O sistema deverá interagir, gerenciar, compartilhar e controlar conteúdos (vídeo e imagens) em diversos painéis de Led Wall.

Deverá ser fornecido um único software de gerenciamento e visualização para a operação do sistema, com capacidade de colaboração entre usuários e painéis de Led Wall.

As ferramentas de software deverão controlar o conteúdo a ser exibido nos painéis de Led Wall.

As ferramentas de software deverão permitir ligar e desligar os módulos individualmente, de maneira local ou remota.

Deverá ser possível a exibição de imagens oriundas de câmeras IP em painéis de Led Wall.

As imagens capturadas deverão ser exibidas nos painéis de Led Wall em taxa mínima de 30 (trinta) frames (quadros) por segundo.

O software de controle deverá possibilitar o acesso e controle remoto de suas funcionalidades por um ou mais operadores de modo simultâneo através da rede local ou de uma rede remota LAN ou WAN.

O sistema de colaboração deverá ser fornecido acompanhado das respectivas licenças perpétuas com direito de uso permanente, que sejam necessárias à execução das tarefas e aplicativos descritos e/ou que sejam disponibilizados pela solução ofertada.

A ferramenta deverá criar nos painéis Led Wall uma área de trabalho única, onde diversas imagens possam ser executadas, livremente posicionadas e redimensionadas em qualquer um dos painéis.

Deverá permitir criar, salvar e carregar perspectivas (conjunto de fontes de vídeo) e compartilhá-las com os diversos dispositivos de imagem (Led Wall).

Deverá permitir a operação remota do Vídeo Wall a partir de teclado e mouse das estações de trabalho simultâneas, através da conexão LAN/WAN.

Deverá permitir aos usuários ou grupo de usuários privilégios diferenciados por meio de senha.

O software deverá ser compatível com Modo de Aplicação de Diretório Ativo (Active Directory Application Mode – ADAM) ou LDAP.

O software deverá ser compatível com API's (Interface Programável de Aplicativos), para a visualização e geração de alarmes de diferentes aplicativos com funções pré-programadas de sequenciamento de ações.

O software de colaboração deverá permitir que cada usuário ou grupo de usuários tenha permissão de visualizar somente determinadas fontes definidas pelo administrador do sistema (câmeras ou aplicativos).

O software de colaboração deverá permitir que cada usuário ou grupo de usuários tenha permissão de exibir as fontes preestabelecidas no Led Wall.

O software deve possuir interface gráfica amigável, com comandos entre outros do tipo arrastar e soltar.

O sistema de colaboração deverá prever funcionalidade para o compartilhamento de conteúdo com os Led Wall, permitindo aos usuários, mediante níveis de permissões, receber imagens, capturas remotas, streaming de vídeo e compartilhar informações, através de simples ação de "arrastar e soltar" (Drag C Drop) e utilizando a infraestrutura de rede TCP/IP, com renderização preferencialmente no Led Wall.

A ferramenta deverá permitir que cada operador envie o conteúdo completo de seu desktop ou uma aplicação ativa em execução no mesmo através de captura por TCP/IP (cropping) a uma janela independente no Led Wall.

Deverá possuir funções de geração e exibição de: nome da fonte de vídeo, data, horário, logo, ticker, status da fonte e borda de alarme.

Deverá possuir pré-visualização nas estações de trabalho de fontes de imagens e das informações exibidas no Led Wall.

A ferramenta deverá permitir que cada operador possa controlar a área de trabalho do Led Wall, de maneira que cada um possa mover e redimensionar as aplicações do painel.

Os usuários poderão ter acesso a um menu de atalhos diretamente no aplicativo instalado em sua estação de trabalho, de maneira a permitir rápido acesso a aplicativos do mesmo.

O sistema de colaboração deverá ser comprovadamente integrável com os principais VMSs (Video Monitoring System) de mercado, sendo no mínimo aceita a integração com Genetec ou ISS ou Digifort, devendo ser realizado por captura com no mínimo 30 fps.

Deverá permitir utilizar o sistema de colaboração em dispositivo móvel (Tablet), sendo que o usuário deverá ser autenticado. As licenças devem ser compatíveis e colaborativas com os demais equipamentos.

O licenciamento deverá ser perpétuo, sendo que deverá contemplar a atualização durante o período de 60 (sessenta) meses.

13. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – COMUNICAÇÃO TELEFÔNICA INTERNA

[TEL01] – COMUNICAÇÃO TELEFÔNICA INTERNA

A comunicação telefônica interna deverá ser implementada por meio de solução híbrida, integrando sistema de telefonia IP com capacidade de operação local e interface com serviços em nuvem. A arquitetura deverá garantir alta disponibilidade, segurança, escalabilidade e interoperabilidade, assegurando a continuidade das comunicações em regime 24x7, mesmo em cenários de falha das redes externas. A solução deverá contemplar:

- Plataforma IP-PBX com suporte a ramais físicos e virtuais;
- Integração com serviços VoIP externos por meio de trunk SIP seguro;
- Compatibilidade com protocolos SIP, TLS e SRTP para comunicação segura;
- Suporte a recursos de comunicação por voz, incluindo discagem direta, chamadas em grupo, conferência, transferência e gravação;
- Gerenciamento centralizado de usuários, permissões, logs e dispositivos;
- Capacidade de expansão modular, permitindo o crescimento de usuários e a integração com outras estruturas de comunicação;

- Interoperabilidade com sistemas de alerta, controle de acesso, videomonitoramento, rádios e plataformas de colaboração;
- Priorização de tráfego de voz na rede de dados por meio de QoS (Quality of Service).

[TEL02] TELEFONE IP

Características Principais:

- **Protocolos/Padrões:** SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS, DHCP, PPPoE, entre outros.
- **Interfaces de Rede:** Duas (2) portas Ethernet Gigabit de 10/100/1000 Mbps com detecção automática.
- **Contas SIP:** Suporte para no mínimo 4 (quatro) contas SIP e 8 (oito) linhas.
- **Display:** LCD TFT colorido de no mínimo 2,8 polegadas (320x240 pixels) com luz de fundo.
- **Áudio:** Áudio em alta definição (HD) no aparelho (handset) e no viva-voz (speakerphone), com suporte a áudio de banda larga (wideband).
- **Teclas Programáveis:** Mínimo de 4 (quatro) teclas sensíveis ao contexto (softkeys) e até 32 teclas virtuais BLF (Busy Lamp Field) de discagem rápida na tela.
- **Conectividade Auxiliar:** Bluetooth integrado (versão 4.0 ou superior) para sincronização com dispositivos móveis e headsets sem fio.
- **Conectividade Headset:** Conector físico dedicado tipo RJ9 para fones de ouvido com fio, preferencialmente compatível com EHS (Electronic Hook Switch).
- **Alimentação:** Suporte a PoE (Power over Ethernet) integrado (802.3af), além de fonte de alimentação universal externa inclusa.
- **Conferência:** Capacidade de conferência de voz de 4 vias local.
- **Funcionalidades:** Espera, transferência, encaminhamento, chamada em espera, não perturbe (DND), rediscagem, entre outras funcionalidades telefônicas padrão.
- **Segurança:** Suporte a senhas de usuário e administrador, autenticação MD5, arquivos de configuração criptografados, TLS, SRTP, 802.1X, entre outros.
- QoS, Qualidade de Serviço de camada 2 (802.1Q, 802.1P) e camada 3 (ToS, DiffServ).
- **Instalação:** Suporte para instalação em mesa com dois ângulos e suporte para montagem em parede incluso.
- **Provisionamento:** Suporte a provisionamento automático (via TR-069 ou arquivos de configuração XML criptografados).
- **Idiomas:** Suporte a múltiplos idiomas, incluindo o idioma português (Brasil).

[TEL03] HEADSET PARA ESCRITÓRIO/CALL CENTER

Características Principais:

- **Tipo:** Headset monoauricular ou biauricular (a definir pela licitante), com fio ou sem fio (Bluetooth).

- **Conectividade (com fio):** Conector físico tipo RJ9 (4P4C) para conexão direta ao terminal telefônico. É fundamental que o fornecedor garanta a compatibilidade pinagem/posição do plug RJ9 com o terminal a ser utilizado.
- **Conectividade (sem fio):** Tecnologia Bluetooth integrada (versão 4.0 ou superior) para emparelhamento com terminais telefônicos compatíveis.
- **Qualidade de Áudio:** Áudio em alta definição (HD) com suporte a banda larga (wideband), proporcionando clareza de voz superior.
- **Microfone:** Microfone com cancelamento de ruído para isolamento de sons indesejados do ambiente e maior clareza na comunicação. Haste do microfone flexível e ajustável.
- **Proteção Auditiva:** Tecnologia para atenuação de sons excessivamente altos (proteção contrachoque acústico), mantendo o volume em níveis seguros e agradáveis.
- **Design e Conforto:** Design ergonômico, leve, com tiara ajustável para conforto em uso prolongado. Protetor auricular em material confortável (ex: espuma, couro sintético).
- **Controles:** Controles de volume e atendimento/encerramento de chamadas integrados (no cabo para modelos com fio, ou no próprio headset para modelos sem fio).
- **Compatibilidade EHS:** Opcional: Compatibilidade com Electronic Hook Switch (EHS) para atendimento remoto de chamadas (se o terminal suportar e for um requisito do edital).

14. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – SISTEMA DE ÁUDIO VISUAL

Mão-de-obra para instalação

Para a instalação deve-se prever:

- Elaboração de projeto executivo de instalação.
- Preparo do suporte de fixação para os módulos (pantográficos ou basculantes).
- Montagem da estrutura metálica de suporte dos painéis.
- Alinhamento e nivelamento dos módulos LCD conforme especificações.
- Fixação segura de cada módulo de 55” nos suportes.
- Organização e fixação de cabos (HDMI/DisplayPort, energia, rede).
- Instalação dos servidores de colaboração e controladores de vídeo wall em rack.
- Conexão dos servidores aos módulos via cabos digitais (HDMI/DisplayPort).
- Configuração da arquitetura distribuída com redundância (N+1).
- Instalação do sistema operacional e softwares de controle e colaboração.
- Configuração do gerenciamento gráfico e integração com fontes de vídeo (ex: VMS, câmeras IP).
- Criação de perfis e permissões de usuários.
- Configuração de sincronização entre controladoras e testes de failover automático.

- Teste de exibição em todos os painéis simultaneamente.
- Calibração de cor, brilho e alinhamento entre os módulos.
- Testes de controle remoto e de colaboração simultânea.
- Ensaios de redundância e recuperação automática (failover).
- Elaboração de manuais de operação e relatórios de configuração.
- Entrega de topologia lógica e física da solução implementada.
- Checklist técnico de conformidade com edital.
- Treinamento dos operadores e administradores do sistema.
- Sessão prática com simulações de uso e falhas.
- Entrega do termo de aceitação com checklist validado.

[SAV01] – Sistema de automação áudio visual

Só deverão ser aceitos fornecimento de fabricantes presentes ou com representação comprovada no mercado brasileiro;

A solução deve compreender os itens de automação e gestão de seus recursos para atendimento aos eventos da sala.

A solução deverá se basear nos seguintes equipamentos:

- **Dispositivo Centralizado de Automação:**
    - O sistema deve possuir automação centralizada para controle de todos os equipamentos, incluindo monitores, sonorização, áudio conferência, vídeo conferência e iluminação.
    - Deve permitir a seleção da entrada de vídeo e áudio que deverá ser visualizado nos displays;
    - Deverá ser compatível com os seguintes protocolos de forma nativa ou com gateways: SIP (Session Initiation Protocol), H.323 para transmissão de áudio e vídeo em tempo real através de redes IP, WebRTC (Web Real-Time Communication) ou SIP over WebSocket
    - Deverá prover solução de automação para a sala de videoconferência com os seguintes itens:
- **Mesa de Som e Gerenciamento de Áudio;**
    - Fornecer sistemas de sonorização que permitam reproduzir o áudio de qualquer uma das entradas inclusive áudio conferência. Por padrão deve ser selecionado o áudio da imagem exibida no monitor 1;
    - Captação de áudio integrado com a Vídeo Conferência através de microfones direcionados para as posições dos participantes evitando ruídos do ambiente;
    - O sistema de captação de voz deve utilizar equipamentos de teto ou mesa com microfones de cobertura customizáveis com 2 cápsulas cardioide e LED indicador;
    - Processador de áudio capaz de gerenciar, balancear e equalizar as entradas e saídas dos equipamentos, compatibilidade com sistemas de comunicação Dante e áudio conferência com cancelamento de eco;
    - 6 (seis) autofalantes da linha profissional com no mínimo 40W de potência cada;

- Amplificador profissional para os autofalantes com alta impedância (70/100V);
    - A mesa de som deve ter:
        - No mínimo, 8 canais;
        - Deve possuir controle de volume, equalizador de frequência e efeito de reverberação;
        - Deve ser capaz de receber sinais de áudio de diferentes fontes, como computadores, telefones celulares, tablets e outros dispositivos de reprodução de som;
        - Deve ter entradas de áudio XLR e P10 para conectar microfones e outros dispositivos.

- **Microfones;**
    - A solução também deve compreender os microfones integrados à mesa de som e sistemas de automação para funcionamento junto à conferências. Os microfones que deverão ser fornecidos na solução devem ser:
    - Microfones de mesa: devem ter uma frequência de resposta de pelo menos 50 Hz a 16 kHz e um nível de pressão sonora máximo de pelo menos 120 dB.
    - Microfone sem fio: deve ter uma frequência de resposta de pelo menos 50 Hz a 16 kHz e um nível de pressão sonora máximo de pelo menos 120 dB. Além disso, deve ser capaz de operar em uma faixa de frequência livre de interferência.
    - Os microfones de mesa e sem fio deverão:
        - Ser de boa qualidade, capazes de captar vozes de forma clara e precisa;
        - Ser direcionais e possuir boa captação de som ambiente;
        - Ser dinâmicos e possuir boa resposta de frequência;
        - Ser resistentes e duráveis.

- **Vídeo**
    - Deve permitir a comutação de fontes de entrada e saída de até 08 fontes de imagens HDMI sendo capaz de receber os comandos de seleção via rede.
    - Deve possuir dois pontos de conexão de mesa com HDMI, USB e tomada de energia em sistema de pop-up;
    - A conexão entre dispositivos de vídeo deve ser em arquitetura TX e RX via cabo UTP com distâncias de até 40 metros com transmissão de todos sinais e protocolos necessários.
    - Compatibilidade com resoluções até FullHD por dispositivo.
    - Deve permitir a visualização das imagens selecionadas em tela retrátil e televisores instalados no auditório e em vídeo wall na sala de crise;
    - Câmera: deve ter uma resolução mínima de 720p e uma taxa de quadros mínima de 30 fps. Além disso, deve ter recursos como zoom óptico e panorâmica/inclinação;
    - O sistema deverá controlar até 08 circuitos de iluminação com funções de ON/OFF e 4 canais dimerizáveis de acordo com a programação dos cenários;
    - Todos os equipamentos deverão ser montados em Rack padrão 19”.

15. SISTEMA DE COMUNICAÇÃO SATELITAL FIXO DE ALTA DISPONIBILIDADE

A solução a ser projetada e implantada deverá garantir conectividade de dados via satélite, em regime de alta disponibilidade, com desempenho compatível com as necessidades operacionais de um Centro de Gestão de Desastres. O objetivo é assegurar a continuidade das comunicações mesmo em cenários de indisponibilidade total ou parcial das redes terrestres.

Esse tipo de conexão utiliza satélites geoestacionários (GEO) para fornecer internet de forma independente da infraestrutura terrestre. A comunicação ocorre entre a antena parabólica VSAT instalada no local do cliente, apropriada para ambientes críticos e de missão essencial. A estrutura deve prever base física de fixação permanente, respeitando normas técnicas e condições ambientais da edificação e o hub central da operadora, via satélite.

- A solução deverá suportar múltiplas conexões simultâneas, com desempenho suficiente para garantir o funcionamento dos sistemas de tecnologia da informação e comunicação do centro, incluindo acesso à internet, VPNs, sistemas de monitoramento e comunicação interinstitucional;
- A largura de banda deverá ser dimensionada conforme o perfil de uso de um centro de operações de emergência, assegurando velocidade de transmissão e recepção compatíveis com o fluxo de dados previsto;
- A infraestrutura deverá operar em regime de alta disponibilidade, com mecanismos de supervisão e controle de falhas;
- A arquitetura deverá permitir operação integrada com outras tecnologias de comunicação disponíveis (como redes terrestres), garantindo a alternância automática (failover) em caso de falha da rede principal.

Integração com Rede Local e Segurança

- A solução satelital deverá ser plenamente integrável à rede lógica existente no centro, por meio de infraestrutura de conectividade física e lógica;
- Devem ser considerados os requisitos mínimos de segurança da informação, com recursos que viabilizem a comunicação segura, protegida e rastreável, conforme os padrões de segurança vigentes no setor público.

Licenciamento e Regularização:

- A solução deverá estar em conformidade com as normas e regulamentações da Agência Nacional de Telecomunicações (ANATEL), sendo de responsabilidade da contratada todas as providências relacionadas ao licenciamento, homologações, registros e autorizações necessárias à sua operação;
- A solução deverá prever meios de monitoramento remoto do desempenho da conexão e notificação de falhas, preferencialmente com painel de controle acessível aos operadores do centro.

Os componentes do sistema estão descritos a seguir:

- Antena Parabólica com diâmetro entre 75cm e 1,8m de diâmetro em alumínio ou aço galvanizado, com pintura anticorrosiva para resistência as intempéries. Montagem em estrutura fixada em base de concreto ou poste metálico, com orientação precisa para o satélite;
- BUC (Block Upconverter): Responsável por enviar os dados ao satélite. Fica acoplado ao braço da antena parabólica;
- LNB (Low-Noise Block): Responsável por receber o sinal do satélite e reduzir o ruído. Fica também no braço da antena;
- Modem Satelital (Indoor Unit): Instalado dentro do empreendimento (rack ou mesa). Conecta a antena via cabo coaxial e se liga ao roteador ou firewall local via Ethernet;
- Cabos Coaxiais: RG-6 ou RG-11, com no máximo 30 metros de comprimento entre modem e antena, para evitar perda de sinal;
- Fonte de Energia, 110~220V com consumo estimado entre 30W e 100W.

16. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – AUTOMAÇÃO PREDIAL E BMS

A Solução tem por objetivo fornecer o monitoramento da infraestrutura que atende a Sala Técnica da CONTRATANTE, visando a gestão ambiental e gestão de energia. A solução deve possuir características de alta confiabilidade para monitoramento contínuo, possuindo os seguintes requisitos mínimos:

- Deverá ser fornecida com estrutura de hardware e software;
- Deverá ser fornecido todos os dispositivos e sensores necessários para implantação da solução, visando atendimento a todas as funcionalidades e requisitos descritos neste Termo de Referência.

A solução a ser implantada deve atender toda a infraestrutura instalada pela CONTRATADA, incluindo os equipamentos:

- Geradores;
- UPS;
- Climatização de precisão;
- Climatização de conforto para sala de equipamentos;
- Painéis elétricos com multimedidores;
- Sensores de temperatura e umidade nos ambientes:
    - Sala UPS;
    - Sala POP;
    - Salas Técnicas;
    - Salas operacionais 24x7x365.

Requisitos de Interface da Solução BMS

A Solução de BMS deverá apresentar todas as informações em língua portuguesa. Deve possuir a capacidade de configuração de limites máximos e mínimos de aceitação para cada grandeza monitorada, incluindo níveis de severidade para alertas e alarmes.

Deve gerar avisos sonoros e visuais com identificação do nível de criticidade por código de cores. Esses avisos deverão ser apresentados na interface gráfica da solução e enviados por e-mail.

Deve possuir a capacidade de apresentação dos equipamentos sobre a planta baixa dos ambientes monitorados.

Deve possuir interface gráfica para apresentação em tempo real e gráficos de tendências das grandezas monitoradas (energia, temperatura, umidade etc.), bem como de todos os equipamentos existentes e integrados à Solução BMS.

Requisitos de Licenciamento

A solução deve permitir o acesso ilimitado de usuários, bem como, 5 (Cinco) acessos concorrentes, no mínimo.

O fornecedor da solução deve oferecer o licenciamento perpétuo do software, independente da unidade de quantidade licenças necessárias para o atendimento do escopo.

O levantamento do licenciamento deverá ser apresentado à CONTRATANTE e validado antes do início da implementação.

A solução deve prover todos os módulos necessários para o atendimento do escopo desse Termo de Referência.

17. INSTALAÇÕES DE TELECOMUNICAÇÕES, LÓGICA – TREINAMENTO E COMISSIONAMENTO

17.1 Treinamento e comissionamento

Treinamento de infraestrutura de suporte às instalações.

Antes do início das operações do ambiente deverão ser ministrados os treinamentos necessários aos usuários, de forma que estes adquiram conhecimento sobre os ambientes que compõem o Centro e sua operação.

Deverá ser ministrado o treinamento técnico para no mínimo 10 pessoas, nas instalações do cliente, de forma capacitar os operadores da contratante a realizarem a operação, ajustes, configuração e administração dos produtos (hardware e software) a serem fornecidos.

O curso deverá ser aplicado nas instalações do cliente imediatamente após o startup do sistema com duração aproximada de 16 horas.

O treinamento deverá ser ministrado em português por profissionais com ampla experiência, com o objetivo a possibilitar aos participantes efetuarem o suporte ao ambiente.

Ainda deverá ser fornecido material de apoio como materiais de Hardware, Software, Catálogos, Desenhos, Esquemas Orientativos etc.

17.2 Comissionamento

Deverão ser realizados serviços especializados para vistoria da obra e testes funcionais e integrados dos sistemas elétrico, ar-condicionado, detecção/combate a incêndio, CFTV e controle de acesso do Centro.

Os sistemas e equipamentos envolvidos no comissionamento da Sala Técnica deverão ser:

Sistema Elétrico:

- Painéis de baixa tensão;
- Geradores;
- UPS;

Sistema Mecânico:

- Evaporadoras de precisão;
- Condensadoras de precisão;

Sistema de Detecção e Combate Incêndio:

- Sistemas de detecção de incêndio convencional;
- Sistema de detecção precoce a laser;
- Sistema de Controle de Acesso;
- Sistema de CFTV;

Testes funcionais:

- Após o término da obra e das instalações dos sistemas de missão crítica, deverão ser feitos testes de funcionamento dos equipamentos, visando identificar problemas de não conformidades com o projeto e especificações, de funcionamento e desempenho.
- O objetivo dos testes individuais é garantir a funcionalidade de cada equipamento da infraestrutura de missão crítica pertencente ao Centro.

Testes integrados:

- O objetivo deste teste é validar a funcionalidade dos sistemas, elétrico, ar-condicionado, detecção e combate a incêndio instalados nas áreas de missão crítica do centro e sala técnica onde os sistemas serão testados de forma conjunta e integrada, sendo confrontado seu funcionamento com as especificações de projeto.
- Todos os equipamentos e sistemas de missão crítica deverão ser testados quanto a sua perfeita funcionalidade de forma integrada, onde se consiste em simulações de falhas nos equipamentos relevantes de cada disciplina e no fornecimento de energia pela concessionária com objetivo de constatar a redundância dos sistemas e a confiabilidade do site.

Seguem os testes de falhas que deverão ser executados durante os testes integrados:

- Simulação de falha de energia fornecida pela concessionária;
- Simulação de falha do sistema de energia ininterrupta (UPS);
- Simulação de falha das máquinas de ar-condicionado de precisão;
- Integração com os sistemas de detecção e combate a incêndio.