Especificações Técnicas do Sistema de Vigilância

Este documento descreve os requisitos funcionais detalhados para a implementação de uma solução robusta de videomonitoramento e vigilância inteligente, abrangendo os módulos de **Segurança de Acesso** e **Administração Operacional**. As especificações aqui apresentadas servem como referência técnica para administradores de sistemas, equipes de segurança e integradores responsáveis pela configuração, implantação, integração e manutenção da plataforma em ambientes críticos.

O sistema foi concebido para apoiar a prevenção de incidentes, o monitoramento contínuo de áreas sensíveis e a resposta rápida a eventos operacionais ou de segurança. Seu escopo pode incluir centros de controle, instalações corporativas, unidades industriais, centros logísticos, ambientes públicos e qualquer local que exija supervisão em tempo real, rastreabilidade de ocorrências e evidências confiáveis para análise posterior.

Além da captura e visualização de imagens, a solução contempla processos de autenticação, controle de permissões, registro de auditoria, armazenamento seguro e gestão de alertas. O objetivo é garantir uma operação consistente, escalável e alinhada às necessidades de segurança física, conformidade interna e governança tecnológica.

Este material também oferece um panorama técnico de alto nível sobre a arquitetura do sistema, os principais componentes envolvidos, os fluxos de integração com outros subsistemas e os critérios mínimos esperados para desempenho, disponibilidade e confiabilidade. A documentação é fundamental para padronizar decisões de projeto, reduzir ambiguidades durante a implementação e apoiar a operação contínua ao longo do ciclo de vida da solução.

As especificações devem ser interpretadas em conjunto com políticas corporativas, requisitos contratuais e normas aplicáveis de privacidade, proteção de dados e retenção de registros. Dependendo do contexto de uso, podem existir obrigações adicionais relacionadas ao tratamento de imagens, acesso a gravações, prazo de armazenamento, notificação de incidentes e controles de segurança cibernética. O cumprimento desses requisitos é essencial para reduzir riscos jurídicos, operacionais e reputacionais.

Em conjunto, este documento estabelece a base técnica necessária para garantir que a solução de vigilância seja implementada de forma previsível, auditável e sustentável, oferecendo suporte à operação diária e à tomada de decisão baseada em evidências.

REFERÊNCIA TÉCNICA V1.0

Estrutura do Documento

Visão Geral dos Módulos

O documento está organizado em dois grandes blocos temáticos, cada um contendo requisitos específicos que devem ser atendidos pela solução de vigilância. A seguir, um resumo dos capítulos e de suas respectivas abordagens, com foco na forma como cada parte contribui para a operação, a segurança e a administração da plataforma.

Em conjunto, esses capítulos definem tanto as capacidades de proteção e controle de acesso quanto os recursos de gestão operacional, permitindo que a solução funcione de maneira consistente, auditável e alinhada às necessidades do ambiente onde será implantada.

🔒 Segurança

Reúne os requisitos voltados à proteção do acesso, ao rastreamento de sessões e ao controle de uso dos dispositivos e arquivos associados ao sistema. Este bloco é essencial para reduzir riscos, preservar a integridade das informações e garantir que apenas usuários autorizados executem ações sensíveis.

- Identificação e histórico de sessões, para registrar quem acessou o sistema e em que contexto.
- Controle de dispositivos por bloqueio e desbloqueio, permitindo restringir o uso de recursos conforme a política definida.
- Gestão de tipos de arquivos anexados, organizando os conteúdos que podem ser associados a eventos e registros.

Esses tópicos formam a base de confiança da solução e sustentam os controles necessários para conformidade, auditoria e resposta a incidentes.

⚙️ Administração

Concentra os recursos de organização, classificação, consulta e manutenção operacional da plataforma. Este módulo orienta como os dados e os ativos de vigilância são estruturados para facilitar o uso cotidiano e a escalabilidade da solução.

- Hierarquia e grupos de câmeras, para organizar dispositivos por áreas, níveis ou critérios operacionais.
- Listas de interesse, que ajudam a destacar elementos relevantes para acompanhamento prioritário.
- Gestão de usuários e perfis, definindo permissões e responsabilidades de cada operador.
- Busca e análise de vídeo arquivado, permitindo localizar evidências e apoiar investigações.
- Integração com Active Directory, conectando o sistema à infraestrutura corporativa de identidade.

Esse conjunto de funções facilita a administração centralizada e assegura que os controles de segurança sejam aplicados de forma coerente ao longo do uso da plataforma.

Embora apresentados separadamente, os dois módulos são complementares: a **Segurança** estabelece as regras de proteção e rastreabilidade, enquanto a **Administração** estrutura a operação diária, os cadastros e as consultas. Juntos, eles fornecem a base para uma solução que seja funcional, governável e preparada para ambientes críticos.

CAPÍTULO 1

Módulo de Segurança

O módulo de segurança da solução é responsável por garantir rastreabilidade, controle de acesso a dispositivos e conformidade no uso de arquivos. Os requisitos a seguir definem as capacidades mínimas exigidas para proteger o ambiente operacional e assegurar auditabilidade completa das ações realizadas pelos usuários.

Em um sistema de vigilância, a segurança não é apenas um componente complementar: ela é a base que sustenta a confiabilidade de toda a plataforma. Sem controles adequados, o ambiente fica exposto a acessos indevidos, uso não autorizado de dispositivos, manipulação de informações sensíveis e perda de evidências que podem ser essenciais para investigações, auditorias e respostas a incidentes.

Esse módulo atua sobre riscos comuns em operações críticas, como tentativa de acesso por usuários não autorizados, uso indevido de credenciais, exploração de sessões abandonadas, alteração de registros e circulação descontrolada de arquivos associados a eventos. Ao definir regras claras de acesso e monitoramento, a solução reduz a superfície de ataque e reforça a integridade das informações tratadas no dia a dia.

A auditabilidade e a rastreabilidade são especialmente importantes porque permitem identificar **quem** acessou o sistema, **quando** o acesso ocorreu, **o que** foi executado e **em qual contexto** a ação aconteceu. Esse histórico é fundamental para atender exigências de conformidade, apoiar a apuração de incidentes e criar um registro confiável das operações, evitando lacunas que comprometam a confiança sobre os dados gerados.

Em termos de escopo, este capítulo cobre um conjunto de sub-requisitos voltados à proteção e ao controle do ambiente, incluindo:

- identificação de usuários e histórico de sessões, para registrar acessos e permitir acompanhamento posterior;
- bloqueio e desbloqueio de dispositivos, restringindo o uso conforme regras operacionais e políticas de segurança;
- controle sobre tipos de arquivos anexados, evitando o tratamento inadequado de conteúdos sensíveis ou fora do padrão permitido;
- mecanismos de registro e auditoria, para que ações relevantes fiquem documentadas de forma verificável;
- apoio à conformidade operacional, garantindo que o uso da plataforma esteja alinhado a políticas internas e exigências regulatórias.

Assim, o módulo de segurança estabelece as condições necessárias para que a solução de vigilância opere de forma confiável, controlada e defensável. Ele protege tanto o uso cotidiano quanto os registros produzidos pelo sistema, preservando a integridade do ambiente e a validade das informações nele armazenadas.

Identificação e Histórico de Sessão

O sistema mantem um registro completo, consistente e auditável de todas as sessões iniciadas por usuários, incluindo dados suficientes para rastrear ações, identificar origens de acesso, correlacionar eventos e detectar comportamentos anômalos. Essa funcionalidade é essencial para conformidade com políticas de segurança corporativa, trilhas de auditoria internas e análise posterior de incidentes.

O histórico de sessão deve permitir reconstruir, com precisão, **quem** acessou o sistema, **de onde** o acesso ocorreu, **em qual dispositivo** a sessão foi iniciada, **quando** começou e terminou, e **quais ações** foram executadas durante sua vigência. Sem esse nível de detalhamento, torna-se difícil validar responsabilidade operacional, investigar acessos indevidos e comprovar aderência a controles de segurança.

Para cada sessão, a solução deverá capturar e armazenar, no mínimo, os seguintes dados:

Campo	Descrição requerida
ID do usuário	Identificador único do usuário autenticado, associado ao perfil, nome exibido e nível de acesso.
Endereço IP	IP de origem da sessão, útil para correlação com rede, localidade e padrões de acesso.
Timestamps	Data e hora de início, autenticação, renovação, inatividade e encerramento da sessão.
Informações do dispositivo	Identificador persistente do dispositivo, tipo de equipamento, sistema operacional e navegador quando aplicável.
Ações executadas	Eventos relevantes realizados durante a sessão, incluindo acessos, alterações, exclusões, exportações e tentativas bloqueadas.
Status da sessão	Indicação de sessão ativa, expirada, desconectada, encerrada manualmente ou invalidada por política.

Além desses campos, recomenda-se registrar também contexto de autenticação, como método utilizado, motivo de encerramento, falhas de login associadas e eventuais trocas de privilégio ao longo da sessão. Esses elementos ampliam a capacidade de detectar uso indevido de credenciais, reutilização suspeita de sessões e acessos simultâneos fora do padrão esperado.

Identificação do Usuário

Registro do usuário que iniciou a sessão, com ID único, nome completo, login e perfil de acesso associado. Permite rastrear quem realizou cada ação dentro do sistema e vincular eventos a um responsável específico.

ID de Dispositivo Único

Cada dispositivo utilizado para acesso deve possuir um identificador único persistente, vinculado ao histórico de sessões. Isso facilita identificar terminais conhecidos, novos ou não autorizados, além de apoiar bloqueios preventivos.

Endereço IP

Registro do endereço IP de origem de cada sessão, permitindo correlacionar acessos com localizações de rede específicas, faixas corporativas permitidas e tentativas de acesso externo não previsto.

Datas e Horários

Registro preciso de início, última atividade, interrupções, expiração por inatividade e encerramento da sessão. Esses dados são essenciais para reconstrução de linha do tempo e detecção de padrões incomuns.

Status Online/Offline

Indicação em tempo real se o usuário está com sessão ativa (online) ou inativa (offline), possibilitando o monitoramento de utilização concorrente, a identificação de abandono de sessão e a detecção de encerramentos inesperados.

Ações Realizadas

Registro das operações relevantes executadas na sessão, como visualização, inclusão, edição, exclusão, exportação, login, logout e tentativa de acesso negada. Esse histórico é fundamental para auditoria e resposta a incidentes.

Os registros de sessão devem ser mantidos pelo período mínimo definido pelas políticas internas de segurança, conformidade e retenção documental. Na ausência de uma política específica, recomenda-se retenção por prazo suficiente para suportar auditorias periódicas, investigações forenses e exigências regulatórias aplicáveis, garantindo que os logs permaneçam íntegros e recuperáveis durante todo o período estipulado.

Essa retenção é importante porque sessões antigas podem ser necessárias para comprovar a origem de uma ação, identificar abuso de credenciais, reconstruir a sequência de eventos e verificar se um incidente foi causado por erro humano, uso indevido ou comprometimento de conta. Quanto mais completa e confiável for a trilha de sessão, maior a capacidade da organização de responder rapidamente a suspeitas e cumprir obrigações de prestação de contas.

Em investigações de incidentes, o histórico de sessão apoia a correlação entre usuários, dispositivos, redes e operações executadas. A partir dele, é possível identificar desde acessos fora do padrão até movimentos laterais, uso de credenciais comprometidas, alterações não autorizadas e exportações indevidas de informações. Também permite comparar o comportamento esperado com o comportamento efetivamente observado, acelerando a triagem e reduzindo o tempo de resposta.

Assim, a identificação e o histórico de sessão constituem uma camada essencial de segurança operacional. Eles fornecem rastreabilidade, contexto e evidências para auditoria, ajudam a prevenir usos indevidos e fortalecem a capacidade de investigação da solução ao longo de todo o ciclo de vida dos acessos.

Controle de Acesso por Dispositivo

A solução deverá disponibilizar uma interface gráfica intuitiva para o gerenciamento de dispositivos autorizados, bloqueados e pendentes de validação. Esse mecanismo garante que apenas terminais confiáveis e previamente homologados possam estabelecer conexão com o sistema, reduzindo a superfície de ataque e prevenindo acessos não autorizados originados de equipamentos comprometidos, compartilhados ou não reconhecidos pela política de segurança.

O controle deve operar por meio de uma **lista de acesso/permissão** e uma **lista de bloqueio**, com avaliação a cada tentativa de acesso. Quando um dispositivo estiver presente na lista de permitidos, a conexão deve ser aceita normalmente. Quando estiver na lista de bloqueio, a conexão deve ser negada automaticamente. Se o dispositivo não estiver em nenhuma das listas, a solução deverá tratá-lo como **não autorizado**, registrando o evento e aplicando o fluxo definido de análise e aprovação.

O processo de autorização de novos dispositivos deve permitir que um administrador ou perfil equivalente avalie o terminal com base em seus identificadores persistentes, contexto de acesso e justificativa operacional. A aprovação pode ocorrer de forma imediata ou após análise manual, conforme a política interna. Uma vez autorizado, o dispositivo deve ser associado ao usuário, à organização ou ao escopo definido pela regra de negócio, permanecendo disponível para uso até eventual revogação.

Quando um dispositivo não autorizado tentar se conectar, a solução deverá impedir o acesso, exibir mensagem clara de bloqueio e registrar todos os dados relevantes para auditoria, incluindo identificador do dispositivo, IP de origem, usuário informado, data e hora, resultado da autenticação e motivo da negação. Se aplicável, o sistema também poderá notificar os administradores responsáveis para revisão do evento e eventual inclusão do dispositivo na lista de bloqueio ou na fila de aprovação.

Os identificadores de dispositivo devem ser tratados como dados persistentes e rastreáveis, com suporte a mais de um atributo de identificação, como fingerprint do equipamento, identificador de instalação, navegador quando aplicável, sistema operacional, nome do host e outros sinais técnicos permitidos pela política. A solução deverá manter a integridade desses identificadores ao longo do tempo, controlando alterações suspeitas e permitindo a comparação entre sessões distintas para detectar troca de equipamento, clonagem ou falsificação.

Além disso, a interface administrativa deve oferecer visão consolidada da base de dispositivos, com status, histórico de alterações, data de primeiro acesso, último acesso, responsável pela decisão e observações operacionais. O objetivo é permitir gestão rápida e auditável, com filtros, busca, ordenação e trilha de eventos suficiente para suportar investigações, revisões de segurança e processos de conformidade.

Bloqueio de Dispositivo

O administrador poderá bloquear o acesso de qualquer dispositivo identificado diretamente pela interface gráfica, sem necessidade de comandos via linha de comando ou acesso ao banco de dados. A ação deve ser imediata e registrada no log de auditoria. Quando bloqueado, o dispositivo passa a ser recusado em todas as tentativas subsequentes de autenticação, inclusive se o usuário estiver corretamente autenticado em outro contexto, salvo exceção formalmente aprovada por perfil autorizado.

Desbloqueio da Lista de Bloqueio

Dispositivos previamente bloqueados poderão ser reabilitados a partir da mesma interface, mediante autorização do perfil competente. A lista de bloqueio deve exibir todos os dispositivos bloqueados, com data/hora da ação e o responsável pelo bloqueio. Antes do desbloqueio, a solução deve permitir a conferência do histórico do dispositivo, a revisão do motivo original do bloqueio e, quando aplicável, a inclusão de observações sobre a liberação realizada.

Requisitos funcionais

- Manter lista de dispositivos permitidos com atualização em tempo real.
- Manter lista de dispositivos bloqueados com exibição de motivo, data/hora e responsável.
- Permitir cadastro, aprovação, bloqueio e desbloqueio de dispositivos pela interface gráfica.
- Registrar cada tentativa de acesso de dispositivo não autorizado, bloqueado ou desconhecido.
- Associar identificadores persistentes do dispositivo ao histórico de sessões e auditoria.
- Exibir histórico de alterações por dispositivo, incluindo criação, aprovação, bloqueio, desbloqueio e edição.
- Permitir busca, filtragem e ordenação por usuário, status, data de último acesso e origem.
- Restringir a administração dos dispositivos aos perfis Supervisor ou superior.
- Garantir que qualquer mudança de status produza evento de auditoria imutável.
- Permitir revisão manual de dispositivos pendentes antes da autorização final.

Gestão de Tipos de Arquivos Anexados

É permitido que os administradores definam e restrinjam os tipos de arquivos que podem ser anexados ao registro de pessoas de interesse cadastradas no sistema. Esse controle é fundamental para reduzir a exposição a arquivos maliciosos, evitar a execução de conteúdos não autorizados, preservar a integridade do banco de dados e padronizar a documentação associada a cada registro, garantindo maior rastreabilidade e segurança operacional.

A gestão de tipos permitidos deve ser aplicada no contexto do cadastro da pessoa de interesse, de forma que cada registro aceite apenas anexos compatíveis com a política definida pela organização. Isso permite manter um histórico documental confiável, facilitar a consulta pelos usuários autorizados e impedir que arquivos inadequados comprometam a análise, o armazenamento ou a conformidade do sistema.

Configuração Centralizada

A lista de extensões e tipos MIME permitidos deve ser configurável centralmente pelo administrador geral, sem necessidade de reinicialização do serviço. A política deve poder ser atualizada conforme a necessidade da operação, com aplicação imediata para novos anexos e registro de auditoria da alteração realizada.

Tipos Suportados

Exemplos típicos: imagens (JPG, PNG), documentos (PDF), planilhas controladas (XLSX) e vídeos curtos (MP4), quando houver justificativa operacional. Tipos de risco elevado, como executáveis, scripts, arquivos compactados com conteúdo oculto e extensões ambíguas, devem ser bloqueados por padrão ou liberados apenas mediante exceção formal.

Validação na Camada de Aplicação

A validação do tipo de arquivo deve ocorrer tanto no frontend quanto no backend, impedindo tentativas de bypass por renomeação de extensão ou manipulação de headers. O backend deve revalidar o conteúdo real do arquivo, comparar extensão, MIME e assinatura quando aplicável, e rejeitar inconsistências antes de persistir o anexo.

Critérios de segurança e governança

O controle de tipo de arquivo é importante porque anexos podem ser usados como vetor de ataque, especialmente quando permitem código executável, macros, scripts, arquivos com dupla extensão ou conteúdo disfarçado. Ao limitar os formatos aceitos, a solução reduz a chance de infecção por malware, protege os usuários que irão consultar os registros e diminui o risco de exposição de dados sensíveis em documentos não autorizados.

Além da proteção contra ameaças, a política de anexos também ajuda na governança do cadastro de pessoas de interesse. Arquivos padronizados facilitam revisão, pesquisa, classificação e integração com processos de análise, garantindo que a documentação armazenada tenha consistência mínima para uso operacional e auditoria.

Exemplos de categorias de arquivos

Categoria	Exemplos permitidos	Observações
Imagens	JPG, JPEG, PNG	Usadas para fotos, documentos digitalizados e evidências visuais.
Documentos	PDF, DOCX	Preferir formatos de leitura estável e com menor risco de execução.
Planilhas	XLSX	Devem ser usadas apenas quando houver necessidade operacional clara.
Vídeos	MP4	Restringir a casos justificados, considerando tamanho e custo de armazenamento.
Bloqueados por padrão	EXE, BAT, CMD, JS, VBS, MSI, SCR	Formatos com potencial de execução ou automação devem ser rejeitados.

Regras de configuração administrativa

- Permitir cadastro, edição e remoção de extensões autorizadas por perfil administrativo permitido.
- Associar cada regra de anexos a uma política global ou a um escopo específico, quando necessário.
- Exibir a lista de extensões e MIME types aceitos em tela de administração com validação imediata.
- Manter histórico de alterações com data/hora, responsável e justificativa da mudança.
- Permitir que o administrador defina mensagens de erro padronizadas para anexos rejeitados.
- Aplicar a configuração sem reiniciar o serviço e sem impactar anexos já armazenados.

Comportamento quando um arquivo não permitido é enviado

Quando um usuário tentar anexar um arquivo fora da política definida, a solução deverá bloquear o envio, apresentar mensagem clara ao usuário e impedir que o conteúdo seja persistido no registro da pessoa de interesse. O sistema também deve registrar o evento para auditoria, incluindo nome do arquivo, extensão informada, tipo detectado, usuário responsável, data e hora, e o motivo da rejeição.

Se o arquivo apresentar inconsistência entre extensão, tipo MIME ou conteúdo real, a validação deverá tratá-lo como suspeito e negar a submissão. Em situações de repetidas tentativas com formatos proibidos, o evento poderá ser sinalizado para revisão administrativa, reforçando o monitoramento de uso indevido.

Integração com o registro de pessoas de interesse

Os anexos permitidos devem ser vinculados diretamente ao cadastro da pessoa de interesse, respeitando permissões de acesso e trilha de auditoria do sistema. Cada anexo deve ficar associado ao identificador do registro, ao autor do envio, à data de inclusão e à categoria do arquivo, de modo que a documentação permaneça organizada e consultável ao longo do ciclo de vida do cadastro.

Essa integração também deve garantir que os anexos possam ser revisados posteriormente por usuários autorizados, mantendo coerência entre o conteúdo documental e o estado do registro. Caso a política de tipos seja alterada no futuro, os arquivos já cadastrados podem permanecer disponíveis, mas novos envios devem seguir imediatamente a regra atualizada.

CAPÍTULO 2

Módulo de Administração

O módulo de administração concentra as funcionalidades responsáveis pela organização lógica dos dispositivos de captura, gestão de usuários, controle de acesso hierárquico, análise de vídeo arquivado e integração com diretórios corporativos. Sua correta configuração é determinante para a eficiência operacional da central de monitoramento e para o cumprimento de requisitos de governança e conformidade.

Na prática, esse módulo atua como a camada de orquestração da plataforma, reduzindo a complexidade de operar múltiplos dispositivos, perfis de usuário e regras de uso em ambientes com alta demanda. Em operações distribuídas, ele ajuda a evitar configurações inconsistentes entre unidades, facilita a padronização de procedimentos e oferece uma visão centralizada do parque tecnológico, permitindo que equipes administrativas mantenham o sistema organizado mesmo quando o número de câmeras, operadores e locais monitorados cresce continuamente.

Entre as principais capacidades oferecidas estão o cadastro e a manutenção de dispositivos, a definição de grupos e perfis de acesso, a administração de permissões por função ou hierarquia, e a vinculação com serviços corporativos de autenticação e diretório. O módulo também apoia a gestão de vídeo arquivado, tornando mais simples localizar registros, aplicar critérios de retenção e atender solicitações internas de consulta ou auditoria. Com isso, o dia a dia da operação se torna mais previsível, com menos retrabalho e maior controle sobre quem pode visualizar, alterar ou administrar cada recurso da plataforma.

Do ponto de vista de escalabilidade, a administração centralizada é essencial para que a solução evolua sem perda de controle. À medida que novos dispositivos, novos usuários e novas áreas de cobertura são incorporados, o módulo permite expandir a infraestrutura sem dispersar regras ou duplicar tarefas de configuração. Isso reduz o risco de erro humano, melhora a rastreabilidade das alterações e garante que as políticas operacionais sejam aplicadas de forma uniforme em toda a plataforma.

Esse módulo também se conecta diretamente ao módulo de segurança, complementando suas funções de proteção e controle. Enquanto a segurança define barreiras, políticas e mecanismos de proteção do ambiente, a administração fornece os meios para aplicar essas regras de maneira consistente, gerenciar exceções autorizadas e manter a operação alinhada às necessidades reais da central de monitoramento. Essa integração assegura que a governança não fique apenas no plano técnico, mas faça parte da rotina administrativa e operacional da solução.

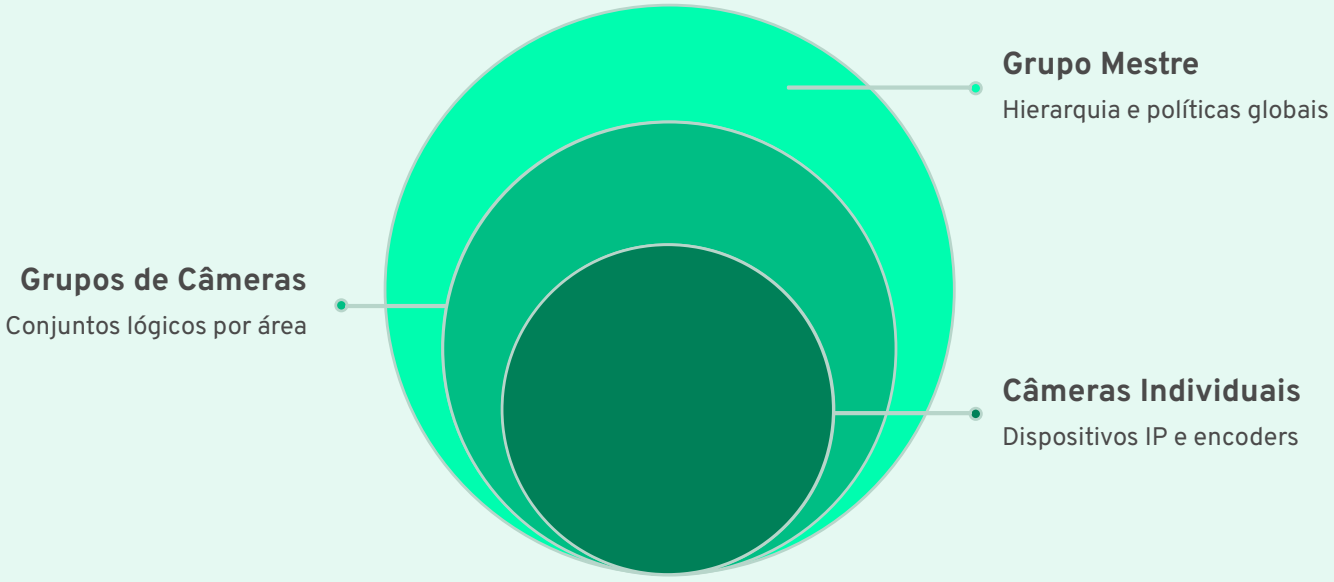
Criação e Hierarquização de Grupos de Câmeras

O modulo de administração do Cluebase permite aos administradores organizem os dispositivos de captura — câmeras IP, encoders e similares — em grupos lógicos com hierarquia configurável. Essa capacidade é indispensável em instalações de médio e grande porte, onde dezenas ou centenas de câmeras precisam ser gerenciadas de forma eficiente e contextualizada por localização, função ou nível de criticidade.

A estrutura recomendada é do tipo **árvore**, permitindo grupos principais e subgrupos aninhados em múltiplos níveis. Assim, um grupo corporativo pode conter unidades, prédios, andares, alas, salas, perímetros ou áreas externas, mantendo a organização alinhada à topologia física ou operacional do ambiente. Essa abordagem facilita a navegação em instalações complexas e reduz o esforço necessário para localizar rapidamente um conjunto específico de câmeras.

Além da posição hierárquica, cada grupo pode receber metadados administrativos para apoiar sua gestão. Entre os atributos mais comuns estão nome, descrição, código interno, localidade, responsável, nível de criticidade, tags operacionais, data de criação, status de ativação e observações de uso. Esses campos ajudam a padronizar o cadastro, melhoram a rastreabilidade e tornam a manutenção mais simples ao longo do ciclo de vida da instalação.

A relação entre grupos e permissões de usuários é um dos principais benefícios do modelo hierárquico. Permissões podem ser aplicadas no nível do grupo mestre, herdadas pelos subgrupos ou sobrescritas quando necessário, permitindo controlar de forma granular quem pode visualizar, operar, exportar ou administrar cada conjunto de câmeras. Dessa forma, a estrutura lógica da organização se reflete diretamente na política de acesso, evitando exposições indevidas e simplificando a gestão de perfis.



Em uma instalação aeroportuária, por exemplo, os grupos podem ser organizados por terminal, portão, saguão, controle de acesso, estacionamento e área de carga. Em campi universitários, a divisão pode seguir blocos acadêmicos, laboratórios, bibliotecas, refeitórios e áreas de circulação. Em redes corporativas e indústrias, a lógica pode refletir plantas, linhas de produção, docas, almoxarifados e perímetros externos. Em todos os casos, a hierarquia facilita a operação diária e torna a expansão da infraestrutura mais previsível.

Do ponto de vista operacional, o agrupamento lógico melhora a clareza da interface, reduz a complexidade na busca de ativos e acelera ações como monitoramento em massa, aplicação de políticas e revisão de eventos por área. Também favorece a padronização entre unidades diferentes, evita duplicidade de cadastros e simplifica a adoção de critérios consistentes de nomenclatura, manutenção e auditoria.

Requisitos funcionais

- Permitir criação de grupos e subgrupos em estrutura hierárquica do tipo árvore.
- Suportar associação de câmeras IP, encoders e outros dispositivos de captura a qualquer nível da hierarquia.
- Permitir a atribuição de metadados aos grupos, como nome, descrição, responsável, localidade e criticidade.
- Aplicar permissões por grupo, com herança para subgrupos e possibilidade de exceções controladas.
- Disponibilizar interface gráfica para criação, edição, movimentação e reorganização dos grupos.
- Manter visibilidade segmentada conforme o perfil do usuário e seu escopo de atuação.
- Facilitar a administração em ambientes distribuídos, com múltiplas unidades, prédios ou zonas operacionais.

A criação dos grupos deve ser realizada por interface gráfica, sem necessidade de edição de arquivos de configuração. Dessa forma, administradores podem ajustar a estrutura organizacional conforme a operação evolui, mantendo a plataforma alinhada às necessidades reais da central de monitoramento e aos requisitos de governança e controle de acesso.

Listas de Interesse

É possível criar e gerir inúmeras listas de interesse, que são coleções de indivíduos, veículos, objetos ou padrões definidos previamente para acionar alertas automáticos, facilitar buscas direcionadas ou aplicar filtros nos fluxos de vídeo designados. As listas funcionam como uma camada de inteligência operacional sobreposta à vigilância passiva, permitindo que o sistema reconheça eventos relevantes com base em critérios previamente cadastrados.

Essas listas podem ser criadas e mantidas por perfis administrativos ou por operadores autorizados, com suporte a nomeação padronizada, descrição, tags operacionais, nível de criticidade, validade temporal, responsáveis e histórico de alterações. Dependendo da política da instalação, também pode haver controle de versões, revisão por aprovação e auditoria de quem incluiu, removeu ou editou cada item.

Os elementos adicionados a uma lista podem incluir pessoas específicas, rostos associados a identidades conhecidas, veículos por placa ou características visuais, documentos fotográficos, perfis biométricos e padrões comportamentais ou contextuais, como presença em áreas restritas ou recorrência em determinados horários. Em operações mais avançadas, a lista também pode incorporar variações e atributos auxiliares, como apelidos, alias, marcas de veículo, cor, modelo, região de origem e observações operacionais.

Criação e Edição

Criação de múltiplas listas nomeadas, com inclusão de perfis biométricos, veículos, documentos fotográficos, padrões ou outros critérios relevantes para a operação.

Associação a Câmeras

Cada lista poderá ser vinculada a câmeras individuais ou grupos de câmeras, determinando o escopo de monitoramento ativo para aquela lista.

Acionamento de Alertas

Quando um indivíduo ou alvo da lista for identificado nas câmeras associadas, o sistema deverá gerar alertas em tempo real com priorização configurável por nível de risco.

Filtros em Buscas

A lista de interesse poderá ser usada como critério de filtragem em buscas no vídeo arquivado, limitando os resultados às entidades cadastradas naquela lista específica.

Na prática, a integração com análise de vídeo permite que o mecanismo opere sobre detecções automáticas geradas por reconhecimento facial, leitura de placas, classificação de objetos, comparação de imagens e outros analytics disponíveis na plataforma. Quando há correspondência com um item cadastrado, o sistema pode registrar o evento, associar metadados da câmera, horário, local, confiança da detecção e evidências visuais, além de encaminhar a ocorrência para painéis de monitoramento, filas de atendimento ou integrações externas.

As listas podem assumir diferentes finalidades operacionais. **Watchlists** são listas de observação, usadas para monitorar alvos de interesse e gerar visibilidade antecipada sem necessariamente bloquear nenhuma ação. Já **blocklists** representam listas restritivas, voltadas a perfis ou entidades cuja presença exige resposta imediata, escalonamento ou bloqueio operacional conforme a política vigente. Essa distinção ajuda a separar monitoramento preventivo de situações de maior criticidade.

Os alertas podem ser configurados por tipo de entidade, câmera, faixa horária, nível de confiança e criticidade da lista. Assim, uma lista de alto risco pode disparar notificações prioritárias, enquanto uma lista de observação pode apenas gerar registros de evento ou avisos de menor severidade. Também é possível configurar regras para evitar duplicidade de alarmes, aplicar janelas de supressão e consolidar múltiplas detecções do mesmo alvo em um único incidente.

Watchlist

Lista de observação para acompanhamento de pessoas, veículos ou padrões de interesse, com foco em monitoramento e rastreabilidade.

Blocklist

Lista restritiva usada para alertas críticos, escalonamento imediato e acionamento de respostas operacionais previamente definidas.

Lista Temporária

Conjunto válido por período determinado, útil para investigações pontuais, operações especiais ou eventos com duração limitada.

Lista Compartilhada

Lista reutilizável entre unidades, centros de controle ou filiais, mantendo critérios consistentes em ambientes distribuídos.

Tipos de listas e usos operacionais

- **Pessoas de interesse:** indivíduos monitorados por imagem facial, biometria ou associação a registros operacionais.
- **Veículos de interesse:** automóveis, motos, caminhões ou frotas identificados por placa, cor, modelo ou atributos visuais.
- **Padrões e comportamentos:** repetições contextuais, presença recorrente em áreas específicas ou eventos associados a regras analíticas.
- **Listas de exclusão:** entidades que exigem tratamento diferenciado, geração de alerta ou bloqueio de fluxo conforme a política da instalação.
- **Listas temporárias:** cadastros válidos apenas durante investigações, auditorias, operações especiais ou campanhas de segurança.

Entre os principais casos de uso estão controle de acesso, proteção de perímetros, monitoramento de visitantes recorrentes, detecção de veículos suspeitos, apoio a investigações, acompanhamento de ordens judiciais e supervisão de eventos de grande circulação. Em instalações críticas, as listas também ajudam a acelerar triagens operacionais, priorizar equipes de resposta e localizar rapidamente ocorrências em gravações históricas.

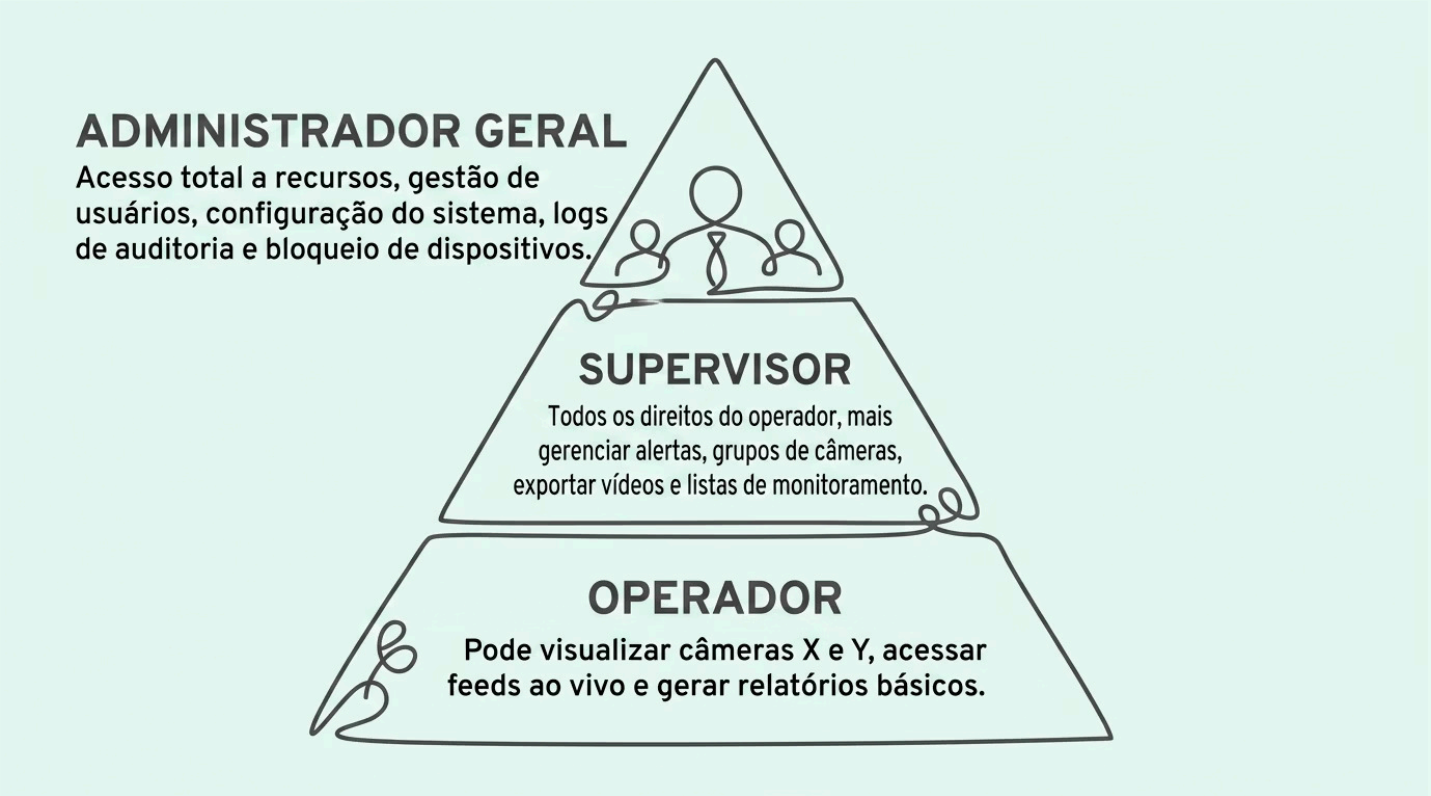
A administração dessas listas deve oferecer recursos de inclusão manual, importação em lote, associação por critérios automáticos e remoção controlada, sempre preservando trilhas de auditoria. Dessa forma, a solução consegue apoiar operações preventivas e reativas de maneira consistente, escalável e alinhada às políticas de segurança da organização.

Gestão de Usuários e Perfis de Acesso

O modulo de gestão de usuários do Cluebase opera de forma granular de gestão de usuários, e suporta ate três níveis hierárquicos de operadores do sistema. Cada perfil deve ter permissões individualizadas para acesso a funcionalidades, câmeras, menus de configuração, exportação de conteúdo e demais operações disponíveis na plataforma. A criação de perfis personalizados, além dos níveis padrão, também deve ser suportada.

O desenho de acesso deve seguir o princípio do **menor privilégio**, garantindo que cada usuário receba apenas as permissões estritamente necessárias para executar suas funções. Isso reduz o risco operacional, limita impactos em caso de credencial comprometida e permite que a administração mantenha um controle mais preciso sobre ações sensíveis, como alteração de configurações, acesso a gravações, gerenciamento de dispositivos e exportação de evidências.

Os perfis podem ser criados a partir de modelos padrão ou definidos manualmente por administradores, com possibilidade de associação por cargo, unidade, turno, projeto ou operação específica. A atribuição deve poder ocorrer de forma individual, por grupos ou por estrutura organizacional, permitindo herança de permissões quando apropriado e sobrescrita de regras em casos excepcionais. Dessa forma, perfis-base podem ser reutilizados em diferentes contextos sem exigir reconfiguração completa a cada novo usuário.



Na prática, a hierarquia de acesso costuma ser estruturada em três níveis principais. **Operador** é o perfil de base, voltado à rotina de monitoramento e execução assistida, com permissões restritas às telas, câmeras e ações necessárias para acompanhamento operacional. **Supervisor** amplia essas capacidades, permitindo gestão de filas, tratamento de alertas, revisão de ocorrências e exportações controladas. **Administrador Geral** concentra atribuições críticas, como gerenciamento de usuários, configuração da plataforma, políticas de retenção, perfis de segurança, integrações, auditoria e governança global do ambiente.

A o Cluebase permite que permissões sejam herdadas de perfis superiores ou de grupos-base, mas também sobrescritas quando houver necessidade de limitação adicional. Por exemplo, um supervisor pode herdar capacidades padrão de monitoramento e receber apenas um subconjunto de permissões administrativas, enquanto um operador pode ter acesso ampliado a um conjunto específico de câmeras sem ganhar acesso às configurações gerais do sistema. Esse modelo flexível evita permissões excessivas e facilita a adequação a políticas internas e requisitos regulatórios.

Em implantações de grande porte, a gestão centralizada é essencial para manter consistência entre múltiplos sites, centrais de monitoramento, unidades operacionais e equipes com responsabilidades distintas. Um repositório único de usuários e perfis simplifica auditoria, reduz retrabalho, acelera onboarding e desligamento de colaboradores, e assegura que alterações de acesso sejam propagadas de forma controlada e rastreável. Também é importante suportar trilhas de auditoria com histórico de criação, alteração, ativação, desativação e remoção de usuários e perfis, incluindo data, responsável e motivo da mudança.

Além disso, o módulo deve contemplar mecanismos de governança como expiração de permissões temporárias, revisão periódica de acessos, bloqueio automático por inatividade ou política de segurança, e segregação entre perfis operacionais e administrativos. Em conjunto, esses recursos garantem uma administração escalável, segura e aderente às necessidades de ambientes com múltiplos níveis de responsabilidade.

Detalhamento dos Níveis de Acesso

A seguir, a descrição técnica das capacidades e restrições associadas a cada nível hierárquico de acesso. O princípio de menor privilégio deve ser aplicado como padrão, garantindo que usuários recebam apenas as permissões estritamente necessárias para o desempenho de suas funções.

Cada nível foi concebido para atender a cenários operacionais distintos, desde a rotina de monitoramento até a administração completa da plataforma. A separação de responsabilidades reduz riscos, evita exposição indevida de funcionalidades sensíveis e facilita a governança de ambientes com múltiplas equipes, unidades e centros de operação.

Nível	Permissões principais	Restrições	Uso típico
Operador	Visualização de câmeras autorizadas, consulta de eventos, acompanhamento de alarmes recebidos, geração de relatórios básicos e execução de ações operacionais previamente permitidas.	Sem acesso a menus de configuração, gestão de usuários, políticas da plataforma, exportação irrestrita de evidências ou alterações em dispositivos e integrações.	Monitoramento diário, triagem inicial de eventos, suporte à operação em tempo real e atendimento a rotinas assistidas.
Supervisor	Todos os direitos do Operador, além de gestão de alertas, administração de listas de interesse, exportação controlada de vídeos, acesso a grupos de câmeras sob sua responsabilidade e revisão de ocorrências.	Não pode alterar configurações globais do sistema, criar perfis de segurança, administrar usuários em nível global nem modificar integrações externas críticas.	Coordenação de equipe, validação de eventos, apoio a investigações operacionais e supervisão de áreas ou turnos específicos.
Administrador Geral	Acesso completo à plataforma, incluindo criação e exclusão de usuários, definição de perfis, parametrização geral, gestão de dispositivos, integrações externas, auditoria e políticas de segurança.	Não possui limitações funcionais dentro do escopo administrativo, mas suas ações devem ser auditadas e, quando aplicável, submetidas a trilhas de aprovação.	Governança da plataforma, configuração inicial, manutenção evolutiva, resposta a incidentes, administração centralizada e conformidade.

1

Operador

O Operador é o perfil de entrada para uso cotidiano da solução. Seu foco é a execução de tarefas de monitoramento e suporte operacional, com acesso apenas ao necessário para observar o ambiente e registrar acontecimentos relevantes. Em geral, esse perfil é utilizado por equipes de vigilância, centrais de monitoramento e colaboradores responsáveis por acompanhamento assistido em tempo real.

Entre suas permissões estão a visualização de câmeras previamente liberadas, a consulta a eventos e registros associados, a navegação por painéis operacionais e a emissão de relatórios básicos padronizados. Dependendo da política da organização, o Operador também pode reconhecer alertas, marcar ocorrências como visualizadas e encaminhar situações para validação de um nível superior.

O Operador não deve acessar configurações do sistema, menus administrativos, perfis de acesso, parâmetros de retenção, integrações externas, exportações de vídeo sem controle ou qualquer funcionalidade capaz de alterar o comportamento global da plataforma. Esse isolamento reduz o risco de mudanças acidentais e preserva a integridade do ambiente.

Na prática, esse perfil é indicado para tarefas como vigilância de perímetro, acompanhamento de áreas críticas, apoio ao atendimento de ocorrências e suporte a operações que exigem consulta frequente a imagens, mas não requerem capacidade de administração.

2

Supervisor

O Supervisor herda as permissões do Operador e adiciona capacidades de coordenação e tratamento avançado de eventos. Trata-se do perfil intermediário, normalmente atribuído a líderes de turno, responsáveis por área, analistas sêniores ou profissionais encarregados de validar ocorrências e direcionar ações da equipe.

Suas funções incluem gerenciar alertas, priorizar eventos, acompanhar grupos de câmeras sob sua responsabilidade, manter listas de interesse, realizar exportações controladas e revisar ocorrências para apoiar investigações ou auditorias internas. Em algumas implantações, também pode registrar comentários, anexar observações operacionais e encaminhar casos para níveis administrativos.

Apesar das prerrogativas ampliadas, o Supervisor continua impedido de alterar parâmetros estruturais da solução, definir políticas globais, criar perfis de segurança, administrar usuários fora do seu escopo ou modificar integrações que afetem todo o ambiente. Essa separação garante que a gestão operacional permaneça descentralizada, sem comprometer a governança central.

Esse nível é especialmente útil em salas de controle, centros de comando e operações multi-turno, nas quais uma camada intermediária precisa reagir rapidamente aos incidentes sem abrir mão da rastreabilidade e do controle institucional.

3

Administrador Geral

O Administrador Geral possui acesso irrestrito às funcionalidades da plataforma e é responsável pela governança completa do ambiente. Esse perfil deve ser atribuído com critérios rigorosos, pois concentra as permissões mais sensíveis e impacta diretamente a segurança, disponibilidade e conformidade do sistema.

Entre suas capacidades estão a criação, alteração, ativação, desativação e exclusão de usuários; a definição de perfis e regras de acesso; a configuração de dispositivos; a administração de integrações externas; a parametrização global; e a consulta a logs e trilhas de auditoria. Também pode ajustar políticas de retenção, organizar estruturas hierárquicas, revisar permissões temporárias e validar exceções operacionais.

Na prática, esse nível é usado por administradores de TI, responsáveis pela segurança da informação, times de suporte especializado e gestores de plataforma. É o perfil indicado para implantação inicial, manutenção evolutiva, resposta a incidentes e adequações regulatórias.

Por concentrar poderes amplos, suas ações devem ser sempre registradas em auditoria detalhada, com data, responsável, justificativa e histórico de alterações. Quando possível, recomenda-se a adoção de revisão periódica, segregação de funções e controles adicionais para operações críticas.

Os níveis se relacionam de forma hierárquica e cumulativa. O Supervisor incorpora as permissões do Operador e adiciona funções de coordenação, enquanto o Administrador Geral engloba todas as capacidades anteriores e inclui o poder de administrar a própria estrutura de acesso. Isso significa que permissões podem ser herdadas de um nível para outro, mas não devem ser ampliadas sem controle explícito.

Na implementação prática, o Operador depende de autorizações concedidas por perfis superiores para ampliar seu escopo de câmeras ou funções. O Supervisor, por sua vez, pode receber acesso adicional a grupos específicos, porém sem extrapolar o domínio operacional definido para sua equipe. Já o Administrador Geral é o único perfil que pode criar, revisar e revogar esses vínculos de acesso em escala global.

Esse modelo facilita a escalabilidade da solução em organizações com múltiplas unidades, diferentes turnos e responsabilidades distintas. Ao mesmo tempo, simplifica auditoria, onboarding e desligamento, pois cada perfil possui um papel claro, com expectativas bem definidas sobre o que pode e o que não pode ser executado.

⚠ Perfis personalizados devem ser documentados e versionados, garantindo rastreabilidade das alterações de permissão realizadas ao longo do tempo. Quando um perfil derivado for criado, sua relação com o perfil-base deve permanecer explícita para facilitar auditoria, revisão periódica e eventuais correções de acesso.

Permissões Granulares por Funcionalidade

Além dos níveis hierárquicos fixos, a solução deve permitir a criação de perfis personalizados com controle granular sobre cada funcionalidade disponível. Isso possibilita cenários como operadores com acesso de exportação mas sem acesso a configurações, ou supervisores restritos a um subconjunto de câmeras.

Na prática, a granularidade de permissões permite separar o que um usuário pode **ver**, **executar**, **alterar** e **auditar**. Em vez de depender apenas de um perfil genérico, a organização pode combinar permissões específicas para refletir responsabilidades reais do cargo, do turno, da unidade ou da operação em andamento. Isso reduz exceções manuais, melhora a aderência ao princípio de menor privilégio e torna o ambiente mais seguro e mais fácil de administrar.

Esses perfis podem incluir, por exemplo, acesso apenas à visualização de câmeras ao vivo, exportação de vídeos com restrições, reconhecimento de alarmes, bloqueio de dispositivos específicos, consulta de trilhas de auditoria, gerenciamento de listas de interesse, ou alteração limitada de parâmetros de câmera. O objetivo não é liberar tudo ou nada, mas sim conceder exatamente as ações necessárias para cada contexto operacional.

Funcionalidade	Operador	Supervisor	Adm. Geral
Visualizar câmeras ao vivo	✅ Parcial	✅ Parcial	✅ Total
Acessar menus de configuração	❌	❌	✅
Exportar vídeos	❌	✅	✅
Apagar eventos	❌	❌	✅
Gerenciar usuários	❌	❌	✅
Bloquear dispositivos	❌	✅	✅
Gerenciar listas de interesse	❌	✅	✅
Visualizar logs de auditoria	❌	❌	✅

Como perfis personalizados são construídos

Um perfil personalizado normalmente parte de um perfil-base, como Operador ou Supervisor, e recebe ajustes finos conforme a necessidade do ambiente. A criação pode seguir uma lógica por módulos, por exemplo: monitoramento, eventos, vídeo, dispositivos, usuários, auditoria e administração. Em cada módulo, o administrador define quais ações ficam liberadas, quais ficam somente para leitura e quais permanecem bloqueadas.

Esse modelo facilita composições como:

- Operador com permissão para exportar vídeo, mas sem acesso a usuários ou configurações;
- Supervisor com poder de gerenciar alertas e listas de interesse, mas sem editar parâmetros globais;
- Perfil de auditoria com leitura de logs e eventos, sem possibilidade de alterar qualquer cadastro;
- Perfil de resposta rápida com bloqueio temporário de dispositivos e acesso restrito a um conjunto definido de câmeras.

Exemplos de permissões granulares

As permissões podem ser detalhadas em níveis como **visualizar**, **criar**, **editar**, **excluir**, **aprovar**, **exportar**, **bloquear**, **desbloquear**, **reconhecer** e **auditar**. Também é possível restringir por escopo, como câmera específica, grupo de câmeras, unidade operacional, turno, filial ou região. Dessa forma, a mesma funcionalidade pode existir para vários perfis, mas com limites de alcance diferentes.

Permissão exemplo	Descrição	Perfis comuns	Observação
Ver câmeras ao vivo	Permite assistir transmissões autorizadas em tempo real.	Operador, Supervisor, Adm. Geral	Pode ser limitada por grupo, local ou horário.
Exportar vídeo	Permite gerar arquivos de evidência com trilha de auditoria.	Supervisor, Adm. Geral	Pode exigir justificativa e aprovação.
Gerenciar alertas	Permite reconhecer, priorizar ou encaminhar alarmes.	Supervisor, Adm. Geral	Útil em centrais com múltiplos turnos.
Configurar câmeras	Permite ajustar parâmetros operacionais e vínculos do dispositivo.	Adm. Geral	Requer atenção especial por impactar o ambiente.
Gerenciar usuários	Permite criar, editar, desativar e revisar contas e perfis.	Adm. Geral	Normalmente associado à segregação de funções.
Acessar logs de auditoria	Permite consultar histórico de ações e alterações.	Adm. Geral	Importante para conformidade e investigação.
Bloquear dispositivos	Permite isolar equipamentos com comportamento suspeito.	Supervisor, Adm. Geral	Geralmente controlado por escopo e motivo.
Gerenciar listas de interesse	Permite incluir, remover e atualizar itens monitorados.	Supervisor, Adm. Geral	Bom exemplo de permissão operacional intermediária.

Casos de uso para perfis com permissões mistas

Perfis mistos são especialmente úteis quando a operação real não se encaixa perfeitamente em categorias rígidas. Um usuário pode, por exemplo, precisar exportar evidências durante um incidente, mas não ter qualquer autonomia para alterar configurações do sistema. Outro caso comum é o de um supervisor que administra apenas um conjunto específico de câmeras, enquanto permanece bloqueado para áreas de outras unidades.

Também é possível atender equipes especializadas, como suporte técnico, segurança patrimonial, auditoria interna ou resposta a incidentes. Cada grupo recebe permissões adequadas ao seu papel, evitando que a solução fique engessada por perfis excessivamente amplos ou que dependa de autorizações temporárias difíceis de controlar.

Flexibilidade operacional com segurança

O principal benefício desse modelo é equilibrar flexibilidade e proteção. Ao conceder apenas o conjunto necessário de permissões, a organização reduz o risco de uso indevido, limita o impacto de erros humanos e melhora a rastreabilidade das ações. Ao mesmo tempo, evita bloqueios desnecessários que atrasariam a operação ou forçariam a criação de exceções informais.

Esse equilíbrio é reforçado por mecanismos como escopo limitado, aprovação para ações críticas, auditoria de alterações, revisões periódicas de acesso e documentação dos perfis derivados. Assim, a plataforma permanece adaptável a diferentes cenários operacionais sem abrir mão da governança, da conformidade e da segurança da informação.

Módulo de Busca e Análise de Vídeo Arquivado

O módulo de busca e análise de vídeo arquivado é um dos componentes mais estratégicos da solução. Ele deverá ser capaz de realizar filtragem simultânea e combinada com base em múltiplos critérios identificados por algoritmos de visão computacional. Essa capacidade transforma o vídeo arquivado de um repositório passivo em uma ferramenta ativa de investigação e inteligência operacional.

Seu objetivo é permitir que equipes de segurança, auditoria e resposta a incidentes localizem rapidamente eventos relevantes em grandes volumes de gravações, reduzindo o tempo gasto em revisão manual e aumentando a precisão na identificação de pessoas, veículos, objetos e comportamentos de interesse. Em vez de depender de buscas lineares em longos períodos de vídeo, o usuário pode partir de um indício parcial — como uma faixa horária, uma característica física, uma placa, uma roupa específica ou uma zona da câmera — e refinar a pesquisa até chegar ao trecho exato desejado.

Os critérios de filtragem estão organizados em três grandes categorias: **Atributos Biométricos e Físicos**, **Classificação Demográfica e Comportamental**, e **Contexto Operacional**. A combinação de filtros de diferentes categorias em uma única consulta é requisito fundamental para eficiência nas investigações. Isso permite, por exemplo, buscar uma pessoa de determinada aparência em um intervalo de tempo específico, em câmeras de uma área restrita, com associação a veículos, objetos ou eventos detectados pelo sistema.

A análise é alimentada por IA e computação visual, que processam os frames e metadados do vídeo para extrair características estruturadas. Entre os recursos esperados estão detecção de presença, rastreamento de alvos, reconhecimento de atributos visuais, agrupamento por similaridade, identificação de padrões de movimentação e correlação entre eventos. O sistema deve ser capaz de interpretar o conteúdo gravado de forma contínua, gerando índices pesquisáveis que aceleram consultas posteriores e ampliam a confiabilidade dos resultados.

Na prática, isso viabiliza buscas como: localizar uma pessoa com determinada vestimenta ou cor predominante, identificar veículos por tipo, cor ou elementos visuais, encontrar ocorrências em uma área geográfica específica da planta, rastrear o deslocamento de um alvo entre câmeras, ou recuperar trechos em que houve interação com portas, acessos, bloqueios, objetos abandonados ou aglomerações incomuns. Quanto mais rico for o contexto capturado, mais útil se torna a investigação.

Para garantir uso em cenários operacionais reais, o módulo precisa ser responsivo mesmo diante de grandes bases de gravação e múltiplas câmeras. As consultas devem suportar intervalos extensos, múltiplos critérios simultâneos, paginação eficiente e retorno rápido de resultados relevantes. Também é importante que a solução preserve rastreabilidade, registrando a consulta executada, os filtros aplicados e o acesso aos trechos analisados.

Os resultados devem ser apresentados de forma clara e investigável, com linha do tempo, miniaturas dos trechos encontrados, indicação das câmeras envolvidas, marcações dos objetos ou eventos detectados e possibilidade de refinar a busca sem recomeçar do zero. Sempre que possível, o usuário deve conseguir abrir o trecho correspondente, revisar o contexto anterior e posterior, comparar ocorrências semelhantes e salvar evidências para uso posterior.

Os critérios de filtragem estão organizados em três grandes categorias: Atributos Biométricos e Físicos, Classificação Demográfica e Comportamental, e Contexto Operacional. A combinação de filtros de diferentes categorias em uma única consulta é requisito fundamental para eficiência nas investigações.

Atributos Biométricos e Físicos

Somos capazes de identificar e filtrar indivíduos no vídeo arquivado com base em características biométricas e físicas detectadas automaticamente pelos algoritmos de visão computacional. Esses atributos permitem localizar com precisão uma pessoa específica ou um grupo de pessoas com características similares em grandes volumes de vídeo gravado, mesmo quando a cena contém múltiplos alvos, baixa iluminação ou diferentes ângulos de captura.

Na prática, o sistema converte pixels em atributos estruturados. Os modelos de IA analisam os frames, detectam pessoas e extraem padrões visuais como contornos do rosto, proporções corporais, vestuário, cabelos, acessórios e marcas distintivas. Esses dados são então transformados em filtros pesquisáveis, permitindo consultas combinadas por mais de um critério ao mesmo tempo.

Reconhecimento Facial

Detecta rostos em cada frame, identifica pontos-chave faciais e cria uma assinatura biométrica comparável com cadastros ou buscas por similaridade. É usado para localizar uma pessoa específica em todas as câmeras e períodos selecionados.

Medições Corporais

Estima altura relativa, porte físico, largura dos ombros, proporção tronco/pernas e silhueta geral a partir da detecção do corpo completo. Esses dados ajudam a filtrar indivíduos com constituição semelhante, mesmo quando o rosto não está visível.

Roupas e Vestuário

Classifica tipo de roupa, cor predominante, padrão, comprimento e combinação de peças, como camisa, jaqueta, calça ou uniforme. O usuário pode buscar por pessoas com vestimenta específica em um intervalo de tempo ou área da câmera.

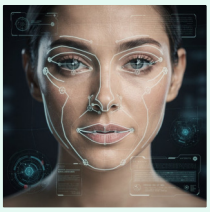
Cabelo, Acessórios e Marcas Distintivas

Reconhece cor e estilo de cabelo, além de acessórios como bonés, óculos, máscaras, bolsas e relógios. Também pode registrar tatuagens, cicatrizes e outras marcas visíveis para refinar a identificação.

Análise de Marcha

Analisa o modo de caminhar, a cadência dos passos e a movimentação dos membros para criar um padrão comportamental útil quando o rosto está parcialmente oculto ou distante. Esse filtro é valioso em câmeras de longo alcance ou cenas com baixa resolução.

Os atributos podem ser usados isoladamente ou combinados em consultas mais precisas. Por exemplo, é possível buscar uma pessoa com **rosto reconhecido**, **camisa escura**, **óculos** e **cabelo curto** em uma janela de horário específica. Em outro cenário, a busca pode considerar apenas **porte físico**, **cor da roupa** e **padrão de marcha** para localizar um indivíduo mesmo sem confirmação facial.



Reconhecimento Facial

Busca por pessoa específica através de reconhecimento facial, permitindo localizar aparições de um indivíduo cadastrado em todas as câmeras e períodos selecionados.

Uso de Máscara

Identificação de indivíduos com máscara de proteção respiratória, sem máscara, ou com uso inadequado (abaixo do nariz, no queixo etc.).

Barba e Óculos

Filtros para presença ou ausência de barba, óculos de grau e óculos de sol, facilitando a identificação de indivíduos mesmo após mudanças de aparência.

Além desses exemplos, a plataforma pode ampliar a busca com outros atributos visuais relevantes, como cor da pele em contextos permitidos, formato de barba, tipo de calçado, presença de mochila ou bolsa, e outros elementos detectáveis conforme a qualidade do vídeo e o modelo de IA disponível. Quanto melhor a qualidade da imagem e maior a continuidade da gravação, maior será a confiabilidade da indexação e da pesquisa posterior.

Os resultados devem ser apresentados de maneira investigável, permitindo comparar ocorrências semelhantes, revisar os trechos adjacentes ao evento encontrado e aplicar novos filtros sem reiniciar a busca. Assim, os atributos biométricos e físicos deixam de ser apenas observações visuais e passam a compor um mecanismo estruturado de investigação em vídeo.

Classificação Demográfica e Comportamental

Além dos atributos físicos, a solução deverá suportar filtros baseados em classificações demográficas e na análise de expressões emocionais e padrões de comportamento dos indivíduos detectados. Esses critérios ampliam o poder investigativo do sistema, permitindo triagem rápida de grandes volumes de vídeo, identificação de grupos de interesse e detecção de situações atípicas que merecem revisão humana.

Na prática, a plataforma combina detecção de pessoas, estimação de pose, análise temporal entre frames e modelos de classificação visual para extrair sinais como faixa etária aproximada, gênero percebido, emoção aparente, densidade de aglomeração, permanência prolongada em uma área e movimentos incompatíveis com o fluxo normal da cena. O resultado é um conjunto de filtros pesquisáveis e acionáveis, úteis tanto para investigação retrospectiva quanto para monitoramento operacional.

Classificação por Grupo Etário

O sistema deverá categorizar automaticamente os indivíduos detectados nas seguintes faixas etárias estimadas pelo algoritmo:

- Criança
- Adolescente
- Adulto
- Idoso

A estimativa de faixa etária é normalmente obtida por modelos treinados em grandes bases de faces ou corpos, que aprendem padrões de proporção facial, textura de pele, postura e constituição corporal. Como se trata de uma inferência probabilística, o sistema deve apresentar o resultado como faixa estimada e não como idade exata.

Em investigações, esse filtro ajuda a localizar pessoas com perfil etário aproximado em cenários como escolas, espaços públicos, eventos ou áreas restritas. Também pode ser combinado com horário, local, vestuário e direção de deslocamento para reduzir falsos positivos.

Classificação por Gênero e Aparência Percebida

O sistema deverá ser capaz de identificar e filtrar indivíduos com base em classificação de gênero percebido pelo algoritmo de visão computacional, quando essa funcionalidade estiver habilitada pelas políticas da organização e pela legislação aplicável.

- Masculino percebido
- Feminino percebido
- Indeterminado / baixa confiança

Esse tipo de inferência costuma ser baseado em características visuais aprendidas pelo modelo, como contornos faciais, cabelo, vestuário e contexto corporal. Por depender de aparência e contexto, a saída deve ser tratada como hipótese de classificação, e não como verdade absoluta sobre identidade ou identidade de gênero.

Seu uso investigativo deve ser restrito a cenários justificados, com trilha de auditoria, controle de acesso e revisão humana obrigatória quando o resultado puder impactar decisões sensíveis.

Classificação por Emoções Detectadas

O sistema deverá ser capaz de identificar e filtrar indivíduos com base em expressões emocionais reconhecidas pelo algoritmo de visão computacional:

- Neutro
- Feliz
- Irritado / Raiva
- Surpreso
- Triste

Essa análise normalmente utiliza detecção facial, extração de pontos-chave e classificação de expressões a partir de redes neurais treinadas para reconhecer padrões musculares do rosto. Em alguns casos, o sistema também considera contexto temporal, pois expressões isoladas podem ser ambíguas e mudar rapidamente entre frames.

Em investigação, o recurso pode auxiliar na triagem de eventos com potencial conflito, pânico, reação a incidentes ou comportamento emocionalmente carregado em determinadas áreas e horários. Ainda assim, emoções inferidas por IA têm alto grau de incerteza e devem ser usadas como indicador auxiliar, nunca como prova conclusiva.

Densidade de Multidão e Ocupação do Espaço

O sistema deverá detectar concentração de pessoas em áreas específicas do vídeo, estimando densidade de aglomeração, fluxo e ocupação espacial.

- Baixa densidade
- Moderada densidade
- Alta densidade / aglomeração
- Formação de fila ou bloqueio

A técnica pode combinar contagem de pessoas, segmentação de cena, mapeamento de calor e análise de ocupação por região. Isso permite identificar lotação excessiva, áreas congestionadas e mudanças bruscas de fluxo em espaços como entradas, corredores, pátios, terminais e ambientes comerciais.

Para investigações, essa classificação é útil para reconstruir cenas de incidentes, verificar picos de ocupação, identificar pontos de concentração e correlacionar a presença de multidões com eventos suspeitos, como tumultos ou movimentações coordenadas.

Loitering e Permanência Suspeita

O sistema deverá detectar indivíduos que permanecem por tempo acima do esperado em uma zona delimitada, sem aparente finalidade operacional. A lógica geralmente compara posição, duração da presença e padrão de deslocamento dentro da área monitorada.

Esse tipo de alerta é útil em cenários como portas de acesso, caixas, corredores, estacionamentos e perímetros sensíveis. Em investigações, pode indicar vigilância, tentativa de abordagem, reconhecimento de rotina ou espera por uma oportunidade de ação.

Corrida e Movimento Incomum

O sistema deverá reconhecer deslocamentos acelerados, corridas, mudanças bruscas de direção, queda súbita, agitação corporal ou movimentos incompatíveis com a marcha normal. Para isso, os modelos podem usar estimativa de pose, rastreamento temporal e análise de velocidade e aceleração.

Na prática investigativa, esse filtro ajuda a localizar fugas, perseguições, dispersão repentina de pessoas, tentativa de evasão ou situações de pânico. Também pode ser combinado com outras pistas visuais para delimitar o início de um evento relevante.

Comportamento em Grupo e Interação

Além de sinais individuais, a solução pode observar comportamento coletivo, como aproximação súbita de várias pessoas, formação de pequenos grupos, dispersão anormal ou permanência conjunta em determinada área. Esses padrões são inferidos por rastreamento multiobjeto e análise de trajetórias ao longo do tempo.

Esse recurso apoia análises de eventos em massa, identificação de aglomerações suspeitas e reconstrução de dinâmica de cena antes e depois de um incidente.

Os atributos podem ser usados isoladamente ou combinados em consultas mais precisas. Por exemplo, é possível buscar um **adulto** com **expressão irritada**, que tenha permanecido por mais de alguns minutos em uma área de acesso e, em seguida, tenha iniciado uma corrida. Em outro cenário, a busca pode considerar apenas **alta densidade de pessoas** e **movimento acelerado** para localizar momentos de tumulto ou evacuação.

Do ponto de vista técnico, a solução pode empregar diferentes modelos em conjunto: detector de pessoas para localizar alvos no frame, classificador demográfico para inferir faixa etária e gênero percebido, classificador de emoções para faces detectadas, e rastreadores temporais para medir permanência, velocidade e trajetória. Em cenas com oclusão, baixa resolução ou ângulos laterais, a confiança deve ser reduzida e o sistema precisa sinalizar incerteza ao operador.

⚠ A detecção de emoções, gênero percebido e faixa etária são funcionalidades sensíveis do ponto de vista ético, legal e operacional. Seu uso deve estar em conformidade com a LGPD, normas internas de privacidade, políticas de retenção e princípios de minimização de dados. Sempre que possível, os resultados devem ser tratados como indicadores auxiliares, com auditoria, controle de acesso e revisão humana antes de qualquer decisão relevante.

Também é recomendável documentar a finalidade de cada filtro, limitar o uso a contextos legítimos de segurança ou investigação e evitar interpretações automáticas que possam gerar vieses ou discriminação. Em especial, classificações demográficas e emocionais nunca devem ser utilizadas como única base para conclusões sobre identidade, intenção ou risco.

Contexto Operacional na Busca de Vídeo

Os filtros de contexto operacional permitem delimitar o escopo de uma busca com base em parâmetros relacionados à infraestrutura de câmeras, à posição dentro da cena e ao intervalo temporal dos eventos. Esses critérios são frequentemente combinados com atributos biométricos e demográficos para refinar os resultados de uma investigação, reduzir o volume de material analisado e acelerar a localização de trechos relevantes.

Na prática, o objetivo desses filtros é transformar uma busca ampla em uma consulta precisa. Em vez de revisar horas ou dias de gravação manualmente, o operador pode restringir o universo de análise a uma câmera específica, a um grupo de câmeras, a um conjunto de horários, a zonas da imagem e a tipos de evento observáveis. Isso torna a triagem mais eficiente, melhora a reprodutibilidade da investigação e ajuda a organizar a revisão humana de forma mais objetiva.

Câmera Específica

Filtragem dos resultados limitada a uma câmera selecionada individualmente pelo operador de busca.

Esse recurso é útil quando já existe conhecimento prévio sobre o ponto exato onde o evento ocorreu, como uma entrada principal, um corredor interno, um estacionamento ou um caixa de atendimento. Ao focar em uma única câmera, o sistema elimina ruído e evita que imagens de áreas irrelevantes consumam tempo de análise.

Grupo de Câmeras

Busca restrita a um grupo previamente configurado, permitindo varreduras contextuais por setor, andar ou área de cobertura.

Em investigações mais amplas, o operador pode trabalhar com grupos de câmeras por prédio, bloco, pavimento, perímetro externo ou zona operacional. Isso é especialmente útil quando o trajeto do indivíduo é desconhecido e é necessário acompanhar sua passagem por diferentes pontos da instalação.

Lista de Interesse

Aplicação de uma lista de interesse como critério de filtragem, retornando apenas aparições de indivíduos cadastrados naquela lista.

Embora a lista de interesse não seja um filtro estritamente espacial ou temporal, ela costuma ser combinada com contexto operacional para acelerar a busca por uma pessoa já identificada. O operador pode, por exemplo, restringir a consulta a uma área e a um horário específicos antes de aplicar a lista, reduzindo drasticamente o número de ocorrências a revisar.

Data e Hora

Definição de intervalo temporal preciso para a busca, com seleção de data inicial, data final, hora de início e hora de término.

Esse tipo de recorte é essencial em ambientes com grande volume de gravação contínua. A busca pode ser limitada a um turno de trabalho, a uma janela de minutos antes ou depois de um incidente, ou ainda a horários de abertura e fechamento, quando o comportamento observado tende a ser mais previsível.

Zonas de Localização no Quadro

O sistema pode permitir que a busca considere apenas uma região específica dentro do campo de visão da câmera, como lado esquerdo, lado direito, centro, entrada, faixa de passagem, área de espera ou perímetro de interesse. Esses recortes ajudam a ignorar movimentos irrelevantes e a priorizar a área onde a ação realmente aconteceu.

- Região superior, inferior, central ou lateral do quadro
- Áreas delimitadas por polígonos, linhas virtuais ou máscaras
- Zonas de entrada, saída, abordagem ou permanência
- Setores sensíveis, como portões, balcões, corredores e acessos restritos

Em uma investigação, esse filtro pode ser usado, por exemplo, para localizar apenas pessoas que atravessaram uma catraca, veículos que pararam em uma baia específica ou indivíduos que permaneceram próximos a uma porta por um intervalo incomum. Quando combinado com detecção de movimento ou rastreamento de trajeto, o sistema reduz falsos positivos e destaca interações relevantes dentro da cena.

Filtros por Tipo de Evento

Além da localização e do tempo, a busca pode ser refinada por eventos observáveis, como passagem, permanência, corrida, aglomeração, queda, aproximação, invasão de área, objeto abandonado ou cruzamento de linha. Esses eventos normalmente são derivados de modelos de detecção e análise temporal aplicados ao vídeo.

- Entrada ou saída de uma área monitorada
- Permanência prolongada em um ponto da cena
- Movimento acelerado, corrida ou fuga
- Aglomeração, dispersão ou formação de fila
- Queda, colisão ou comportamento anômalo

Em contextos investigativos, os eventos funcionam como marcadores para filtrar rapidamente momentos críticos. Em vez de revisar todo o vídeo de um período, o operador pode procurar apenas ocorrências de um tipo específico de comportamento, o que facilita a reconstrução da sequência dos fatos e a identificação do instante inicial de um incidente.

Filtros de tempo também podem ser refinados por **dia da semana**, permitindo limitar a pesquisa a segundas-feiras, fins de semana, feriados ou a um padrão recorrente observado em múltiplas ocorrências. Em investigações de rotina, isso é útil para verificar se um evento acontece sempre no mesmo turno, em dias específicos ou em horários de menor supervisão.

Na prática, a combinação desses filtros cria uma busca em camadas. O operador pode começar pelo local e pela câmera, depois restringir por data e hora, aplicar uma zona no quadro e, por fim, selecionar o tipo de evento. Cada etapa diminui o volume de resultados e aumenta a precisão da análise, sem depender de revisão manual exaustiva.

Exemplos comuns incluem localizar um indivíduo que foi visto em um corredor específico entre 18h e 19h em dias úteis, rastrear um veículo apenas nas câmeras de acesso do perímetro durante o turno da madrugada, ou encontrar registros de aglomeração próximos a uma entrada somente em finais de semana. Em um caso de furto interno, por exemplo, a combinação de câmera do almoxarifado, janela temporal de 15 minutos, zona de prateleiras e evento de permanência pode revelar o momento exato da ação. Em uma ocorrência de segurança perimetral, o operador pode usar grupo de câmeras externas, faixa horária noturna e evento de corrida para destacar uma movimentação suspeita em poucos segundos.

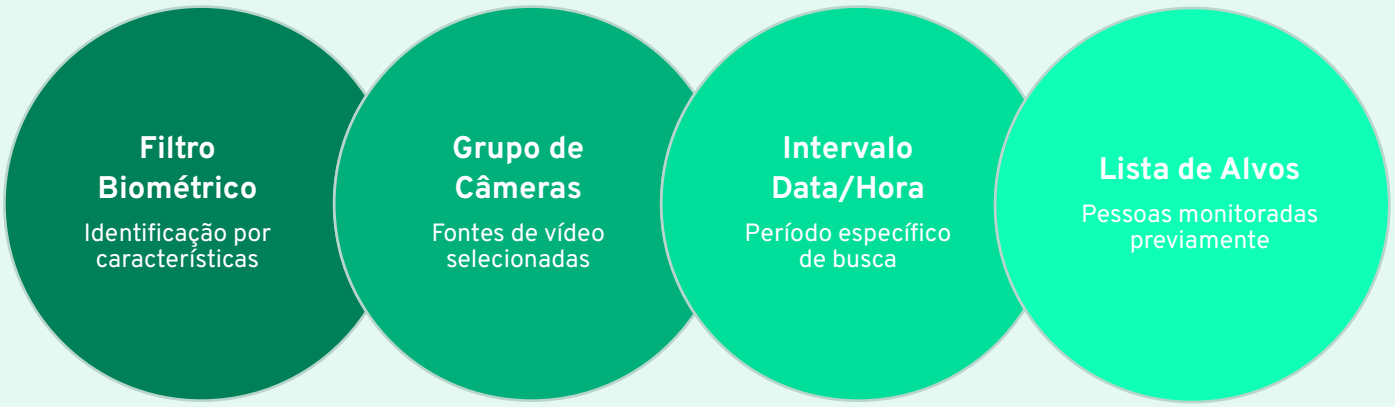
Do ponto de vista operacional, esses filtros tornam a busca mais escalável em ambientes com grande quantidade de câmeras e retenção extensa de imagens. Eles também ajudam a padronizar o processo investigativo, porque cada consulta fica associada a critérios explícitos de seleção, facilitando auditoria, revisão posterior e compartilhamento de evidências com outras equipes.

Combinação de Filtros na Busca

A capacidade de combinar filtros de diferentes categorias em uma única consulta é o diferencial central do módulo de análise. A solução deve suportar consultas compostas, onde os critérios podem ser aplicados simultaneamente com operadores lógicos **AND** e **OR**, resultando em buscas altamente precisas mesmo em repositórios com centenas de horas de vídeo gravado.

Na prática, o operador usa **AND** quando todos os critérios precisam ser verdadeiros ao mesmo tempo — por exemplo, uma pessoa com determinadas características biométricas *e* registrada em um grupo específico de câmeras *e* dentro de uma janela temporal delimitada. Já o **OR** amplia a consulta, permitindo retornar resultados que satisfaçam uma entre várias condições, como "barba **ou** óculos", "câmera A **ou** câmera B", ou "evento de corrida **ou** evento de fuga". Quando necessário, a interface deve deixar claro como os filtros estão agrupados, para que o usuário entenda a lógica aplicada antes de iniciar a análise.

Em consultas mais complexas, o sistema deve aceitar combinações encadeadas, como: **sexo masculino AND idade estimada adulta AND (barba OR bigode) AND sem máscara AND (Entrada Principal OR Estacionamento Sul) AND intervalo entre 08h e 12h**. Esse tipo de construção é comum em investigações em que o suspeito não foi identificado com precisão, mas há pistas parciais suficientes para restringir significativamente o universo de busca. Também é útil quando a equipe precisa cruzar atributos visuais com contexto operacional, como pontos de acesso, faixa horária e lista de interesse.



A lógica de combinação também precisa lidar com filtros potencialmente conflitantes. Se o usuário selecionar parâmetros incompatíveis — por exemplo, **sem máscara** e **com máscara** no mesmo bloco AND, ou duas faixas de horário que não se sobrepõem — o sistema deve sinalizar a inconsistência antes da execução ou retornar zero resultados de forma explicável. Em vez de falhar silenciosamente, a interface pode destacar o conflito, sugerir a remoção de um critério e mostrar quais condições estão tornando a consulta inviável. Isso reduz erros operacionais e evita interpretações equivocadas durante a investigação.

Outro aspecto importante é o tratamento de filtros com sobreposição parcial. Em uma consulta de período, por exemplo, o usuário pode combinar um intervalo principal de busca com dias da semana, feriados ou turnos específicos. Em cenários operacionais reais, isso é frequente: um analista pode querer ver apenas eventos ocorridos em noites de sexta-feira, ou somente em horários de abertura e fechamento. O sistema deve preservar a intenção do operador, aplicando a interseção entre os critérios quando necessário e deixando claro quando um filtro amplia a busca e quando a restringe.

O desempenho é um fator crítico para consultas compostas. Quanto maior o número de filtros, maior a necessidade de otimização, especialmente quando a busca envolve múltiplas câmeras, longas janelas temporais e critérios biométricos. A solução deve priorizar a aplicação dos filtros mais seletivos primeiro, reduzir o conjunto de candidatos antes das etapas mais custosas e manter a interface responsiva com feedback de progresso. Em buscas muito grandes, é desejável que o sistema informe se a consulta está em processamento, quantos resultados parciais já foram encontrados e se a execução pode ser refinada para acelerar a resposta.

Os resultados também devem ser ordenados de forma útil para a investigação. Em geral, a lista pode ser classificada por maior aderência aos filtros, pela confiabilidade da detecção, pela proximidade temporal com o evento de interesse ou pela relevância operacional definida pelo usuário. Por exemplo, quando há múltiplas ocorrências da mesma pessoa em intervalos diferentes, o sistema pode priorizar as passagens mais próximas da janela temporal solicitada ou as capturas com maior qualidade de visualização facial. Se a consulta incluir uma lista de alvos, resultados que coincidam com essa lista podem aparecer no topo, seguidos por correspondências parciais ou secundárias.

Em termos práticos, a busca composta permite situações como localizar um homem adulto com barba, sem máscara e expressão irritada, visto no Grupo de Câmeras "Entrada Principal" entre 08h e 12h no último mês e presente na Lista de Interesse "Suspeitos Prioritários". Em outro caso, uma equipe de segurança pode procurar um veículo em área restrita usando **placa parcialmente reconhecida AND câmera do acesso AND horário noturno AND evento de parada prolongada**. Já em uma investigação de varejo, pode ser necessário cruzar **pessoa não cadastrada OR correspondência parcial na lista de alvos** com uma janela curta de tempo e a zona da área de estoque para localizar uma possível subtração de mercadorias.

Esses cenários mostram que combinar filtros não é apenas uma forma de reduzir volume, mas uma estratégia de investigação. Ao cruzar biometria, contexto operacional, período temporal e listas de interesse, o analista transforma uma varredura extensa em uma consulta guiada por hipóteses. Isso acelera a triagem, melhora a rastreabilidade das decisões e aumenta a chance de encontrar o momento exato em que um evento relevante ocorreu.

Do ponto de vista operacional, a melhor experiência é aquela em que o usuário consegue montar, revisar e ajustar consultas complexas sem perder clareza. Por isso, a interface deve tornar explícito o agrupamento lógico dos filtros, indicar quando uma condição está limitando demais a busca e oferecer um resultado final ordenado de maneira consistente com a prioridade da investigação.

Resumo dos Critérios de Filtragem

A tabela abaixo consolida todos os critérios de filtragem suportados pelo módulo de busca e análise de vídeo arquivado, organizados por categoria e com indicação de tipo de dado e origem do dado (algoritmo ou configuração manual).

Para interpretar o quadro, leia cada linha como um critério disponível na interface: a coluna **Categoria** agrupa filtros com finalidade semelhante; **Critério** descreve o que o sistema consegue buscar; **Tipo** indica como aquele valor é representado internamente; e **Origem** mostra se a informação vem de inferência automática por IA ou de parametrização feita pelo operador. Essa distinção é importante porque afeta a confiabilidade esperada, a forma de validação e a maneira como o resultado deve ser exibido ao usuário.

Categoria	Critério	Tipo	Origem
Biométrico/Físico	Pessoa específica (reconhecimento facial)	Identidade	Algoritmo IA
Biométrico/Físico	Máscara: com / sem / uso inadequado	Booleano/enum	Algoritmo IA
Biométrico/Físico	Barba: com / sem	Booleano	Algoritmo IA
Biométrico/Físico	Óculos de grau: com / sem	Booleano	Algoritmo IA
Biométrico/Físico	Óculos de sol: com / sem	Booleano	Algoritmo IA
Demográfico	Grupo etário (criança/adulto/idoso)	Enum	Algoritmo IA
Comportamental	Emoção detectada	Enum	Algoritmo IA
Operacional	Câmera específica	Seleção	Configuração
Operacional	Grupo de câmeras	Seleção	Configuração
Operacional	Lista de interesse	Seleção	Configuração
Operacional	Data e hora do evento	Intervalo	Manual

Em termos de origem, os filtros gerados por **Algoritmo IA** dependem da capacidade de detecção do modelo aplicado ao vídeo e, portanto, podem variar conforme iluminação, ângulo da câmera, oclusão parcial, resolução do arquivo e qualidade do enquadramento. Já os critérios vindos de **Configuração** ou **Manual** são definidos pelo ambiente operacional e tendem a ser mais estáveis, pois representam ativos cadastrados, agrupamentos de câmeras, listas de interesse e janelas temporais escolhidas pelo usuário. Na prática, isso significa que filtros automáticos precisam ser avaliados com tolerância à incerteza, enquanto filtros configuracionais devem ser validados principalmente quanto à integridade do cadastro e à consistência da seleção.

Requisitos de qualidade dos dados por tipo de filtro

Para que a filtragem funcione de forma confiável, cada tipo de critério depende de um nível mínimo de qualidade de dados. Em filtros biométricos e físicos, como máscara, barba e óculos, a imagem precisa ter nitidez suficiente para permitir a leitura visual desses atributos; frames muito comprimidos, com pouca luz ou com o rosto parcialmente encoberto reduzem a precisão. No caso de reconhecimento facial, a exigência é ainda maior: o sistema precisa de um rosto razoavelmente frontal, com boa resolução facial e baixa interferência de movimento para evitar falsos negativos.

Nos filtros demográficos e comportamentais, a qualidade do dado está associada à robustez da inferência do modelo em cenários reais. Grupo etário e emoção detectada devem ser tratados como classificações probabilísticas, e não como verdades absolutas, especialmente quando há baixa definição, distância excessiva ou grande variação de pose. Por isso, a interface e os testes devem considerar que esses campos podem apresentar incerteza maior do que filtros operacionais.

Já os filtros operacionais dependem menos da qualidade do vídeo e mais da qualidade do cadastro. Câmeras, grupos de câmeras e listas de interesse precisam estar corretamente configurados, com nomes consistentes, vínculos atualizados e sem duplicidade. O filtro de data e hora do evento exige sincronização confiável do relógio do sistema e preservação adequada dos metadados temporais, para que a busca não seja afetada por divergência de fuso, atraso de ingestão ou inconsistência entre origem e índice.

> Como regra prática, quanto mais o filtro depende de inferência visual automática, maior deve ser a atenção a qualidade de imagem, contexto da cena e margem de erro esperada. Quanto mais o filtro depende de cadastro manual, maior deve ser o foco em consistência de configuração e rastreabilidade.

Uso do resumo em validação e aceitação

Este resumo também serve como base para validação funcional e aceitação do sistema. Durante os testes, a equipe pode usar a tabela para confirmar se cada critério aparece na interface, se o tipo de dado está correto, se a origem está coerente com a implementação e se as combinações de filtros produzem resultados esperados. Isso facilita a criação de casos de teste com cobertura por categoria, reduz ambiguidades entre negócio e tecnologia e ajuda a verificar se o módulo responde adequadamente a entradas válidas, inválidas e parcialmente preenchidas.

Além disso, o documento apoia a definição de critérios de aceite, pois explicita quais filtros são automáticos, quais são configuráveis e quais dependem de intervalo temporal. Dessa forma, fica mais fácil validar não apenas a presença dos campos, mas também o comportamento esperado em cenários reais de operação, como seleção de câmera, cruzamento com lista de interesse, combinação de atributos biométricos e refinamento por janela de tempo.

Integração com Active Directory

Possuímos integração nativa com serviços de diretório corporativo, com suporte especial ao Microsoft Active Directory (AD). Essa integração é estratégica para organizações que já utilizam o AD como repositório central de identidades, eliminando a necessidade de manutenção paralela de bases de usuários e reduzindo a superfície de ataque por credenciais duplicadas.

A integração deve ser realizada utilizando protocolos padrão de mercado (LDAP/LDAPS), garantindo compatibilidade com as principais versões do Active Directory e com serviços de diretório compatíveis, como o OpenLDAP. A configuração deve ser realizada de forma centralizada pelo Administrador Geral, por interface gráfica dedicada.

Autenticação Única (SSO)

Um dos benefícios centrais da integração com o Active Directory é a habilitação do Single Sign-On (SSO), que permite que os usuários autentiquem-se na solução de vigilância utilizando as mesmas credenciais corporativas já utilizadas para acesso ao Windows, e-mail, ERP e demais sistemas da organização. Isso elimina a necessidade de múltiplas senhas e simplifica a gestão do ciclo de vida de credenciais.

1

Login Corporativo

Usuário insere credencial Windows (usuário@dominio.com) na tela de login da solução de vigilância.

2

Autenticação no AD

A solução encaminha as credenciais para validação no Active Directory via LDAP/S, sem armazenar a senha localmente.

3

Mapeamento de Perfil

O grupo do AD ao qual o usuário pertence é mapeado para o perfil de acesso correspondente na solução (Operador, Supervisor, Administrador).

4

Acesso Concedido

O usuário acessa a plataforma com os privilégios correspondentes ao seu perfil, sem necessidade de nova autenticação.

Sincronização de Usuários e Grupos

Além da autenticação, a integração deverá suportar a criação e sincronização automática de usuários e grupos a partir do Active Directory. Isso significa que quando um novo colaborador é adicionado ao AD e incluído em um grupo mapeado, ele automaticamente recebe acesso à solução de vigilância sem necessidade de cadastro manual pelo administrador.

Sincronização Automática

- Criação automática de usuário ao primeiro login
- Atualização de perfil ao mudar de grupo no AD
- Desativação automática ao remover do grupo ou desativar no AD
- Frequência de sincronização configurável

Mapeamento de Grupos AD → Perfis

- GRP-CFTV-Operadores → Perfil Operador
- GRP-CFTV-Supervisores → Perfil Supervisor
- GRP-CFTV-Admins → Perfil Administrador Geral
- Mapeamentos personalizáveis pelo administrador

Requisitos Técnicos da Integração LDAP/S

A integração com o Active Directory deve seguir especificações técnicas precisas para garantir compatibilidade, segurança e desempenho adequados. Os parâmetros abaixo são os requisitos mínimos que a solução deve suportar para configuração da conexão com o serviço de diretório.

Parâmetro	Requisito
Protocolo	LDAP (porta 389) e LDAPS (porta 636)
Versão do protocolo LDAP	LDAPv3
Segurança de transporte	TLS 1.2 ou superior obrigatório para LDAPS
Autenticação de bind	Simple Bind com conta de serviço dedicada
Atributos sincronizados	sAMAccountName, mail, displayName, memberOf
Base DN	Configurável por interface gráfica
Filtro de busca	Customizável por expressão LDAP
Compatibilidade	Active Directory 2012 R2, 2016, 2019, 2022 e Azure AD DS

⚠ Recomenda-se fortemente o uso de LDAPS (porta 636) em ambiente de produção para proteger as credenciais de bind e os dados dos usuários durante o trânsito na rede.

Segurança na Integração com Diretório

A integração com o Active Directory deve ser implementada seguindo boas práticas de segurança para minimizar riscos de exposição de credenciais e garantir a integridade do processo de autenticação. O cumprimento dessas recomendações é condição para a homologação da solução em ambientes corporativos auditados.

Conta de Serviço com Privilégio Mínimo

A conta utilizada para bind no AD deve possuir apenas permissão de leitura no escopo de OU necessário, sem direitos administrativos ou de modificação no diretório.

Armazenamento Seguro de Credenciais

As credenciais da conta de serviço devem ser armazenadas de forma criptografada no banco de dados da solução, nunca em texto plano em arquivos de configuração.

Auditoria de Autenticações

Todas as tentativas de autenticação via AD devem ser registradas no log de auditoria da solução, incluindo sucessos, falhas e razão da rejeição.

Fallback de Autenticação

Em caso de indisponibilidade do servidor AD, o Administrador Geral deve conseguir autenticar-se com credencial local de emergência, previamente cadastrada.

Consolidação dos Requisitos

A tabela abaixo apresenta uma visão consolidada de todos os requisitos funcionais descritos neste documento, organizados por módulo e com indicação de criticidade e área funcional impactada. Esta tabela serve como lista de verificação para integradores durante o processo de implantação e homologação da solução.

Módulo	Requisito	Área Impactada	Criticidade
Segurança	Histórico de sessão com usuário, device ID, IP e status	Auditoria	Alta
Segurança	Bloqueio/desbloqueio de dispositivos pela GUI	Controle de Acesso	Alta
Segurança	Restrição de tipos de arquivos em anexos	Integridade de Dados	Média
Administração	Hierarquização de grupos de câmeras	Organização Operacional	Alta
Administração	Criação e gestão de listas de interesse	Inteligência Operacional	Alta
Administração	Módulo de usuários com 3 níveis hierárquicos	Governança de Acesso	Alta
Administração	Filtragem combinada no vídeo arquivado	Investigação/Análise	Alta
Administração	Integração LDAP/S com Active Directory e SSO	Identidade Corporativa	Alta

Conclusão e Próximos Passos

Este documento consolidou os requisitos funcionais essenciais para a implantação de uma solução de vigilância inteligente com capacidades avançadas de segurança e administração. O atendimento integral a esses requisitos é condição necessária para que a plataforma seja homologada e posta em operação no ambiente corporativo.

01

Validação de Requisitos

Revisão e aprovação formal deste documento pelos stakeholders técnicos e de negócio, com registro de eventuais adendos ou ajustes de escopo.

02

Avaliação de Fornecedores

Análise das soluções disponíveis no mercado com base nos critérios aqui definidos, incluindo prova de conceito (PoC) para os requisitos mais críticos.

03

Planejamento de Implantação

Definição do cronograma de implantação, ambientes (desenvolvimento, homologação, produção), responsabilidades e marcos de entrega.

04

Configuração e Integração

Execução da implantação técnica, incluindo configuração do AD, criação de perfis, grupos de câmeras e parametrização dos algoritmos de visão computacional.

05

Homologação e Go-Live

Testes de aceitação com base nos requisitos deste documento, correção de não-conformidades e autorização formal para entrada em produção.

Documento aprovado para distribuição aos integradores e equipes técnicas responsáveis pela avaliação e implantação da solução.