



TERMO DE REFERÊNCIA

1. OBJETO

1.1. O presente Termo de Referência (TR) tem por objeto a aquisição de equipamentos e softwares especializados para captura, processamento, tratamento, transmissão e armazenamento de imagens, acompanhada de serviços de instalação, configuração e treinamento, bem como da prestação continuada de serviços de manutenção preventiva, corretiva e suporte técnico mensal, conforme condições e especificações estabelecidas neste Termo de Referência e seus anexos.

LOTE ÚNICO			
Item	Descrição de itens	Unidade de Medida	Qtd Total
1.1	Conjunto para monitoramento perimetral	Conjunto	61
1.2	Câmera tipo 2	Peça	62
1.3	Câmera tipo 3	Peça	19
1.4	Câmera tipo 4	Peça	428
1.5	Câmera tipo 5	Peça	162
1.6	Câmera tipo 6	Peça	49
1.7	Câmera tipo 7	Peça	41
1.8	Switch	Peça	52
1.9	NVR tipo 1	Peça	05
1.10	NVR tipo 2	Peça	07
1.11	NVR tipo 3	Peça	02
1.12	Plataforma de gerenciamento	Conjunto	01
1.13	Central de monitoramento	Conjunto	01

1.14	Estação de trabalho	Conjunto	11
1.15	Serviço de projeto executivo	Serviço	12
1.16	Serviço de instalação de 10 dispositivos	Serviço	95
1.17	Serviço de instalação de NVR	Serviço	14
1.18	Serviço de instalação da plataforma de gerenciamento	Serviço	1
1.19	Serviço de instalação da central de monitoramento	Serviço	1
1.20	Serviço de instalação de estação de trabalho	Serviço	11
1.21	Unidade de serviço técnico (UST)	Serviço	1000
1.22	Serviço mensal de suporte, manutenção e sustentação (inicial)	Serviço	36
1.23	Serviço mensal de suporte, manutenção e sustentação (complemento)	Serviço	252

Tabela 1

2. DA JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. O Serviço Social do Comércio – Administração Regional do Distrito Federal – Sesc-AR/DF, por concentrar suas atividades em diversas unidades escolares, centros técnicos e setores administrativos, recebe diariamente um intenso fluxo de alunos, colaboradores, visitantes e prestadores de serviço. Esse movimento constante, aliado à localização urbana e à variedade de atividades desenvolvidas, expõe a instituição a diferentes tipos de crimes: contra a pessoa, o patrimônio, a dignidade sexual e a incolumidade pública. Esse contexto impõe desafios crescentes à segurança física e patrimonial, exigindo medidas robustas e integradas de prevenção e proteção.

2.2. Incidentes recentes em instituições de ensino no Brasil, amplamente noticiados nos últimos anos, revelam um aumento significativo de episódios como invasões, furtos, depredações, agressões e ameaças à integridade física de estudantes e servidores. Esses eventos geram impacto direto na sensação de segurança da comunidade escolar, prejudicam o ambiente educacional e comprometem o patrimônio público.

• 08/07/2025 — Estação/RS — Ataque com arma branca: adolescente invade escola municipal; 1 criança morre e há feridos.



<https://www.cnnbrasil.com.br/nacional/sul/rs/ataque-a-escola-deixa-uma-crianca-morta-e-duas-feridas-no-rs/>

• 23/10/2023 — São Paulo/SP (Sapopemba) — Ataque a tiros: estudante atira em colegas; 1 aluna morre e 3 ficam feridos.

<https://www.nexojornal.com.br/extra/2023/10/23/aluna-morre-e-3-ficam-feridos-em-ataque-a-tiros-em-escola-de-sp>

• 27/03/2023 — São Paulo/SP (Vila Sônia) — Ataque com faca: aluno fere docentes e aluno; professora morre.

<https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/professora-morre-e-5-pessoas-sao-feridas-em-ataque-contr-escola-em-sp>

• 05/04/2023 — Blumenau/SC — Ataque em creche: invasor mata 4 crianças.

<https://agenciabrasil.ebc.com.br/geral/noticia/2023-04/homem-invade-creche-em-blumenau-e-mata-quatro-criancas>

• 19/06/2023 — Cambé/PR — Ataque a tiros: ex-aluno entra armado em colégio estadual; 2 estudantes morrem.

<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2023/06/19/ataque-tiros-escola-cambe.htm>

• 25/11/2022 — Aracruz/ES — Ataques a tiros em duas escolas: 4 mortos e vários feridos; autor usou arma do pai.

<https://agenciabrasil.ebc.com.br/geral/noticia/2022-11/es-adolescente-usa-arma-do-pai-e-simbolo-nazista-em-ataque-escolas>

• 21/08/2024 — Planaltina/DF — Professora feita refém com faca: suspeito invade escola e é preso; docente liberada sem ferimentos graves.

<https://www.cnnbrasil.com.br/nacional/adolescente-invade-escola-e-faz-professora-refem-no-df/>

• 13/06/2024 — Contagem/MG — Furto em massa de TI: criminosos levam 124 Chromebooks, 13 notebooks, 11 tablets e 8 projetores de escola municipal.

<https://www.cnnbrasil.com.br/nacional/ladros-furtam-mais-de-130-computadores-de-escola-em-mg-itens-haviam-sido-entregues-na-semana-passada/>

• Ago/2025 — São Paulo/SP (Mooca) — Furtos de cabos: EMEI sofre furtos repetidos de fiação; aulas ficam suspensas/afetadas.

<https://globoplay.globo.com/v/13824769/>

• Mar/2025 — Sumaré/SP — Furto de fios: escola municipal fica sem energia; aulas seguem sem ventilação/ar-condicionado.

<https://globoplay.globo.com/v/13465802/>



- Jul/2025 — Maringá/PR — Escola vandalizada: GCM encontra unidade municipal depredada; prefeitura atribui danos a menores.

<https://globoplay.globo.com/v/13793205/>

- Jul/2025 — Vila Velha/ES — Prisão de professor por abuso de alunas (8 anos): ação da DPCA; investigação aponta crimes dentro da sala de aula.

<https://pc.es.gov.br/Not%C3%ADcia/dpca-prende-professor-investigado-por-estuprar-aluna-em-escola-particular-de-vila-velha>

- Nov/2024 — Novo Brasil/GO — Professor preso por crimes sexuais contra alunas: caso em escola local; investigações em curso.

<https://globoplay.globo.com/v/12893206/>

- Out/2024 — SP — Professor de escola estadual investigado por abuso sexual: caso exibido no SP2 (Globo/G1).

<https://globoplay.globo.com/v/12970910/>

- Abr/2023 – Em uma semana, SP registra 279 ameaças de ataques em escolas, diz Polícia Civil.

<https://www.cnnbrasil.com.br/nacional/em-uma-semana-sp-registra-279-ameacas-de-ataques-em-escolas-diz-policia-civil/>

2.3. Segundo o ministério da justiça, recentemente houve aumento de ataques e de ameaças online a escolas, o que motivou operações federais e estaduais de monitoramento e prisões preventivas. Isso reforça a necessidade de prevenção, resposta rápida e integração com autoridades.

Fonte: <https://www.gov.br/mj/pt-br/assuntos/noticias/lancada-em-abril-operacao-escola-segura-ja-efetuoou-400-prisoos-e-apreensoes>

2.4. Ênfase em incidentes ocorridos no DF:

- 2025 - Esfaqueamento dentro de escolas em 2025 – um no Centro de Ensino Médio 01 do Gama (31/03) e outro no Centro Educacional 02 de Brazlândia (08/04)

<https://www.cl.df.gov.br/-/populacao-pede-controles-de-acesso-as-escolas-do-df>

“O aluno era exemplar, com família presente. Mas ele passou no portão da escola e esfaqueou 5 pessoas”.

Silvia Maria Cavalcante - coordenadora do Centro Educacional 01 São José, em São Sebastião

- 2023 – Pais com medo de enviar filhos para escolas no DF após onda de violência

<https://www.correiobraziliense.com.br/euestudante/educacao-basica/2023/04/5086702-escolas-e-pais-do-df-se-mobilizam-contr-onda-de-violencia.html>

2.5. Além disso, segundo dados recentes do Grupo Dados para um Debate Demográfico na Educação, o Brasil registrou 42 ataques violentos em escolas entre 2001 e 2024,



resultando em 44 mortes e 113 feridos, sendo que quase 65% desses episódios ocorreram apenas em dois anos, alertando sobre a crescente frequência e gravidade desse tipo de ocorrência.

2.6. No mesmo sentido, um estudo inédito do Fórum Brasileiro de Segurança Pública em parceria com a empresa Timelens revelou que, entre 2021 e 2025, houve um aumento de 360% nas postagens com ameaças a escolas em redes sociais, totalizando mais de 88 mil menções até maio de 2025, sendo que boa parte dessas ameaças circula abertamente na internet comum, potencializando o risco real de violência.

2.7. Esses dados reforçam a urgência de uma solução robusta e preventiva, que permita ao SESC-DF responder de forma efetiva a múltiplas formas de risco – do ataque físico à escalada de ameaças digitais – por meio de monitoramento integrado e governança de segurança.

2.8. Vale notar que a violência nas escolas nem sempre vem de invasores externos – conflitos entre os próprios alunos também são frequentes. Entre janeiro e agosto de 2024, registraram-se 1.023 ocorrências de brigas e agressões em escolas do DF; no mesmo período de 2025 foram 730 casos, uma redução de 29% atribuída a ações preventivas e maior patrulhamento escolar¹. Apesar da queda, os números mostram que centenas de incidentes violentos ainda ocorrem anualmente, exigindo atenção contínua.

2.9. Para mitigar tais riscos, torna-se necessária a implantação de um serviço especializado de videomonitoramento abrangendo todas as unidades do SESC-DF, com operação contínua, recursos de análise inteligente e capacidade de resposta rápida a eventos. A solução deve ser gerida de forma centralizada, com infraestrutura moderna, de alta disponibilidade, e contemplar a manutenção e atualização tecnológica ao longo de todo o contrato.

2.10. A inexistência de um sistema integrado limita a capacidade de prevenção, investigação e documentação de ocorrências, dificultando a adoção de medidas corretivas e preventivas eficazes. Assim, a contratação proposta é estratégica para preservar a integridade física de pessoas, proteger os bens da instituição e assegurar a continuidade das atividades educacionais.

2.11. Em última análise, como benefícios resultantes desta contratação espera-se dotar o SESC-DF de mecanismos que possibilitem a implementação de medidas de proteção dos recursos humanos e patrimoniais.

3. O ESCOPO DO PROJETO

¹ Fonte: <https://jornaldebrasil.com.br/brasil/brigas-em-escolas-do-df-caem-29-em-um-ano-segundo-a-pm/>



3.1. O escopo consiste, resumidamente, na implantação de uma solução integrada de videomonitoramento inteligente e gestão unificada de segurança, abrangendo diversas unidades do SESC-DF, com aquisição de hardware, software e serviços técnicos especializados, assegurando a continuidade operacional, a eficiência no monitoramento, a prevenção de incidentes e o apoio às áreas técnicas e operacionais.

4. DO REGISTRO DE PREÇO

4.1. A opção pela modalidade de Registro de Preço, prevista no Artigo 44 da Resolução SESC Nº 1.593/2024, se justifica plenamente para a contratação de serviços organizacionais para o tratamento de informações, condicionados aos fluxos negociais, finalísticos e administrativos do SESC-AR/DF. Esta modalidade oferece flexibilidade operacional, eficiência administrativa e vantagens econômicas, adequando-se às necessidades estratégicas da contratação.

4.2. De acordo com o inciso I do Art. 44, o Registro de Preço é recomendado quando a aquisição demanda entregas parceladas, como é o caso da Expansão da infraestrutura de atendimento as demandas computacionais da instituição, com garantia de disponibilidade, confidencialidade, integridade e legalidade. A solicitação de aquisição e fornecimento dos itens do objeto será gradual, o que torna o fornecimento parcelado a alternativa mais eficiente para garantir o cumprimento das especificações técnicas sem sobrecarregar o processo logístico e financeiro de uma única vez.

4.3. Essa demanda constante torna o registro de preço o mecanismo ideal para otimizar a gestão de compras, permitindo que o Sesc-AR/DF realize novas aquisições conforme necessário, mantendo a coerência com o planejamento orçamentário e técnico, sem a necessidade de iniciar novos processos licitatórios a cada compra adicional.

4.4. O inciso IV do Art. 44, o Registro de Preço possibilita a contratação de bens e serviços por mais de um serviço social autônomo. Isso se alinha à visão estratégica do SESC-AR/DF de permitir que outros departamentos ou unidades do SESC-AR/DF ou do Sistema S possam, futuramente, aderir à Ata de Registro de Preço. Desta forma, o SESC e outras entidades podem ampliar os benefícios econômicos e operacionais dessa contratação, aumentando o poder de negociação e garantindo a padronização das soluções tecnológicas em diferentes unidades.

4.5. O uso do Registro de Preço garante maior controle e flexibilidade, uma vez que as contratações podem ser ajustadas conforme as necessidades específicas de cada unidade do SESC-AR/DF e outros possíveis aderentes, sem comprometer o prazo de execução ou o orçamento previamente estabelecido. O modelo também permite maior eficiência na gestão dos fornecedores e das garantias contratuais, conforme definido nos artigos 53 a



55 da Resolução SESC Nº 1.593/2024, assegurando que as aquisições sejam feitas de acordo com as condições e os prazos registrados, sem prejuízos para as partes envolvidas.

5. DA JUSTIFICATIVA DO MENOR PREÇO GLOBAL

5.1. Aplica-se a modalidade de licitação por Pregão Eletrônico, com julgamento por menor preço global, visando dar celeridade e desburocratização ao procedimento licitatório, bem como sem perder a qualidade nas propostas, uma vez que a competitividade nesta modalidade de licitação possui como uma grande característica, a ampla concorrência.

5.2. A contratação por preço global ensejará o planejamento e a racionalização do trabalho, a melhor gestão dos contratos, o adequado cumprimento de prazos e padrões de qualidade, além da atribuição de responsabilidade pelos serviços executados.

6. LOTE ÚNICO

6.1. Tendo em vista que os equipamentos, hardwares, softwares e serviços objeto deste Termo de Referência convergem para a implantação de um sistema unificado de videomonitoramento e gestão de segurança, resta plenamente justificado o agrupamento dos itens em lote único.

6.2. O conjunto contratado apresenta relação de interdependência técnica e necessidade de plena compatibilidade entre os componentes, de modo que a fragmentação da licitação em itens isolados acarretaria riscos significativos de interoperabilidade, de sobreposição de responsabilidades e de inviabilização do funcionamento integrado da solução.

6.3. Adicionalmente, o lote único garante a padronização tecnológica, simplifica a gestão contratual, concentra em um único fornecedor a responsabilidade pela entrega e pelo desempenho global do sistema e assegura a manutenção homogênea ao longo do ciclo de vida da solução.

6.4. Sob a ótica econômica, o agrupamento também promove economia de escala, permitindo melhores condições de aquisição, implantação e suporte, além de reduzir custos indiretos decorrentes de disputas contratuais fragmentadas.

6.5. Assim, o agrupamento dos itens em lote único se apresenta como a solução mais eficiente, segura e econômica para atender ao interesse público e às necessidades do SESC-DF.

7. DA DOTAÇÃO ORÇAMENTÁRIA

7.1. A despesa decorrente do objeto do presente TR correrá no presente exercício.

8. DA LEGISLAÇÃO DE REFERÊNCIA



8.1. As licitações do SESC não estão sujeitas à Lei Federal nº 14.133/2021, mas sim aos seus regulamentos próprios, conforme decisões 907/97 de 11/12/1997 e 461/98 de 22/07/1998, do Plenário do Tribunal de Contas da União (TCU) e as determinações contidas no Acórdão nº 1.664/2004, constante na Relação nº 033/2004 – 1ª Câmara, de 13/07/2004, e Acórdão nº 457/2005, da 2ª Câmara, de 29/03/2005, ambos do TCU.

8.2. As licitações do SESC-AR/DF seguem a Resolução nº 1.593/2024, aprovada em 02/05/2024. A norma, em vigor desde o dia 02 de maio de 2024, altera, modifica e consolida o Regulamento de Licitações e Contratos do SESC e revoga a Resolução SESC nº 1.570/2023. No SESC-AR/DF, as licitações são realizadas pela Seção de Licitações.

8.3. LEI Nº 12.305, DE 2 DE AGOSTO DE 2010. DOU de 03.08.2010. Institui a Política Nacional de Resíduos Sólidos; altera a Lei nº 9.605, de 12 de fevereiro de 1998.

9. QUALIFICAÇÃO TÉCNICA

9.1. Requisitos Técnicos:

9.1.1. De acordo com a tabela 02 – Especificações Técnicas – Anexo I deste processo.

9.1.2. No Anexo I estão especificados os requisitos mínimos e obrigatórios para todos os itens da Tabela 01 – Escopo de Fornecimento, onde a licitante deverá apresentar junto a sua proposta comercial, as seguintes informações:

9.1.3. A composição de cada item do escopo de fornecimento, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, dentre outras informações que sejam necessárias ou solicitadas pelo SESC-AR/DF, com o objetivo de se identificar claramente os produtos utilizados para o fornecimento e prestação dos serviços.

9.1.4. Os documentos mencionados no item 9.1.3., poderão ser objetos de diligência a fim de se esclarecer quaisquer dúvidas quanto ao seu conteúdo.

9.1.5. Justificativa: a exigência desses documentos formais visa assegurar a legitimidade das informações apresentadas, a rastreabilidade das responsabilidades e a conformidade com as melhores práticas administrativas, prevenindo riscos de procedência duvidosa ou de suporte técnico inadequado.

9.1.6. Qualquer informação inexata ou inverídica, apurada pelo pregoeiro nos documentos de capacitação técnica, implicará na inabilitação da respectiva licitante.

9.2. Comprovações da Especificação Técnica:

9.2.1. Para comprovação da qualificação técnica, a licitante deverá apresentar Atestados de Capacidade Técnica (ACTs) emitidos por pessoas jurídicas de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto desta contratação.

9.2.2. Serão aceitos ACTs que comprovem experiência em:



9.2.2.1. Instalação e configuração de sistemas de câmeras IP com plataforma de gerenciamento centralizado com quantitativo de pelo menos 50% da quantidade prevista neste projeto.

9.2.2.2. Implantação de centrais de monitoramento com videowall.

9.2.2.3. Instalação de NVRs, storages e servidores para gravação e armazenamento de imagens.

9.2.3. Os documentos solicitados para comprovação da qualificação técnica da licitante, deverão ser enviados juntamente com a proposta comercial e tem o objetivo de garantir seu pleno atendimento ao instrumento convocatório. O não envio destes implicará em desclassificação.

10. SERVIÇO DE SUPORTE TÉCNICO E INSTALAÇÃO

10.1. O serviço de suporte técnico das soluções deverá ser prestado diretamente pela CONTRATADA, com apoio do fabricante caso necessário, com vistas a promover o correto funcionamento das soluções.

10.2. Os serviços de suporte técnico deverão ser prestados sem custos adicionais ao SESC-AR/DF durante toda vigência do contrato.

10.3. Entende-se por suporte técnico todo auxílio, imediato ou programado que tem como prioridade manter a operacionalidade do sistema, bem como o atendimento de requisições solicitadas pelo SESC.

10.4. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes da solução, no regime 8x5 todos os dias úteis da semana em horário comercial.

10.5. O suporte técnico deve corrigir o problema/incidente, seja ele de baixa, média e alta complexidade, em cada um de seus níveis de atendimento e suporte de acordo com o SLA estabelecido.

10.6. A abertura de chamados para suporte técnico deverá ser efetuada por correio eletrônico.

10.7. O atendimento do serviço de suporte técnico deverá ocorrer preferencialmente de forma remota, podendo o SESC solicitar atendimento presencial caso necessário.

10.8. A CONTRATADA deverá possuir corpo técnico especializado nas soluções ofertadas.

10.9. Os serviços profissionais de instalação têm como objetivo de se manter a implementação correta de todos os equipamentos e sistemas necessários para garantir o funcionamento pleno e seguro da solução de comunicação, mesmo após a mudança de



endereço do Sesc-DF. Durante a instalação, técnicos especializados realizam as adequações físicas e lógicas, respeitando as especificações do projeto e as normas vigentes de segurança e qualidade.

10.10. O monitoramento constante do ambiente implantado permite detectar preventivamente falhas ou quedas de performance. Com isso, é possível atuar de forma proativa, ajustando configurações ou realizando intervenções pontuais para manter a estabilidade e a qualidade do serviço.

10.11. A manutenção contínua garante que todos os componentes e recursos permaneçam atualizados e operando de acordo com as melhores práticas do mercado. Isso inclui a aplicação de patches de segurança, atualizações de firmware e revisões periódicas de desempenho.

10.12. Essa abordagem completa, que vai da instalação até o suporte e a manutenção contínua, oferece um ambiente de comunicação robusto, confiável e adaptável às constantes mudanças e demandas do Sesc-DF, e alinhado com seus objetivos de crescimento e inovação.

11. ACORDO DE NÍVEL DE SERVIÇO

11.1. O prazo para a prestação do serviço de suporte técnico deve garantir a observância ao atendimento do seguinte acordo de níveis de serviços (ANS) e sua severidade:

11.1.1. Severidade alta – solução totalmente inoperante em um site.

- Prazo máximo de para primeiro atendimento de até 06 horas úteis contadas a partir do horário de abertura do chamado.

- Prazo máximo de resolução do problema de até 16 horas úteis contadas a partir do início do atendimento.

11.1.2. Severidade média – quando há falha, simultânea, que cause indisponibilidade de pelo menos 8 câmeras (câmeras off line) em um site.

- Prazo máximo de início de atendimento de até 8 horas úteis contadas a partir do horário de abertura do chamado.

- Prazo máximo de resolução do problema de até 16 horas contadas a partir do início do atendimento.

11.1.3. Severidade baixa – quando há falha, simultânea, que cause indisponibilidade de menos que 8 câmeras em um site.

- Prazo máximo de início de atendimento de até 10 horas úteis contadas a partir do horário de abertura do chamado.

- Prazo máximo de resolução do problema de até 20 horas contadas a partir do início do atendimento.

11.1.4. Suporte – aplicado para solicitações/alterações de configurações e novas funcionalidades – necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

- Prazo máximo de início de atendimento de até 12 horas úteis contadas a partir do horário de abertura do chamado.

- Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

11.1.5. Dúvidas técnicas – solicitações de informações diversas ou dúvidas sobre a solução.

- Prazo máximo de resposta de até 3 dias úteis, contados a partir da data de abertura da ocorrência.

11.2. Os tempos de resolução dos problemas descritos acima não são válidos para situações que dependam do fabricante, como substituição de equipamentos ou correção de falhas (bugs) de software.

11.3. É possível que surjam chamados técnicos cujas causas não sejam cobertas pelo presente contrato, posto que a causa da natureza técnica não tenha relação direta com o objeto deste contrato, tais como: problemas relacionados ao link de rede WAN ou Internet (interrupção da comunicação, alta latência, perda de pacotes, baixa taxa de transmissão, etc.), falta de energia elétrica, problemas com o cabeamento lógico ou elétrico, ações de terceiros que afetem a operação do sistema, entre outros. Neste sentido, estes chamados não deverão ser enquadrados em nenhuma severidade.

11.4. Um chamado técnico somente poderá ser fechado após a confirmação do responsável do SESC-DF e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde está instalado.

11.5. Na abertura de chamados técnicos, será informado pelo SESC a severidade do chamado.

11.6. A severidade do chamado poderá ser reavaliada pelo SESC, quando verificado que foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

11.7. A contratada poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

Indicador de início de atendimento (IIA): mostra o nível de cumprimento do prazo previsto para início de atendimento dos chamados.

11.8. Deve ser apurado separadamente, por linha de serviço, conforme serviços que estejam em uso pela contratante:

Indicador IIA		
1	Periodicidade	A apuração deve ser medida considerando os chamados concluídos entre o primeiro e o último dia de cada mês.
2	Método de Medição (Fórmula)	$IIA = (\sum \text{quantidade de chamados concluídos que atenderam o ANS Início de atendimento}) / (\text{total de chamados concluídos no período}).$

3	Glosa	O percentual de glosa IIA será aplicado, sobre cada índice obtido, seguindo a tabela abaixo:	
		% Índice IIA	Percentual de Glosa do Valor Mensal
		95% a 100%	0%
		80% a 94,99%	2%
4	Cálculo da Glosa	Abaixo de 80%	5%
		Valor da Glosa (R\$) = (% da glosa IIA) x (Valor total do serviço a ser pago no mês de apuração).	

12. SERVIÇO DE OPERAÇÃO ASSISTIDA

12.1. O serviço de operação assistida das soluções consiste na gestão, operação diária, suporte técnico, monitoramento, análise, projetos de melhorias e evolutivos dos itens contratados.

12.2. Os serviços serão prestados mensalmente, no regime 08 horas x 05 dias da semana, com a abertura de ordem de serviço (os) exclusiva para esse fim.

12.3. Durante toda a vigência do contrato, a equipe técnica da contratada realizará monitoramento constante para garantir que os sistemas permaneçam operando de forma eficiente. Isso inclui a identificação antecipada de possíveis problemas e a execução de manutenções preventivas para evitar interrupções.

12.4. A operação assistida irá incluir ajustes periódicos e atualizações para manter as soluções em linha com as melhores práticas e com as evoluções tecnológicas.

12.5. Devem ser realizadas reuniões periódicas entre o fornecedor e o SESC para avaliar a eficácia das soluções e ajustar as estratégias conforme necessário.

12.6. Durante toda a vigência do contrato, o suporte técnico será disponibilizado de forma contínua, com uma equipe capacitada para resolver quaisquer problemas que surjam, garantindo a estabilidade e o desempenho da solução.

13. DA VIGÊNCIA CONTRATUAL, ADITIVO E REAJUSTE

13.1. O prazo de vigência deste contrato será 12 (doze) meses, a contar da data da última assinatura eletrônica/digital, sendo prorrogada obrigatória e automaticamente por períodos iguais e sucessivos, pelo período mínimo de 36 (trinta e seis) meses, observado o limite máximo de 10 (dez) anos, conforme o art. 33, da Resolução nº. SESC 1.593/2024.

13.2. De acordo com a legislação vigente, o Contrato poderá sofrer acréscimos e reduções, de acordo com a necessidade do SESC-AR/DF, até o limite de 50% (cinquenta por cento), nas mesmas condições contratadas.



13.3. O contrato poderá ser reajustado mediante negociação entre as partes e a formalização do pedido de compras, tendo como limite máximo a variação do Índice Nacional de Preços ao Consumidor Amplo - IPCA, ou outro indexador que venha a substituí-lo, ocorrida nos últimos 12 (doze) meses contados da data da apresentação da proposta ou do último reajuste.

14. DA PRESTAÇÃO DE GARANTIA CONTRATUAL

14.1. A CONTRATADA deverá apresentar ao SESC, no prazo máximo de 10 (dez) dias, contados da data de assinatura do contrato, comprovante de prestação de garantia, que cubra todo o prazo contratual acrescido de 90 (noventa) dias, correspondente ao percentual de 5% (cinco por cento) do valor atualizado do contrato, podendo optar por caução em dinheiro, fiança bancária ou seguro garantia;

14.2. A garantia mencionada neste item deverá ser renovada a cada prorrogação do Contrato, se houver, devendo seu valor ser atualizado nas mesmas condições contratuais.

14.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- a) prejuízos advindos do não cumprimento do objeto do Contrato;
- b) prejuízos diretos causados ao SESC-AR/DF, decorrentes de culpa ou dolo durante a execução do Contrato;
- c) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela licitante vencedora.
- d) serviços que tenham que ser contratados com terceiros para corrigir falhas dos serviços executados pela licitante vencedora;
- e) multas aplicadas por órgãos públicos;
- f) débitos porventura existentes para com o INSS e FGTS; e
- g) danos contra terceiros não cobertos pelo seguro específico.

14.4. A garantia do contrato terá vigência durante todo o prazo de execução da obra ou serviços, devendo se estender até o prazo de 3 (três) meses, após término da vigência contratual.

14.5. Se o valor da garantia for utilizado total ou parcialmente, em pagamento de qualquer obrigação, a empresa contratada deverá proceder à respectiva reposição no prazo de 3 (três) dias úteis, contada da data em que for notificada pelo SESC-AR/DF.

14.6. Após o cumprimento fiel e integral do Contrato, a garantia prestada será liberada ou restituída à adjudicatária, no prazo de até 10 (dez) dias úteis, após formalizada sua solicitação.

14.7. Ao término da vigência do Contrato, a garantia retida somente será liberada ante a comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas, se for o



caso, decorrentes da Contratação. Caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo SESC-AR/DF.

15. GARANTIA DE PROPOSTA

15.1. A Garantia de Proposta corresponde ao valor exigido do licitante no momento da apresentação da proposta, sendo limitada a 1% (um por cento) do valor estimado do contrato.

15.2. A garantia da proposta será devolvida aos licitantes no prazo de 10 (dez) dias úteis, contado da assinatura do contrato ou a data que for declarada fracassada a Licitação.

15.3. A Garantia de Proposta poderá ser apresentada por meio de uma das seguintes modalidades:

15.4. Caução em dinheiro, por meio de depósito em conta específica a ser informada pelo SESC DF;

15.5. Fiança bancária, emitida por instituição financeira autorizada pelo Banco Central do Brasil;

15.6. Seguro-garantia, emitido por empresa devidamente registrada na Superintendência de Seguros Privados (SUSEP).

15.7. O comprovante da Garantia de Proposta deverá ser apresentado junto à documentação de habilitação da empresa.

Devolução e Retenção

15.8. A Garantia de Proposta será devolvida aos licitantes:

15.8.1. Após a assinatura do contrato pelo vencedor da licitação;

15.8.2. No caso de inabilitação ou desclassificação da proposta, após a conclusão da fase de julgamento.

15.8.3. Implicará execução do valor integral da garantia de proposta a recusa em assinar o contrato ou a não apresentação dos documentos para a contratação.

15.8.4. Se for constatada fraude ou má-fé na participação do certame.

Penalidades por Descumprimento

15.9. O não cumprimento da exigência de apresentação da Garantia de Proposta resultará na inabilitação automática do licitante, sem prejuízo de outras penalidades previstas no edital.

15.10. Caso ocorra a retenção da Garantia de Proposta por descumprimento das condições estabelecidas, a empresa poderá ser penalizada conforme a legislação vigente, incluindo impedimento de participação em novos certames por período determinado.

16. DO PAGAMENTO

16.1. As notas fiscais/faturas, bem como os documentos/relatórios, incluindo ANSs (Acordos de Níveis de Serviço) e glosas, que devem acompanhá-las, deverão ser apresentadas pela CONTRATADA, referente aos itens executados.

16.2. Os pagamentos serão realizados até 30 dias, após o aceite do objeto, aqui representado por meio da homologação pela CONTRATANTE do Produto/Serviço entregue e ateste das respectivas notas fiscais/faturas, mediante ordem bancária creditada na conta corrente da CONTRATADA.

17. REQUISITOS DA PROPOSTA

17.1. Para fins de registro e controle das propostas e lances durante a fase pública do pregão, o objeto licitado foi configurado em quantidades como ITEM, com base no preço unitário utilizado na composição do preço de referência. Esses preços unitários de referência representam o valor MÁXIMO que o SESC-AR/DF está disposto a pagar pelo equipamento, conforme pesquisa de mercado prévia realizada junto às empresas.

17.2. Deverá ser comprovado pela LICITANTE, na fase aceitação como anexo da proposta de preço, por meio de documento expedido pelo fabricante, que os equipamentos descritos na proposta de preços continuam sendo fabricados;

17.3. A LICITANTE deverá apresentar, juntamente com sua Proposta de Preços, carta ou declaração dos fabricantes ou distribuidores oficiais dos equipamentos comprovando ser revendedora autorizada dos produtos ofertados.

17.4. Tal solicitação justifica-se por:

17.4.1. Garantia e Suporte Técnico: Revendedores autorizados têm um relacionamento formal com o fabricante, o que pode facilitar a obtenção de suporte técnico e garantias mais eficientes. Isso é importante para garantir a manutenção adequada dos equipamentos ao longo do tempo.

17.4.2. Qualidade e Conformidade: Fabricantes geralmente impõem padrões rigorosos para seus revendedores autorizados. Ao exigir que os licitantes sejam revendedores autorizados, a entidade licitante pode buscar garantir que os equipamentos adquiridos atendam aos padrões de qualidade e conformidade estabelecidos pelo fabricante.

17.4.3. Acesso a Atualizações e Peças de Reposição: Revendedores autorizados têm mais chances de ter acesso a atualizações de software, firmware e peças de reposição originais. Isso é crucial para manter os equipamentos funcionando de maneira eficiente e segura ao longo do tempo.

17.4.4. Treinamento Especializado: Revendedores autorizados muitas vezes recebem treinamento especializado diretamente do fabricante. Isso significa que estão



mais bem preparados para instalar, configurar e manter os equipamentos de acordo com as especificações do fabricante.

17.4.5. Evitar Falsificações e Produtos Ilegítimos: Exigir que os licitantes sejam revendedores autorizados pode ajudar a evitar a aquisição de equipamentos falsificados, adulterados ou de procedência duvidosa. Isso contribui para a integridade e segurança das operações da entidade licitante.

17.4.6. Atualização Tecnológica: Revendedores autorizados geralmente estão mais atualizados em relação às últimas tecnologias e inovações dos produtos do fabricante. Isso pode ser crucial, especialmente em setores onde a tecnologia está em constante evolução.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. Prestar todas as informações e os esclarecimentos que venham a ser solicitados pela Contratada;

18.2. Responsabilizar-se pela observância das leis, decretos, regulamentos, portarias e demais normas legais, federal, estadual e municipal, direta e/ou indiretamente, aplicáveis ao Contrato;

18.3. Responsabilizar-se pela lavratura do respectivo contrato, com base resolução 1593/2024;

18.4. Assegurar os recursos orçamentários e financeiros para custear o contrato;

18.5. Pagar a importância correspondente à aquisição ou aquisições;

18.6. Fiscalizar a execução do contrato, através de servidor especialmente designado.

18.7. Rejeitar qualquer material entregue equivocadamente ou em desacordo com as especificações mínimas exigidas neste termo de referência.

18.8. Nomear Gestor e Fiscal para acompanhar e fiscalizar a execução dos contratos;

18.9. Receber o objeto do certame prestado pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

18.10. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis.

19. DAS OBRIGAÇÕES DA CONTRATADA

19.1. Fornecer serviços nos prazos e condições pactuadas, de acordo com as exigências constantes neste documento;

19.2. Emitir fatura no valor pactuado, apresentando-as ao CONTRATANTE para ateste e Pagamento;

19.3. Atender prontamente as orientações e exigências inerentes à execução do objeto contratado;



19.4. Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer; qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste termo de referência;

19.5. Responsabilizar-se pela garantia dos serviços empregados nos itens solicitados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência;

19.6. Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência

19.7. O descumprimento das especificações solicitadas implicará no não recebimento dos serviços por parte do SESC-AR/DF;

19.8. A inobservância ao disposto nos itens anteriores, deste item, implicará no não pagamento do valor devido ao fornecedor, até que ocorra a necessária regularização.

19.9. Caso seja verificada alguma inconformidade nos serviços entregues, a Contratada será acionada para recolher e substituir ou reparar no prazo indicado pelo SESC;

19.10. A Contratada deverá apresentar documento fiscal válido correspondente ao fornecimento, no momento da entrega;

19.11. Prestar os serviços conforme especificações das legislações, normas técnicas e resoluções pertinentes, mantendo disponíveis equipamentos, softwares e pessoal especializado, em quantidades compatíveis;

19.12. Instalar, implantar e ativar os equipamentos relacionados no OBJETO deste instrumento, nos locais, quantidades e prazos definidos por cada ordem de serviço;

19.13. Responsabilizar-se por qualquer dano ou prejuízo causado a CONTRATANTE, seus bens e de terceiros, decorrentes da execução do Contrato;

19.14. A CONTRATADA deverá observar as obrigações abaixo relacionadas:

19.15. Executar fielmente o contrato avençado, de acordo com as cláusulas avençadas no Edital e seus ANEXOS, solicitação da CONTRATANTE, especificações, condições, prazo, locais e os termos da proposta ofertada, caso haja descontinuidade de produção do objeto oferecido, poderá ser entregue modelo atualizado sem ônus para a CONTRATANTE;

19.16. Cumprir as normas vigentes, respondendo pelas consequências de sua inexecução total ou parcial ou atraso injustificado.

19.17. Manter preposto, aceito pela CONTRATANTE, para representá-lo na execução do contrato;

19.18. Reparar, corrigir, remover, reconstituir ou substituir, as suas expensas, no total ou em parte o objeto de contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;



19.19. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificações exigidas na licitação;

19.20. Prestar esclarecimentos que lhe forem solicitados, atendendo prontamente as eventuais reclamações/ notificações relacionadas com os objetos fornecidos;

19.21. É expressamente proibida, também a veiculação de publicidade acerca deste contrato, salvo de houver previa autorização da Administração do CONTRATANTE;

19.22. É expressamente proibido à empresa contratada subcontratar outras empresas para realizar o objeto da presente licitação;

19.23. Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

19.24. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

19.25. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

19.26. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

19.27. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

20. DAS CARACTERÍSTICAS DA CONTRATAÇÃO

20.1. O fornecedor será selecionado por meio de procedimento licitatório na modalidade PREGÃO, sob a forma ELETRÔNICA, adotando o critério de julgamento de MENOR PREÇO GLOBAL.

21. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

21.1. É vedada a participação de consórcio de empresas, qualquer que seja sua forma de constituição.

21.2. Justificativa para a vedação:

21.2.1. A ausência de consórcio não trará prejuízos a competitividade do certame, a vedação visa tratar exatamente o oposto que seria o estímulo da competição entre os fornecedores do ramo;

21.2.2. Corroborando essa tese, o professor Marçal Justen Filho, no seu livro Lei de Licitações e Contratos Administrativos, leciona que:

“Em regra, o consórcio não é favorecido ou incentivado pelo nosso Direito. Como instrumento de atuação empresarial, o consórcio pode conduzir a resultados indesejáveis. A formação de consórcios acarreta risco de dominação do mercado, através de pactos de eliminação de competição entre os empresários. No campo de licitações, a formação de consórcios poderia reduzir o universo da disputa. O Consórcio poderia retratar uma composição entre eventuais interessados, em vez de estabelecerem disputa entre si, formalizariam acordo para eliminar a competição”;

21.3. A vedação visa também prevenir outros riscos, conforme abaixo:

21.3.1. Dificuldade de avaliação das propostas: em licitações que envolvem consórcios, pode ser mais difícil avaliar as propostas apresentadas, uma vez que várias empresas estão envolvidas no processo. Isso pode prejudicar a transparência e a competitividade do certame, bem como aumentar o risco de erros ou favorecimentos;

21.3.2. Complexidade na execução do contrato: a execução de contratos com consórcios pode ser mais complexa e demandar maior coordenação entre as empresas envolvidas. Isso pode aumentar o risco de atrasos, conflitos e problemas na entrega do objeto contratado; e

21.3.3. Risco de inadimplência: a participação de consórcios pode aumentar o risco de inadimplência, uma vez que a responsabilidade pelos compromissos assumidos é dividida entre as empresas participantes. Isso pode gerar incertezas quanto à capacidade do consórcio de cumprir com as obrigações do contrato.

22. DIREITOS AUTORAIS E DE PROPRIEDADE INTELECTUAL

22.1. Pertencem ao SESC-AR/DF o direito patrimonial e a propriedade intelectual das informações e dados que forem manipulados nos equipamentos e resultados produzidos em consequência da licitação, entendendo-se por resultados, quaisquer estudos, relatórios, descrições técnicas e documentação didática, em papel ou em mídia eletrônica;

22.2. Não será permitida a cessão, citação ou qualquer referência pública a nenhum dos trabalhos realizados com a exceção dos autorizados pelo SESC-AR/DF.

23. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

23.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da entrega dos equipamentos entregues, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados.



23.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da entrega do produto do contrato.

23.3. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle.

23.4. Durante a execução do objeto, o fiscal deverá monitorar o nível de qualidade dos produtos para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

23.5. O fiscal deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizados.

23.6. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

23.7. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha sua relação detalhada, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

23.8. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

23.9. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual.

23.10. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos.

24. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

24.1. Os produtos deverão ser entregues de acordo com a necessidade do CONTRATANTE, em 20 (Vinte) dias, após a emissão e comprovação de recebimento da Ordem de Compras.

24.2. Os produtos poderão ser rejeitados, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser



corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades;

24.3. Se, durante o recebimento provisório, constatar-se que os produtos estão em desacordo com o solicitado, fora da especificação ou incompletos, a CONTRATADA será notificada e deverá sanar as pendências em até 30 (trinta) dias corridos ficando suspenso o prazo de recebimento definitivo. As despesas referentes ao saneamento das pendências, inclusive frete, correrá às expensas da CONTRATADA.

24.4. O gestor do contrato analisará toda documentação apresentada pela fiscalização técnica e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções; e

24.5. O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços de implantação, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

24.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

25. SANÇÕES ADMINISTRATIVAS

25.1. Em caso de inexecução total, parcial, ou qualquer outra inadimplência, sem motivo de força maior, a empresa contratada estará sujeita, sem prejuízo da responsabilidade civil e criminal, no que couber, garantida a prévia defesa, às penalidades previstas na legislação aplicável, para as seguintes hipóteses:

25.1.1. por atraso injustificado:

25.1.1.1. multa de 1% (um por cento) ao dia, até o 30º (trigésimo) dia, incidente sobre o valor correspondente a Ordem de Compra – OC, limitado esse percentual a 10% (dez por cento); e

25.1.1.2. multa de 1,5% (uma vírgula cinco por cento) ao dia, a partir do 31º (trigésimo primeiro) dia de atraso, incidente sobre o valor da OC, sem prejuízo da rescisão deste a partir do 60º (sexagésimo) dia de atraso.

25.1.2. por inexecução parcial ou total:

25.1.2.1. advertência;

25.1.2.2. multa de 5% (cinco por cento) sobre o valor do Contrato; e

25.1.2.3. suspensão do direito de licitar ou contratar com a contratante, por um prazo não superior a 3 (três) anos, inclusive quando recusar-se a assinar o Contrato.



25.2. Impedimento do direito de licitar com abrangência Nacional, por prazo mínimo de 4(quatro) e máximo de 6(seis) anos:

25.2.1. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

25.2.2. Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

25.2.3. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

25.2.4. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.

25.3. Quando não pagos em dinheiro, os valores das multas eventualmente aplicadas serão deduzidos, pelo SESC- AR/DF, do pagamento devido e, quando for o caso, cobrados judicialmente.

25.4. Quando se tratar de inexecução parcial, o valor da multa deverá ser proporcional ao valor do produto que deixou de ser entregue.

25.5. Em caso de reincidência por atraso injustificado, será a adjudicatária penalizada nos termos da Resolução SESC nº. 1.593/2024.

26. DA SUBCONTRATAÇÃO

26.1. O A CONTRATADA não poderá subcontratar, no todo ou em parte, os serviços/fornecimentos objeto deste contrato.

26.2. A subcontratação dos serviços/dos fornecimentos pela CONTRATADA, ou de parte deles, será considerada inadimplemento contratual e permitirá:

26.2.1. Solicitar a imediata paralisação dos serviços/fornecimentos ou de parte deles;

26.2.2. Exigir a desmobilização imediata da subcontratada;

26.2.3. Aplicar as penalidades previstas no contrato;

26.2.4. Solicitar a rescisão do contrato.

27. DOS CRITÉRIOS AMBIENTAIS, SOCIAIS E CULTURAIS ADOTADOS

27.1. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade.

27.2. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao



longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos.

27.3. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens.

27.4. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar:

a) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e

b) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC).

27.5. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono.

28. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

28.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no Edital.

28.2. Os critérios de qualificação econômica a serem atendidos pelos Licitantes estão previstos no Edital.

28.3. Os critérios para a Qualificação Técnica devem ser atendidos pelas Licitantes, por meio dos seguintes documentos:

28.4. O(s) licitante(s) deverá(ão) apresentar atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, comprovando a experiência da licitante em prestação de serviços e venda de equipamentos de áudio e vídeo com automação, incluindo a prestação de serviços de instalação, suporte técnico e operação assistida.



28.5. No(s) atestado(s) devem estar explícitos: a identificação da pessoa jurídica que está fornecendo o atestado, o responsável pelo setor encarregado do objeto em questão e a especificação dos serviços executados ou em execução. Poderá ser necessário diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando obter informações sobre o serviço prestado;

28.6. Os atestados deverão ser válidos e conter a descrição pormenorizada do serviço prestado incluindo equipamentos e sistemas, bem como informações sobre o número do contrato vinculado, a sua vigência e a data de início dos serviços prestados; e

28.7. Somente poderão ser aceitos atestados de capacidade técnica expedidos após a conclusão do contrato ou se decorrido, no mínimo, um ano do início de sua execução, exceto se houver sido firmado para ser prestado em prazo inferior.

28.8. Será permitido o somatório de atestados ou declarações para fins de comprovação da qualificação técnica da licitante.

29. DA COMUNICAÇÃO

29.1. GARANTIA ON-SITE.

29.2. A CONTRATADA deverá manter um responsável pelo projeto de implantação da solução, capaz de resolver questões técnicas e administrativas, o qual deverá ser o ponto de contato com a equipe do SESC-AR/DF.

29.3. O mecanismo formal de comunicação entre o SESC-AR/DF e a contratada se dará mediante emissão de correspondência com os respectivos anexos que venham a ser necessários para o eficaz entendimento da comunicação e sua formalização.

29.4. A CONTRATADA disponibilizará para abertura de chamados e-mail, número 0800 ou site as suas expensas para solicitação de substituição de peças ou equipamentos.

29.5. A abertura de chamados técnicos deverá ser realizada por telefone (0800 ou de custo local em Brasília), ou por sistema WEB/e-mail.

29.6. Os chamados técnicos terão origem em decorrência de qualquer problema detectado pela equipe do SESC-AR/DF no tocante ao pleno estado de funcionamento do(s) equipamento(s), inclusive problemas relacionados com instalação, configuração e atualização.

29.7. Na abertura do chamado técnico junto à Central de Atendimento serão fornecidas, no mínimo, as seguintes informações:

29.8. Marca, modelo e número de série do(s) equipamento(s);

29.9. Problema observado;

29.10. Nome, telefone, e-mail do profissional do SESC-AR/DF responsável pela solicitação;



29.11. Nível de severidade do chamado.

29.12. O fornecedor informará o número do chamado técnico no ato da comunicação efetuada pela equipe do SESC-AR/DF, o qual servirá de referência para acompanhamento do chamado, inclusive após o encerramento do chamado.

30. DA SEGURANÇA DA INFORMAÇÃO

30.1. A CONTRATADA e seus profissionais envolvidos no projeto deverão seguir os seguintes procedimentos e premissas de segurança envolvidos na prestação dos serviços:

30.2. Manter sigilo sobre todo e qualquer assunto de interesse do SESC-AR/DF ou de terceiros de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

30.3. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do SESC-AR/DF;

30.4. Não veicular publicidade acerca do contrato, salvo se houver prévia autorização do SESC-AR/DF;

30.5. Manter sigilo de todas as informações a que tiveram acesso inclusive após o término da vigência contratual ou eventual rescisão; e

30.6. Assinar Termo de Termo de Confidencialidade e Sigilo.

30.7. na utilização de aplicações como VoIP, streaming de dados e Videoconferência, que requerem uma alta disponibilidade e baixa latência.

30.8. O modelo do Termo de Confidencialidade e Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no SESC-AR/DF, a ser assinado pelo representante legal da CONTRATADA, se encontra no Apêndice II.

30.9. O modelo do Termo de Confidencialidade e Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no SESC-AR/DF, a ser assinado pelo representante legal da CONTRATADA, se encontra no Apêndice II.

30.10. O modelo do Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes no SESC-AR/DF, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação se encontra no Apêndice III.

31. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL



31.1. A CONTRATADA deverá atender os critérios de sustentabilidade e observar as regras ambientais para atividades potencialmente poluidoras previstas na legislação pertinente.

31.2. A CONTRATADA se compromete a destinar todos os resíduos de forma ambientalmente correta, sempre priorizando materiais que sejam menos agressivos ao meio ambiente e possibilitem reutilização futura, bem como deverá dar ênfase nos princípios da redução, reutilização e reciclagem.

31.3. O desfazimento de qualquer material gerado para uso no SESC-AR/DF deve ser de acordo com a Política Nacional de Resíduos Sólidos (Lei 12.305/2010) e manejado adequadamente até sua destinação e/ou disposição final.

31.4. Para cumprir essa obrigação legal, a empresa que irá fazer o descarte dos resíduos deverá dar prioridade à destinação final ambientalmente adequada de resíduos que inclui a reutilização, a reciclagem, a compostagem, a recuperação, o aproveitamento energético e por último a disposição final em aterros sanitários visando mitigar danos adversos ao meio ambiente e os riscos à saúde pública. Caso os resíduos sejam reaproveitados fora do SESC-AR/DF, os resíduos devem ser descaracterizados.

31.5. O material licitado não deverá conter substâncias perigosas em concentração acima da recomendada na diretiva RoCHS (Restriciton of Certain Hazardous Substances), tais como mercúrio (Hg), CHUMBO (Pb), dentre outros.

31.6. Toda coleta de resíduos deve ser acompanhada de Manifesto de Transporte de Resíduos (MTR) e Certificado de Destinação.

32. LOCAL DE ENTREGA

32.1. Local de entrega:

Unidades	Endereço:
SESC Nova SEDE Administrativa e suas expansões	Setor de Indústria e Abastecimento – SIA, Trecho 04, Lotes 80/90 e 100/110. CEP: 71.200-040

33. CONDIÇÕES GERAIS

33.1. Sob nenhum pretexto serão recebidas propostas em desacordo com o Termo de Referência, bem como aquelas que não forem entregues conforme as normas de apresentação e prazos determinados;

33.2. O Distrito Federal é domicílio e foro competente para dirimir quaisquer dúvidas referentes ao processo e a procedimentos dele resultantes, renunciando as partes a qualquer outro, por mais privilegiado que seja;



33.3. A participação neste processo de cotação implica conhecimento e aceitação integral deste Termo de Referência, caso haja, bem como a observância de regulamentos, normas administrativas e técnicas aplicáveis;

33.4. A licitante que apresentar proposta estará vinculada a ela e se responsabilizará pela prestação do serviço licitado nas condições oferecidas, através de profissional competente e com Certidão de Acervo Técnico devidamente registrado pelo CREA em quantidades e especificidades iguais ou equivalentes de montagem ou desmontagem da estrutura do objeto sendo obrigatoriamente ser do mesmo Fabricante, assim garantindo para a Contratante a fiel execução do contrato sem perdas para a Contratante por desconhecimento.

34. DOCUMENTOS ANEXOS

34.1. Seguem Anexos a este Termo de Referência os seguintes documentos:

34.1.1. ANEXO I – Especificações Técnicas;

34.1.2. ANEXO II – Modelo do Termo de Confidencialidade e Sigilo

34.1.3. ANEXO III – Modelo do Termo de Ciência

34.1.4. ANEXO IV – Modelo de Proposta de Preço; e

BRASÍLIA, ____ de _____ de 2025.

Edital elaborado por:

Nome	Cargo	Matrícula
Paulo Henrique Castanheira	Gerente de Área	6600
Unidade Demandante: Gerencia de Tecnologia da Informação - GETEC		

Informações: Gestor, Fiscal e Substituto do Contrato

Nome	Cargo	Matrícula
Paulo Henrique Castanheira	Gestor Contrato	6888
Ricardo Bitencourt Soares	Fiscal de Contrato	2630
Jonatas Silva Perim	Fiscal Substituto	4469

ANEXO I AO TERMO DE REFERÊNCIA

Tabela 01 – ESPECIFICAÇÕES TÉCNICAS

Item	Especificações
1	1. Conjunto para monitoramento perimetral 1.1. O conjunto deverá ser composto por 2 câmeras bullet, um alto-falante e um switch industrial, conforme especificações a seguir. Câmera tipo 1 1.2. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 1.3. A câmera deve ser IP do tipo bullet para vídeo monitoramento outdoor ou indoor. 1.4. A câmera deve possuir resolução mínima para monitoramento de 4.0MP (2688 × 1520), operando com uma taxa mínima de 30 quadros por segundo em sua resolução máxima. 1.5. A câmera deverá adotar sensor de imagem CMOS com varredura progressiva, em dimensão próxima a 1/3", garantindo captação de imagens em alta definição. 1.6. Deve possuir compressão de vídeo nos padrões MJPEG, H.264 e H.265, além de suportar padrões complementares otimizados como H.264+ e H.265+, com alta relação de compressão. 1.7. A câmera deve suportar velocidade de shutter variando de aproximadamente 1/3 s até 1/100.000 s. 1.8. A câmera deverá possuir capacidade de gerar imagem colorida em condições de luminosidade extremamente baixa, em torno de 0,003 lux, e operar em 0 lux mediante acionamento do iluminador infravermelho. 1.9. A câmera deve possuir iluminadores IR integrados com alcance mínimo de 60 metros. 1.10. Possuir lente fixa de 4 mm com ângulo de visualização horizontal mínimo de 83°. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lente solicitado, uma margem para mais e para menos de 5% nos valores, desde que seja

	comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado. 1.11. A câmera deverá possuir função Dia e Noite com filtro de IR comutável automaticamente. 1.12. O sistema deverá oferecer função de codificação diferenciada em área marcada da câmera (ROI), garantindo que regiões críticas possuam resolução máxima configurada. 1.13. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contra forte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com pelo menos 2 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 1.14. O equipamento deverá incorporar função de redução digital de ruído 3D DNR ajustável, assegurando clareza de imagem em ambientes de baixa luminosidade. 1.15. O sistema deverá permitir a criação de máscaras de privacidade, possibilitando ocultar áreas específicas do campo de visão. 1.16. A câmera deverá possuir suporte a eventos de proteção perimetral como cruzamento de linha, detecção de intrusão, entrada e saída de áreas. 1.17. O sistema de detecção deverá suportar classificação de alvos por tipo, distinguindo entre pessoas e veículos. 1.18. A câmera deverá possuir capacidade de captura facial, permitindo aplicações de segurança que demandem identificação de indivíduos. 1.19. O equipamento deverá dispor de interface para armazenamento local com suporte a cartões de memória de até 512 GB. Não é necessário o fornecimento do cartão de memória. 1.20. O equipamento deverá suportar protocolos e recursos de rede abrangentes, incluindo TCP/IP, HTTPS, TLS, IPv6, SNMP, 802.1x e QoS, garantindo compatibilidade e segurança. 1.21. O sistema deverá assegurar mecanismos de proteção cibernética, como autenticação por credenciais complexas, criptografia de tráfego e registros de auditoria de segurança. 1.22. O equipamento deverá ser alimentado via PoE conforme padrão 802.3af, Classe 3, simplificando a infraestrutura de instalação.
--	---

	1.23. O invólucro da câmera deverá possuir proteção mínima IP66, assegurando resistência contra poeira e água, adequado para ambientes externos com variação térmica de 0 °C a 60 °C. 1.24. A câmera deverá ser fornecida com suportes e acessórios homologados para fixação em parede, teto ou poste, de acordo com a necessidade do projeto. Alto-falante 1.25. A solução deverá impreterivelmente adotar corneta IP com processamento digital embarcado, apta a difusão sonora programada, transmissões ao vivo e acionamentos emergenciais, com possibilidade de vinculação por eventos e comunicação em duas vias, de modo a viabilizar atuação reativa no perímetro sem dependência de processamento central para as funções de áudio operacional. 1.26. Deverá apresentar potência nominal não inferior a aproximadamente 6 W, assegurando nível de pressão sonora adequado em aplicações externas e internas. 1.27. O sistema deverá garantir sensibilidade de referência próxima de 110 dB a 1 metro com 1 W, contribuindo para alto desempenho com baixa potência disponível. 1.28. O equipamento deverá alcançar nível máximo de pressão sonora superior à 120 dB SPL, permitindo ampla cobertura em áreas abertas. 1.29. O conjunto deverá operar em faixa útil de resposta compreendida entre aproximadamente 250 Hz a 15 kHz, assegurando inteligibilidade vocal e reprodução de mensagens. 1.30. A diretividade deverá ser controlada, com abertura próxima de 70° no plano horizontal e 90° no plano vertical, favorecendo focalização do feixe sonoro na área de interesse e mitigação de vazamentos acústicos. 1.31. A eletrônica embarcada deverá implementar algoritmos de processamento de áudio incluindo AEC, AGC, ANS e DRC, garantindo inteligibilidade e estabilidade de ganho em distintos cenários operacionais. 1.32. O dispositivo deverá suportar comunicação em duas vias para atendimento/negociação remota no ponto de instalação. 1.33. O equipamento deverá fornecer TTS com disponibilidade de Português (Brasil) entre os idiomas suportados, permitindo emissão de mensagens contextuais sem pré-renderização externa.
--	--

	1.34. O caminho de áudio deverá contemplar bitrates e formatos compatíveis com integrações de segurança: G.711 μ-law/a-law (64 Kbps) e MP3 (128 Kbps), além de reprodução MP3/WAV. 1.35. A unidade deverá sincronizar eventos e difusões por NTP, assegurando integridade cronológica dos registros. 1.36. A integração de rede deverá contemplar protocolos abertos e amplamente adotados, incluindo IPv4, HTTP, HTTPS, SIP, SSL/TLS, DNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP e SSH, garantindo compatibilidade e segurança na implantação. 1.37. A interface com plataformas e softwares de mercado deverá apoiar padrões de interoperabilidade não proprietários, contemplando SIP, RTP e ONVIF. 1.38. A interface física deverá ser RJ45 10/100M adaptativa, com auto-negociação e compatibilidade com infraestruturas Ethernet convencionais. 1.39. A alimentação deverá ocorrer por PoE conforme IEEE 802.3at, simplificando cabeamento e assegurando reserva de potência para picos dinâmicos de áudio. 1.40. Deverá estar disponível saída auxiliar de 12 VDC de baixa corrente para suprimento de dispositivos locais de baixa potência. 1.41. A unidade deverá possibilitar armazenamento de arquivos de áudio (pelo menos 1GB), permitindo difusão autônoma mesmo em contingências de rede. 1.42. A interface de I/O deverá contemplar entrada de alarme e entrada de linha (line-in), possibilitando correlação com sensores e fontes sonoras analógicas locais. 1.43. O sistema deverá observar relação sinal-ruído mínima em torno de 85 dB, contribuindo para emissão clara de mensagens e alarmes audíveis. 1.44. O invólucro deverá ser confeccionado em material metálico e apresentar proteção mínima IP66, assegurando operação em ambientes externos severos. 1.45. O equipamento deverá operar de forma estável em temperaturas de 0 °C a 60 °C, com umidade menor que 90% (sem condensação), garantindo disponibilidade em condições climáticas adversas. 1.46. A solução deverá observar conformidades eletromagnéticas, de segurança e ambientais aplicáveis, incluindo CE-EMC, CB/CE-LVD, RoHS, WEEE e REACH, assegurando aderência regulatória em projetos públicos e privados. Switch tipo 1
--	--

	1.47. O equipamento deverá ser um switch industrial não gerenciável, capaz de suportar quatro portas PoE Gigabit e duas portas SFP Gigabit para conexão via fibra óptica, garantindo flexibilidade em topologias industriais. 1.48. A solução deverá dispor de suporte a fornecimento de até 90 W em uma de suas portas (Hi-PoE), permitindo energizar equipamentos de maior demanda diretamente pela rede de dados. 1.49. O switch deverá estar em conformidade com os padrões IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt, garantindo interoperabilidade plena com dispositivos de diferentes fabricantes. 1.50. O sistema deverá implementar mecanismo de detecção inteligente de dispositivos alimentados, associado a proteção contra sobrecarga em nível de sistema, assegurando confiabilidade operacional. 1.51. O equipamento deverá oferecer proteção contra surtos elétricos de até 6 kV, mitigando riscos em ambientes industriais sujeitos a descargas atmosféricas e interferências elétricas. 1.52. A solução deverá assegurar ampla faixa de operação térmica, suportando temperaturas de 0 °C a 60 °C, compatível com aplicações industriais em ambientes severos. 1.53. O invólucro deverá ser confeccionado em material metálico, em design sem ventoinhas, garantindo maior robustez e confiabilidade em aplicações contínuas. 1.54. O equipamento deverá apresentar consumo máximo próximo de 120 W, com alimentação em corrente contínua de 48–57 V DC, assegurando eficiência energética e adequação a sistemas de energia industriais. 1.55. O dispositivo deverá permitir instalação em trilho DIN, além de montagem em mesa, garantindo flexibilidade de aplicação em campo. 1.56. O switch deverá possuir capacidade de comutação de 12 Gbps, assegurando desempenho adequado para redes de missão crítica. 1.57. O equipamento deverá apresentar tabela de endereços MAC de pelo menos 2K entradas, cache interno de 1.0 Mbits e taxa de encaminhamento de pacotes de, no mínimo, 8 Mpps. 1.58. As portas PoE deverão fornecer até 30 W cada, com orçamento total de potência PoE não inferior a 110 W, permitindo operação simultânea de múltiplos dispositivos terminais.
--	---

	1.59. O equipamento deverá atender normas de conformidade eletromagnética, segurança e ambientais aplicáveis, incluindo CE-EMC, IC, RCM, CB, CE-LVD, RoHS, WEEE e REACH. 1.60. Deverá ser fornecido com 02 mini gbic e fonte própria para operação. Licenciamento 1.61. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
2	2. Câmera tipo 2 2.1. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 2.2. A câmera deve ser IP do tipo bullet para vídeo monitoramento outdoor ou indoor. 2.3. Resolução mínima para monitoramento de 4.0MP (2688 × 1520) operando com uma taxa mínima de 60 quadros por segundo em sua resolução máxima. 2.4. Sensor de imagem CMOS 1/2" ou maior, com varredura progressiva. 2.5. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão. 2.6. O produto deverá estar em conformidade comprovada com os perfis ONVIF Profile S, Profile G, Profile M e Profile T, devendo a comprovação ser realizada por meio do site oficial da ONVIF (www.onvif.org/conformant-products). 2.7. Suportar velocidade de shutter de 1s a 1/100.000s. 2.8. Suporte para cinco streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo. 2.9. Deverá possuir capacidade de gerar imagem colorida em 10 metros quadrados com 0,005 lúmens e 0 Lux com IR acionado. 2.10. Deve possuir iluminadores IR integrados, com alcance mínimo de 60 metros. 2.11. Possuir lente varifocal P-iris de no mínimo 2.8 mm a 12 mm com ângulo de visualização horizontal mínimo de 110° a 45°. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será

	aceito para o cálculo de lentes solicitado uma margem para mais e para menos de 5% nos valores de FOV e PPM, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado 2.12. Função Dia e Noite com filtro de IR com troca automática. 2.13. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI). 2.14. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contra forte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com pelo menos 3 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 2.15. Deve possuir função para redução de ruído ajustável na intensidade de ação espacial e temporal. 2.16. Deve possuir sistema de estabilização de imagem. 2.17. Possuir recurso que permita a inclusão de máscaras de privacidade, sendo no mínimo 8 (oito). 2.18. A câmera deverá suportar os seguintes eventos de proteção perimetral: 2.19. Cruzamento de linha, intrusão, entrada e saída de áreas; 2.20. A câmera deve suportar alarmes acionados por tipos de alvos especificados (pessoa e veículo) 2.21. A câmera deve suportar realização de alertadas baseados nos eventos de proteção perimetral de forma combinada; 2.22. A câmera deve ser capaz de detectar pelo menos 100 faces simultaneamente, capturando pelo menos 30 imagens faciais frame simultâneo e realizar o envio de no mínimo 10 imagens faciais por segundo para o software de gerenciamento, a captura facial deverá realizar extração de no mínimo 7 atributos faciais. 2.23. A câmera deve ser capaz de reconhecer identidade facial por meio de modelagem, classificação e comparação em biblioteca de imagens-alvo. Para a comparação deve suportar no mínimo 5 bibliotecas, cada uma configurável, com capacidade total de pelo menos 10mil faces.
--	--

	2.24. A câmera deve suportar analíticos de extração de atributos de alvos, sendo eles: 2.25. Deverá suportar de forma simultânea a captura de: 7 atributos faciais, 13 atributos de corpo humano e no mínimo 2 atributos veiculares; 2.26. A câmera deve suportar contagem do número de alvos que cruzam uma linha por tipo, incluindo corpo humano, veículo não motorizado e veículo motorizado. 2.27. A câmera deverá permitir aplicação de mais de um analítico simultâneo, permitindo otimizar a operação onde haja a necessidade de realizar mais de um analítico, sendo eles: 2.28. Extração de atributos de alvos (corpo, face e veículo) e proteção de perímetro (intrusão, cruzamento de linha); 2.29. Extração de atributos de alvos (corpo, face e veículo) e comparação de faces; 2.30. Extração de atributos de alvos (corpo, face e veículo) e gerenciamento de pessoas (contagem regional); 2.31. Reconhecimento facial e proteção de perímetro (intrusão, cruzamento de linha); 2.32. Metadados: 2.33. A câmera deve fornecer metadados que permitam a recuperação e busca ágil de imagens relevantes no banco de dados. 2.34. Os metadados devem abranger eventos como detecção de intrusão, detecção de cruzamento de linha, detecção de entrada em região, detecção de saída de região, captura de face e extração de alvos. 2.35. A câmera deve oferecer plataforma aberta de IA para instalar e executar até 4 modelos de aplicação adicionais, sem que haja a necessidade de licenças adicionais. 2.36. Não será aceito soluções em que o fluxo de vídeo da câmera necessita ser encaminhado a um servidor centralizado para a captura de face e corpo humano ou extração de atributos faciais e corporais. 2.37. O processamento do reconhecimento facial deve acontecer no local de instalação, de maneira remota, não sendo permitido que o fluxo de vídeo vá até um software ou appliance centralizado. Poderá ser ofertado a instalação de appliance de aplicação nível industrial para realizar essa integração de maneira
--	--

	local no ponto de monitoramento, e seu custo deve estar previsto no fornecimento deste item. 2.38. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 1 TB, sendo fornecido com unidade de 64 GB destinada exclusivamente a aplicações de videomonitoramento contínuo, com suporte a criptografia de dados local. A mídia deverá adotar tecnologia NAND Flash do tipo 3D TLC (Triple-Level Cell), assegurando maior densidade, eficiência energética e resistência a ciclos intensivos de gravação. 2.39. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 2.40. A câmera deverá possuir suporte multiprotocolos e padrões de segurança: 2.41. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar. 2.42. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 2.43. Protocolo que permita realizar priorização de tráfego de dados na rede; 2.44. Protocolo de transferência de arquivos; 2.45. Protocolo que permita realizar a câmera realizar envios de e-mail para um destino especificado; 2.46. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação; 2.47. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 2.48. Deve possuir padrão de autenticação 802.1x; 2.49. Protocolos que criem um canal criptografado com os dados que serão transmitidos da câmera até um servidor externo, envelopando as informações e
--	--

	garantindo que apenas o remetente e o destinatário possam entender o conteúdo da comunicação; 2.50. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 2.51. O sistema deverá permitir a definição de credenciais de acesso que imponham restrições de composição e robustez, exigindo diversidade de caracteres e estruturas mínimas que reduzam a exposição a ataques por tentativa sucessiva. 2.52. A solução deverá implementar protocolo de segurança de transporte com capacidade de negociação criptográfica robusta, autenticação mútua e resistência a ataques de interceptação e retrocesso de versão. 2.53. A arquitetura deverá suportar protocolo de segurança de última geração com redução de latência, criptografia com segredo direto (forward secrecy) e eliminação de algoritmos legados, assegurando proteção aprimorada para os dados em trânsito. 2.54. O equipamento deverá incorporar módulo criptográfico embarcado em hardware, com proteção física contra violação, armazenamento seguro de chaves e validação da integridade do ambiente, com conformidade com normas internacionais de segurança em nível elevado. 2.55. Deve ser alimentada via PoE, simplificando sua infraestrutura de instalação, compatível PoE (802.3af) ou PoE+ (802.3at). 2.56. O invólucro externo do dispositivo deverá apresentar conformidade com padrões internacionais de proteção eletromecânica, oferecendo resistência aprimorada contra penetração de partículas sólidas, jatos de água em alta pressão e ambientes com presença de agentes corrosivos, sendo adequado para aplicações em áreas externas sujeitas a intempéries severas, ambientes industriais e atmosferas salinas. 2.57. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 2.58. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução. 2.59. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o
--	--

	fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros. Licenciamento 2.60. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
3	3. Câmera tipo 3 3.1. A câmera descrita a seguir pode ser fornecida em um único conjunto embarcado e integrado em um mesmo corpo, ou em dois conjuntos ópticos separados, desde que atenda todas as especificações abaixo. 3.2. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 3.3. A câmera deverá possuir tecnologia de inteligência Artificial de larga escala, para análise perimetral. 3.4. Doravante, não importando se o ofertado é um conjunto único ou duas câmeras, denominaremos a solução ofertada apenas como "Câmera", quando necessária distinção entre os conjuntos ópticos indicaremos "Câmera Bullet" e "Câmera Speed Dome" ou "Câmera Móvel". 3.5. A Câmera ofertada deve prover dois campos de visão simultaneamente, um fixo, e outro móvel, com movimento de pan, tilt e zoom. 3.6. Caso seja ofertada a solução com dois conjuntos ópticos, todo licenciamento de software e analíticos deve estar contemplada neste item para os equipamentos ofertados, de maneira que a solução funcione plenamente, sem prejuízo para o CONTRATANTE. 3.7. A câmera deve operar de forma autônoma ou com hardware e software exclusivos, porém estes como parte integrante do custo do item, mesmo que seja proporcional à quantidade solicitada. 3.8. O conjunto ofertado deve possuir resolução mínima de 3680x1656 no canal fixo e 2688x1520 no canal PTZ.

	3.9. O conjunto óptico fixo deve ter campo de visão horizontal mínimo de 85°, Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lente solicitado, uma margem para mais e para menos de 5% nos valores, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado. 3.10. Deve permitir a geração de imagens coloridas com baixa iluminação a no mínimo 0,0005 Lux na Câmera Móvel, e 0,0005 Luz na Câmera fixa. 3.11. Possuir três fluxos de vídeo independentes e com resoluções e taxas de frames por segundo (fps) ajustáveis independentemente; 3.12. Deve possuir compressão de vídeo padrão H.265 e, ao menos, um padrão compressão de vídeo superior ao mesmo com alta relação de compressão; 3.13. Deve possuir iluminador de suplementar embarcado em seu conjunto móvel com alcance mínimo de 300m, e no conjunto fixo de 30m. Não será aceito o fornecimento de iluminadores externos ao corpo da câmera. 3.14. Possuir tempo do obturador configurável de 1/25 s a 1/30000 s 3.15. Permitir zoom óptico de, no mínimo, 25x 3.16. Possuir zoom digital de, no mínimo, 16x; 3.17. Possuir configuração de ajuste de foco para automático / semiautomático / manual; 3.18. Permitir configuração de até 300 presets; 3.19. Permitir configuração de até 8 patrulhas com, no mínimo, 32 presets cada. 3.20. Possuir Modo Dia&Noite com acionamento automático do filtro de IR, no conjunto móvel. 3.21. Possuir funções de aprimoramento de imagens como Redução Digital de Ruídos 3D (3D DNR), EIS (Estabilização Eletrônica da Imagem), Antinevoeiro (Defog), HLC (Compensação de luz alta); 3.22. Possuir função de Máscara de Privacidade de até, no mínimo, 20 zonas; 3.23. Possuir função Controle de Ganho automático (AGC); 3.24. A câmera deverá suportar os seguintes eventos de proteção perimetral: 3.25. Cruzamento de linha, intrusão, entrada e saída de área, objeto deixado ou removido; 3.26. A Câmera Speed Dome deve possuir função de rastreamento inteligente de objetos, sendo capaz de acompanhar apenas humanos ou veículos identificados no campo de visão da câmera fixa.
--	--

	3.27. O canal PTZ deverá possuir capacidade de detecção simultânea de múltiplos tipos de alvos, contemplando corpo humano, face e veículo, com captura dedicada no fluxo de vídeo. Já o canal fixo deverá suportar análise de densidade de pessoas, permitindo estimar o nível de ocupação em áreas configuradas. 3.28. A câmera deverá possuir grau de proteção contra intempéries mínimo IP66; 3.29. Possuir no mínimo 6 entradas de alarme e 2 saídas de alarme para acionamento de dispositivos; 3.30. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 1 TB, sendo fornecido com unidade de 64 GB destinada exclusivamente a aplicações de videomonitoramento contínuo, com suporte a criptografia de dados local. A mídia deverá adotar tecnologia NAND Flash do tipo 3D TLC (Triple-Level Cell), assegurando maior densidade, eficiência energética e resistência a ciclos intensivos de gravação. 3.31. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 3.32. No caso do fornecimento de conjuntos ópticos separados, os dois devem atender aos requisitos de cartão de memória descritos anteriormente. 3.33. A câmera deverá possuir suporte multiprotocolos e padrões de segurança: 3.34. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar. 3.35. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 3.36. Protocolo que permita realizar priorização de tráfego de dados na rede; 3.37. Protocolo de transferência de arquivos; 3.38. Protocolo que permita realizar a câmera realizar envios de e-mail para um destino especificado; 3.39. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação;
--	--

	3.40. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 3.41. Deve possuir padrão de autenticação 802.1x; 3.42. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 3.43. Deverá possuir alimentação 36 VDC. 3.44. Permitir trabalhar entre temperaturas na faixa de 0°C a 60°C e humidade na faixa de 90% ou inferior. 3.45. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 3.46. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução. 3.47. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros. Licenciamento 3.48. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
4	4. Câmera tipo 4 4.1. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 4.2. A câmera deve ser IP do tipo dome para vídeo monitoramento outdoor ou indoor. 4.3. Resolução mínima para monitoramento de 3200 × 1800 operando com uma taxa mínima de 25 quadros por segundo em sua resolução máxima.

	4.4. Sensor de imagem CMOS 1/2" ou maior, com varredura progressiva. 4.5. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão. 4.6. O produto deverá estar em conformidade comprovada com os perfis ONVIF Profile S, Profile G, Profile M e Profile T, devendo a comprovação ser realizada por meio do site oficial da ONVIF (www.onvif.org/conformant-products). 4.7. Suportar velocidade de shutter de 1s a 1/100.000s. 4.8. Suporte para quatro streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo. 4.9. Deverá possuir capacidade de gerar imagem colorida em 10 metros quadrados com 0,005 lúmens e 0 Lux com IR acionado. 4.10. Deve possuir iluminadores IR integrados, com alcance mínimo de 40 metros. 4.11. Possuir lente fixa com ângulo de visualização horizontal mínimo de 108°. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lentes solicitado uma margem para mais e para menos de 5% nos valores de FOV e PPM, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado 4.12. Função Dia e Noite com filtro de IR com troca automática. 4.13. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI). 4.14. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contra forte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com pelo menos 2 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 4.15. Deve possuir função para redução de ruído ajustável na intensidade de ação espacial e temporal. 4.16. Deve possuir sistema de estabilização de imagem.
--	--

	4.17. Possuir recurso que permita a inclusão de máscaras de privacidade, sendo no mínimo 8 (oito). 4.18. A câmera deverá suportar os seguintes eventos de proteção perimetral: 4.19. A câmera deverá suportar eventos de detecção de movimento, adulteração de vídeo e exceções, com acionamento de alarmes diferenciados por tipo de alvo (humano e veículo). Deverá ainda contemplar eventos inteligentes como detecção de alteração de cena, exceção de áudio e desfoque. 4.20. A câmera deverá implementar funções avançadas de análise embarcada, incluindo captura facial, contagem de pessoas e proteção perimetral (cruzamento de linha, intrusão, entrada e saída de região), com alarmes acionados por tipos de alvos especificados (humano e veículo). 4.21. Deverá possuir capacidade inteligente para diferenciar humanos e veículos; 4.22. Deverá possuir analítico embarcado para captura de face humana, contagem de pessoas e segmentação e captura simultânea de múltiplos alvos. 4.23. No modo de captura facial deve detectar, rastrear e capturar no mínimo 20 faces por frame que passam por seu campo de visão. Não serão aceitas câmeras que não sejam capazes de realizar o recorte da quantidade de faces especificado, câmeras que realizam apenas a detecção, sem a capacidade de realizar o recorte na quantidade especificada não serão aceitas. 4.24. A segmentação e captura simultânea de múltiplos alvos de abranger: Veículos automotores, Veículos não motorizados, Faces humanas e Corpos humanos. 4.25. A função de múltiplos alvos deverá realizar extração automática dos seguintes atributos veiculares: Tipo do veículo e Cor predominante do veículo (somente para veículos em sentido frontal). 4.26. A função de múltiplos alvos deverá realizar extração automática dos seguintes atributos faciais e corporais: Gênero, Faixa etária estimada, Presença de óculos, Uso de chapéu ou boné, Uso de máscara facial, tipo e cor da vestimenta superior e inferior, Transporte de mochila, Transporte de objetos nas mãos, Estilo de cabelo. Deve ainda ser capaz de detectar humanos pilotando motocicletas, bicicletas e triciclos, sendo capaz de identificar o uso de capacete e a quantidade de ocupantes. 4.27. Deve possuir capacidade de aplicar no mínimo os analíticos perimetrais por movimento, detecção por intrusão em uma área definida na imagem, detecção por cruzamento de linha definida na imagem, detecção por entrada, saída de uma área
--	---

	definida na imagem e caso a câmera seja rotacionada para uma nova cena deverá detectar esta mudança gerando alerta. 4.28. A câmera deve permitir a instalação de novos analíticos customizados e treinados de acordo com a biblioteca de desenvolvimento disponível pelo fabricante, caso a câmera não suporte esta função, deverá ser fornecido para cada local de instalação appliance de processamento de analíticos já licenciado e contemplado nos custos da câmera, sem prejuízo a CONTRATANTE. 4.29. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 512 GB. 4.30. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 4.31. Deverá possuir tecnologia de redução de ruído baseado em inteligência artificial. 4.32. O equipamento deverá dispor de microfone embutido, possibilitando captação de áudio em tempo real com alta qualidade, além de entrada e saída de áudio adicionais. 4.33. A câmera deverá possuir suporte multiprotocolos e padrões de segurança: 4.34. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar. 4.35. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 4.36. Protocolo que permita realizar priorização de tráfego de dados na rede; 4.37. Protocolo de transferência de arquivos; 4.38. Protocolo que permita realizar a câmera realizar envios de e-mail para um destino especificado; 4.39. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação;
--	---

	4.40. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 4.41. Deve possuir padrão de autenticação 802.1x; 4.42. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 4.43. O sistema deverá permitir a definição de credenciais de acesso que imponham restrições de composição e robustez, exigindo diversidade de caracteres e estruturas mínimas que reduzam a exposição a ataques por tentativa sucessiva. 4.44. A arquitetura deverá suportar protocolo de segurança de última geração com redução de latência, criptografia com segredo direto (forward secrecy) e eliminação de algoritmos legados, assegurando proteção aprimorada para os dados em trânsito. 4.45. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 4.46. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução. 4.47. Os firmwares de atualização de produto, devem ser criptografados ou autenticados, para que as informações críticas incluídas, não possam ser arbitrariamente analisadas, falsificadas ou violadas. 4.48. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros. Licenciamento 4.49. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
5	5. Câmera tipo 5

	5.1. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 5.2. A câmera deve ser IP do tipo dome para vídeo monitoramento outdoor ou indoor. 5.3. Resolução mínima para monitoramento de 3200 × 1800 operando com uma taxa mínima de 25 quadros por segundo em sua resolução máxima. 5.4. Sensor de imagem CMOS 1/2" ou maior, com varredura progressiva. 5.5. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão. 5.6. Suportar velocidade de shutter de 1s a 1/100.000s. 5.7. Suporte para quatro streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo. 5.8. Deverá possuir capacidade de gerar imagem colorida em 10 metros quadrados com 0,005 lúmens e 0 Lux com IR acionado. 5.9. Deve possuir iluminadores IR integrados, com alcance mínimo de 40 metros. 5.10. Possuir lente varifocal com ângulo de visualização horizontal mínimo de 40°. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lentes solicitado uma margem para mais e para menos de 5% nos valores de FOV e PPM, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado 5.11. Função Dia e Noite com filtro de IR com troca automática. 5.12. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI). 5.13. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contraforte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com
--	--

	pelo menos 2 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 5.14. Deve possuir função para redução de ruído ajustável na intensidade de ação espacial e temporal. 5.15. Deve possuir sistema de estabilização de imagem. 5.16. Possuir recurso que permita a inclusão de máscaras de privacidade, sendo no mínimo 8 (oito). 5.17. A câmera deverá suportar os seguintes eventos de proteção perimetral: 5.18. A câmera deverá suportar eventos de detecção de movimento, adulteração de vídeo e exceções, com acionamento de alarmes diferenciados por tipo de alvo (humano e veículo). Deverá ainda contemplar eventos inteligentes como detecção de alteração de cena, exceção de áudio e desfoque. 5.19. A câmera deverá implementar funções avançadas de análise embarcada, incluindo captura facial, contagem de pessoas e proteção perimetral (cruzamento de linha, intrusão, entrada e saída de região), com alarmes acionados por tipos de alvos especificados (humano e veículo). 5.20. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 512GB. 5.21. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 5.22. Deverá possuir tecnologia de redução de ruído baseado em inteligência artificial. 5.23. O equipamento deverá dispor de microfone embutido, possibilitando captação de áudio em tempo real com alta qualidade, além de entrada e saída de áudio adicionais. 5.24. A câmera deverá possuir suporte multiprotocolos e padrões de segurança: 5.25. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar.
--	--

	5.26. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 5.27. Protocolo que permita realizar priorização de tráfego de dados na rede; 5.28. Protocolo de transferência de arquivos; 5.29. Protocolo que permita realizar a câmera realizar envios de e-mail para um destino especificado; 5.30. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação; 5.31. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 5.32. Deve possuir padrão de autenticação 802.1x; 5.33. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 5.34. O sistema deverá permitir a definição de credenciais de acesso que imponham restrições de composição e robustez, exigindo diversidade de caracteres e estruturas mínimas que reduzam a exposição a ataques por tentativa sucessiva. 5.35. A arquitetura deverá suportar protocolo de segurança de última geração com redução de latência, criptografia com segredo direto (forward secrecy) e eliminação de algoritmos legados, assegurando proteção aprimorada para os dados em trânsito. 5.36. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 5.37. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução. 5.38. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros.
--	--

	Licenciamento 5.39. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
6	6. Câmera tipo 6 6.1. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 6.2. A câmera deve ser IP do tipo bullet para vídeo monitoramento outdoor ou indoor. 6.3. Resolução mínima para monitoramento de 3200 × 1800 operando com uma taxa mínima de 25 quadros por segundo em sua resolução máxima. 6.4. Sensor de imagem CMOS 1/2" ou maior, com varredura progressiva. 6.5. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão. 6.6. O produto deverá estar em conformidade comprovada com os perfis ONVIF Profile S, Profile G, Profile M e Profile T, devendo a comprovação ser realizada por meio do site oficial da ONVIF (www.onvif.org/conformant-products). 6.7. Suportar velocidade de shutter de 1s a 1/100.000s. 6.8. Suporte para quatro streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo. 6.9. Deverá possuir capacidade de gerar imagem colorida em 10 metros quadrados com 0,005 lúmens e 0 Lux com IR acionado. 6.10. Deve possuir iluminadores IR integrados, com alcance mínimo de 40 metros. 6.11. Possuir lente fixa com ângulo de visualização horizontal mínimo de 93°. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lentes solicitado uma margem para mais e para menos de 5% nos valores de FOV e PPM, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado 6.12. Função Dia e Noite com filtro de IR com troca automática.

	6.13. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI). 6.14. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contra forte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com pelo menos 2 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 6.15. Deve possuir função para redução de ruído ajustável na intensidade de ação espacial e temporal. 6.16. Deve possuir sistema de estabilização de imagem. 6.17. Possuir recurso que permita a inclusão de máscaras de privacidade, sendo no mínimo 8 (oito). 6.18. A câmera deverá suportar os seguintes eventos de proteção perimetral: 6.19. A câmera deverá suportar eventos de detecção de movimento, adulteração de vídeo e exceções, com acionamento de alarmes diferenciados por tipo de alvo (humano e veículo). Deverá ainda contemplar eventos inteligentes como detecção de alteração de cena, exceção de áudio e desfoque. 6.20. A câmera deverá implementar funções avançadas de análise embarcada, incluindo captura facial, contagem de pessoas e proteção perimetral (cruzamento de linha, intrusão, entrada e saída de região), com alarmes acionados por tipos de alvos especificados (humano e veículo). 6.21. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 512GB. 6.22. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 6.23. Deverá possuir tecnologia de redução de ruído baseado em inteligência artificial. 6.24. O equipamento deverá dispor de microfone embutido. 6.25. A câmera deverá possuir suporte multiprotocolos e padrões de segurança:
--	--

	6.26. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar. 6.27. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 6.28. Protocolo que permita realizar priorização de tráfego de dados na rede; 6.29. Protocolo de transferência de arquivos; 6.30. Protocolo que permita a câmera realizar envios de e-mail para um destino especificado; 6.31. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação; 6.32. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 6.33. Deve possuir padrão de autenticação 802.1x; 6.34. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 6.35. O sistema deverá permitir a definição de credenciais de acesso que imponham restrições de composição e robustez, exigindo diversidade de caracteres e estruturas mínimas que reduzam a exposição a ataques por tentativa sucessiva. 6.36. A arquitetura deverá suportar protocolo de segurança de última geração com redução de latência, criptografia com segredo direto (forward secrecy) e eliminação de algoritmos legados, assegurando proteção aprimorada para os dados em trânsito. 6.37. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 6.38. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução.
--	--

	6.39. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros. Licenciamento 6.40. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
7	7. Câmera tipo 7 7.1. A solução deverá impreterivelmente trabalhar com equipamentos que possuam inteligência de detecções de forma embarcada, ou seja, o processo de detecção deverá acontecer na borda, onde os equipamentos estiverem instalados ou através das próprias câmeras. 7.2. A câmera deve ser IP do tipo fish eye para vídeo monitoramento outdoor ou indoor. 7.3. Resolução mínima para monitoramento de 2560x1920 operando com uma taxa mínima de 25 quadros por segundo em sua resolução máxima. 7.4. Sensor de imagem CMOS 1/3" ou maior, com varredura progressiva. 7.5. Deve possuir compressão de vídeo padrão MJPEG, H.264, H.265 e, ao menos, um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão. 7.6. Suportar velocidade de shutter de 1/3s a 1/100.000s. 7.7. Suporte para dois streams de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo. 7.8. Deverá possuir capacidade de gerar imagem colorida em 0.017 Lux e 0 com IR ativo. 7.9. Deve possuir iluminadores IR integrados, com alcance mínimo de 8 metros. 7.10. Possuir lente fixa com ângulo de visualização horizontal mínimo de 180°, o campo de visão deverá ser de no mínimo 0.1m. Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito para o cálculo de lentes solicitado uma margem para mais e para menos de

	5% nos valores de FOV e PPM, desde que seja comprovado a utilização de ferramentas de cálculos do fabricante ou outras comumente utilizadas no mercado 7.11. Função Dia e Noite com filtro de IR com troca automática. 7.12. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente na área marcada a imagem possua a resolução máxima configurada na câmera (ROI). 7.13. Deve ter a capacidade de prover imagem visível de dois campos de visão, próximo e distante, mesmo contraforte luz de fundo, de maneira que o objeto de interesse no campo de visão próximo fique perfeitamente visível ao mesmo tempo que um segundo objeto de interesse, em segundo plano, em um campo de visão distante também esteja visível. A câmera deve realizar essa funcionalidade com pelo menos 2 quadros com diferentes tempos de exposição para formar o quadro final com a visão clara dos dois campos de visão. 7.14. Deve possuir função para redução de ruído ajustável na intensidade de ação espacial e temporal. 7.15. Possuir recurso que permita a inclusão de máscaras de privacidade. 7.16. O sistema deve dispor de funcionalidade de contagem de pessoas, com capacidade de registrar entradas, saídas e passagens, assegurando armazenamento local em memória interna dedicada e disponibilizando exportação de dados em ciclos estatísticos, além de permitir transmissão em tempo real. 7.17. Deverá possuir de forma embarcada funcionalidade de mapa de calor. 7.18. O equipamento deverá dispor de interface para armazenamento local com suporte a capacidades de, no mínimo, 512GB. 7.19. Deve ter a capacidade na ocorrência de uma interrupção de comunicação de dados, sincronizar as capturas e gravações realizadas neste período, armazenadas em seu cartão de memória, com a Solução de Armazenamento e a Solução de Processamento de Analíticos. Desta maneira garantindo a confiabilidade do sistema e integridade do sistema. 7.20. O equipamento deverá dispor de microfone embutido. 7.21. A câmera deverá possuir suporte multiprotocolos e padrões de segurança: 7.22. Protocolo que permita a interface de configuração da câmera seja aberta e apresentada em navegador WEB o digitar o endereço IP dela. A câmera deve dispor de duas versões desse protocolo, sendo uma com criptografia e outra sem criptografia, permitindo selecionar na interface de câmera qual função ela irá operar.
--	---

	7.23. Protocolo que ajude a diagnosticar problemas de comunicação, fornecendo informações sobre erros e congestionamento de rede; 7.24. Protocolo que permita realizar priorização de tráfego de dados na rede; 7.25. Protocolo de transferência de arquivos; 7.26. Protocolo que permita realizar a câmera realizar envios de e-mail para um destino especificado; 7.27. Protocolo ou conjunto de protocolos que possibilite a câmera envie em tempo real fluxo vídeo e áudio, bem como controle a entrega do fluxo, gerenciando a negociação; 7.28. Protocolo que permita a câmera obtenha automaticamente informações de configuração de uma rede, como por exemplo: Endereço IP, Máscara de Sub- rede e Gateway; 7.29. Deve possuir padrão de autenticação 802.1x; 7.30. Protocolo que permita a câmera realize conexões com provedores de banda larga, onde o acesso à Internet requer autenticação através de um nome de usuário e senha fornecidos pelo provedor de serviços. 7.31. O sistema deverá permitir a definição de credenciais de acesso que imponham restrições de composição e robustez, exigindo diversidade de caracteres e estruturas mínimas que reduzam a exposição a ataques por tentativa sucessiva. 7.32. Deve ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. 7.33. Acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução. 7.34. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como, responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros. Licenciamento 7.35. Deverão ser fornecidas todas as licenças necessárias para conexão dos equipamentos à Plataforma de Gerenciamento proposta. Quaisquer outras
--	---

	licenças necessárias para atendimento dos requisitos descritos neste documento deverão estar incluídas.
8	8. Switch 8.1. Deve possuir altura máxima 1 (um) rack unit (RU) 8.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC; 8.3. Deve possuir 24 (vinte e quatro) portas 10/100/1000 Mbps, usando conectores RJ-45; 8.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático; 8.5. Deve possuir, no mínimo, 4 (duas) portas 10 Gbps SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado; 8.6. Deve possuir capacidade de processamento igual ou superior a 96 (noventa e seis) Mpps; 8.7. Deve possuir capacidade de switching igual ou superior a 125 (cento e vinte e cinco) Gbps; 8.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes; 8.9. Deve possuir, pelo menos, 2 GB de memória DRAM; 8.10. Deve possuir, pelo menos, 8 GB de memória NVRAM; 8.11. Deve ser do tipo compacto e fanless; 8.12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+); 8.13. Deve implementar os protocolos IEEE 802.3at Power over Ethernet (PoE Max PoE+ Class 4 ports (30 W) em pelos menos 12 portas; 8.14. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts; 8.15. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C; 8.16. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas; 8.17. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento; 8.18. Deve possuir botão de reset para voltar a para configuração default de fábrica; 8.19. Deve implementar o padrão IEEE 802.3az (Energy-Efficient Ethernet);

	8.20. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet; 8.21. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC; 8.22. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo; 8.23. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas; 8.24. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree); 8.25. Deve ser compatível com o protocolo PVST / PVST+ e PRST; 8.26. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree; 8.27. Deve implementar BPDU Guard e Root Guard; 8.28. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta; 8.29. Deve permitir a criação VLANs privadas; 8.30. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ; 8.31. Deve implementar selective QinQ; 8.32. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDAP (Device Link Detection Protocol) ou similar; 8.33. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet; 8.34. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast; 8.35. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown); 8.36. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls; 8.37. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
--	--

	8.38. Deve implementar MLD snooping v1 e v2; 8.39. Deve implementar protocolo de proteção de topologia em anel; 8.40. Deve possuir DHCP Server para IPv4 e IPv6; 8.41. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta; 8.42. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv; 8.43. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas; 8.44. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino; 8.45. Deve permitir a configuração de Rate Limiting de entrada; 8.46. Deve permitir a configuração de Rate Shaping de saída; 8.47. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR; 8.48. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando perfis definidas por um servidor RADIUS externo; 8.49. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X; 8.50. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X; 8.51. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas; 8.52. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas: 8.52.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x; 8.52.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x; 8.52.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x; 8.53. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
--	--

	8.54. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x; 8.55. Deve implementar “Change of Authorization” de acordo com a RFC 5176; 8.56. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+; 8.57. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv; 8.58. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv; 8.59. Deve implementar ACLs de entrada e ACLs de saída para IPv4; 8.60. Deve implementar ACLs de entrada e ACLs de saída para IPv6; 8.61. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List); 8.62. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança; 8.63. Deve permitir a criação de filtros de endereço MAC de origem e destino; 8.64. Deve possuir protocolos para proteção de ataques de Denial of Service; 8.65. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping; 8.66. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”; 8.67. Deve implementar IP Source Guard em IPv4 e IPv6; 8.68. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf; 8.69. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing; 8.70. Deve implementar RADsec conforme RFC6614; 8.71. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3; 8.72. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
--	--

	8.73. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6; 8.74. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão; 8.75. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL; 8.76. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto; 8.77. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada; 8.78. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada; 8.79. Deve implementar pelo menos 4 (quatro) grupos de RMON; 8.80. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status; 8.81. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link; 8.82. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada; 8.83. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização; 8.84. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP; 8.85. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED; 8.86. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
--	--

	8.87. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash. 8.88. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada; 8.89. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header; 8.90. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável. 8.91. Garantia do fabricante na modalidade LIFETIME para equipamento ofertado, incluindo a evolução para novas versões. 8.92. Todos os equipamentos, componentes, produtos ou softwares necessários devem ser novos, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação(end-of-life) e nem de vendas (end-of-sale), ainda que futura, na data de entrega da proposta. 8.93. Deverá ser fornecido com 02 Módulos MINI-GBIC (GIGABIT INTERFACE CONVERTER) e fonte tipo industrial própria para operação.
9	9. NVR tipo 1 9.1. O gravador digital de vídeo em rede deve operar de forma autônoma e autossuficiente, unicamente com os recursos de hardware e software internos contidos em seu gabinete, com desempenho pleno e integral de suas funções. Exclui-se deste conceito os NVR montados com base em PC, que utilizem sistemas operacionais comuns a microcomputadores convencionais, não originalmente desenvolvidos em fábrica para o fim único e específico de atuar como NVR monobloco; 9.2. O sistema deverá suportar nativamente conexão e gravação de não menos que 64 canais IP. 9.3. O equipamento deverá possuir de forma nativa analíticos de inteligência artificial de larga escala. 9.4. O equipamento deve oferecer decodificação de até 32 streams em 1080p, ou até 20 streams em 1080p com funções de IA habilitadas, garantindo flexibilidade entre desempenho bruto e analítico.

	9.5. O sistema deve dispor de motor analítico duplo, permitindo o processamento à captura/comparação de faces ou à indexação e busca avançada por metadados. 9.6. Na aplicação de reconhecimento facial, o NVR deverá executar no mínimo 8 canais de comparações faciais, em casos onde a câmera realiza o envio da captura da face e até 4 canais a 2 MP, onde o NVR realiza o processo por análise do stream de vídeo recebido. 9.7. O NVR deve disponibilizar bibliotecas faciais com pelo menos 10 listas e armazenamento de pelo menos 10.000 imagens. 9.8. O sistema deve possuir mecanismo de pesquisa avançada por metadados estruturados gerados pelas câmeras. 9.9. A solução deverá possuir funcionalidade nativa de busca avançada multimodal, capaz de correlacionar descrições textuais com o conteúdo visual armazenado. O equipamento deverá utilizar mecanismo de indexação que mapeie imagens e descrições em um espaço vetorial comum, permitindo consultas abertas por texto. O sistema deverá possibilitar que o operador digite frases curtas ou palavras-chave (mínimo de 64 caracteres suportados) em linguagem natural, retornando automaticamente os trechos de vídeo mais relevantes, ordenados por similaridade semântica entre a consulta e os vetores previamente gerados a partir do vídeo. 9.10. O sistema de armazenamento deve contemplar mínimo de 8 interfaces SATA internas, aceitando HDDs de até 20 TB cada, totalizando mais de 150 TB de capacidade bruta. Devendo ser fornecido com 1 HDs com 16 TB. 9.11. O sistema de gravação deverá suportar arquitetura de armazenamento redundante, suportando pelo menos os principais níveis de agrupamento de discos utilizados em ambientes corporativos críticos, contemplando desde arranjos básicos de espelhamento e distribuição até configurações híbridas que conciliem desempenho e alta tolerância a falhas. Deverá abranger obrigatoriamente níveis equivalentes a RAID 0, RAID 1, RAID 5, RAID 6 e RAID 10. 9.12. Deve oferecer múltiplas saídas de vídeo HDMI e VGA independentes, com resoluções de até 4K no HDMI1 e Full HD nos demais, permitindo exibição simultânea em múltiplos monitores. 9.13. Deve contemplar 16 entradas e 9 saídas de alarme, além de interfaces seriais RS-232 e RS-485, garantindo integração com sistemas externos. 9.14. A comunicação em rede deve ser assegurada por duas interfaces Ethernet RJ-45 autoadaptativas de 10/100/1000 Mbps.
--	--

	9.15. Deve suportar até 128 conexões remotas simultâneas e protocolos abertos de integração, incluindo ONVIF (S/G), RTSP, iSCSI, HTTPS, SNMP. 9.16. O sistema deve operar em faixa de temperatura de 0 °C a 50 °C, com umidade relativa de até 90% sem condensação, consumo máximo de ≤50 W (sem HDD). Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito margem para mais e para menos de 5% nos valores.
10	10. NVR tipo 2 10.1. O gravador digital de vídeo em rede deve operar de forma autônoma e autossuficiente, unicamente com os recursos de hardware e software internos contidos em seu gabinete, com desempenho pleno e integral de suas funções. Exclui-se deste conceito os NVR montados com base em PC, que utilizem sistemas operacionais comuns a microcomputadores convencionais, não originalmente desenvolvidos em fábrica para o fim único e específico de atuar como NVR monobloco; 10.2. O sistema deverá suportar nativamente conexão e gravação de não menos que 128 canais IP. 10.3. O equipamento deve oferecer decodificação de até 32 streams em 1080p, garantindo flexibilidade entre desempenho bruto e analítico. 10.4. Na aplicação de reconhecimento facial, o NVR deverá executar no mínimo 16 canais de comparações faciais, em casos onde a câmera realiza o envio da captura da face (24 imagens por segundo) e até 8 canais a 2 MP, onde o NVR realiza o processo por análise do stream de vídeo recebido. 10.5. O NVR deve disponibilizar bibliotecas faciais com pelo menos 20 listas e armazenamento de pelo menos 100.000 imagens. 10.6. O sistema deve possuir mecanismo de pesquisa avançada por metadados estruturados gerados pelas câmeras. 10.7. O sistema de armazenamento deve contemplar mínimo de 16 interfaces SATA internas, aceitando HDDs de até 20 TB cada, totalizando mais de 300 TB de capacidade bruta. Devendo ser fornecido com 1 HDs com 16 TB. 10.8. O sistema de gravação deverá suportar arquitetura de armazenamento redundante, suportando pelo menos os principais níveis de agrupamento de discos utilizados em ambientes corporativos críticos, contemplando desde arranjos básicos de espelhamento e distribuição até configurações híbridas que conciliem

	desempenho e alta tolerância a falhas. Deverá abranger obrigatoriamente níveis equivalentes a RAID 0, RAID 1, RAID 5, RAID 6 e RAID 10. 10.9. Deve oferecer múltiplas saídas de vídeo HDMI e VGA independentes, com resoluções de até 4K no HDMI1 e Full HD nos demais, permitindo exibição simultânea em múltiplos monitores. 10.10. Deve contemplar 32 entradas e 16 saídas de alarme, além de interfaces seriais RS-232 e RS-485, garantindo integração com sistemas externos. 10.11. A comunicação em rede deve ser assegurada por quatro interfaces Ethernet RJ-45 autoadaptativas de 10/100/1000/2500 Mbps. 10.12. Deve suportar até 256 conexões remotas simultâneas e protocolos abertos de integração, incluindo ONVIF (S/G), RTSP, iSCSI, HTTPS, SNMP. 10.13. O sistema deve operar em faixa de temperatura de 0 °C a 50 °C, com umidade relativa de até 90% sem condensação, consumo máximo de ≤100 W (sem HDD). Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito margem para mais e para menos de 5% nos valores.
11	11. NVR tipo 3 11.1. O gravador digital de vídeo em rede deve operar de forma autônoma e autossuficiente, unicamente com os recursos de hardware e software internos contidos em seu gabinete, com desempenho pleno e integral de suas funções. Exclui-se deste conceito os NVR montados com base em PC, que utilizem sistemas operacionais comuns a microcomputadores convencionais, não originalmente desenvolvidos em fábrica para o fim único e específico de atuar como NVR monobloco; 11.2. O sistema deverá suportar nativamente conexão e gravação de não menos que 256 canais IP. 11.3. O equipamento deve oferecer decodificação de até 32 streams em 1080p, garantindo flexibilidade entre desempenho bruto e analítico. 11.4. Na aplicação de reconhecimento facial, o NVR deverá executar no mínimo 16 canais de comparações faciais, em casos onde a câmera realiza o envio da captura da face (24 imagens por segundo) e até 8 canais a 2 MP, onde o NVR realiza o processo por análise do stream de vídeo recebido. 11.5. O NVR deve disponibilizar bibliotecas faciais com pelo menos 20 listas e armazenamento de pelo menos 100.000 imagens.

	11.6. O sistema deve possuir mecanismo de pesquisa avançada por metadados estruturados gerados pelas câmeras. 11.7. O sistema de armazenamento deve contemplar mínimo de 16 interfaces SATA internas, aceitando HDDs de até 20 TB cada, totalizando mais de 300 TB de capacidade bruta. Devendo ser fornecido com 1 HDs com 16 TB. 11.8. O sistema de gravação deverá suportar arquitetura de armazenamento redundante, suportando pelo menos os principais níveis de agrupamento de discos utilizados em ambientes corporativos críticos, contemplando desde arranjos básicos de espelhamento e distribuição até configurações híbridas que conciliem desempenho e alta tolerância a falhas. Deverá abranger obrigatoriamente níveis equivalentes a RAID 0, RAID 1, RAID 5, RAID 6 e RAID 10. 11.9. Deve oferecer múltiplas saídas de vídeo HDMI e VGA independentes, com resoluções de até 4K no HDMI1 e Full HD nos demais, permitindo exibição simultânea em múltiplos monitores. 11.10. Deve contemplar 32 entradas e 16 saídas de alarme, além de interfaces seriais RS-232 e RS-485, garantindo integração com sistemas externos. 11.11. A comunicação em rede deve ser assegurada por quatro interfaces Ethernet RJ-45 autoadaptativas de 10/100/1000/2500 Mbps. 11.12. Deve suportar até 512 conexões remotas simultâneas e protocolos abertos de integração, incluindo ONVIF (S/G), RTSP, iSCSI, HTTPS, SNMP. 11.13. O sistema deve operar em faixa de temperatura de 0 °C a 50 °C, com umidade relativa de até 90% sem condensação, consumo máximo de ≤100 W (sem HDD). Observação: Visto que existem pequenas variações de parâmetros entre os diversos fabricantes do mercado, será aceito margem para mais e para menos de 5% nos valores.
12	12. Plataforma de gerenciamento 12.1. A Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, ofertada pela CONTRATADA, deverá ser fornecida como uma solução de gerenciamento centralizado, segura e escalável, capaz de gerenciar, configurar e monitorar todos os Pontos de Imagens, servidores de processamento analítico, servidores de armazenamento, dispositivos de operação, videowall e demais elementos integráveis, ainda que alocados em redes distintas ou locais geograficamente dispersos. 12.2. O sistema de gerenciamento de vídeo deve apresentar arquitetura corporativa de nível empresarial, permitindo controle unificado de múltiplos

	subsistemas, incluindo vídeo, controle de acesso e detecção de alarmes, assegurando continuidade operacional em implantações de grande porte. 12.3. A solução deve dispor de arquitetura leve, capaz de reduzir o consumo de recursos computacionais, assegurando eficiência consistente na gestão de sistemas de diferentes portes. 12.4. O sistema deve possibilitar combinação de múltiplos plug-ins sob uma arquitetura unificada e sob demanda, permitindo colaboração entre diferentes segmentos de negócio e expansão contínua para novas necessidades. 12.5. A plataforma deve ser compatível com aplicações de análise avançada baseadas em deep learning e estatísticas, assegurando recursos de inteligência ampliada. 12.6. O sistema deve possuir arquitetura aberta, permitindo integração com sistemas e hardwares de terceiros de forma simples e interoperável. 12.7. O sistema deve disponibilizar gerenciamento de vídeo eficiente e abrangente, incluindo busca rápida de incidentes, exportação de vídeos, adaptação a redes de baixa largura de banda e armazenamento confiável. 12.8. A solução deve suportar mecanismo de busca inteligente baseado em linguagem natural, capaz de classificar alvos em categorias como pessoas, veículos, objetos e animais, utilizando modelos de inteligência artificial em larga escala. 12.9. A plataforma deve possuir módulo de gerenciamento de acesso com estratégias avançadas, integração empresarial, autenticação multifatorial, registro de funcionários, impressão de crachás, políticas de permanência em áreas sensíveis e mecanismos de bloqueio automático em emergências. 12.10. O sistema deve permitir integração de controle de acesso com credenciais móveis, como Bluetooth e NFC, oferecendo maior conveniência e segurança. 12.11. A plataforma deve possuir módulo de registro e gestão de visitantes, incluindo permissões temporárias, rastreabilidade de acessos, relatórios detalhados e experiência personalizada com design e impressão de crachás. 12.12. O sistema deve suportar detecção de alarmes de diferentes tipos, permitindo gerenciamento centralizado, relatórios customizados e ações de enlace flexíveis. 12.13. A plataforma deve suportar módulo de análise inteligente, com painéis interativos baseados em inteligência artificial, permitindo análises estendidas e aplicações digitais específicas.
--	---

	12.14. O sistema deve suportar gerenciamento de exibição comercial, incluindo programação centralizada de conteúdos digitais, modelos pré-instalados e publicação de campanhas. 12.15. A solução deve possuir módulo de controle de tempo e presença, permitindo múltiplos métodos de registro, modelos de jornada de trabalho, relatórios diversificados e integração com sistemas de folha de pagamento. 12.16. O sistema deve suportar mecanismos para gestão de dispositivos portáteis, incluindo reconhecimento rápido, importação automática de dados por docking stations e relatórios estatísticos detalhados. 12.17. A plataforma deve suportar gerenciamento de vídeo wall inteligente, com exibição de vídeos de alarmes em tempo real em janelas pop-up e programação de layouts dinâmicos. 12.18. A plataforma deve suportar gerenciamento unificado de evidências, incluindo vídeos, imagens, áudios e documentos, assegurando arquivamento, exportação e recuperação centralizada de registros. 12.19. O sistema deve possuir módulo de mecanismos de realidade aumentada, permitindo associação entre câmeras e mapas, além de interação rápida com recursos através de operações intuitivas. 12.20. A solução deve suportar gerenciamento de patrulhas, com definição de rotas, disparo de alarmes durante inspeções e geração de relatórios de desempenho. 12.21. A plataforma deve ter módulo para inspeções de segurança inteligentes, com identificação de itens proibidos, auditoria detalhada e redução de falhas de operação. 12.22. O sistema deve possuir módulo de evacuação de emergência, com definição de pontos de encontro, monitoramento em tempo real da movimentação de pessoas e relatórios de presença. 12.23. A solução deve suportar gerenciamento remoto de múltiplos sites em uma única plataforma, oferecendo supervisão centralizada de dispositivos, usuários e recursos distribuídos. 12.24. A plataforma deverá suportar o gerenciamento centralizado de servidores em cluster, assegurando continuidade operacional em cenários de falha e suporte a armazenamento em larga escala.
--	---

	12.25. O sistema deve contemplar ferramentas de manutenção e monitoramento de saúde de dispositivos, incluindo visualização de topologia, alarmes de falha e relatórios de risco e exceções. 12.26. A plataforma deve possuir módulo para gerenciamento unificado de evidências, incluindo vídeos, imagens, áudios e documentos, assegurando arquivamento, exportação e recuperação centralizada de registros. A Plataforma deverá abranger os requisitos mínimos a seguir: 12.27. A solução deverá incorporar um serviço centralizado de gerenciamento de sistema que concentre as funções de autenticação, delegação de permissões e administração de usuários, funções, dispositivos e serviços, além de prover interface técnica para integração com sistemas de terceiros. 12.28. O sistema deverá contemplar componente dedicado à intermediação de comunicação entre a estrutura de gerenciamento e dispositivos externos de terceiros, permitindo interoperabilidade e ampliação do ecossistema através de gateway compatível. 12.29. A arquitetura deverá dispor de mecanismo específico para encaminhamento e distribuição de fluxos audiovisuais em tempo real, com suporte para até 200 canais de vídeo em entrada e 200 canais em saída, ambos operando com largura de banda de até 2 Mbps por canal, compatível com transmissões simultâneas ao vivo ou reprodução, sem dependência de interface web. 12.30. Deverá estar presente serviço responsável pela gestão de conteúdo estático e mediação de configuração de dispositivos via proxy reverso, atuando como elemento de sinalização e controle interno da plataforma. 12.31. A solução deverá oferecer suporte a dispositivos de controle remoto por meio de teclado em rede, com intermediação via serviço dedicado, permitindo operação ao vivo sobre ambientes visuais como videowalls. 12.32. O sistema deverá dispor de serviço específico voltado ao gerenciamento e controle de videowalls, com capacidade de integração com os demais módulos da plataforma. 12.33. A solução deverá permitir a conexão simultânea de, no mínimo, 100 dispositivos clientes, com acesso por meio de cliente leve ou completo em ambiente Windows, ou via aplicativo em dispositivos móveis com sistemas iOS ou Android, sem necessidade de licenciamento adicional de software cliente.
--	--

	12.34. A solução deverá oferecer suporte à integração com serviços de diretório corporativo, permitindo autenticação e gestão de usuários baseada em Active Directory, tanto para clientes de controle quanto para aplicativos móveis. 12.35. As funções de administração e operação da solução deverão ser acessíveis separadamente por meio de clientes web, clientes de controle e aplicativos móveis, com conectividade via LAN, WAN ou Internet, sem exigência de software adicional para administração. 12.36. 12.37. A solução deverá permitir a conexão simultânea de, no mínimo, 100 dispositivos clientes, com acesso por meio de cliente leve ou completo em ambiente Windows, ou via aplicativo em dispositivos móveis com sistemas iOS ou Android, sem necessidade de licenciamento adicional de software cliente. 12.38. A solução deverá oferecer suporte à integração com serviços de diretório corporativo, permitindo autenticação e gestão de usuários baseada em Active Directory, tanto para clientes de controle quanto para aplicativos móveis. 12.39. A administração do sistema deverá ser possível via cliente web acessado por navegador, sem necessidade de instalação de software adicional, com conectividade via LAN, WAN ou Internet. 12.40. As funcionalidades de operação de segurança deverão ser acessíveis via cliente de controle conectado à rede local ou remota, permitindo gerenciamento de permissões, dispositivos e eventos. 12.41. As funções básicas de operação deverão estar disponíveis via cliente móvel, com acesso remoto ou local à plataforma, para atividades de visualização e controle simplificado. 12.42. A solução deverá oferecer suporte a múltiplos formatos de codificação de vídeo, incluindo H.264, H.264+, H.265 e H.265+, assegurando compatibilidade com diferentes perfis de compressão e qualidade. 12.43. A plataforma deverá permitir a gestão do licenciamento para garantir a operação contínua do sistema, bem como suporte à atualização da plataforma de forma supervisionada. 12.44. A solução deverá disponibilizar funcionalidade de exportação de registros de eventos e operações por meio do gerenciador de serviços, permitindo o acesso e auditoria dos logs do sistema.
--	--

	12.45. A solução deverá permitir a configuração de múltiplos fusos horários e suporte a horário de verão, possibilitando sincronismo adequado em ambientes geograficamente distribuídos. 12.46. A solução deverá dispor de mecanismo de proteção de senha embarcado, funcional de forma autônoma e independente de servidor externo. 12.47. O sistema deverá implementar mecanismo de autenticação de usuário, assegurando o controle de acesso individualizado à plataforma. 12.48. O processo de ativação deverá incluir verificação automática da complexidade da senha definida pelo usuário, com base em critérios estabelecidos pelo fabricante. 12.49. O sistema deverá classificar e exibir o nível de segurança da senha atribuída, identificando-a como fraca, média ou forte conforme parâmetros internos. 12.50. As senhas definidas no sistema deverão conter, no mínimo, dois tipos distintos de caracteres entre letras minúsculas, letras maiúsculas, números ou caracteres especiais. 12.51. O sistema deverá restringir o uso de caracteres em senhas ao conjunto ASCII, bloqueando símbolos não reconhecidos por esse padrão. 12.52. A senha mínima permitida pelo sistema deverá conter ao menos oito caracteres, independentemente do tipo de usuário. 12.53. A solução deverá implementar fluxo de autenticação baseado em troca de sinalização entre o cliente (Web, Controle ou Móvel) e o servidor central, com validação do nome de usuário e senha (incluindo nome de domínio) e retorno da resposta ao cliente. 12.54. A solução deverá permitir que, quando cliente, dispositivo e servidor estiverem na mesma rede local (LAN), o cliente possa requisitar diretamente o fluxo de vídeo ao dispositivo, sem mediação adicional, recebendo a transmissão correspondente de forma direta. 12.55. A solução deverá dispor de mecanismo de mediação de vídeo ao vivo por meio de servidor de streaming, possibilitando que fluxos de vídeo originados dos dispositivos sejam requisitados pelo cliente, encaminhados pelo servidor de stream e entregues de forma otimizada, especialmente em cenários com múltiplos clientes acessando o mesmo dispositivo.
--	---

	12.56. A solução deverá permitir controle remoto de câmeras motorizadas (PTZ), com fluxo de sinalização em que o cliente envia requisição de comando ao sistema central, que por sua vez encaminha o controle ao dispositivo correspondente. 12.57. A solução deverá permitir agendamento de gravação por evento ou por faixa horária, com encaminhamento da programação do servidor ao NVR, que então requisita o fluxo ao dispositivo conforme a agenda e realiza a gravação do conteúdo recebido. 12.58. A solução deverá permitir que, ao ser configurado um alarme, o cliente de controle possa obter diretamente o fluxo de vídeo associado ao evento, com base na sinalização proveniente do dispositivo e da programação definida pelo cliente web. 12.59. A solução deverá permitir que, ao ser configurado um alarme, o cliente de controle obtenha o fluxo de vídeo relacionado ao evento por meio de servidor de streaming, utilizando fluxo de sinalização baseado na programação definida e no encaminhamento da requisição via servidor de streaming. 12.60. A solução deverá permitir a exibição de vídeo proveniente de dispositivos conectados diretamente, sobre infraestrutura de videowall, por meio de fluxo estruturado envolvendo o cliente, o sistema central e um decodificador. O processo deverá incluir a solicitação do cliente para obtenção da URL de transmissão junto ao servidor, o retorno dessas informações à interface de exibição do videowall, seguido da solicitação de exibição à unidade de decodificação. Esta, por sua vez, deverá ser responsável por requisitar o fluxo diretamente ao dispositivo de origem e executar a decodificação para apresentação no videowall. 12.61. A solução deverá possibilitar a exibição de vídeo em videowall por meio de servidor de streaming, utilizando fluxo de sinalização encadeado entre cliente, sistema central, decodificador, servidor de streaming e dispositivo de origem. O processo deverá contemplar a solicitação inicial do cliente para obtenção da URL com informações do dispositivo e do videowall; o retorno dessas informações pelo sistema ao cliente; a solicitação de exibição ao decodificador; e a requisição em cadeia do fluxo até a câmera, passando pelo servidor de streaming. O fluxo de vídeo deverá retornar à cadeia de transmissão até alcançar o decodificador, que então deverá realizar a decodificação e encaminhar o sinal ao videowall. 12.62. A solução deverá permitir a exibição automática de vídeo de alarme no videowall, originado de dispositivo diretamente conectado, mediante sinalização entre servidor, decodificador e câmera. O processo deverá incluir o envio da
--	--

	informação de alarme pela câmera ao servidor, a solicitação deste para exibição no videowall, a requisição de fluxo pelo decodificador diretamente ao dispositivo de origem, o recebimento do fluxo pela unidade de decodificação e, por fim, a exibição do vídeo no painel de visualização. 12.63. A solução deverá contemplar arquitetura composta por servidor, cliente, componente de serviço e SDK de plataforma, assegurando interoperabilidade plena entre esses elementos. 12.64. A comunicação entre servidor, cliente, componentes de serviço e SDK de plataforma deverá ocorrer sobre protocolos seguros, incluindo suporte a HTTP e HTTPS. 12.65. Todos os dados sensíveis armazenados no servidor deverão ser protegidos por meio de mecanismos criptográficos que assegurem confidencialidade da informação, mesmo em repouso. 12.66. Informações sensíveis que não demandem leitura deverão ser criptografadas utilizando algoritmos irreversíveis, impossibilitando qualquer tentativa de decodificação posterior. 12.67. Informações sensíveis que exijam leitura futura deverão ser protegidas por esquemas de criptografia que permitam a decriptação controlada, conforme política da aplicação. 12.68. A plataforma deverá adotar algoritmos de criptografia reconhecidos no padrão de mercado, incluindo RSA, AES, SHA e MD5. 12.69. Todos os algoritmos de criptografia utilizados deverão ser baseados em biblioteca de código aberto compatível com OpenSSL-1.0.2K. 12.70. A versão do OpenSSL utilizada pela plataforma deverá estar em conformidade com as políticas vigentes do laboratório de segurança do fabricante. 12.71. A solução deverá permitir acesso via protocolo HTTP como padrão para acesso web, garantindo conectividade básica entre cliente e sistema. 12.72. A plataforma deverá oferecer, como opção, o uso de protocolo HTTPS para transmissão segura de dados, por meio da importação de certificado digital compatível. 12.73. Para garantir segurança adicional no acesso remoto via serviços de visualização ao vivo ou reprodução, a autenticação do dispositivo deverá ocorrer no nível do servidor de streaming.
--	--

	12.74. A autenticação na plataforma deverá ser baseada, no mínimo, em nome de usuário e senha, com validação dos dados conforme regras definidas no sistema. 12.75. A complexidade da senha e o limite de tentativas de login deverão ser configuráveis de forma separada, permitindo ajustes distintos para força de senha e política de bloqueio. 12.76. A plataforma deverá permitir que, em caso de esquecimento de senha por parte do administrador, seja possível realizar a redefinição da senha com uso de licença específica. 12.77. Durante o processo de autenticação, as informações de entrada (input) deverão ser ocultadas visualmente durante a digitação da senha, garantindo proteção contra exposição local. 12.78. A senha deverá ser criptografada utilizando algoritmo RSA durante a transmissão, tanto em conexões HTTP quanto HTTPS, assegurando a integridade da autenticação. 12.79. O mecanismo de verificação de login deverá combinar usuário, senha e endereço IP como forma de proteção contra-ataques de força bruta. 12.80. A plataforma deverá aplicar bloqueio temporário caso a senha seja digitada incorretamente por cinco vezes consecutivas, impedindo novo acesso por um período de 30 minutos. 12.81. O parâmetro de bloqueio de usuário deverá estar ativado por padrão, garantindo a aplicação imediata de medidas de segurança ao detectar tentativas incorretas de login. 12.82. O sistema deverá permitir configuração de limite de tentativas de login por endereço IP, com bloqueio automático do IP ao atingir o valor pré-definido. 12.83. Após login bem-sucedido, a solução deverá gerar dinamicamente uma sessão única por cliente, com tempo de vida limitado, a fim de reduzir riscos associados a repetição de tentativas de autenticação. 12.84. Uma vez expirada a sessão, o sistema deverá exigir novo login para restabelecimento de acesso. 12.85. Em conexões HTTP, cada sessão deverá conter um token exclusivo com mecanismo de proteção contra replay, invalidado imediatamente após cada requisição e criptografado com algoritmo AES.
--	---

	12.86. A solução deverá empregar políticas de segurança distintas para o tratamento de dados sensíveis, como nome de usuário e senha, em conformidade com os diferentes cenários de uso. 12.87. Todas as informações sensíveis trocadas entre cliente e servidor deverão ser criptografadas durante a comunicação. 12.88. Em conexões HTTP, deverá ser gerada uma chave AES aleatória a cada sessão de login, assegurando que os dados não sejam facilmente expostos. 12.89. Em conexões HTTPS, o sistema deverá utilizar criptografia SSL certificada. 12.90. O sistema deverá adotar diferentes esquemas de armazenamento para dados sensíveis, conforme exigência dos requisitos funcionais e de segurança. 12.91. Para mitigar riscos de vazamento por replicação de chaves entre plataformas, o sistema deverá adotar algoritmos dinâmicos para senhas armazenadas localmente. 12.92. Para evitar o vazamento da senha do usuário causado por leitura indevida do sistema, a senha deverá ser criptografada com algoritmo SHA e armazenada em formato cifrado. Funcionalidades: 12.93. A plataforma deverá permitir o registro de informações de pessoas, incluindo dados básicos, níveis de acesso, agenda de turnos, associação a bibliotecas faciais, grupos de docas, informações de residente e dados públicos, contemplando ainda atributos como ID alfanumérico, departamento, nome, sobrenome, temperatura superficial da pele, data de validade de registro, e-mail, telefone, permissões especiais, credenciais estendidas, PIN, observações e informações privadas customizadas. 12.94. O sistema deverá permitir a alteração da organização à qual um indivíduo está vinculado. 12.95. A aplicação deverá permitir a exportação de todas as informações de pessoas cadastradas em arquivo compactado (ZIP), com senha para descompressão dos dados. 12.96. O sistema deverá suportar segmentação das informações de pessoas por abas na interface de adição de novos registros. 12.97. A solução deverá viabilizar a exportação de informações de pessoas incluindo itens adicionais, conforme necessidade de configuração.
--	---

	12.98. A aplicação deverá possibilitar a exportação de fotos de perfil de pessoas selecionadas em arquivo ZIP, com definição de senha para criptografia do conteúdo. 12.99. O sistema deverá suportar exportação de informações e dados adicionais sobre pessoas selecionadas, assegurando rastreabilidade detalhada. 12.100. A aplicação deverá permitir a importação de informações de pessoas por meio de modelos que aceitem itens adicionais, de forma a ampliar a flexibilidade de cadastro. 12.101. O sistema deverá permitir adicionar pessoas a grupos de contagem de emergência, assegurando controle específico em situações críticas. 12.102. A solução deverá permitir a edição de credenciais vinculadas a pessoas (como cartões, impressões digitais, face e íris) dentro da lista de indivíduos cadastrados. 12.103. O sistema, quando configurado com a função de dispositivo de registro via cliente web, deverá sincronizar automaticamente na plataforma as informações de novos usuários e credenciais adicionadas ou editadas localmente no dispositivo. 12.104. A aplicação deverá permitir habilitar ou desabilitar a função de exigir autorização administrativa para exclusão de departamentos e registros de pessoas; quando ativada, será necessário informar a senha de login do administrador para concluir a exclusão. 12.105. A plataforma deverá permitir o ajuste em lote do período de validade associado aos registros de pessoas. 12.106. O sistema deverá possibilitar a filtragem e exportação em lote de registros de pessoas cujo período de validade tenha expirado. 12.107. A aplicação deverá manter recurso de exportação em lote de relatórios de perdas de cartões vinculados a registros pessoais. 12.108. O sistema deverá suportar a desativação e posterior restauração de níveis de acesso atribuídos a pessoas de forma massiva. 12.109. A solução deverá permitir a personalização de até 20 campos de informações privadas e até 4 tipos de campos por item (texto, valor, data e seleção única), respeitando permissões da plataforma. 12.110. A aplicação deverá permitir a personalização de até 20 campos de informações públicas e um tipo de campo (somente texto), respeitando as permissões estabelecidas.
--	--

	12.111. A plataforma deverá permitir que o administrador habilite/desabilite o login de autoatendimento de funcionários e configure senhas de acesso vinculadas ao ID. 12.112. O sistema deverá suportar que os funcionários realizem login por autoatendimento na plataforma. 12.113. A aplicação deverá bloquear o IP de acesso de um usuário por período específico após múltiplas tentativas de login fracassadas. 12.114. O sistema deverá suportar configuração de comprimento máximo de senha para usuários. 12.115. A aplicação deverá obrigar o usuário a trocar a senha no primeiro login, emitir notificações quando a senha estiver próxima do vencimento e possibilitar redefinição em caso de esquecimento. 12.116. O sistema deverá expirar logins após período de inatividade, solicitando novo acesso. 12.117. A plataforma deverá suportar o preenchimento de informações pessoais via autoatendimento, acessível por QR code ou link de registro, com submissão dos dados diretamente para a plataforma. 12.118. O sistema deverá permitir habilitar a verificação de identidade facial como requisito na etapa de autoatendimento, com opção de tornar obrigatória a validação. 12.119. A aplicação deverá manter recurso de revisão de registros submetidos por autoatendimento, permitindo aprovação administrativa antes da efetiva inserção na base de dados. 12.120. O sistema deverá suportar que informações inseridas por autoatendimento sejam atribuídas por padrão a uma organização específica, com possibilidade de redefinição. 12.121. A solução deverá permitir que administradores realizem verificação e aprovação/rejeição/remoção de informações submetidas via autoatendimento antes da integração definitiva à plataforma. 12.122. A plataforma deverá permitir a importação de informações de pessoas via arquivo Excel, com parâmetros para definição de tratamento de duplicidades de registros e números de cartão. 12.123. O sistema deverá permitir a importação de fotos de pessoas em formato ZIP, com opção de habilitar ou desabilitar avaliação de qualidade facial durante o processo.
--	---

	12.124. A aplicação deverá suportar a importação de registros de pessoas diretamente a partir de dispositivos integrados. 12.125. O sistema deverá suportar a configuração de relação de mapeamento entre domínio AD e registros de pessoas na plataforma. 12.126. A solução deverá possibilitar a sincronização do domínio AD com registros de pessoas ou grupos de pessoas cadastrados. 12.127. A aplicação deverá permitir a sincronização do domínio AD com grupos de segurança. 12.128. O sistema deverá suportar sincronização de registros de pessoas ou grupos oriundos do domínio Azure AD. 12.129. A solução deverá suportar vinculação de IDs de pessoas com itens equivalentes do domínio AD. 12.130. A plataforma deverá possibilitar a limpeza rápida de permissões atribuídas a pessoas. 12.131. O sistema deverá suportar detecção do status de permissões atribuídas a pessoas. 12.132. A aplicação deverá permitir desabilitar e restaurar níveis de acesso em lote, garantindo flexibilidade na gestão de permissões. 12.133. O sistema deverá manter recursos para gestão de desligamento de pessoas, incluindo o tratamento de permissões e registros associados. 12.134. A plataforma deverá permitir a exclusão automática de níveis de acesso de pessoas desligadas na data de rescisão. 12.135. A aplicação deverá suportar habilitar ou desabilitar o cálculo de frequência/assiduidade no período compreendido entre a solicitação de desligamento e a data efetiva de saída. 12.136. O sistema deverá permitir a pesquisa de registros de acesso e de frequência associados a pessoas desligadas. 12.137. A plataforma deverá suportar cartões de até 20 dígitos ou um número de cartão. 12.138. O sistema deverá permitir a adição de até cinco cartões a um único registro de pessoa. 12.139. A aplicação deverá permitir a inserção manual de número de cartão durante o processo de matrícula/cadastro. 12.140. O sistema deverá permitir leitura de números de cartão a partir de estações de matrícula integradas.
--	---

	12.141. A solução deverá possibilitar que, ao utilizar uma estação de matrícula de cartão, sejam suportados formatos padrão como Wiegand 26 ou Wiegand 34. 12.142. A aplicação deverá suportar o registro de cartões via número completo (Full Byte Card No.) ou via número de cartão enrolado (Card Enrolled No.). 12.143. O sistema deverá permitir que, durante o processo de matrícula de cartão, seja possível selecionar condições de acesso relacionadas ao cartão. 12.144. A plataforma deverá permitir criptografia de setores de cartão (um setor por vez), quando utilizada estação de matrícula habilitada para leitura/gravação, comunicando-se com a plataforma via USB. 12.145. O sistema deverá suportar leitura de cartões em estação de matrícula integrada à rede, contemplando cartões de diferentes padrões, tais como EM, M1, ID, DESfire, FelCa e CPU. 12.146. A aplicação deverá permitir leitura de cartões em estação de matrícula comunicando-se via USB, contemplando múltiplos padrões de cartão. 12.147. O sistema deverá suportar leitura de números de cartão a partir de qualquer leitor de dispositivos de controle de acesso remoto. 12.148. A plataforma deverá suportar múltiplos tipos de cartões, incluindo: comum, duração limitada e de descarte. 12.149. O sistema deverá permitir a emissão de cartões em lote. 12.150. A aplicação deverá suportar relatórios de perda de cartões e possibilitar cancelamento de registros de perda. 12.151. A plataforma deverá permitir o cadastro de até 10 impressões digitais por pessoa. 12.152. O sistema deverá suportar estações de matrícula de impressões digitais dedicadas para captura de dados biométricos. 12.153. A aplicação deverá possibilitar captura de impressões digitais por estação de matrícula conectada em rede. 12.154. O sistema deverá permitir captura de impressões digitais por estação de matrícula conectada via USB. 12.155. A plataforma deverá permitir leitura de impressões digitais por leitores remotos de controle de acesso. 12.156. O sistema deverá suportar múltiplos tipos de impressões digitais, incluindo comum, de coação e de descarte. 12.157. A aplicação deverá manter mecanismos de checagem de duplicidade e avaliação de qualidade para impressões digitais cadastradas.
--	--

	12.158. A plataforma deverá permitir que apenas uma foto de rosto seja cadastrada por pessoa. 12.159. O sistema deverá suportar o upload de imagens faciais locais diretamente na plataforma. 12.160. A aplicação deverá permitir captura de fotos faciais utilizando câmera USB ou câmera de notebook. 12.161. O sistema deverá suportar ajuste automático de espelhamento ao capturar imagens faciais por câmera USB. 12.162. A aplicação deverá permitir captura de imagens faciais via estação de matrícula conectada em rede. 12.163. O sistema deverá permitir captura de imagens faciais via estação de matrícula conectada via USB. 12.164. A plataforma deverá permitir a coleta de imagens faciais por dispositivos de controle de acesso remoto. 12.165. O sistema deverá possibilitar exportação em arquivo ZIP contendo todas as imagens faciais de pessoas cadastradas, com definição de senha para descompactação. 12.166. A aplicação deverá suportar exclusão de credenciais faciais inválidas ou exclusão em massa de registros faciais de pessoas. 12.167. O sistema deverá suportar ocultar imagens faciais corrompidas ou ilegíveis para que não sejam exibidas na plataforma. 12.168. A plataforma deverá permitir testes de qualidade de imagens faciais em dispositivos de controle de acesso e câmeras de vídeo, garantindo integridade biométrica. 12.169. O sistema deverá suportar validação de qualidade de imagens faciais em cancelas/balizadores de passagem integrados a terminais de reconhecimento facial dedicados. 12.170. A plataforma deverá permitir o cadastro de até duas amostras de palma/veia por pessoa. 12.171. O sistema deverá suportar a coleta de amostras de palma/veia via dispositivos USB. 12.172. A aplicação deverá suportar a coleta remota de amostras de palma/veia em terminais dedicados. 12.173. A plataforma deverá permitir o cadastro de até duas íris por pessoa.
--	--

	12.174. O sistema deverá suportar a coleta remota de íris por dispositivos dedicados, permitindo utilizá-las como credencial de acesso e aplicando permissões diretamente aos dispositivos. 12.175. A aplicação deverá permitir a geração de códigos QR estáticos baseados no número de cartão da pessoa cadastrada. 12.176. O sistema deverá permitir a visualização e o download de códigos QR estáticos, para posterior distribuição aos colaboradores. 12.177. A plataforma deverá possibilitar a definição do modo de QR Code como estático ou dinâmico. 12.178. O sistema deverá permitir a configuração do período de validade do QR Code dinâmico (mínimo de 1 minuto por padrão). 12.179. A aplicação deverá permitir que colaboradores visualizem QR Codes dinâmicos atualizados automaticamente em intervalos definidos, além de suportar atualização manual após login no cliente móvel. 12.180. O sistema deverá suportar a gravação automática dos parâmetros da estação de matrícula, garantindo a restauração da última configuração utilizada após novo login. 12.181. A plataforma deverá suportar a configuração de senha exclusiva para cada pessoa, contendo entre 4 e 8 dígitos, assegurando que apenas uma senha esteja vinculada a cada registro individual. 12.182. O sistema deverá possibilitar a geração automática de códigos PIN vinculados a registros de pessoas. 12.183. A aplicação deverá permitir a customização de modelos de cartões, incluindo definição de layout vertical ou horizontal, ajuste de margens e posicionamento de campos de informações de pessoas. 12.184. O sistema deverá permitir a inserção de imagens em modelos de cartão personalizados. 12.185. A solução deverá suportar a impressão de QR Codes estáticos em cartões de pessoas cadastradas. 12.186. A plataforma deverá permitir a visualização prévia do cartão antes da impressão final. 12.187. O sistema deverá suportar configuração de alinhamento de texto nos cartões impressos. Dos eventos e alarmes:
--	--

	12.188. O sistema deve classificar os eventos de disparo por módulos, incluindo vídeo, controle de acesso, veículo, alarme, grupo de análise inteligente, sinalização digital, manutenção, usuário, evento definido pelo usuário, evento genérico, visitante, broadcast e inspeção de segurança. 12.189. A página de alarme deve disponibilizar ícone para configuração remota da fonte do disparo, permitindo ao usuário abrir a página de configuração remota do dispositivo ou servidor. 12.190. A plataforma deve permitir configurar, para eventos genéricos, o tipo de transporte como TCP, UDP, HTTP ou HTTPS. 12.191. O sistema deve permitir definir o tipo de correspondência de eventos genéricos como “Search by Expression”, “Match by Expression” ou “Search by keyword”, e especificar palavras-chave da fonte de dados, título e descrição. 12.192. A plataforma deve permitir selecionar operadores lógicos AND ou OR como expressão para os eventos genéricos. 12.193. O sistema deve permitir importar em lote eventos genéricos. 12.194. A solução deve permitir monitorar eventos genéricos por meio de mapa. 12.195. O sistema deve permitir configurar evento auto-definido quando os eventos monitorados pelo sistema ou os eventos genéricos não atenderem à necessidade dos usuários. 12.196. A plataforma deve permitir selecionar modelo de agenda de recebimento de eventos, incluindo modelos All-Day, Weekday e Holiday, podendo ser utilizados modelos definidos pela plataforma ou modelos personalizados. 12.197. A página Event Receiving and Alarm deve permitir habilitar a função de ignorar eventos ou alarmes recorrentes, com possibilidade de configurar a duração da condição de ignorar. 12.198. A plataforma deve permitir configurar grupos de destinatários de alarmes, de modo que, após adicionar usuários como destinatários, estes recebam notificações quando alarmes forem disparados. 12.199. O sistema deve suportar adição em lote de usuários como destinatários de alarmes. 12.200. A página Edit Alarm deve permitir selecionar destinatários de alarme ou grupo de destinatários de alarme para cada alarme. 12.201. A plataforma deve permitir configurar um ou múltiplos feriados para um modelo de agenda de recebimento de alarmes. Dos gatilhos de alarme:
--	--

	12.202. A plataforma deve permitir configurar cores para eventos. 12.203. O sistema deve suportar adição de modelos de cores para uso futuro. 12.204. A solução deve permitir definir como ação de enlace a captura de imagem, configurando a duração do período de captura anterior ou posterior ao evento. 12.205. O sistema deve suportar definir como ação de enlace a gravação, iniciando antes do evento, continuando após a ocorrência e vinculando os vídeos gravados ao estado de bloqueio. 12.206. A plataforma deve permitir configurar como ação de enlace o acionamento de PTZ, incluindo seleção de chamada de preset, patrulha ou padrão da câmera vinculada. 12.207. O sistema deve suportar definir como ação de enlace a criação de tag nos vídeos, com seleção das câmeras para gravação, definição de armazenamento dos arquivos e configuração de pesquisa por tag. 12.208. A solução deve suportar definir como ação de enlace o vínculo de pontos de acesso, associando todos ou pontos específicos. 12.209. A plataforma deve permitir definir como ação de enlace a associação de entradas de alarme, podendo estas ser ativadas ou desativadas quando o evento ocorrer. 12.210. O sistema deve suportar definir como ação de enlace a saída de alarme, com possibilidade de configurar diferentes modos de saída, incluindo manter estado de ligado/desligado ou acionar/desacionar automaticamente. 12.211. A solução deve permitir configurar como ação de enlace recurso de terceiros integrado, podendo selecionar operações de controle específicas que ocorrerão quando o evento acontecer. 12.212. O sistema deve permitir definir como ação de enlace o envio de e-mail, possibilitando selecionar modelo de e-mail definido ou criar modelo personalizado, com envio das informações de alarme de acordo com a configuração. 12.213. O sistema deve permitir definir como ação de enlace unidade de áudio, de modo que após vincular, seja possível enviar áudio ao dispositivo selecionado e reproduzi-lo quando o evento for disparado. 12.214. A plataforma deve permitir configurar como ação de enlace a associação de partições de alarme, de modo que partições configuradas possam ser armadas ou desarmadas conforme a ocorrência do evento. Gerenciamento de alarmes em tempo real:
--	--

	12.215. A janela pop-up de alarmes deve permitir editar a prioridade do alarme. Por padrão, devem estar disponíveis três níveis: alto, médio e baixo. 12.216. A janela pop-up de alarmes deve permitir editar o tipo do alarme. Por padrão, devem estar disponíveis quatro tipos: true, false, to be acknowledged e to be verified. 12.217. O cliente Web deve permitir configurar se um evento pode ser tratado como alarme, incluindo a seleção de destinatários do alarme e a definição de sua prioridade. 12.218. O cliente Web deve suportar a configuração do tempo restrito de tratamento de alarme, de forma que a saída de alarme vinculada ou eventos definidos pelo usuário sejam disparados após o período configurado expirar. 12.219. O cliente Web deve suportar habilitar múltiplas funções associadas a alarmes: exibição de janela pop-up, exibição de vídeo relacionado ao alarme em visualização pequena, associação do alarme a um mapa e disparo de alerta sonoro. 12.220. Quando a ação de enlace for gravação, a plataforma deve permitir selecionar se a gravação exibida será proveniente de vídeo gravado ou de visualização ao vivo no momento em que o alarme ocorreu. 12.221. A plataforma deve suportar o reconhecimento automático de alarmes pelo próprio sistema. Quando o tempo configurado expirar, o alarme deve ser automaticamente reconhecido. 12.222. A plataforma deve suportar exibir alarmes não tratados múltiplos e o número total de alarmes não tratados em uma janela pop-up de alarmes no cliente de controle. Das combinações de alarme: 12.223. A plataforma deve suportar vincular um alarme combinado com uma área de alarme disparada, sendo utilizado para contabilizar os alarmes ocorridos nessa área. 12.224. O sistema deve suportar habilitar a função de ignorar alarmes recorrentes, permitindo configurar a duração da condição de ignorar. 12.225. A plataforma deve suportar definir quaisquer tipos de fonte de disparo como parte da lógica de um alarme combinado. 12.226. O sistema deve suportar até quatro lógicas de disparo de alarmes, bem como configurar o intervalo de disparo entre dois alarmes.
--	---

	12.227. A plataforma deve suportar habilitar ou desabilitar alarmes. Ao desabilitar, o usuário deve poder definir hora de início e tempo de duração, sendo que, durante o período desativado, não devem ser recebidas notificações desses alarmes. 12.228. O sistema deve suportar definir todas as ações de enlace, exceto impressora de link. 12.229. A plataforma deve suportar configurar, por meio de lógica de disparo de alarme (uma das lógicas disponíveis), condições do tipo: “se um evento ocorreu, mas outro não ocorreu”, bem como suportar configuração de dois eventos de origem e do intervalo entre eles. 12.230. A plataforma deve suportar adicionar um alarme combinado ao mapa. 12.231. O sistema deve permitir copiar as configurações de um alarme combinado para outros alarmes combinados. 12.232. A plataforma deve suportar testar um alarme combinado. 12.233. O sistema deve permitir filtrar alarmes combinados por nome, área, prioridade e status. Configuração e gerenciamento: 12.234. A plataforma deve suportar, ao adicionar um evento, a seleção de múltiplos eventos de disparo e fontes. 12.235. O sistema deve suportar a exclusão rápida de todos os eventos inválidos por meio do botão “Delete All Invalid Items”. 12.236. A plataforma deve permitir definir múltiplos eventos como alarmes em lote. 12.237. O sistema deve permitir habilitar e desabilitar múltiplos alarmes em lote. 12.238. A plataforma deve suportar a realização de testes de alarmes. 12.239. O sistema deve permitir aplicar filtros para eventos definidos como alarmes. 12.240. A plataforma deve suportar filtros de eventos e alarmes por tipo de fonte, nome do evento e alarme, área, origem e evento de disparo. 12.241. O sistema deve destacar alarmes anormais com uma marca de exclamação vermelha. 12.242. A plataforma deve destacar eventos e alarmes não suportados pelas fontes configuradas. 12.243. O sistema deve suportar estatísticas de eventos e alarmes. 12.244. A plataforma deve permitir classificar eventos e alarmes por módulos. Central de alarme e controle:
--	---

	12.245. A plataforma deve suportar a seleção de diferentes layouts do Alarm Center no Control Client, incluindo opções: Related Video & Picture, Map e ambos combinados. 12.246. O sistema deve suportar a exibição de alarmes em tempo real, incluindo área, vídeo e imagem em uma tela auxiliar. 12.247. A plataforma deve suportar a seleção de itens exibidos na lista de alarmes, tais como status, prioridade, fonte, nome do evento e evento de disparo. 12.248. O sistema deve suportar a personalização de ícones exibidos na coluna de operação do Alarm Center. 12.249. A plataforma deve suportar a seleção de vídeo ou imagem como conteúdo exibido na informação do alarme, com recomendação do uso de imagem em casos de baixa largura de banda. 12.250. O sistema deve suportar a configuração do fluxo de vídeo padrão para exibição em janela pop-up de alarme. 12.251. A plataforma deve suportar o disparo de janela pop-up de alarme. 12.252. O sistema deve permitir habilitar aviso sonoro para alarmes. 12.253. A plataforma deve permitir configurar som de alarme diferenciado por prioridade. 12.254. O sistema deve suportar configurar o tempo de reprodução do som de alarme. 12.255. A plataforma deve suportar aplicação de filtros de alarmes em tempo real por prioridade, status de marcação e status de alarme. 12.256. O sistema deve suportar desabilitar o prompt de voz após reconhecer certos alarmes. 12.257. A plataforma deve suportar configuração de alarmes de baixa prioridade sem som de alarme. 12.258. O sistema deve suportar reconhecimento em lote de alarmes, com limite máximo de 2.000 alarmes reconhecidos simultaneamente. 12.259. A plataforma deve permitir classificar os alarmes por tempo e agregá-los por nome de alarme no Alarm Center do Control Client. 12.260. O sistema deve suportar adicionar categoria para personalizar as condições de filtro conforme a necessidade do usuário no Alarm Center. 12.261. O usuário deve poder visualizar um alarme no mapa, consultar detalhes no mapa e reconhecer um alarme diretamente no mapa. Busca e exportação de alarmes:
--	---

	12.262. A plataforma deve suportar a pesquisa de eventos por critérios como tempo, área, tipo de evento e nome do evento. 12.263. O sistema deve permitir a pesquisa de alarmes por parâmetros como hora de disparo, status de marcação, prioridade, tipo de alarme, status de reconhecimento, área, tipo de evento e nome do evento/alarme. 12.264. A plataforma deve suportar a pesquisa conjunta de eventos e alarmes sob as mesmas condições de filtragem. 12.265. Após a busca de eventos e alarmes, a solução deve permitir visualizar os detalhes do evento/alarme e os registros de operação associados. 12.266. O registro de operações de um alarme deve conter todas as ações relacionadas, incluindo registros de encaminhamento, ocultação, recebimento, marcação, desabilitação e informações do usuário responsável. 12.267. O sistema deve suportar exibir o mapa vinculado na janela pop-up de alarme e na página de detalhes do alarme, incluindo fontes de alarme, recursos de alarme e área de cobertura. O mapa deve ainda permitir ignorar alarmes em lote, iniciar áudio bidirecional e habilitar áudio de aviso. 12.268. A plataforma deve suportar abrir a janela do mapa vinculada a partir da janela pop-up de alarme e da página de detalhes do alarme, permitindo realizar operações relacionadas diretamente via mapa. 12.269. Após pesquisa de eventos e alarmes, a plataforma deve permitir exportar os resultados em arquivo CSV/PDF, suportando até 5.000 registros de informação. 12.270. O sistema deve suportar exportação de imagens relacionadas aos alarmes, com limite de até 500 registros. 12.271. A plataforma deve permitir exportar alarmes que coincidam ou não coincidam com as condições de busca, incluindo informações detalhadas como número do alarme, localização, número de cartão, número da placa do veículo e outros dados associados. Segurança do sistema: 12.272. A plataforma deve suportar protocolo de transmissão HTTPS e permitir configurar endereços IP para recebimento de informações de dispositivo. 12.273. O sistema deve permitir definir senha para o banco de dados local. 12.274. A plataforma deve suportar perguntas de segurança; caso a senha seja esquecida, administradores devem poder acessar o sistema respondendo corretamente às perguntas.
--	---

	12.275. O sistema deve suportar redefinição de senhas por meio de perguntas de segurança. 12.276. A solução deve suportar emissão de certificado de serviço, incluindo Streaming Service e Cloud Storage Service. 12.277. A plataforma deve suportar configuração de marcas d'água, incluindo nome do usuário, data e hora, conteúdo customizado, transparência, rotação do ângulo e espaçamento. 12.278. O sistema deve suportar definição de estratégias de login, incluindo bloqueio de IP em tentativas de login mal-sucedidas além do limite, habilitação de senha efetiva, expiração de senha, bloqueio do cliente após tempo ocioso e configuração de autenticações adicionais. 12.279. A plataforma deve suportar configuração de permissões por papéis, incluindo permissões de acesso a recursos, permissões de função, permissões de configuração e operação, status de usuário (ativo ou inativo) e período de validade da função. 12.280. O sistema deve permitir salvar permissões de um papel como modelo para aplicação em outros papéis de usuários, aplicável a cenários com grande número de usuários que compartilham mesma permissão de função mas diferentes permissões de recurso. 12.281. A solução deve permitir habilitar/desabilitar a função "Allow Remembering Password" quando do login via Mobile Client / Control Client. 12.282. A plataforma deve suportar configurar o tempo de inatividade nos clientes Web, Control Client e Mobile App, de forma que os usuários sejam automaticamente bloqueados se não houver operação durante o período configurado. 12.283. O sistema deve permitir adição e exclusão manual de usuários e grupos, bem como importação de usuários de domínio AD (Active Directory), com possibilidade de ativar/desativar, forçar logout e demais controles. 12.284. A solução deve suportar atualização automática dos clientes via Web Client, permitindo que sejam atualizados quando novas versões estiverem disponíveis. 12.285. A plataforma deve suportar backup de dados para o PC local, incluindo dados de configuração e registros. 12.286. O sistema deve suportar restauração de dados.
--	---

	12.287. A plataforma deve suportar backup de dados para servidor FTP, incluindo dados de configuração e registros. 12.288. O sistema deve suportar a função hot spare, permitindo configurar a propriedade hot spare (servidor principal e servidor de backup). Logs do sistema: 12.289. A plataforma deve suportar pesquisa de logs conforme critérios como local remoto, tipo de log, gatilho do log, recurso filtrado e tempo selecionado. 12.290. O sistema deve suportar exportação de logs de site remoto e logs centrais em formato EXCEL ou CSV. 12.291. A plataforma deve suportar pesquisa de logs locais de dispositivos de codificação, controle de segurança, dispositivos de decodificação, controle de acesso, controle de elevadores e dispositivos de rede. 12.292. O sistema deve suportar exportação de logs locais dos dispositivos. 12.293. A solução deve permitir exportar logs online/offline de múltiplos dispositivos. 12.294. O sistema deve suportar exportação de logs online/offline de dispositivos individuais. 12.295. A plataforma deve suportar exibir em gráficos e listas a duração online de dispositivos e o tempo mais recente de desconexão. 12.296. O sistema deve permitir exportação de logs de recursos. 12.297. A plataforma deve suportar pesquisa de status de gravação dos recursos. 12.298. O sistema deve suportar visualização do status de gravação em cada ponto de tempo. 12.299. A plataforma deve suportar pesquisa de logs online/offline dos recursos. 12.300. O sistema deve permitir exibição em gráfico e lista sobre a duração online dos recursos e o tempo mais recente de desconexão. 12.301. A plataforma deve suportar exportação de logs de manutenção dos recursos. 12.302. O sistema deve suportar pesquisa de logs de manutenção conforme tarefas pendentes, objetos em verificação de integridade, nível de risco, responsável pela manutenção, tempo de atendimento e status de manuseio. 12.303. A plataforma deve suportar visualização de status de manutenção em cada ponto de tempo. 12.304. O sistema deve permitir pesquisa de logs de manutenção online/offline. 12.305. A plataforma deve suportar visualização de logs de manutenção.
--	---

	O sistema deve permitir exportação de logs de manutenção. Módulo de BI 12.306. A plataforma deve permitir personalizar os relatórios exibidos no dashboard, incluindo contagem de pessoas, análise de densidade, análise de mapa de calor, fila, atributos de pessoas e veículos. 12.307. O sistema deve permitir configurar o tipo de análise, podendo ser definido por grupo de recurso ou por canal. 12.308. A plataforma deve suportar alternar o modo de visualização no dashboard, permitindo também a edição do tipo e do horário do relatório exibido. 12.309. O sistema deve suportar a atualização manual do conteúdo dos relatórios exibidos no dashboard. 12.310. A plataforma deve permitir a exportação do conteúdo dos relatórios exibidos no dashboard. 12.311. O sistema deve permitir exportar relatórios diretamente no dashboard. 12.312. A plataforma deve suportar a seleção do nome do relatório para exportação. 12.313. O sistema deve permitir exportação de relatórios em formatos Excel, CSV e PDF. 12.314. A plataforma deve suportar a configuração de relatórios agendados diários, semanais ou mensais. 12.315. O sistema deve suportar a configuração do horário de envio de relatórios agendados. 12.316. A plataforma deve permitir configuração do modelo de e-mail para envio de relatórios agendados. 12.317. O sistema deve permitir selecionar o idioma dos relatórios exportados de forma agendada. 12.318. A plataforma deve suportar o envio de relatórios agendados de eventos e alarmes para servidor SFTP. 12.319. O sistema deve permitir salvar em armazenamento local os relatórios agendados de eventos e alarmes exportados. 12.320. A plataforma deve suportar geração de relatórios de análise multi-alvo, exibindo informações como número de pessoas, veículos motorizados e veículos não motorizados em período especificado.
--	--

	12.321. O sistema deve suportar visualização de relatórios do tipo: Daily Report, Weekly Report, Monthly Report, Annual Report e Custom Time Interval Report, contendo estatísticas de visitantes por hora, dia e mês. 12.322. A plataforma deve permitir exportação de relatórios em formato PDF, EXCEL ou CSV. 12.323. O sistema deve permitir selecionar múltiplas câmeras e leitores de cartão como recursos estatísticos de grupos de contagem de pessoas. 12.324. A plataforma deve permitir configurar entradas e saídas de portas como recursos no grupo de contagem de pessoas. 12.325. O sistema deve permitir configurar tempo para limpeza periódica de dados de contagem de pessoas. 12.326. A plataforma deve suportar habilitar capacidade máxima e configurar número máximo de pessoas autorizadas a entrar. 12.327. O sistema deve suportar configuração de alarmes para grupos de contagem de pessoas quando número de indivíduos ultrapassar limite de threshold configurado. 12.328. A plataforma deve permitir monitoramento em tempo real de grupos de contagem de pessoas selecionados, exibindo visualização ao vivo de múltiplos grupos simultaneamente. 12.329. O sistema deve suportar visualização do número de pessoas restantes em grupo de contagem e número de pessoas já passadas durante o período de contagem. 12.330. A plataforma deve permitir correção manual dos dados de contagem de pessoas. 12.331. O sistema deve suportar configuração de exibição bilíngue para grupos de contagem de pessoas. 12.332. A plataforma deve suportar exibir resultados de análise por câmeras ou por grupos de contagem de pessoas. 12.333. O sistema deve permitir classificação de grupos de recursos de ranking e câmeras de acordo com o número de pessoas que entraram e o número de pessoas que saíram. 12.334. A plataforma deve permitir configurar a direção da análise estatística como Entrando, Saindo ou Entrando & Saindo. 12.335. O sistema deve suportar exibir número de pessoas que entraram, pessoas que passaram e taxa de entrada.
--	---

	12.336. A plataforma deve suportar exibir relatórios dos tipos: Daily Report, Weekly Report, Monthly Report, Annual Report e Custom Time Interval. 12.337. O sistema deve suportar exibição de comparativos estatísticos com períodos anteriores (ontem, semana anterior, mês anterior, ano anterior e tempo customizado). 12.338. A plataforma deve permitir exibir o pico de pessoas por diferentes dimensões. 12.339. O sistema deve suportar exportação de relatórios de análise. 12.340. A plataforma deve permitir adicionar e gerenciar grupos de análise de características de pessoas. 12.341. O sistema deve suportar exibir resultados de análise por câmeras ou por grupos de análise de características de pessoas. 12.342. A plataforma deve suportar exibir relatórios de grupos de características de pessoas nos formatos Daily, Weekly, Monthly, Annual e Custom Time Interval. 12.343. O sistema deve permitir selecionar conteúdo estatístico por tempo para grupos de características de pessoas. 12.344. A plataforma deve suportar exibir resultados de análise em gráfico de pizza. 12.345. O sistema deve permitir exportação de relatórios de análise de características de pessoas. 12.346. A plataforma deve suportar seleção de múltiplas câmeras e leitores de cartão de portas selecionadas como recurso estatístico para grupos de análise de calor. 12.347. O sistema deve suportar configuração da direção como Entrando ou Saindo para recursos no grupo de análise de calor. 12.348. A plataforma deve suportar seleção de múltiplas câmeras como recurso estatístico para análise de calor. 12.349. A plataforma deve suportar exibir resultados de análise por câmeras ou por grupos de contagem de pessoas. 12.350. O sistema deve suportar classificação de grupos de recursos e câmeras de acordo com parâmetros como contagem de pessoas, tempo médio de permanência, número de pessoas que permaneceram e tempo médio de permanência. 12.351. A plataforma deve suportar três tipos de estatísticas: tempo de permanência, quantidade de pessoas e taxa média de permanência.
--	--

	12.352. O sistema deve permitir definir intervalos de tempo que serão considerados como permanência: >0s, >15s, >30s, >60s. 12.353. A plataforma deve suportar exibir mapa global de calor, permitindo vincular múltiplas câmeras ao mapa. 12.354. O sistema deve suportar exibição de diferentes cores para regiões distintas no mapa de calor, assim como visualizar mapa de calor de câmera individual. 12.355. A plataforma deve suportar exibição de comparativos estatísticos com períodos anteriores (ontem, semana anterior, mês anterior, ano anterior, promoções anteriores e tempo customizado). 12.356. O sistema deve suportar exibição do pico de pessoas e taxa de permanência por diferentes dimensões. 12.357. A plataforma deve suportar relatórios nos formatos: diário, semanal, anual e customizado. 12.358. O sistema deve suportar exportação de relatórios de análise. 12.359. A plataforma deve suportar adicionar múltiplas câmeras ao mapa e configurar suas localizações para análise de trajeto. 12.360. O sistema deve permitir relatórios de análise de trajeto nos formatos diário, semanal, anual e customizado. 12.361. A plataforma deve permitir selecionar conteúdo estatístico por tempo na análise de trajeto. 12.362. O sistema deve suportar exibir resultados de análise de trajeto no mapa, incluindo cor do calor de cada trajeto e número de pessoas em cada trajeto. 12.363. A plataforma deve suportar exportação de relatórios de análise de trajeto. 12.364. O sistema deve suportar relatórios de análise de fila nos formatos diário, semanal e anual. 12.365. A plataforma deve permitir seleção de conteúdo estatístico por tempo em relatórios de análise de fila. 12.366. A plataforma deve suportar dois tipos de análise de filas: duração de espera e comprimento da fila. 12.367. O sistema deve suportar a exibição do número de exceções, considerando situações de tempo de espera excedido. 12.368. A plataforma deve permitir a exibição da duração de espera para filas com diferentes quantidades de pessoas. 12.369. O sistema deve permitir a exibição do número de exceções quando a quantidade de pessoas ultrapassar o limite configurado.
--	---

	12.370. A plataforma deve suportar a exibição de estatísticas de contagem de pessoas em filas, considerando diferentes durações de espera. 12.371. O sistema deve permitir a exportação dos relatórios de análise de filas. 12.372. A plataforma deve suportar relatórios de análise de densidade de pessoas nos formatos diário, semanal, mensal, anual e por intervalo de tempo personalizado. 12.373. O sistema deve permitir a exibição de resultados da análise de densidade de pessoas em gráfico de linhas. 12.374. A plataforma deve permitir a exportação de relatórios de análise de densidade de pessoas. 12.375. O sistema deve suportar relatórios de análise de temperatura nos formatos diário, semanal, mensal, anual e por intervalo de tempo personalizado. 12.376. A plataforma deve permitir a seleção por hora em relatórios diários, exibindo as temperaturas máxima e mínima registradas em intervalos de um minuto. 12.377. O sistema deve permitir a exibição da quantidade de exceções detectadas nos pontos de triagem de temperatura. 12.378. A plataforma deve permitir a comparação entre a temperatura mais alta e a mais baixa registrada em diferentes pontos de triagem de temperatura. 12.379. O sistema deve permitir a exportação de relatórios de análise de temperatura. Módulo de busca avançada 12.380. Deverá ainda de forma integrada a Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, ofertar módulo de inteligência baseado em tecnologia de inteligência artificial de larga escala, com as seguintes funcionalidades: 12.381. A solução deverá possibilitar a realização de pesquisas em registros de vídeo por meio de interpretação em linguagem natural, incluindo a capacidade de identificação e localização rápida de diferentes alvos como pessoas, veículos, veículos não motorizados, animais e objetos, estabelecendo correlação entre textos de entrada e conteúdos audiovisuais. 12.382. A plataforma deverá viabilizar a pesquisa em registros de visitantes utilizando linguagem natural, contemplando a extração de informações individuais e registros de captura, além da busca avançada de pessoas por meio de imagens faciais previamente armazenadas.
--	---

	12.383. A aplicação deverá disponibilizar funcionalidades para consulta de registros de acesso mediante uso de linguagem natural, contemplando dados de identificação de pessoas e respectivos registros de captura, incluindo mecanismos de busca para reconhecimento e associação de imagens faciais a registros de interesse. 12.384. O software deverá oferecer a possibilidade de armazenar e recuperar textos de pesquisa frequentemente utilizados, permitindo a configuração destes como favoritos de forma a otimizar consultas recorrentes. 12.385. A ferramenta deverá contemplar a capacidade de processar consultas em múltiplos idiomas no âmbito da pesquisa textual, assegurando abrangência no atendimento a diferentes contextos linguísticos. Módulo para gerenciamento de videowall 12.386. A plataforma deve ser capaz de realizar a detecção e integração de dispositivos em rede local, abrangendo funcionalidades como identificar automaticamente equipamentos disponíveis, adicionar manualmente via endereço IP, segmento e porta, bem como estabelecer configuração remota para decodificadores de vídeo, controladores de painel e visualização de status de sinal e saídas, assegurando integração plena com a infraestrutura de vídeo. 12.387. O sistema deve oferecer gestão avançada de painel LCD, abrangendo a inclusão, edição e remoção de murais, definição em lote das resoluções de saída dos decodificadores e associação dinâmica entre janelas de exibição e recursos de decodificação, permitindo inclusive a liberação dessa vinculação conforme necessidade operacional. 12.388. Deve haver suporte à configuração de portas de áudio dedicadas ao painel, bem como à definição de parâmetros estéticos e informativos da exibição, incluindo a aplicação de cores de fundo ou imagens de referência nas áreas de exibição. 12.389. A solução deve assegurar controle sobre as portas de decodificação utilizadas, com possibilidade de exibição em tela cheia, configuração do tipo de fluxo (principal/sub) e alternância automática em caso de indisponibilidade, garantindo continuidade operacional. 12.390. O sistema deve viabilizar a sobreposição do identificador de câmeras no painel, a exportação e armazenamento dessas identificações, bem como a reprodução programada de janelas de vídeo em horários previamente definidos, respeitando a janela de tempo configurada.
--	---

	12.391. A plataforma deve ser capaz de executar reproduções em lote de vídeos já gravados, apresentando-os em sequência nas janelas do painel a partir de um layout previamente especificado, garantindo consistência na exibição de arquivos históricos. 12.392. O sistema deve contemplar modos de divisão de tela predefinidos, como 4/9/16/36 janelas, além de permitir bloqueio de janelas, redimensionamento, ampliação e restauração de sub-janelas de forma dinâmica e em tempo real. 12.393. A plataforma deve admitir a criação de janelas móveis (“roaming”), com recursos para movimentação, alteração de tamanho e fixação na parte superior ou inferior da tela, garantindo flexibilidade de exibição em ambientes de vigilância de alta demanda. 12.394. O sistema deve permitir a habilitação e desabilitação de regras de análise de vídeo (VCA) diretamente nas janelas do painel, assegurando integração entre visualização e inteligência embarcada. 12.395. O sistema deve permitir a exibição de número de janela, apresentação de fontes de vídeo locais ou remotas (ONVIF, protocolo proprietário ou nome de domínio), além de possibilitar controle de auto-switching de fluxos de vídeo de câmeras em janelas individuais ou múltiplas, ajustando parâmetros de continuidade, repetição e ordem de exibição. 12.396. A plataforma deve contemplar recursos avançados como alternância entre fluxos principal/sub de uma mesma fonte, suporte a controle PTZ e personalização da exibição de identificadores de câmeras diretamente no painel. 12.397. Deve haver capacidade de exibir imagens do cliente em diferentes modos (painel principal, painel de reprodução ou painel de backup), mantendo consistência de apresentação entre decodificação de saídas e estados de sinal, além de permitir adição de elementos gráficos como logotipos e cores de fundo personalizados. 12.398. O painel deve permitir exibição de desktop remoto e suas janelas em tela cheia, assegurando integração entre aplicações de PC e o sistema de vídeo wall. 12.399. O sistema deve oferecer aplicativo complementar (APP) para dispositivos móveis ou pads, capaz de alternar fontes de sinal, operar até 8 murais simultâneos, suportar murais LED e LCD, além de recursos de divisão virtual de tela, janelas dinâmicas roaming, redimensionamento e zoom interativo.
--	--

	12.400. O módulo de painel LED deve contemplar exibições estáticas ou dinâmicas, personalização de layout e funções de união de janelas, além de suportar divisão visual customizada. 12.401. O módulo de visualização (View) deve permitir criação, edição e exclusão de visualizações, alternância de exibições semanais ou em horários específicos, bem como suporte a visualizações públicas e privadas, com miniaturas exibidas ao passar o cursor sobre a lista de views. Servidor 12.402. Para operação da Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, deverão ser fornecidos dois servidores com as configurações abaixo, sendo um dedicado à aplicação do sistema e outro destinado ao banco de dados. 12.403. O servidor deve possuir formato rack 1U, adequado para instalação em racks padrão de 19". 12.404. Deve incorporar processador de última geração, no mínimo Intel Xeon E-2434 (3,4 GHz a 5,0 GHz, cache de 12 MB, 4 núcleos / 8 threads), assegurando desempenho adequado a cargas críticas de inteligência situacional. 12.405. Deve conter no mínimo 16 GB de memória DDR5 ECC UDIMM a 4400 MT/s, com suporte à expansão até 128 GB em quatro slots disponíveis. 12.406. O subsistema de armazenamento deve incluir pelo menos 2 HDDs de 2 TB 7.2K SATA em configuração RAID 1, assegurando redundância e confiabilidade, com possibilidade de expansão até 4 discos de 22 TB cada. 12.407. O servidor deve possuir duas interfaces LAN 10/100/1000 Mbps, além de porta dedicada iDRAC para gerenciamento remoto. 12.408. A fonte de alimentação deve ser redundante, 600 W Platinum, com suporte a 100–240 VAC ou 240 VDC, garantindo operação contínua. 12.409. Deve incluir interface de gerenciamento avançado iDRAC9, com suporte a telemetria, BIOS live scanning, recuperação rápida de sistema operacional, iDRAC Direct, iDRAC RESTful API com Redfish e integração com plataformas como VMware vCenter, Microsoft System Center e ServiceNow. 12.410. Deve suportar múltiplos modelos de gerenciamento, permitindo operação tanto no formato 1:1 quanto 1:Many, assegurando controle remoto completo de dispositivos.
--	---

	12.411. O equipamento deve dispor de conectividade física abrangente, incluindo iDRAC Direct (USB Micro-AB), USB 2.0 frontal, LAN redundante, VGA, USB 3.2 Gen1, Serial e USB traseiros adicionais, garantindo flexibilidade de integração. 12.412. Deve contemplar recursos de segurança de última geração, incluindo firmware assinado criptograficamente, Secure Boot, verificação de integridade de hardware, Secure Erase, Silicon Root of Trust, Data at Rest Encryption, servidor secured-core, TPM 2.0 FIPS/CC-TCG e modo System Lockdown, garantindo confiabilidade corporativa. 12.413. O servidor deve ser fornecido com licença do sistema operacional Windows Server 2019 Standard, com suporte oficial e garantia de 3 anos de plano de serviço (PSP). 12.414. Para operação da Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, deverá ainda ser previsto 3 (três) servidores para stream de vídeo de acordo com as especificações abaixo: 12.415. O servidor de stream deve possuir processador Intel Core i5-12500, operando a 3,0 GHz, cache de 18 MB, com 6 núcleos e 12 threads, assegurando desempenho em ambientes multitarefa de análises situacionais. 12.416. Deve integrar no mínimo 16 GB de memória UDIMM DDR4 a 3200 MT/s (2 × 8 GB), com suporte de expansão até 128 GB (4 × 32 GB), permitindo escalabilidade futura. 12.417. Deve possuir como configuração básica um SSD M.2 de 1 TB para sistema e aplicativos, com possibilidade de expansão para HDD SATA de até 4 TB. 12.418. A placa gráfica deve ser baseada em Intel UHD Graphics 770 integrada ao processador, assegurando capacidade de decodificação de múltiplos fluxos, com possibilidade de expansão via placa gráfica dedicada. 12.419. Deve suportar até quatro saídas independentes de vídeo (HDMI, DisplayPort e VGA), possibilitando a operação simultânea em quatro monitores distintos para gestão eficiente de imagens. 12.420. A estação deve incluir portas de conectividade diversificada, com no mínimo: 1 × Type-C, 4 × USB 3.0, 4 × USB 2.0, 1 × Porta de Áudio universal, 1 × LAN 1GbE, além de saídas de vídeo HDMI/DP/VGA. 12.421. O equipamento deve ser fornecido com sistema operacional Windows 10 multilinguagem pré-instalado, acompanhado de teclado e mouse, assegurando operação imediata (“plug and play”).
--	--

	12.422. Deve apresentar robustez ambiental, operando em faixa de temperatura de 5 °C a 45 °C e umidade de 20% a 80% sem condensação. 12.423. Deve dispor de filtros de poeira, protegendo contra partículas suspensas e poeira ambiente, assegurando longevidade em condições adversas. 12.424. A fonte de alimentação deve ser de 300 W com eficiência 92% (80 Plus Platinum), assegurando eficiência energética e operação confiável. Storage 12.425. Deverão ser fornecidos ainda 2 (dois) storages para armazenamento das imagens, sendo fornecidos cada um com 8 HDs de 16 TB. 12.426. O sistema de armazenamento deve ser projetado em arquitetura modular, com controladora única de 64 bits multi-core, cache de 16 GB expansível até 64 GB, assegurando escalabilidade e estabilidade para cargas críticas de videomonitoramento. 12.427. Deve possuir 24 slots hot-swap para HDDs corporativos (enterprise class), compatíveis com capacidades entre 4 TB e 20 TB, com suporte a discos de até 20 TB, permitindo expansão de longo prazo e manutenção sem interrupção. 12.428. O storage deve suportar múltiplos níveis de RAID corporativo (0, 1, 5, 6, 10, 50, VRAID 2.0 e Hot-Spare), assegurando proteção avançada de dados e alta disponibilidade. 12.429. A solução deve ser capaz de processar até 550 canais de vídeo (≈1100 Mbps) em gravação contínua, com suporte a gravação simultânea de eventos e imagens, assegurando desempenho para grandes parques de câmeras. 12.430. O sistema deve possibilitar desempenho de cópia de segurança (copy-back) em até 275 canais (≈550 Mbps), assegurando eficiência na redundância de dados e transferência para unidades externas. 12.431. O storage deve suportar até 200 canais em modo de evento (≈400 Mbps), com mecanismos de proteção de vídeo incluindo ANR, detecção de perda de vídeo e bloqueio de gravações críticas. 12.432. Deve oferecer 4 interfaces de rede 2,5 GbE; assegurando conectividade de alto desempenho e gestão remota. 12.433. O sistema deve contemplar recursos de backup agendado para transferência automática de gravações históricas de dispositivos, sem necessidade de servidor intermediário. 12.434. Deve suportar protocolos abertos RTSP, ONVIF, SDK, permitindo integração com câmeras e sistemas de múltiplos fabricantes.
--	--

	12.435. O equipamento deve ser fornecido em gabinete 4U, com fonte de alimentação redundante de 550 W, consumo em operação ≤ 674 W.
13	13. Central de monitoramento 13.1. A Central de Monitoramento será composta por: 06 monitores 55" com suporte e decodificador de vídeo; Monitor 13.2. O display LCD profissional, na solução ofertada, deve ser do mesmo fabricante do Encoder e ser totalmente compatível com a Plataforma de Monitoramento. Deve também, ser fornecido com suporte de parede do mesmo fabricante (ou plenamente compatível), garantindo perfeita fixação. 13.3. O tamanho da tela deve possuir o tamanho de 55" (cinquenta e cinco) na diagonal. 13.4. Deve possuir borda com design de moldura extremamente estreita de, no máximo, 1 mm. 13.5. Deve possuir display LCD de alta definição de uso profissional. 13.6. Deve possuir aplicação de uso 24h. 13.7. Deve possuir resolução de 1920×1080; 13.8. Deve possuir brilho de, no mínimo, 500 cd/m². 13.9. Deve possuir profundidade de cor de 10bit. 13.10. Deve possuir contraste mínimo de, no mínimo, 1000 por 1. 13.11. Deve possuir Tempo de Resposta: 8 ms. 13.12. Deve possuir, ao menos, as seguintes entradas: 1 HDMI, 1 DVI, 1 VGA e 1 DP e 1 USB. 13.13. Suportar alimentação de entrada na faixa de 100 a 240 VCA ~ 60Hz. 13.14. Deve operar em faixa de temperatura de 0° a 40° C. 13.15. Acessórios deverão ser do mesmo fabricante do display LCD profissional, ou homologados pela mesma, garantindo a qualidade da solução. 13.16. A solução deve compor toda a infraestrutura e acessórios necessários para a perfeita instalação e funcionamento da solução, seguindo as boas práticas, normas e recomendações dos fabricantes que compõem a solução. 13.17. Visando a qualidade e garantia de continuidade de atualizações e suporte, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros.

	Decoder: 13.18. O decoder, na solução ofertada, deverá ser totalmente compatível com as câmeras e a Plataforma de Monitoramento. Deve operar de forma autônoma e autossuficiente, unicamente com os recursos de hardware e software internos contidos em seu gabinete, com desempenho pleno e integral de suas funções. 13.19. O sistema deverá acomodar entradas de vídeo de estações de trabalho, terminais de videoconferência e fontes HDMI 4K. 13.20. O sistema deverá utilizar câmeras IP, appliances NVR e dispositivos em rede como origens de sinal. 13.21. O sistema deverá entregar saída via HDMI 1.4 e suportar vídeo UHD 4K. 13.22. O sistema deverá empregar H.264 como formato padrão, com suporte opcional a H.265, e permitir codificação de fluxo principal e subfluxo. 13.23. O sistema deverá oferecer pelo menos 100 canais de decodificação de vídeo simultâneos. 13.24. O sistema deverá suportar a junção (splicing) de fontes de sinal no vídeo-wall, a abertura de janelas de fonte de sinal, o roaming de janelas, a alternância de cena e a troca de janelas de sinal. Cada tela deverá suportar até quatro janelas de fonte em 1080p ou duas janelas em 4K. 13.25. Cada janela de fonte de sinal deverá poder ser subdividida em layouts de 1, 2, 4, 6, 8, 9, 12, 16, 25 ou 36 sub-janelas. 13.26. O sistema deverá permitir a configuração dos estados de visualização ao vivo, decodificação, comutação, áudio e a posição de cada janela de fonte de sinal. 13.27. A unidade deverá disponibilizar, no mínimo, duas interfaces Ethernet autonegociáveis em faixa aproximada de 10 – 1000 Mbps (conector padronizado RJ-45) e duas portas ópticas operando em faixa aproximada de 100 – 1000 Mbps. 13.28. A unidade deverá prover no mínimo 6 interfaces de alarme de entrada e 6 de saída, além de interfaces seriais modulares configuráveis para RS-232 e RS-485 (conector tipo modular) e múltiplas portas USB 2.0. 13.29. A unidade deverá suportar, no mínimo, 08 interfaces de saída de vídeo independentes. 13.30. Acessórios deverão ser do mesmo fabricante do decoder, ou homologados pela mesma, garantindo a qualidade da solução. 13.31. A solução deve compor toda a infraestrutura e acessórios necessários para a perfeita instalação e funcionamento da solução, seguindo as boas práticas, normas e recomendações dos fabricantes que compõem a solução.
--	---

	13.32. Os firmwares de atualização de produto, devem ser criptografados ou autenticados, para que as informações críticas incluídas, não possam ser arbitrariamente analisadas, falsificadas ou violadas. 13.33. Visando a qualidade e garantia de continuidade de atualizações e suporte, bem como a responsabilidade acerca da segurança cibernética, é imperativo que o fabricante tenha pleno domínio dos processos de desenvolvimento e manufatura do produto, tanto a nível de hardware quanto de software, não sendo aceitos produtos baseados em OEM, ou apenas "montados", utilizando tecnologia de terceiros.
14	14. Estação de trabalho 14.1. A Estação de Trabalho será composta por: 01 computador, 02 monitores, 01 headset, 01 joystick e 01 kit com mouse e teclado; Computador 14.2. O equipamento deve possuir processador Intel Core i5-12500, operando a 3,0 GHz, cache de 18 MB, com 6 núcleos e 12 threads, assegurando desempenho em ambientes multitarefa de análises situacionais. 14.3. Deve integrar no mínimo 16 GB de memória UDIMM DDR4 a 3200 MT/s (2 × 8 GB), com suporte de expansão até 128 GB (4 × 32 GB), permitindo escalabilidade futura. 14.4. Deve possuir como configuração básica um SSD M.2 de 1 TB para sistema e aplicativos, com possibilidade de expansão para HDD SATA de até 4 TB. 14.5. A placa gráfica deve ser baseada em Intel UHD Graphics 770 integrada ao processador, assegurando capacidade de decodificação de múltiplos fluxos, com possibilidade de expansão via placa gráfica dedicada. 14.6. Deve suportar até quatro saídas independentes de vídeo (HDMI, DisplayPort e VGA), possibilitando a operação simultânea em quatro monitores distintos para gestão eficiente de imagens. 14.7. A estação deve incluir portas de conectividade diversificada, com no mínimo: 1 × Type-C, 4 × USB 3.0, 4 × USB 2.0, 1 × Porta de Áudio universal, 1 × LAN 1GbE, além de saídas de vídeo HDMI/DP/VGA. 14.8. O equipamento deve ser fornecido com sistema operacional Windows 10 multilinguagem pré-instalado, acompanhado de teclado e mouse, assegurando operação imediata ("plug and play").

	14.9. Deve apresentar robustez ambiental, operando em faixa de temperatura de 5 °C a 45 °C e umidade de 20% a 80% sem condensação, além de tolerância a armazenamento em condições extremas (-40 °C a 70 °C e 5% a 95% UR). 14.10. Deve dispor de filtros de poeira personalizados, protegendo contra partículas suspensas e poeira ambiente, assegurando longevidade em condições adversas. 14.11. A fonte de alimentação deve ser de 300 W com eficiência 92% (80 Plus Platinum), assegurando eficiência energética e operação confiável. Headset 14.12. Deve ser fornecido com um headset com, no mínimo, as seguintes características técnicas: 14.12.1. Tipo on-ear com haste ajustável, acolchoamento em couro sintético e design ergonômico para uso prolongado; 14.12.2. Conectividade via USB-C; 14.12.3. Microfone com cancelamento de ruído baseado em IA; 14.12.4. Alto-falantes com resposta de frequência adequada para voz / conversação (100Hz - 8kHz); 14.12.5. Controles integrados no cabo para ajuste de volume, mute do microfone e atendimento de chamadas; 14.12.6. Cabo com comprimento mínimo de 1,5 metro; 14.12.7. Peso máximo de 150 gramas; Joystick 14.13. Deve ser fornecido com um joystick com, no mínimo, as seguintes características técnicas: 14.13.1. Joystick de quatro eixos com botão integrado para controle de câmeras PTZ e navegação em menus; 14.13.2. Deve possuir de porta USB 2.0; 14.13.3. Estrutura em material de alta resistência, adequado para operação contínua em centrais de monitoramento; 14.13.4. Alimentação externa em 12 VDC; 14.13.5. Deve ser compatível com sistemas baseados em Linux; 14.13.6. Faixa de temperatura operacional entre 0 °C e 50 °C; Monitor 14.14. Deve ser fornecido com dois monitores com, no mínimo, as seguintes características técnicas:
--	---

	14.14.1. Tamanho de tela de 27 polegadas, tecnologia de painel IPS com tratamento antirreflexo; 14.14.2. Resolução nativa Full HD (1920 × 1080), proporção de 16:9, brilho típico de 300 cd/m2 e contraste típico de 1500:1; 14.14.3. Ângulo de visão de 178° horizontal e vertical; 14.14.4. Conectividade mínima: 2 portas HDMI 1.4; 14.14.5. 2 alto-falantes integrados com potência mínima de 2 × 5 W; 14.14.6. Ajuste de inclinação de pelo menos -5° a +21°; Demais itens 14.15. Cada estação deverá incluir teclado e mouse.
15	15. Serviço de projeto executivo 15.1. O presente item contempla a elaboração do Projeto Executivo de implantação do sistema de videomonitoramento e correlatos, abrangendo todas as unidades do SESC-DF contempladas nesta contratação. O projeto deverá detalhar tecnicamente a instalação, integração e operação dos equipamentos e softwares previstos, fornecendo documentação completa e padronizada para execução, fiscalização e futuras manutenções. 15.2. Cada unidade (endereço) compreenderá a contratação de uma unidade do serviço de projeto executivo. Escopo do serviço 15.3. Levantamento in loco nas unidades indicadas pelo SESC-DF, com verificação de condições reais de infraestrutura, cabeamento, energia elétrica e pontos de instalação. 15.4. Apontamento das melhorias de infraestrutura necessárias para providências da contratante. 15.5. Elaboração de plantas baixas e desenhos técnicos indicando a posição exata dos dispositivos (câmeras, alto-falantes, switches, racks, NVRs, servidores, storages, estações de trabalho, central de monitoramento). 15.6. Diagrama lógico da solução, contemplando topologia de rede, interligações físicas e lógicas, fluxos de dados e integrações entre os componentes da plataforma. 15.7. Memorial descritivo contendo justificativas técnicas para os posicionamentos definidos, critérios de desempenho (incluindo DORI para câmeras), normas aplicadas (ABNT, ISO, NBR específicas) e parâmetros de segurança da informação.

	15.8. Cronograma executivo sugerindo ordem de execução por unidade, levando em conta prazos, restrições de operação do SESC-DF e minimização de impactos ao funcionamento das unidades. 15.9. Anotação de Responsabilidade Técnica (ART) ou equivalente, emitida por profissional habilitado, abrangendo todo o escopo do projeto. Material de apoio 15.10. O SESC-DF fornecerá as plantas arquitetônicas das unidades em arquivos editáveis (formato DWG, DGN ou equivalente). 15.11. A contratada deverá utilizar essas plantas como base para inserção dos elementos do projeto executivo. Condições gerais 15.12. As visitas técnicas para levantamento deverão ser previamente agendadas com o SESC-DF, respeitando os horários de funcionamento das unidades. 15.13. Todos os documentos deverão ser entregues em versão editável (DWG/DOCX/XLSX ou equivalentes) e em PDF não editável para arquivo oficial. 15.14. O Projeto Executivo deverá ser submetido à aprovação formal do SESC-DF, podendo ser exigidas revisões até sua homologação final.
16	16. Serviço de instalação de 10 dispositivos 16.1. Compreende os serviços necessários para a instalação física, em ambiente interno ou externo, e configuração de 10 dispositivos IP. Entende-se por dispositivos IP: câmeras, alto-falantes. Escopo do serviço 16.2. Planejamento e preparação: validação prévia dos pontos de instalação junto ao contratante, análise de campo de visão, cobertura acústica e avaliação de infraestrutura disponível (energia e rede). 16.3. Fixação mecânica: instalação dos suportes homologados pelo fabricante ou aprovados pelo contratante, em postes, paredes ou tetos, garantindo resistência a intempéries, vibração e vandalismo. 16.4. Infraestrutura elétrica e lógica: realização da conexão de rede (PoE ou fonte dedicada) em circuito elétrico existente, incluindo aterramento existente, e conexão em ponto de rede existente. 16.5. Configuração inicial: atribuição de endereços IP estáticos, atualização de firmware homologado, criação de credenciais seguras e sincronização de data/hora via NTP.

	16.6. Ajustes técnicos: parametrização de imagem (resolução, fps, bitrate, WDR, ROI), calibração de áudio (quando aplicável), testes de detecção de eventos analíticos embarcados e verificação de transmissão ao NVR/VMS. 16.7. Integração: registro dos dispositivos na plataforma de gerenciamento central (VMS/NVR), configuração dos fluxos de vídeo e áudio, alarmes e eventos associados. 16.8. Testes e validação: verificação funcional de cada dispositivo, incluindo visualização ao vivo, gravação, reprodução, emissão de áudio, e validação do enquadramento segundo critérios DORI (no caso de câmeras). 16.9. Documentação: registro fotográfico da instalação, entrega de relatório contendo modelo, número de série, localização física, endereço IP e parâmetros configurados de cada dispositivo. 16.10. Treinamento básico: orientação à equipe técnica designada pelo contratante quanto ao acesso, operação e ajustes primários de imagem e áudio. Condições gerais 16.11. A contratada deverá providenciar todas as ferramentas, insumos e equipamentos necessários para a execução dos serviços, incluindo EPIs, escadas, andaimes, instrumentos de medição e teste, materiais de fixação e proteção, sem ônus adicional ao contratante. 16.12. Em caso de serviços executados em altura, os profissionais deverão cumprir integralmente todas as normas vigentes de segurança do trabalho, incluindo NR-35 (trabalho em altura) e demais legislações correlatas. 16.13. A contratada é responsável pela recomposição de qualquer área afetada pela instalação, mantendo acabamento compatível com o existente. 16.14. O serviço deverá atender integralmente às normas técnicas aplicáveis, incluindo ABNT NBR 5410 (instalações elétricas de baixa tensão), ABNT NBR ISO/IEC 27001 (segurança da informação, quando aplicável) e demais regulamentações específicas do setor. 16.15. Os serviços deverão ser executados preferencialmente em horário comercial, exceto aqueles que possam causar perturbação ao funcionamento normal do SESC (como excesso de ruído). Nestes casos, deverá ser acordada e programada uma janela de serviço fora do horário de expediente. 16.16. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo
--	--

	integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade. 16.17. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 16.18. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens. 16.19. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: c) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e d) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 16.20. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono. Limitações do escopo: 16.21. Não faz parte deste escopo o fornecimento ou adequação de pontos de rede lógica, alimentação elétrica ou infraestrutura mecânica (tais como postes,
--	---

	tubulações, eletrocalhas ou canaletas), exceto pelo uso de elementos de acabamento estritamente necessários à fixação final do dispositivo instalado. 16.22. Caso sejam identificadas necessidades adicionais de infraestrutura durante a execução, estas deverão ser informadas ao contratante para providências ou contratação em separado.
17	17. Serviço de instalação de NVR 17.1. Compreende os serviços necessários para a instalação física, configuração inicial e integração de um NVR (Network Video Recorder), incluindo os discos rígidos fornecidos com o equipamento, no ambiente de videomonitoramento do contratante. Escopo do serviço 17.2. Preparação e posicionamento: validação do local designado pelo contratante para instalação, quanto à ventilação adequada, segurança física e acessibilidade para manutenção. 17.3. Fixação mecânica: instalação do NVR no rack designado pelo contratante, utilizando trilhos, parafusos ou suportes adequados para garantir fixação segura. 17.4. Instalação de discos rígidos: montagem dos discos rígidos internos conforme orientação do fabricante, configuração de arranjos de armazenamento (RAID ou JBOD, quando aplicável) e teste de reconhecimento pelo sistema. 17.5. Conexões físicas: realização das conexões de rede, energia e interfaces auxiliares previstas em projeto, com organização dos cabos no rack utilizando guias, canaletas ou abraçadeiras apropriadas. 17.6. Configuração inicial: atribuição de endereço IP estático, atualização de firmware homologado, criação de credenciais seguras, ajuste de data/hora com sincronização NTP e configuração de parâmetros de armazenamento (retenção, sobregravação, partições de disco). 17.7. Integração e testes: registro de câmeras IP no NVR conforme projeto, configuração de parâmetros de gravação (contínua, por evento ou agendada), testes de gravação, reprodução, exportação e integração com sistema de gerenciamento central (VMS/NVR). 17.8. Documentação: registro fotográfico da instalação e entrega de relatório contendo modelo, número de série, versão de firmware, endereços IP e configuração de armazenamento aplicada.

	17.9. Treinamento básico: orientação à equipe técnica designada pelo contratante quanto ao acesso ao NVR, navegação na interface, busca de gravações e exportação de evidências. Condições gerais 17.10. O NVR será instalado em local e rack previamente designado pelo contratante. 17.11. A contratada deverá providenciar todas as ferramentas, insumos e EPIs necessários para a execução dos serviços. 17.12. Os serviços deverão ser executados preferencialmente em horário comercial. 17.13. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade. 17.14. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 17.15. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens. 17.16. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: e) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e f) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de
--	--

	vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 17.17. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono. Limitações do escopo: 17.18. Não faz parte deste escopo o fornecimento ou adequação de pontos de rede lógica, alimentação elétrica ou infraestrutura mecânica. 17.19. Caso sejam identificadas necessidades adicionais de infraestrutura durante a execução, estas deverão ser informadas ao contratante para providências ou contratação em separado.
18	18. Serviço de instalação da plataforma de gerenciamento 18.1. Compreende os serviços necessários para a instalação física, configuração inicial, integração e validação da Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, assegurando seu pleno funcionamento com todos os dispositivos, servidores e storages associados. 18.2. Os servidores e storages que compõem a solução deverão ser instalados e mantidos em operação em Data Center externo às dependências do SESC-DF, ficando sob inteira responsabilidade da contratada quanto à sua hospedagem, disponibilidade, monitoramento e manutenção durante o tempo de vigência do contrato. 18.3. O Data Center utilizado deverá possuir, no mínimo, classificação Tier III (conforme padrões do Uptime Institute ou equivalente), garantindo infraestrutura redundante em energia, climatização e conectividade, além de assegurar nível elevado de disponibilidade, segurança física e lógica, e conformidade com normas aplicáveis de continuidade de negócios e proteção de dados. Escopo do serviço 18.4. Instalação de sistemas operacionais e dependências: instalação e ativação do sistema operacional especificado (Windows Server/Windows 10) e demais softwares de suporte necessários, conforme requisitos do fabricante da plataforma.

	18.5. Configuração da plataforma: 18.5.1. Instalação do software de gerenciamento central e seus módulos (análise de vídeo, BI, controle de acesso, videowall, busca avançada etc.). 18.5.2. Criação da base inicial de dados e configuração do banco de dados associado. 18.5.3. Parametrização de políticas de retenção, redundância e backup. 18.5.4. Definição de credenciais administrativas e políticas de autenticação seguras (incluindo integração com Active Directory, quando aplicável). 18.6. Integração de dispositivos e subsistemas: 18.6.1. Registro de câmeras IP, NVRs, storages, servidores de stream, estações de operação e videowalls. 18.6.2. Configuração de fluxos de vídeo, alarmes, eventos e regras de acionamento. 18.6.3. Parametrização de módulos adicionais (controle de acesso, análise inteligente, monitoramento embarcado, gestão veicular, BI). 18.7. Testes e validação: 18.7.1. Testes funcionais de gravação, reprodução, busca de eventos e exportação de evidências. 18.7.2. Validação de dashboards, relatórios, alarmes e notificações. 18.7.3. Simulação de falhas para verificar continuidade operacional (failover em cluster, RAID, redundância de energia). 18.8. Documentação - entrega de relatório técnico contendo: 18.8.1. Topologia lógica configurada. 18.8.2. Lista de dispositivos integrados (com modelo, IP, firmware). 18.8.3. Configurações de armazenamento, retenção e segurança aplicadas. 18.8.4. Perfis de usuários e permissões criados. 18.9. Treinamento básico: orientação à equipe técnica do contratante sobre operação do sistema, gerenciamento de usuários, busca de eventos e geração de relatórios. Condições gerais 18.10. Os serviços de configuração poderão ser executados de forma remota. Limitações do escopo: 18.11. Não está incluído neste escopo o desenvolvimento de integrações customizadas com sistemas de terceiros além daquelas suportadas nativamente pela plataforma.
--	--

	18.12. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade. 18.13. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 18.14. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens. 18.15. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: a) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e b) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 18.16. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono.
--	--

19	19. Serviço de instalação da central de monitoramento 19.1. Compreende os serviços necessários para a instalação física, configuração inicial, integração e validação da Central de Monitoramento (VCIM), composta por monitores profissionais e decodificadores de vídeo, assegurando seu pleno funcionamento com a plataforma de gerenciamento e os dispositivos de campo. Escopo do serviço 19.2. Preparação e instalação física: 19.2.1. Instalação dos monitores profissionais de 55" em suportes de parede homologados, conforme layout aprovado pelo contratante. 19.2.2. Fixação e alinhamento de acordo com a composição do videowall, assegurando uniformidade estética e funcional. 19.2.3. Instalação física do decoder em rack ou local designado pelo contratante, com ventilação adequada e organização dos cabos. 19.3. Conexões físicas: 19.3.1. Conectorização de cabos HDMI/DP/DVI/VGA entre monitores e decoder. 19.3.2. Conexão do decoder às redes de dados e energia elétrica, com organização dos cabos em canaletas ou guias. 19.3.3. Verificação das interfaces Ethernet e ópticas, garantindo redundância e desempenho conforme especificações. 19.4. Configuração inicial: 19.4.1. Parametrização dos monitores para operação 24/7, incluindo ajustes de brilho, contraste, resolução e alinhamento de cor. 19.4.2. Configuração do decoder para operação com múltiplos canais simultâneos, definindo fluxos de vídeo, protocolos de transmissão (H.264/H.265) e layouts de exibição. 19.4.3. Criação de perfis de janelas e programação de cenários de exibição conforme necessidades do contratante. 19.5. Integração e testes: 19.5.1. Integração plena com a Plataforma de Gerenciamento e NVRs para exibição de fluxos de vídeo em tempo real. 19.5.2. Testes de junção (splicing), alternância de cena, roaming de janelas e exibição de múltiplos sinais. 19.5.3. Validação de recursos de alarmes, acionamentos e entradas/saídas de áudio e vídeo. 19.6. Documentação - entrega de relatório técnico contendo:
----	--

	19.6.1. Topologia de conexão, lista de equipamentos instalados (com número de série, modelo e firmware), configuração de exibição e cenários programados. 19.6.2. Registro fotográfico do videowall em funcionamento. 19.7. Treinamento básico: orientação à equipe técnica do contratante sobre operação básica do videowall, alteração de layouts, troca de cenários e acionamento de recursos do decoder. Condições gerais 19.8. A contratada deverá prover todas as ferramentas, insumos e EPIs necessários para a execução dos serviços, incluindo instrumentos de medição e fixação, sem ônus adicional ao contratante. 19.9. Deverão ser observadas integralmente as normas de segurança do trabalho. 19.10. A contratada é responsável pela recomposição de quaisquer áreas afetadas pela instalação, mantendo acabamento compatível com o existente. 19.11. Os serviços deverão ser realizados preferencialmente em horário comercial, salvo em casos que possam causar perturbação ao funcionamento do SESC, hipótese em que deverá ser programada janela de serviço fora do expediente. Limitações do escopo: 19.12. Não faz parte deste escopo o fornecimento ou adequação de infraestrutura elétrica, lógica ou mecânica (como rede elétrica dedicada, rede lógica, eletrocalhas ou tubulações), exceto pelos materiais de acabamento necessários para a conexão e fixação dos dispositivos. 19.13. Alterações estruturais no layout físico da sala de monitoramento não estão incluídas neste serviço. 19.14. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade. 19.15. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia
--	---

	elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 19.16. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens. 19.17. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: a) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e b) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 19.18. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono.
20	20. Serviço de instalação de estação de trabalho 20.1. Compreende os serviços necessários para a instalação física, configuração inicial e integração de estações de trabalho destinadas à operação da Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional, incluindo monitor, teclado, mouse e joystick profissional para controle de câmeras PTZ. Escopo do serviço 20.2. Preparação e instalação física: 20.2.1. Instalação física das estações em local designado pelo contratante, incluindo posicionamento ergonômico de monitores, teclado, mouse e joystick.

	20.2.2. Verificação das condições de ventilação e acesso seguro a pontos de energia e rede. 20.3. Conexões físicas: 20.3.1. Conectorização dos cabos de energia e rede, bem como dos periféricos (monitor, teclado, mouse e joystick). 20.3.2. Configuração de múltiplas saídas de vídeo (HDMI/DP/VGA) para operação simultânea, conforme especificação da estação. 20.4. Configuração inicial: 20.4.1. Inicialização do sistema operacional Windows 10 multilinguagem pré-instalado. 20.4.2. Criação de usuários administrativos e operacionais conforme política definida pelo contratante. 20.4.3. Aplicação de atualizações de sistema e drivers homologados pelo fabricante. 20.4.4. Configuração de antivírus e parâmetros básicos de segurança cibernética. 20.5. Integração e testes: 20.5.1. Instalação dos clientes de software da Plataforma Unificada, compatíveis com análise de vídeo, controle de acesso e monitoramento de alarmes. 20.5.2. Parametrização da estação para decodificação de múltiplos fluxos de vídeo e integração com recursos de videowall (quando aplicável). 20.5.3. Configuração e teste do joystick PTZ (via RS-485), validando as funções de Pan, Tilt e Zoom em câmeras compatíveis. 20.6. Treinamento básico: orientação à equipe técnica designada pelo contratante quanto ao uso da estação, navegação no software de gerenciamento e operação do joystick PTZ. Condições gerais 20.7. Os serviços deverão ser realizados preferencialmente em horário comercial, salvo em casos que possam causar perturbação ao funcionamento do SESC, hipótese em que deverá ser programada janela de serviço fora do expediente. 20.8. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade.
--	---

	20.9. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 20.10. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens. 20.11. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: a) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e b) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 20.12. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono. Limitações do escopo: 20.13. Não faz parte deste escopo o fornecimento ou adequação de infraestrutura elétrica, lógica ou mecânica (como rede elétrica dedicada, rede lógica, eletrocalhas ou tubulações), exceto pelos materiais de acabamento necessários para a conexão e fixação dos dispositivos.
--	---

21	21. Unidade de serviço técnico (UST) 21.1. A Unidade de Serviço Técnico (UST) será a métrica oficial para planejamento, execução, acompanhamento e pagamento de serviços técnicos especializados de customização, parametrização, integração e evolução da Plataforma Unificada de Pontos de Imagens, Acessos e Eventos de Inteligência Situacional. Escopo da UST 21.2. Customizações e parametrizações em módulos da plataforma (ex.: dashboards, relatórios, alarmes, BI, integração com AD, controle de acesso). 21.3. Desenvolvimento de novas regras de negócio, workflows e relatórios avançados. 21.4. Integrações com sistemas de terceiros por meio de APIs ou SDKs. 21.5. Evoluções funcionais (ajustes de interface, novos campos, melhorias em módulos). 21.6. Manutenção evolutiva em módulos já implantados. 21.7. Suporte especializado para ajustes finos de desempenho ou segurança. Catálogo de atividades e classificação de complexidade 21.8. O catálogo abaixo é referencial. O consumo final de UST será validado entre contratante e contratada antes da execução. 21.9. Ajuste de relatório existente, criação de usuário com regras específicas, inclusão de campo simples. • Complexidade: baixa • USTs estimadas: 1 a 2 USTs 21.10. Novo relatório com múltiplos filtros, customização de dashboard, parametrização de módulo de alarmes. • Complexidade: média • USTs estimadas: 3 a 5 USTs 21.11. Integração com sistema externo via API, criação de workflow com regras de negócio complexas, customização de BI. • Complexidade: alta • USTs estimadas: 6 a 10 USTs 21.12. Desenvolvimento de novo módulo, integração de múltiplos sistemas simultaneamente, alterações estruturais. • Complexidade: especial • USTs estimadas: >10 USTs (a definir em OS)
----	--

	21.13. Treinamento operacional da solução. • Complexidade: especial • USTs estimadas: >10 USTs (a definir em OS conforme escopo e carga horária) 21.14. Os serviços deverão ser realizados preferencialmente em horário comercial, salvo em casos que possam causar perturbação ao funcionamento do SESC, hipótese em que deverá ser programada janela de serviço fora do expediente. Medição e faturamento: 21.15. O faturamento será baseado no número de USTs executadas e homologadas, mediante aceite formal do contratante. 21.16. O consumo será registrado em relatório mensal, discriminando OS, escopo, complexidade, perfis profissionais envolvidos e quantidade de USTs consumidas. 21.17. Não serão pagas USTs referentes a serviços não homologados ou que não atendam aos requisitos definidos em OS. Condições gerais: 21.18. A contratada deverá observar normas de segurança da informação (ISO 27001, NIST, LGPD) e de boas práticas de desenvolvimento seguro. Limitações do escopo: 21.19. Alterações estruturais que impactem a arquitetura-base da solução poderão demandar negociação adicional, fora do consumo de USTs.
22	22. Serviço mensal de suporte, manutenção e sustentação (inicial) 22.1. O presente item contempla a prestação de serviços mensais de suporte técnico, manutenção corretiva e sustentação preventiva da solução implantada, incluindo plataforma, servidores, storages, NVRs, estações de trabalho, central de monitoramento e dispositivos de campo. 22.2. Esse serviço compreende serviços para a Plataforma de gerenciamento, central de monitoramento e 300 câmeras. Escopo do serviço: 22.3. Suporte técnico: 22.3.1. Atendimento remoto ou presencial para: • Solução de incidentes relacionados a falhas de sistema, configuração ou operação; • Execução de ajustes de configuração necessários para adequação de parâmetros técnicos ou analíticos;

	• Apoio direto aos usuários técnicos e operacionais na resolução de dúvidas ou dificuldades.; 22.4. Manutenção corretiva: 22.4.1. Atendimento remoto e/ou presencial para resolução de incidentes relacionados a falhas de equipamentos, comunicação, desempenho ou operação do sistema. 22.4.2. As atividades de manutenção corretiva compreendem: • Ajustes de posicionamento, ângulo de visão e/ou foco de câmeras; • Limpeza de câmeras; • Reconfiguração de parâmetros de gravação em NVRs e storages; • Reinstalação ou atualização de firmware de dispositivos (câmeras, NVRs, switches, alto-falantes IP); • Reconfiguração de regras de alarme, eventos ou dashboards que apresentarem falhas de funcionamento; • Correção de falhas em monitores e decodificadores da central de monitoramento (ex.: ausência de vídeo ou imagem distorcida); • Reajuste de licenciamento e revalidação de chaves de software na plataforma de gerenciamento; • Correção de inconsistências em relatórios, históricos ou logs da plataforma; • Verificação e troca de fontes de alimentação de dispositivos em caso de falha; • Reinstalação ou reconfiguração de estações de trabalho em caso de falha de sistema operacional ou software cliente da plataforma. • Quaisquer outras atividades de correção relacionadas aos equipamentos e sistemas objeto desse fornecimento. 22.4.3. Em caso de falha de hardware coberto pela garantia do fabricante, a contratada deverá: • Realizar a desinstalação segura do equipamento defeituoso; • Providenciar o envio à assistência técnica autorizada do fabricante; • Realizar a reinstalação e reconfiguração do equipamento quando este retornar da assistência ou for substituído pelo fabricante. • Garantir a plena reintegração do dispositivo à solução, respeitando as regras de segurança e configuração originais. 22.5. Sustentação:
--	--

	22.5.1. Atividades periódicas destinadas a garantir o funcionamento pleno da solução, prevenindo falhas e degradação de desempenho. 22.5.2. As rotinas mensais de manutenção preventiva incluirão: • Verificação de integridade dos servidores, storages, NVRs e estações de trabalho; • Conferência de atualizações críticas de firmware e software, aplicadas de forma controlada em ambiente de homologação antes da produção; • Checagem de conectividade de rede e latência entre dispositivos; • Inspeção dos dispositivos de campo (câmeras, alto-falantes, switches PoE), incluindo limpeza física de lentes, sensores e conectores quando aplicável; • Validação periódica das regras de negócio, alarmes e dashboards configurados; • Testes de redundância e failover em servidores, storages e arranjos RAID; • Revisão de logs de eventos críticos e de segurança; • Emissão de relatório técnico com as atividades realizadas, inconsistências encontradas e recomendações de melhoria. Regime de atendimento e SLA 22.6. Conforme descrito em capítulo específico do TR. Condições gerais 22.7. A contratada deverá adotar todas as medidas necessárias à proteção ambiental, bem como as precauções para evitar a ocorrência de danos ao meio ambiente e a terceiros durante a execução dos serviços, respondendo integralmente por quaisquer danos que venham a ser causados, desde que devidamente caracterizada e comprovada sua responsabilidade. 22.8. Com base na avaliação do Guia Nacional de Contratações Sustentáveis – 6ª edição e nas informações do Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), constatou-se que a implantação e operação de novos equipamentos de videomonitoramento e controle de acesso podem gerar impactos ambientais diretos e indiretos, como consumo contínuo de energia elétrica, geração de resíduos eletrônicos ao longo do ciclo de vida e emissões associadas à fabricação, transporte e instalação dos dispositivos. 22.9. Para mitigar tais impactos, será exigida a priorização de equipamentos energeticamente eficientes, com menor consumo em operação e conformidade com normas ambientais aplicáveis, além da destinação ambientalmente adequada de resíduos e embalagens.
--	--

	22.10. A contratada deverá comprovar que possui compromisso efetivo com a sustentabilidade e histórico positivo de neutralização de emissões de gases de efeito estufa (GEE). Para tanto, deverá apresentar: a) Na fase de habilitação: Certificado de Neutralização de CO₂ referente ao exercício imediatamente anterior ao da licitação, emitido por entidade certificadora reconhecida, que comprove a compensação integral das emissões anuais da empresa; e b) Ao final do contrato: Certificado de Neutralização de CO₂ relativo às emissões geradas durante a execução contratual, a ser apresentado ao final do período de vigência, também emitido por entidade certificadora reconhecida, observando padrões internacionais como Carbon Fair Standard, Gold Standard, Verified Carbon Standard (VCS) ou metodologias auditadas pela United Nations Framework Convention on Climate Change (UNFCCC). 22.11. Esta exigência está em consonância com o disposto no art. 6º, parágrafo único, da Instrução Normativa nº 01, de 19 de janeiro de 2010, garantindo que a empresa contratada não apenas compense as emissões decorrentes da execução contratual, mas também demonstre, de forma prévia e inequívoca, comprometimento contínuo com a gestão ambiental e a neutralização de sua pegada de carbono.
23	23. Serviço mensal de suporte, manutenção e sustentação (complementar) 23.1. O presente item contempla complemento de serviços de suporte, manutenção e sustentação, conforme especificação do item anterior, para um pacote adicional de até 100 câmeras.
	24. Outros requisitos gerais da solução 24.1. O fabricante do software e do hardware dos componentes do Sistema de videomonitoramento deverá possuir certificações e aderência comprovada a normas internacionais de segurança da informação e governança de dados, contemplando a ISO 27001 para gestão de segurança da informação, a ISO 27701 para gestão de informações de privacidade, a ISO 29151 voltada à proteção de dados pessoais, bem como deverá atender ainda à IEC 62443, garantindo proteção em ambientes de automação e controle. 24.2. Os equipamentos do Sistema de videomonitoramento (hardware) deverão ter total integração com a plataforma de software, de modo que permita o aproveitamento de todo o potencial do software e do hardware, além de garantir a segurança e a inviolabilidade nas operações de toda a solução.

24.3. Todos os itens descritos do Sistema de videomonitoramento (câmeras, alto-falantes, NVRs e softwares) deverão operar de forma plenamente integrada, garantindo interoperabilidade funcional e técnica entre os componentes ofertados. Para comprovar tal integração, a LICITANTE deverá apresentar, juntamente com a proposta, Declaração de Compatibilidade de Integração emitida pelos fabricantes dos equipamentos e sistemas propostos, em papel timbrado, assinada por representante legal. A declaração deverá citar nominalmente todos os dispositivos, sistemas e módulos propostos, confirmando sua compatibilidade com a Plataforma de VMS. A não apresentação da declaração, ou a apresentação em desacordo com os critérios estabelecidos, acarretará a desclassificação da proposta.

24.4. Deve comprovar que a solução ofertada dispõe de interface para integração via API, devidamente documentada em ambiente web ou nativa da aplicação de controle. A demonstração deverá abranger obrigatoriamente os seguintes pontos:

24.4.1. Apresentação da documentação técnica das APIs, acessível por meio de navegador web ou cliente, organizada por categorias de recursos e com exemplos de requisições e respostas nos formatos padrão (JSON/HTTPS).

24.4.2. Demonstração de ambiente nativo da própria solução para testes de chamadas de API (simulador de requisições REST), com autenticação segura, permitindo realizar requisições, visualizar respostas e validar comportamentos sem necessidade de ferramentas externas.

24.4.3. Exibição da interface de gerenciamento de credenciais e permissões de acesso à API, permitindo a geração e revogação de chaves (token, AppKey ou equivalente), com controle granular de escopo e segurança baseado em níveis de autorização.

24.5. A demonstração deve comprovar que esses recursos fazem parte nativamente da plataforma ofertada, sem necessidade de aquisição de licenças adicionais, customizações ou integrações com sistemas de terceiros.

25.Requisitos de IA

25.1. Os Modelos de Inteligência Artificial de Grande Escala utilizados no projeto deverão possuir certificação internacional que comprove a qualidade de sua operação e desenvolvimento. Entre as certificações aceitas estão: CSA, AIC4, CAICT ou AI RMF do NIST. Essas certificações têm como objetivo assegurar a qualidade e confiabilidade da solução de IA fornecida pela CONTRATADA.

25.2. Os Modelos de Inteligência Artificial de Larga Escala devem integrar recursos de percepção multimodal, possibilitando a obtenção e o processamento de dados em diferentes formatos. Devem ser capazes de fundir imagem e texto para aumentar a

eficiência na recuperação de informações, realizando a comparação e calibração entre grandes volumes de imagens e suas descrições textuais correspondentes. As imagens deverão ser codificadas em recursos não estruturados (como contornos, texturas e cores), enquanto os textos deverão ser codificados em recursos estatísticos (como ordem de palavras e gramática).

ANEXO II AO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

GERÊNCIA DE COMPRAS E CONTRATOS

PREGÃO ELETRÔNICO Nº __/2025

A empresa [RAZÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente CONTRATADA, por tomar conhecimento de informações sobre o ambiente computacional do Serviço Social do Comércio – Administração Regional do DF, doravante denominado simplesmente CONTRATANTE, aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste **TERMO DE CONFIDENCIALIDADE E SIGILO** é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CONTRATANTE reveladas à CONTRATADA em razão da execução dos serviços objeto do contrato n.º __/20__, doravante denominado simplesmente CONTRATO, bem como assegurar o respeito às normas de segurança vigentes naquele órgão durante a realização dos serviços.

2. A expressão “informação restrita” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, dentre outros.

3. A CONTRATADA compromete-se a não reproduzir e/ou dar conhecimento a terceiros, sem a anuência formal e expressa do CONTRATANTE, das informações restritas reveladas.

4. A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no CONTRATO, as informações restritas reveladas.
5. A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CONTRATANTE, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.
6. A CONTRATADA declara conhecer e se compromete a seguir e divulgar entre seus colaboradores envolvidos na execução do CONTRATO a Política Corporativa de Segurança da Informação do CONTRATANTE e normativos correlatos.
7. A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo, conforme especificado no instrumento convocatório do processo licitatório que deu origem ao CONTRATO.
8. A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo estabelecidas neste Termo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.
9. A CONTRATADA obriga-se a informar ao CONTRATANTE a relação de colaboradores que estarão envolvidos na execução do CONTRATO e a fornecer ao CONTRATANTE a Declaração de Ciência do Termo de Manutenção de Sigilo e das Normas de Segurança Vigentes de cada colaborador.
10. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONTRATANTE, ou uso inadequado de conta de acesso ao ambiente computacional do CONTRATANTE, possibilitará a imediata rescisão de qualquer contrato firmado entre o CONTRATANTE e a CONTRATADA sem qualquer ônus para o CONTRATANTE. Nesse caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridas pelo CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.
11. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONTRATANTE, possibilitará a imediata rescisão de qualquer contrato firmado entre o CONTRATANTE e a CONTRATADA sem qualquer ônus

para o CONTRATANTE. Nesse caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridas pelo CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

12. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CONTRATANTE.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a CONTRATADA assina o presente termo através de seus representantes legais.

Brasília, ____ de _____ de 2025.

[NOME DA EMPRESA CONTRATADA]

Nome:

Nome:

ANEXO III AO TERMO DE REFERÊNCIA
MODELO DE TERMO DE CIÊNCIA

GERÊNCIA DE COMPRAS E CONTRATOS

PREGÃO ELETRÔNICO Nº _/2025

A _____, inscrita no CNPJ sob o n.º _____, com sede _____, _____, por intermédio de seu representante legal _____, portador da Cédula de Identidade n.º _____, expedida pela _____ e CPF n.º _____, DECLARA para fins de atendimento aos procedimentos internos de gestão contratual e, ainda, ao _____, que se compromete a manter em sigilo, ou seja, não revelar ou divulgar as informações identificadas como confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços no SESC-AR/DF, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a ele se referem.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o SESC-AR/DF de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, custas e despesas que porventura venha sofrer como resultado da violação do disposto neste instrumento.

Brasília, ____ de _____ de 2025

Assinatura do representante legal

ANEXO IV AO TERMO DE REFERÊNCIA

MODELO DE PROPOSTA DE PREÇO

GERÊNCIA DE COMPRAS E CONTRATOS

PREGÃO ELETRÔNICO Nº _/2025

Proposta que faz a empresa _____ para a contratação de serviços técnicos e organizacionais especializados para a captura, processamento, tratamento, transmissão e armazenamento de imagens, com implantação de processamento e regras de negócios para geração e sinalização de alertas e *dashboards* operacionais, com foco nas disciplinas e necessidades mantidas pelo SESC-AR/DF, pelo prazo de contrato será 12 (doze) meses, a contar da data da última assinatura eletrônica/digital, sendo prorrogada obrigatória e automaticamente por períodos iguais e sucessivos, pelo período mínimo de 36 (trinta e seis) meses, incluídos a disponibilização de suporte técnico, em formato aquisição de hardware/aquisição de software, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência, Anexo I do Edital, conforme tabela abaixo:

LOTE ÚNICO				
Item	Descrição de itens	Qtd	R\$ Unit.	R\$ total
1.1	Conjunto para monitoramento perimetral	61		
1.2	Câmera tipo 2	62		
1.3	Câmera tipo 3	19		
1.4	Câmera tipo 4	428		
1.5	Câmera tipo 5	162		
1.6	Câmera tipo 6	49		
1.7	Câmera tipo 7	41		
1.8	Switch	52		
1.9	NVR tipo 1	05		

1.10	NVR tipo 2	07		
1.11	NVR tipo 3	02		
1.12	Plataforma de gerenciamento	01		
1.13	Central de monitoramento	01		
1.14	Estação de trabalho	11		
1.15	Serviço de projeto executivo	12		
1.16	Serviço de instalação de 10 dispositivos	95		
1.17	Serviço de instalação de NVR	14		
1.18	Serviço de instalação da plataforma de gerenciamento	1		
1.19	Serviço de instalação da central de monitoramento	1		
1.20	Serviço de instalação de estação de trabalho	11		
1.21	Unidade de serviço técnico (UST)	1000		
1.22	Serviço mensal de suporte, manutenção e sustentação (inicial)	36		
1.23	Serviço mensal de suporte, manutenção e sustentação (complementar)	252		
VALOR TOTAL:				

(anexar catálogos dos equipamentos e softwares ofertados).

Declaramos que atenderemos a todos os dispositivos constantes do Termo de Referência, Anexo I do Edital de Pregão Eletrônico nº __/2025.

Declaramos que os preços contidos nesta Proposta incluem todos os custos e despesas referentes ao objeto da licitação, tais como: custos diretos e indiretos, tributos incidentes, taxa de administração, transporte, mão de obra, encargos sociais, trabalhistas, seguros, lucro e outros necessários ao cumprimento integral do objeto.

Prazo de validade da proposta: __ dias (não inferior a 60 dias).

DADOS DA EMPRESA:

Razão Social:

Inscrição Estadual:

CNPJ:

Endereço:

E-mail:

Telefone:

Dados bancários:

Local e data, _de ____de 2025.

Assinatura do representante legal