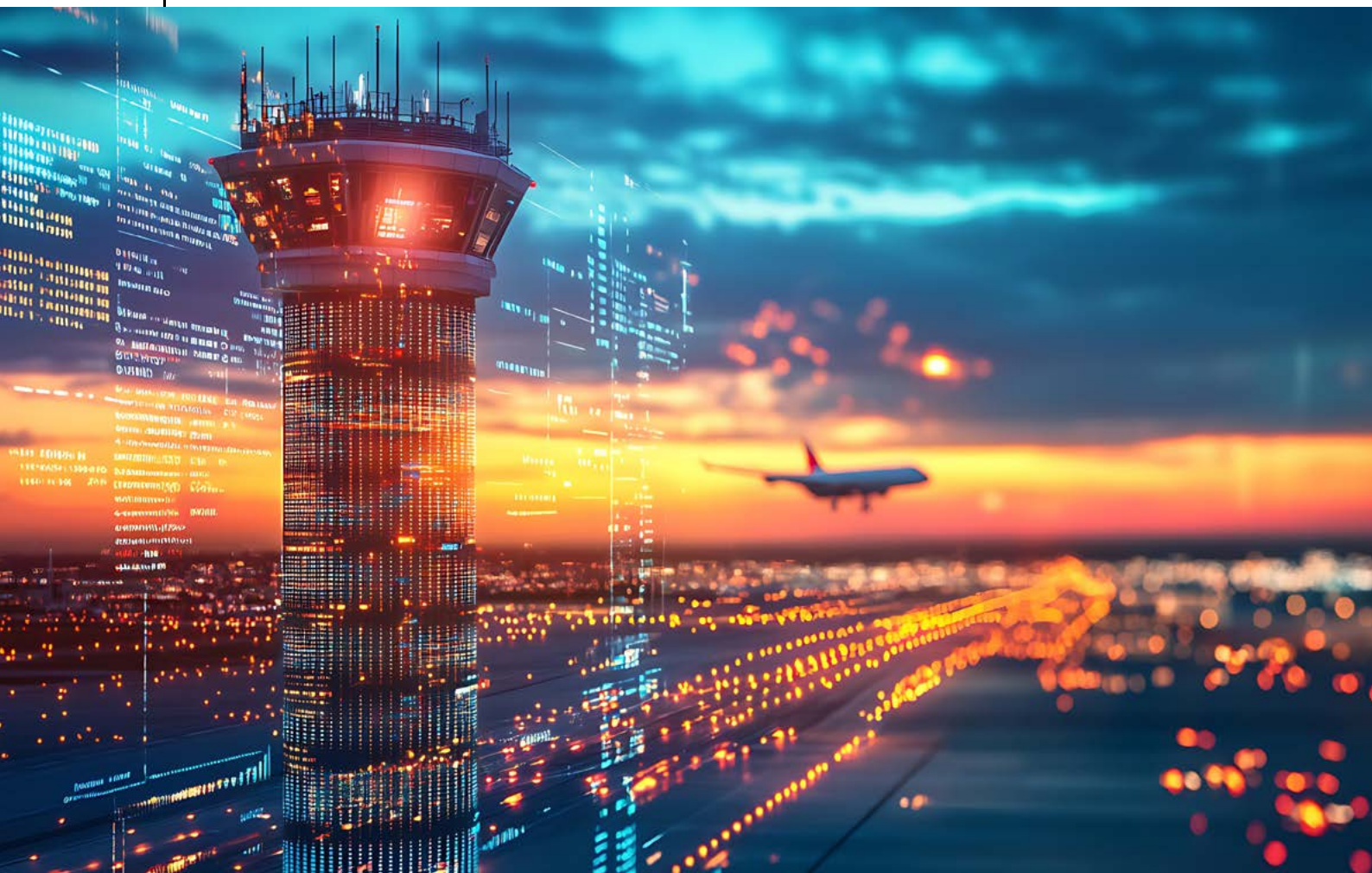


Manual sobre SOLUÇÕES TECNOLÓGICAS PARA REALIZAÇÃO DE VISTORIAS DO PERÍMETRO OPERACIONAL AEROPORTUÁRIO



Brazilian Aviation Security Team – BAsET

Manual sobre soluções tecnológicas para realização de vistorias do perímetro operacional aeroportuário

Trabalho de conclusão do estudo desenvolvido pelo Subgrupo nº 1 do BAsET (Ciclo 2024/2025) com tema relacionado à utilização de novas tecnologias para execução de vistorias e rondas no perímetro operacional do sítio aeroportuário.

SUBGRUPO 1

Coordenador

Wallace Gomes Assis

Dezembro / 2024

SUMÁRIO

1. INTRODUÇÃO	5
2. PRESSUPOSTOS DO ESTUDO	6
3. COMPONENTES DO SUBGRUPO	7
4. PLANO DE TRABALHO	8
5. FATOR MOTIVADOR	9
6. DETALHAMENTO DO ESTUDO	12
6.1. BENEFÍCIOS ESPERADOS	12
6.1.1. MELHORIA NA DETECÇÃO DE INTRUSÕES E AMEAÇAS	12
6.1.2. AUMENTO NA EFICIÊNCIA OPERACIONAL	13
6.1.3. CAPACIDADE DE RESPOSTA APRIMORADA A INCIDENTES	13
6.2. ANÁLISE <i>SWOT</i>	13
6.2.1. FORÇAS (<i>STRENGTHS</i>)	14
6.2.2. FRAQUEZAS (<i>WEAKNESSES</i>)	15
6.2.3. OPORTUNIDADES (<i>OPPORTUNITIES</i>)	16
6.2.4. AMEAÇAS (<i>THREATS</i>)	16
6.3. <i>BENCHMARKING</i> DE AEROPORTOS	17
6.3.1. AEROPORTO INTERNACIONAL DE CINGAPURA (CHANGI)	17
6.3.2. AEROPORTO INTERNACIONAL DE DUBAI (DXB)	18
6.3.3. AEROPORTO INTERNACIONAL DE AMSTERDÃ (SCHIPHOL)	18
6.3.4. AEROPORTO INTERNACIONAL DE GUARULHOS (GRU)	19
6.3.5. AEROPORTO INTERNACIONAL DO RIO DE JANEIRO (GIG)	19
6.3.6. AEROPORTO INTERNACIONAL DE BRASÍLIA (BSB)	20
6.3.7. LIÇÕES APRENDIDAS	20
6.4. SOLUÇÕES TECNOLÓGICAS RECOMENDADAS	20
6.4.1. SISTEMAS DE MONITORAMENTO POR VÍDEO	21
6.4.2. SENSORES DE MOVIMENTO E INTRUSÃO	21
6.4.3. DRONES DE INSPEÇÃO	22
6.4.4. SISTEMAS DE GEOLOCALIZAÇÃO E RASTREAMENTO	22
6.4.5. PLATAFORMAS DE GESTÃO INTEGRADA	22

7. CONSIDERAÇÕES FINAIS	23
ANEXO 1 - SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE SISTEMAS DE VIGILÂNCIA AUTOMATIZADOS, COMO CÂMERAS DE ALTA RESOLUÇÃO COM CAPACIDADES DE VISÃO NOTURNA E TERMOGRÁFICA	25
ANEXO 2 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE DRONES DE PATRULHA PARA DETECÇÃO DE ANOMALIAS E PADRÕES DE COMPORTAMENTO SUSPEITO	39
ANEXO 3 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE SENSORES INTELIGENTES AO LONGO DO PERÍMETRO PARA DETECÇÃO DE ANOMALIAS, PROPORCIONANDO ALERTAS IMEDIATOS ÀS EQUIPES DE SEGURANÇA	49
ANEXO 4 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE PLATAFORMAS DE GESTÃO CENTRALIZADA QUE PERMITEM MONITORAR, EM TEMPO REAL, O STATUS DAS PATRULHAS, INCIDENTES REPORTADOS E A LOCALIZAÇÃO DAS EQUIPES DE SEGURANÇA	58

1. INTRODUÇÃO

A realização de vistorias periódicas no perímetro operacional aeroportuário é uma atividade essencial para manter a segurança, a conformidade regulatória e a integridade das operações aeroportuárias.

Além do mais, por meio das vistorias periódicas no perímetro operacional aeroportuário é possível identificar possíveis brechas ou pontos vulneráveis no perímetro que possam comprometer a segurança do aeroporto, verificar a integridade das cercas, portões, iluminação e outros sistemas de segurança, detectar a presença de obstáculos, vegetação e de outros elementos que possam representar riscos e evitar a entrada de animais, pessoas e de veículos não autorizados na área operacional.

Entretanto, observa-se a necessidade emergente de implementação de novas tecnologias para a realização eficiente de vistorias e rondas no perímetro operacional de sítios aeroportuários.

Frente a isso, este Manual apresentará as principais soluções tecnológicas que podem ser utilizadas para realizar vistorias eficientes do perímetro operacional aeroportuário.

Cada solução será descrita com seus benefícios e considerações importantes para a implementação, com o objetivo de fornecer uma visão geral das principais tecnologias disponíveis para aprimorar a segurança e a eficácia das vistorias do perímetro operacional.

2. PRESSUPOSTOS DO ESTUDO

Como pressupostos de abordagem dos temas envolvidos, no escopo da evolução dos trabalhos do Subgrupo 1 do BASeT (Ciclo 2024/2025), foram propostas e aprovadas, na primeira reunião do Subgrupo, as seguintes diretrizes de gestão para condução dos trabalhos:

- a) livre iniciativa e manifestação dos integrantes do Subgrupo, incluindo a propositura de pautas de discussão;
- b) estímulo à participação de todos os componentes, com destaque para os operadores aeroportuários, haja vista a ideia principal do tema de trabalho;
- c) temas não consensuais seriam descritos nas formas como foram discutidos, com apontamentos de diferenças no trabalho de conclusão do estudo;
- d) enfoque no tema determinado ao Subgrupo, sem possibilidade de extensão ou aumento de escopo (incidência de estudo de outro escopo normativo);
- e) fomento à participação efetiva, com possibilidades de desenvolvimento de estudos por grupos específicos dentro do Subgrupo;
- f) As propostas discutidas não levam em consideração questões que demandem futuros pleitos de reequilíbrios econômicos no escopo de contratos de concessão ou contratos de exploração de infraestrutura aeroportuária; e
- g) o trabalho de conclusão a ser apresentado à ANAC reflète os temas discutidos, as posições e decisões tomadas nas discussões pelo Subgrupo.

A partir da análise do escopo do tema, constatou-se que a utilização de novas tecnologias para execução de vistorias e rondas no perímetro operacional de sítios aeroportuários envolve a necessidade de realização de *benchmarking* detalhado e abrangente. E, ao combinar a análise comparativa com a consulta a especialistas com a revisão de literatura relevante, foi possível obter uma visão completa das melhores práticas, desafios e oportunidades associadas à implementação dessas tecnologias inovadoras em segurança aeroportuária.

A fim de identificar forças, fraquezas, oportunidades e ameaças relacionadas à propositura de utilização de novas tecnologias para execução de vistorias e rondas no perímetro operacional de sítios aeroportuários, os integrantes do Subgrupo foram divididos em equipes de estudo para realização de sondagem tecnológica.

A sondagem tecnológica teve como intuito apresentar o detalhamento dos principais recursos e a funcionalidade de cada uma das soluções tecnológicas para a realização de vistorias e rondas no perímetro aeroportuário. Esse nível de detalhe permitiu uma visão mais completa das soluções tecnológicas disponíveis e a perspectiva de como elas podem ser aplicadas de forma integrada para aprimorar a eficácia das vistorias do perímetro operacional

3. COMPONENTES DO SUBGRUPO

O Subgrupo 1 do BASeT (Ciclo 2024/2025) contou com a participação dos seguintes Componentes designados por Organizações Públicas e privadas:

	AENA BRASIL	Wallace Gomes Assis		RIOGALEÃO	Ramon Lago Moreira
	ABR - AEROPORTOS DO BRASIL	Mariana Silveira de Menezes		VINCI AIRPORTS BRASIL	Edimário Menezes
		Raquel de Britto S. dos Santos Carvalho		ZURICH AIRPORT BRASIL	Camila Fagundes Porto
	AEROPORTOS BRASIL VIRACOPOS	Wesley Ramos Correa			Heinz Schuchardt Burda Filho
		Renata Almeida Lança		ESAERO AIRPORTS	Edna Maria Lima Silva
	ANAC	Roberto Hudson Barros		IINFRAMERICA	Ricardo Caldeira César Brasil
	AZUL LINHAS AÉREAS	José Monteiro da Silva Filho			João Paulo da Silva Barros
		Fábio Alves Lima			
	COSTA DO SOL OPERADORA AEROPORTUÁRIA S/A	Renata de Rezende Fróes		NEWTON CHAVES RISK MANAGEMENT IN AVIATION (Participante Eventual)	Newton Duarte Chaves
		Verônica de Jesus Nascimento Brandão		GRUPO SIMÃO SARKIS (Participante Eventual)	Renata dos S. Carvalho Pereira
	FRAPORT BRASIL	Nathalia Burgos Barbosa		TRÂMITE AIR TRAINING (Participante Eventual)	Diego de Souza Lima
		Tiago Marcelino Martins		TAM AVIAÇÃO EXECUTIVA E TÁXI AÉREO (Participante Eventual)	Clara de Jesus Hilário Catarino
	INFRAERO	Robersivania Albuquerque de Lima	Não se aplica	Participante Eventual	Mwena Gabriel Muxila

4. PLANO DE TRABALHO

Foi proposta e aprovada uma agenda de reuniões *on-line* por meio da plataforma *Microsoft Teams*, conforme cronograma abaixo:

- 14/05/2024 – Reunião remota
- 04/06/2024 – Reunião remota
- 02/09/2024 – Reunião remota
- 08/10/2024 – Reunião remota
- 05/11/2024 – Reunião remota

Ficou acordado que os convites para as reuniões seriam encaminhados pelo *e-mail* do Coordenador do Subgrupo 1 do BAsE T (2024/2025), que as interações sobre o escopo do estudo se dariam pelo grupo do WhatsApp criado, exclusivamente, para essa finalidade e que, por sua vez, será encerrado ao término deste Ciclo.

5. FATOR MOTIVADOR

Atualmente, a segurança e a eficiência das operações aeroportuárias dependem significativamente da precisão e da frequência das inspeções realizadas ao redor das instalações. No entanto, os métodos tradicionais têm mostrado limitações quanto à cobertura completa, à eficiência temporal e à capacidade de resposta a incidentes potenciais.

Os métodos convencionais de execução de vistorias e rondas no perímetro aeroportuário são, muitas vezes, manuais, o que resulta em cobertura irregular, haja vista que a extensão dos sítios aeroportuários dificulta a cobertura completa e regular das equipes de segurança. Além do mais, o tempo lento de resposta a eventos adversos, a necessidade de realizar rondas frequentes, que, por sua vez, consomem recursos significativos e que nem sempre garantem a detecção imediata de intrusões ou de outras ameaças, e as dificuldades quanto à obtenção de dados precisos e em tempo real sobre o estado da segurança perimetral são fatores que, também, comprometem a proteção do perímetro operacional dos aeroportos.

Inobstante, é importante destacar o preconizado nos requisitos normativos AVSEC vigentes:

“O operador do aeródromo manterá permanente vigilância do perímetro da área operacional, conforme atos normativos da ANAC. (Artigo 42 do Decreto nº 11.195/2022 – Programa Nacional de Segurança da Aviação Civil contra Atos de Interferência Ilícita (PNAVSEC)).”

“O operador de aeródromo deve manter vigilância do perímetro e da área operacional, de forma a garantir sua proteção adequada. (Parágrafo 107.81(a) do Regulamento Brasileiro da Aviação Civil – RBAC 107).”

Frente ao exposto, um ponto de destaque na abordagem do escopo deste Manual foi a percepção unânime, pela parte dos operadores de aeródromo presentes no Subgrupo, quanto aos benefícios da adoção de uma nova tecnologia para execução de vistorias e rondas no perímetro operacional do sítio aeroportuário, pois este entendimento não apenas visa a superar as limitações dos métodos convencionais, mas também a fortalecer a segurança, a aumentar a eficiência operacional e a garantir uma resposta mais rápida e eficaz a potenciais ameaças. O avanço tecnológico representa um investimento estratégico para aprimorar a segurança aeroportuária em um ambiente cada vez mais dinâmico e desafiador.

Inobstante, na proeminência das discussões sobre a aplicação de novas tecnologias para vistorias e rondas no perímetro operacional de sítios aeroportuários, o Subgrupo identificou as principais vulnerabilidades de segurança existentes no perímetro operacional de um aeroporto, que incluem:

a) Acesso não autorizado:

- i. Pontos de acesso mal protegidos ou com controle de acesso insuficiente, permitindo a entrada de pessoas não autorizadas.
- ii. Falhas no monitoramento e na vigilância do perímetro, facilitando a invasão.
- iii. Falta de barreiras físicas adequadas, como cercas, muros ou obstáculos, para impedir a entrada de intrusos.

b) Vigilância inadequada:

- i. Cobertura insuficiente de câmeras de segurança, deixando áreas às cegas no perímetro.
- ii. Sistemas de monitoramento e detecção de intrusão obsoletos ou com desempenho limitado.
- iii. Falta de integração entre os diferentes sistemas de segurança (câmeras, sensores, alarmes, etc.).

c) Iluminação Deficiente:

- i. Iluminação insuficiente ou mal posicionada no perímetro, dificultando a visualização e a detecção de atividades suspeitas.
- ii. Falhas no sistema de iluminação, deixando áreas escuras e vulneráveis.

d) Manutenção e gestão inadequadas:

- i. Falta de manutenção preventiva e corretiva dos sistemas de segurança, levando a falhas e a vulnerabilidades.
- ii. Ausência de procedimentos e protocolos claros para a gestão da segurança do perímetro.
- iii. Treinamento insuficiente da equipe de segurança para lidar com incidentes e situações de emergência.

e) Integração tecnológica limitada:

- i. Sistemas de segurança fragmentados e não integrados, dificultando a análise e a resposta a incidentes.
- ii. Falta de interoperabilidade entre os diferentes sistemas de segurança (câmeras, sensores, controle de acesso, etc.).
- iii. Dificuldade em aproveitar os benefícios da integração de tecnologias avançadas, como drones, sensores inteligentes e análise de dados.

f) Ameaças externas:

- i. Proximidade com áreas públicas ou vias de acesso, facilitando a invasão do perímetro.
- ii. Condições climáticas adversas, como neblina, chuva ou vento, que podem afetar a eficácia dos sistemas de segurança.
- iii. Atividades criminosas ou terroristas nas proximidades do aeroporto, representando riscos potenciais.

Para mitigar essas vulnerabilidades, é essencial implementar uma abordagem abrangente de segurança que inclua a adoção de tecnologias avançadas, a melhoria da infraestrutura física, o fortalecimento dos procedimentos operacionais e o treinamento contínuo da equipe de segurança. Além disso, a colaboração com autoridades locais e a integração com os sistemas de segurança do aeroporto como um todo são fundamentais para garantir a proteção efetiva do perímetro operacional.

6. DETALHAMENTO DO ESTUDO

6.1. BENEFÍCIOS ESPERADOS

A aplicação de novas tecnologias para vistorias e rondas no perímetro operacional de sítios aeroportuários não só aborda desafios existentes relacionados à segurança AVSEC, mas também antecipa melhorias significativas na detecção de ameaças, na eficiência operacional e na capacidade de resposta a incidentes. Ao investir em soluções tecnológicas avançadas, os aeroportos não apenas melhoram sua segurança física, mas também fortalecem sua capacidade de adaptar-se e de responder, proativamente, aos desafios emergentes de segurança.

Neste sentido, é importante sinalizar que a utilização de novas tecnologias para execução de vistorias e rondas no perímetro operacional de sítios aeroportuários traz diversos benefícios significativos para a segurança AVSEC. Utilizando a teoria de causa e efeito, é possível identificar os seguintes benefícios antecipados para a segurança AVSEC:

6.1.1. MELHORIA NA DETECÇÃO DE INTRUSÕES E AMEAÇAS:

- a) Identificação do problema: Atualmente, as metodologias tradicionais de vigilância perimetral podem não detectar intrusões de forma eficiente, devido às limitações de cobertura e eficácia.
- b) Causas do problema: Cobertura irregular, pontos cegos nas patrulhas humanas e capacidade limitada de resposta a incidentes imprevistos.
- c) Mudanças das causas do problema: A implementação de tecnologias avançadas, como câmeras de alta resolução, sensores inteligentes e drones equipados com câmeras térmicas e capacidades de visão noturna, pode aumentar, drasticamente, a cobertura e a eficiência na detecção de intrusões.
- d) Benefício antecipado: Com uma cobertura mais abrangente e capacidade de monitoramento contínuo por meio de tecnologias automatizadas, a detecção de intrusões e ameaças potenciais será melhorada. Isso permite às equipes de segurança uma resposta mais rápida e direcionada, minimizando o tempo de detecção até a intervenção efetiva.

6.1.2. AUMENTO NA EFICIÊNCIA OPERACIONAL:

- a) Identificação do problema: As rondas manuais consomem tempo e recursos significativos, resultando em uma cobertura limitada e na necessidade de patrulhas frequentes para garantir a segurança do perímetro.
- b) Causas do problema: Dependência de patrulhas manuais que podem não ser suficientes para cobrir grandes áreas de maneira eficaz e constante.
- c) Mudanças das causas do problema: A introdução de tecnologias como drones automatizados e sistemas de monitoramento baseados em IA pode reduzir a necessidade de patrulhas manuais constantes, liberando recursos humanos para tarefas mais estratégicas e de resposta rápida.
- d) Benefício antecipado: Com a automação e o uso de tecnologias inteligentes, a eficiência operacional será aumentada. Menos recursos serão necessários para a realização de rondas, enquanto a cobertura e a frequência de monitoramento serão melhoradas. Isso resultará em uma segurança mais robusta e eficiente sem comprometer a resposta a emergências.

6.1.3. CAPACIDADE DE RESPOSTA APRIMORADA A INCIDENTES:

- a) Identificação do problema: A resposta a incidentes pode ser comprometida pela falta de detecção precoce e pela comunicação inadequada entre as equipes de segurança.
- b) Causas do problema: Sistemas de vigilância convencionais podem não fornecer alertas imediatos ou informações precisas em tempo real sobre incidentes em potencial.
- c) Mudanças das causas do problema: A adoção de tecnologias avançadas permite a detecção precoce de atividades suspeitas e a comunicação instantânea de dados para os centros de operações de segurança.
- d) Benefício antecipado: Com uma detecção mais rápida e precisa, as equipes de segurança podem responder imediatamente a incidentes, minimizando o impacto e aumentando a eficácia das medidas de contenção. Isso fortalece a segurança global do aeroporto e promove um ambiente mais seguro para passageiros, tripulações e funcionários.

6.2. ANÁLISE *SWOT*

No bojo das discussões sobre a aplicação de novas tecnologias para vistorias e rondas no perímetro operacional de sítios aeroportuários, optou o Subgrupo por uma análise de forças, fraquezas, oportunidades e ameaças em relação à proposta de inovação (análise *SWOT* ou FOFA).

Ademais, a análise *SWOT* é essencial para fornecer uma visão abrangente dos fatores internos e externos que podem impactar o sucesso do projeto, permitindo um planejamento estratégico mais robusto e uma tomada de decisão mais embasada.

Destaca-se que a técnica empregada pelo Subgrupo 1 do BASeT (Ciclo 2024/2025) foi obter de todos os representantes do Subgrupo, previamente, as perguntas que pudessem suscitar quais forças, fraquezas, oportunidades e ameaças a implementação de soluções tecnológicas para vistorias do perímetro operacional aeroportuário poderia incorporar.

Preparadas as perguntas, as respostas foram compiladas e tratadas em grupo, de acordo com o conhecimento adquirido e *expertise* dos representantes dos operadores.

6.2.1. FORÇAS (*STRENGTHS*):

- a) Eficiência Aumentada: As tecnologias podem aumentar a eficiência das vistorias, permitindo uma cobertura mais abrangente em menos tempo.
- b) Precisão e Confiabilidade: Tecnologias como drones, sensores e câmeras de alta definição podem fornecer dados mais precisos e confiáveis.
- c) Análise de Dados em Tempo Real: Capacidade de monitorar e analisar informações em tempo real, possibilitando respostas rápidas a incidentes.
- d) Automatização de Processos: Redução da necessidade de intervenção humana, minimizando erros e aumentando a segurança operativa.
- e) Documentação Facilita: Registro automático das vistorias, ajudando na conformidade regulatória e na auditoria.

6.2.2. FRAQUEZAS (*WEAKNESSES*):

- a) Custo Inicial Elevado: Investimentos iniciais em tecnologia, infraestrutura e treinamento podem ser altos.
- b) Dependência de Tecnologia: Risco de falhas tecnológicas que podem comprometer a segurança e a eficácia das vistorias.
- c) Curva de Aprendizado: O pessoal operacional pode precisar de tempo para se adaptar às novas tecnologias, o que pode atrasar a implementação.
- d) Manutenção e Suporte: A necessidade de manutenção constante e suporte técnico pode aumentar custos operacionais.

6.2.3. OPORTUNIDADES (*OPPORTUNITIES*):

- a) Inovação Contínua: O mercado de tecnologia está em constante evolução, oferecendo novas ferramentas e soluções para otimização das vistorias.
- b) Parcerias Tecnológicas: Possibilidade de colaborações com empresas de tecnologia para desenvolver soluções sob medida.
- c) Aumento da Segurança: Melhoria na segurança do perímetro operacional, reduzindo riscos de invasões ou incidentes.
- d) Sustentabilidade: Tecnologias, como drones elétricos, podem oferecer alternativas mais sustentáveis em comparação com métodos tradicionais.
- e) Expansão de Mercado: Com a experiência adquirida, há potencial para expandir a aplicação de tecnologias para outras áreas de segurança e monitoramento.

6.2.4. AMEAÇAS (*THREATS*):

- a) Regulamentação: Normas e regulamentações governamentais podem limitar ou complicar a implementação de novas tecnologias.
- b) Concorrência: Outras organizações ou aeroportos podem adotar tecnologias similares, tornando o diferencial competitivo mais desafiador.
- c) Cibersegurança: Aumento da vulnerabilidade a ataques cibernéticos com a digitalização e conectividade de dispositivos.
- d) Resistência Cultural: O pessoal pode ser resistente a mudanças, afetando a aceitação das tecnologias implantadas.
- e) Mudanças Climáticas: Condições climáticas extremas podem impactar a eficácia de tecnologias, como nos casos de drones, durante operações de monitoramento.

O balanceamento das forças e fraquezas discutidos remetem a um ganho de eficiência, considerados os benefícios que a inovação traria em termos de oportunidades na melhoria da gestão.

Para mitigar os riscos associados à implementação de novas tecnologias em vistorias e rondas em sítios aeroportuários, algumas estratégias de mitigação podem ser consideradas:

1. Gestão de Cibersegurança:

- Implementar soluções robustas de cibersegurança, como *firewalls*, sistemas de detecção e prevenção de intrusões e criptografia de dados.
- Realizar avaliações regulares de vulnerabilidades e testes de penetração para identificar e corrigir possíveis brechas.
- Desenvolver e implementar planos de resposta a incidentes cibernéticos, incluindo procedimentos de recuperação.
- Capacitar a equipe com treinamentos sobre conscientização e melhores práticas de cibersegurança.

2. Gestão de Mudanças e Envolvimento da Equipe:

- Implementar um programa de gestão de mudanças para facilitar a transição e a adoção das novas tecnologias.
- Envolver a equipe operacional desde o início, fornecendo treinamento e suporte para a utilização das novas ferramentas.
- Incentivar a participação da equipe no processo de seleção e implementação das tecnologias, a fim de obter *feedback* e aumentar a aceitação.
- Estabelecer uma cultura de inovação e melhoria contínua, reconhecendo e recompensando a adoção bem-sucedida das novas tecnologias.

3. Planejamento e Gestão de Riscos:

- Realizar uma análise de risco abrangente, identificando e avaliando os principais riscos associados à implementação das novas tecnologias.
- Desenvolver e implementar um plano de gestão de riscos, com estratégias de mitigação e contingência para cada risco identificado.
- Monitorar constantemente os riscos e ajustar o plano de gestão conforme necessário, com base em mudanças no ambiente ou no surgimento de novos riscos.
- Estabelecer procedimentos de *backup* e recuperação de dados, bem como planos de continuidade de negócios, para garantir a resiliência operacional.

4. Parcerias e Colaboração:

- Estabelecer parcerias com fornecedores de tecnologia e especialistas em segurança cibernética para desenvolver soluções personalizadas e obter suporte técnico.
- Colaborar com outras organizações aeroportuárias e autoridades reguladoras para compartilhar melhores práticas, lições aprendidas e soluções inovadoras.
- Participar de fóruns e grupos de trabalho relacionados à segurança aeroportuária e à adoção de novas tecnologias, a fim de se manter atualizado sobre tendências e regulamentações.

5. Conformidade Regulatória e Governança:

- Manter-se atualizado sobre as regulamentações e normas aplicáveis à implementação de novas tecnologias em sítios aeroportuários.
- Desenvolver e implementar políticas, procedimentos e controles internos para garantir a conformidade com os requisitos regulatórios.
- Estabelecer uma estrutura de governança clara, com responsabilidades e processos de tomada de decisão definidos para a gestão das tecnologias implementadas.
- Realizar auditorias e avaliações periódicas para monitorar a conformidade e identificar oportunidades de melhoria.

Ao adotar essas estratégias de mitigação, a organização poderá gerenciar de forma mais eficaz os riscos associados à implementação de novas tecnologias em vistorias e rondas em sítios aeroportuários, maximizando os benefícios e minimizando os impactos negativos.

6.3. BENCHMARKING DE AEROPORTOS

Para identificar as melhores práticas na implementação de soluções tecnológicas para vistorias do perímetro operacional, no escopo de desenvolvimento dos trabalhos do Subgrupo 1 do BASeT (Ciclo 2024/2025), buscou-se uma oportunidade de conhecimento sobre a existência de aeroportos que adotaram essas tecnologias.

6.3.1. AEROPORTO INTERNACIONAL DE CINGAPURA (CHANGI)

a) Implementou um sistema abrangente de monitoramento com câmeras inteligentes:

- mais de 5.000 câmeras de alta resolução (4K);
- cobertura 360° do perímetro operacional;
- recursos de zoom óptico de até 30x; e
- capacidade de visão noturna e térmica.

- b) Utiliza análise de vídeo avançada, com recursos de detecção de movimento:
 - reconhecimento facial em tempo real;
 - detecção de comportamentos suspeitos;
 - análise preditiva de movimentação; e
 - integração com banco de dados de segurança.
- c) Integrou o sistema de monitoramento com sensores de movimento e intrusão, gerando alertas em tempo real.
- d) Emprega drones de inspeção para cobrir áreas de difícil acesso no perímetro.
- e) Utiliza uma plataforma de gestão integrada que unifica todas as informações de segurança.

6.3.2. AEROPORTO INTERNACIONAL DE DUBAI (DXB)

- a) Implementou um sistema de rastreamento em tempo real, utilizando tecnologias de geolocalização (GPS, RFID) para monitorar a movimentação de veículos e pessoas:
 - tags RFID em todos os veículos autorizados;
 - sensores GPS em equipamentos móveis;
 - monitoramento em tempo real 24/7; e
 - precisão de localização de até 1 metro.
- b) Integrou o sistema de rastreamento com controles de acesso e barreiras físicas ao longo do perímetro.
- c) Utiliza drones equipados com câmeras térmicas e de alta resolução para inspeções aéreas:
 - autonomia de voo de 4 horas;
 - câmeras térmicas de alta precisão;
 - transmissão de dados em tempo real; e
 - sistema anticolisão automático.
- d) Implementou uma plataforma de análise de dados que correlaciona informações de diferentes sistemas de segurança

6.3.3. AEROPORTO INTERNACIONAL DE AMSTERDÃ (SCHIPHOL)

- a) Adotou uma abordagem de "perímetro inteligente", com sensores de movimento e intrusão conectados a um sistema de alarme centralizado:
 - detectores de vibração a cada 50 metros;
 - sensores infravermelhos duplos;
 - cabos de fibra ótica sensores; e
 - sistema de alarme setorizado.
- b) Utiliza câmeras de vídeo com recursos avançados de detecção e reconhecimento integradas a uma plataforma de gerenciamento de vídeo.
- c) Emprega drones de inspeção para monitoramento aéreo do perímetro, com transmissão de imagens em tempo real.
- d) Implementou um centro de controle com uma solução de gestão de incidentes que unifica informações de diferentes sistemas de segurança:
 - *videowall* de 180° com 24 telas;
 - *software* de gestão de incidentes;
 - sistema de comunicação integrado; e
 - redundância de servidores.

6.3.4. AEROPORTO INTERNACIONAL DE GUARULHOS (GRU)

- a) Implementou um sistema de monitoramento por vídeo com mais de 1.500 câmeras de segurança.
- b) Utiliza análise de vídeo para detecção de movimentação suspeita e reconhecimento facial.
- c) Realiza inspeções periódicas com drones equipados com câmeras de alta resolução.

6.3.5. AEROPORTO INTERNACIONAL DO RIO DE JANEIRO (GIG)

- a) Adotou uma abordagem de "perímetro inteligente" com sensores de detecção distribuídos estrategicamente.
- b) Utiliza tecnologias de geolocalização (GPS, RFID) para rastreamento de veículos.
- c) Implementou um centro de controle integrado que unifica informações de diferentes sistemas de segurança.
- d) Realiza testes e simulações regulares para aprimorar os protocolos de resposta a incidentes.

6.3.6. AEROPORTO INTERNACIONAL DE BRASÍLIA (BSB)

- a) Investiu em câmeras de segurança com recursos avançados de detecção e reconhecimento.
- b) Integrou o sistema de monitoramento por vídeo com um centro de operações de segurança.
- c) Estabeleceu parcerias com autoridades locais para compartilhamento de informações e coordenação de ações.

6.3.7. LIÇÕES APRENDIDAS

Com base no *benchmarking* realizado, no escopo da evolução dos trabalhos do Subgrupo 1 do BASeT (Ciclo 2024/2025), algumas lições aprendidas foram observadas:

1. Adotar uma abordagem abrangente e integrada, combinando diferentes soluções tecnológicas para obter uma visão holística da segurança do perímetro.
2. Investir em tecnologias avançadas de monitoramento, detecção e análise, como câmeras inteligentes, sensores de intrusão e drones de inspeção.
3. Priorizar a integração de sistemas de segurança em uma plataforma unificada, facilitando a correlação de informações e a tomada de decisões.
4. Desenvolver capacidades de rastreamento e geolocalização para monitorar a movimentação de ativos e pessoas dentro do perímetro.
5. Estabelecer protocolos e procedimentos claros para a operação e manutenção dos sistemas, garantindo sua eficácia a longo prazo.
6. Investir em treinamento e capacitação da equipe de segurança para a correta utilização das soluções tecnológicas implementadas.

6.4. SOLUÇÕES TECNOLÓGICAS RECOMENDADAS

Durante as discussões sobre a aplicação de novas tecnologias para vistorias e rondas no perímetro operacional de sítios aeroportuários, o Subgrupo identificou um conjunto de soluções tecnológicas adequadas de forma mais eficaz às operações aeroportuárias. Essas tecnologias têm o potencial de aprimorar a eficiência, a precisão e a resposta a incidentes no perímetro do aeroporto.

Essas soluções tecnológicas, quando implementadas de forma integrada e com uma abordagem abrangente de segurança, podem significativamente melhorar a eficácia das vistorias no perímetro operacional dos aeroportos brasileiros, aumentando a detecção de atividades suspeitas, a resposta a incidentes e a conformidade com os requisitos de segurança.

É importante ressaltar que a implementação dessas tecnologias deve ser acompanhada de um planejamento cuidadoso, considerando aspectos como compatibilidade, integração, treinamento da equipe e conformidade regulatória. Além disso, a adoção de uma abordagem de melhoria contínua e a realização de testes e avaliações periódicas são fundamentais para garantir a eficácia e a atualização constante das soluções de segurança.

6.4.1. SISTEMAS DE MONITORAMENTO POR VÍDEO

Sistemas de câmeras de segurança estrategicamente posicionados ao longo do perímetro operacional podem fornecer uma visão abrangente da área, permitindo a detecção e o acompanhamento de possíveis ameaças ou irregularidades. Esses sistemas podem ser integrados a plataformas de análise de vídeo que utilizam inteligência artificial para identificar padrões anormais e gerar alertas em tempo real.

Soluções recomendadas:

- a) Câmeras de alta resolução e com recursos avançados, como detecção de movimento, reconhecimento facial e função analítica de vídeo.
- b) Plataformas de gerenciamento de vídeo que permitem visualização em tempo real, gravação, busca e reprodução de imagens.
- c) Inteligência artificial para detecção automática de atividades suspeitas e geração de alertas.

6.4.2. SENSORES DE MOVIMENTO E INTRUSÃO

A instalação de sensores de movimento e intrusão ao longo do perímetro pode complementar o sistema de monitoramento por vídeo, fornecendo uma camada adicional de detecção. Esses sensores podem ser conectados a um sistema de alarme, acionando notificações imediatas em caso de detecção de atividade suspeita.

Soluções recomendadas:

- a) Sensores infravermelhos, magnéticos e sísmicos posicionados estrategicamente ao longo do perímetro.
- b) Sistemas de alarme que disparam notificações em caso de detecção de atividade.
- c) Câmeras com configuração de zonas de detecção e ajuste de sensibilidade para minimizar falsos alarmes.

6.4.3. DRONES DE INSPEÇÃO

Drones equipados com câmeras de alta resolução podem ser utilizados para realizar inspeções aéreas do perímetro operacional, cobrindo áreas de difícil acesso ou com baixa visibilidade. Esses drones podem ser programados para percorrer rotas predefinidas, capturando imagens e vídeos que podem ser analisados posteriormente.

Soluções recomendadas:

- a) Drones equipados com câmeras de alta resolução, sensores térmicos e outros recursos avançados.
- b) Drones com programação de rotas de voo predefinidas para cobertura sistemática do perímetro.
- c) Drones com capacidade de transmissão de imagens e vídeos em tempo real para análise.

6.4.4. SISTEMAS DE GEOLOCALIZAÇÃO E RASTREAMENTO

A integração de sistemas de geolocalização, como GPS e RFID, pode permitir o rastreamento de ativos e pessoas dentro do perímetro operacional. Isso possibilita o monitoramento da movimentação e a identificação de padrões anormais, auxiliando na detecção de possíveis ameaças.

Soluções recomendadas:

- a) Tecnologias como GPS, RFID e *Bluetooth* para rastreamento de ativos e pessoas.
- b) Sistemas de gerenciamento de acesso e controle de perímetro.
- c) *Software* de geração de relatórios de movimentação e análise de padrões de atividade.

6.4.5. PLATAFORMAS DE GESTÃO INTEGRADA

Plataformas de gestão integrada, como sistemas de segurança física e cibernética, podem unificar as informações provenientes de diferentes soluções tecnológicas em uma interface única. Isso facilita a análise de dados, a tomada de decisões e a coordenação de respostas a incidentes.

Soluções recomendadas:

- a) Unificação de informações de diferentes sistemas de segurança (física e cibernética) em uma interface única.
- b) Recursos avançados de análise de dados, correlação de eventos e geração de relatórios.
- c) *Software* para facilitar na tomada de decisões e na coordenação de respostas a incidentes.

7. CONSIDERAÇÕES FINAIS

A adoção de soluções tecnológicas para a realização de vistorias do perímetro operacional pode trazer diversos benefícios, como:

- a) aumento da eficiência e eficácia das vistorias;
- b) detecção precoce de ameaças e irregularidades;
- c) melhoria na segurança e proteção dos ativos e pessoas; e
- d) geração de registros e históricos para análise e auditoria.

No entanto, é importante considerar fatores como compatibilidade, integração, treinamento de equipes e manutenção contínua das soluções implementadas. Uma abordagem holística e planejada é essencial para garantir o máximo aproveitamento dessas tecnologias.

Ao combinar essas soluções tecnológicas, é possível criar um sistema de segurança robusto e eficaz para a realização de vistorias do perímetro operacional, aumentando a detecção precoce de ameaças, a proteção de ativos e a eficiência das operações.

TERMO DE TRATAMENTO DE INFORMAÇÕES

A coordenação do Subgrupo 1 do BASeT (Ciclo 2024/2025) declara que as informações contidas neste estudo são de responsabilidade de seus idealizadores e não devem ser veiculadas sem que haja o devido tratamento dos dados.

As informações contidas neste documento poderão ser compartilhadas com autoridades públicas, sem que isso se limite ao Departamento de Polícia Federal, quando demandado, mas também a outras, quando demandadas. Além disso, o compartilhamento também poderá ocorrer, caso necessário, para finalidades contidas no objeto deste estudo, desde que sejam respeitados os princípios de boa-fé, finalidade, adequação, necessidade, transparência, segurança e responsabilização pelos dados.

E, por estarem justas e acordadas, a coordenação do Subgrupo assina o presente Relatório de Estudo.

São Paulo, 20 de dezembro de 2024.

Wallace Gomes Assis

Coordenador AVSEC

Coordenador do Subgrupo 1 do BASeT (Ciclo 2024/2025)

ANEXO 1 - SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE SISTEMAS DE VIGILÂNCIA AUTOMATIZADOS, COMO CÂMERAS DE ALTA RESOLUÇÃO COM CAPACIDADES DE VISÃO NOTURNA E TERMOGRÁFICA

CONSIDERAÇÕES INICIAIS:

Ao considerar a utilização de sistemas de vigilância automatizados, como câmeras de alta resolução com capacidades de visão noturna e termográfica no ambiente aeroportuário, há alguns aspectos iniciais importantes:

1. Avaliação das Necessidades e Requisitos:

- Realizar uma análise detalhada das necessidades de segurança e monitoramento do perímetro e áreas críticas do aeroporto.
- Identificar os principais desafios e lacunas que precisam ser abordados, como a cobertura de áreas de baixa luminosidade, detecção de ameaças e integração com outros sistemas.
- Definir os requisitos técnicos e operacionais, como resolução de imagem, alcance de visão noturna e termográfica, funcionalidades avançadas de detecção e rastreamento.

2. Planejamento da Arquitetura do Sistema:

- Projetar a disposição e o posicionamento estratégico das câmeras ao longo do perímetro, considerando a cobertura, ângulos de visão e áreas de sobreposição.
- Avaliar a necessidade de integração com outros subsistemas, como iluminação, controle de acesso e plataforma de gerenciamento de segurança unificada.
- Definir os requisitos de infraestrutura, como alimentação elétrica, comunicação de dados e armazenamento de imagens e vídeos.

3. Seleção de Tecnologias Adequadas:

- Analisar as soluções de câmeras de alta resolução disponíveis no mercado, comparando suas especificações técnicas e recursos avançados.
- Avaliar a compatibilidade e interoperabilidade das câmeras com os sistemas e protocolos existentes no aeroporto.
- Considerar a escalabilidade e a capacidade de expansão futura do sistema de vigilância.

4. Implementação e Integração:

- Desenvolver um plano detalhado de implantação, incluindo etapas de instalação, configuração e testes.
- Garantir a integração eficiente das câmeras com a plataforma de gerenciamento de segurança, permitindo a correlação de dados, a geração de alertas e a coordenação de respostas.
- Estabelecer procedimentos operacionais claros para o monitoramento, a análise de eventos e a tomada de ações corretivas.

5. Treinamento e Capacitação da Equipe:

- Capacitar a equipe de segurança na operação, monitoramento e manutenção dos sistemas de vigilância automatizados.
- Desenvolver programas de treinamento contínuo para garantir a atualização de conhecimentos e a eficácia na utilização das tecnologias.
- Estabelecer protocolos de comunicação e coordenação entre a equipe de segurança e os sistemas de vigilância.

6. Manutenção e Atualização Constante:

- Implementar um plano de manutenção preventiva e corretiva para garantir o funcionamento contínuo e a confiabilidade dos sistemas.
- Acompanhar o desenvolvimento tecnológico e avaliar oportunidades de atualização e modernização do sistema de vigilância.
- Realizar testes periódicos e ajustes necessários para manter a eficácia do sistema de acordo com as necessidades em evolução.

Ao considerar essas etapas iniciais, o aeroporto poderá implementar um sistema de vigilância automatizado, com câmeras de alta resolução e capacidades avançadas, de forma estratégica e alinhada com os requisitos de segurança, operação e integração com os demais sistemas do ambiente aeroportuário.

IDENTIFICAÇÃO DA TECNOLOGIA:

Para o sistema de vigilância automatizado, como câmeras de alta resolução com capacidades de visão noturna e termográfica para o perímetro aeroportuário, a indústria dispõe dos seguintes recursos:

1. Câmeras de Alta Resolução:

- Resolução mínima recomendada: 4K (3840 x 2160 pixels) ou superior.
- Características desejáveis:
 - » lentes com zoom óptico avançado (30x ou mais);
 - » sensores de imagem de alto desempenho, com boa sensibilidade em baixa luminosidade;
 - » capacidade de captura de imagens em alta taxa de quadros (60 FPS ou mais); e
 - » opções de montagem fixa, PTZ (*pan-tilt-zoom*) ou em rede de câmeras.



2. Visão Noturna:

- Tecnologias de iluminação integrada:
 - » iluminadores de infravermelho (IR) para visão noturna ativa; e
 - » sensores de luz de baixa luminosidade para visão noturna passiva.
- Características desejáveis:
 - » alcance de visão noturna de, no mínimo, 100 metros;
 - » capacidade de ajuste automático da iluminação IR com base nas condições de luminosidade; e
 - » opções de filtros e lentes especiais para minimizar ofuscamento e reflexos.



3. Visão Termográfica:

- Câmeras com sensores de infravermelho (IR) para detecção de calor.
- Características desejáveis:
 - » resolução térmica mínima de 320 x 240 pixels;
 - » sensibilidade térmica de 0,05°C ou melhor;
 - » capacidade de detecção de alvos a uma distância de, no mínimo, 200 metros; e
 - » opções de paletas de cores e modos de exibição adaptáveis às necessidades de segurança.



As especificações apresentadas fornecem uma visão geral das principais características e funcionalidades desejáveis para um sistema de vigilância automatizado, com destaque em câmeras de alta resolução, visão noturna e termográfica, a fim de aprimorar a segurança e o monitoramento do perímetro aeroportuário. A implementação desse tipo de solução pode contribuir significativamente para a detecção precoce de ameaças e a melhoria da resposta a incidentes.

DESAFIOS DO SETOR QUE A TECNOLOGIA AUXILIARÁ:

O emprego de câmeras de alta resolução com capacidades de visão noturna e termográfica pode auxiliar o setor aeroportuário a enfrentar diversos desafios, entre eles:

1. Vigilância Eficaz do Perímetro:

- Desafio: Garantir a cobertura e o monitoramento constante de todo o perímetro do aeroporto, mesmo em condições de baixa luminosidade.
- Solução: As câmeras com visão noturna e termográfica permitem a detecção e o acompanhamento de atividades suspeitas ao longo do perímetro, independentemente das condições de iluminação.

2. Detecção Precoce de Ameaças:

- Desafio: Identificar rapidamente a presença de intrusos, veículos não autorizados e objetos suspeitos no perímetro.
- Solução: Os recursos avançados de detecção e rastreamento de movimento, aliados à capacidade de reconhecimento de padrões, possibilitam a identificação precoce de ameaças, permitindo uma resposta rápida e eficaz.

3. Monitoramento em Áreas de Difícil Acesso:

- Desafio: Garantir a vigilância de áreas do perímetro com pouca ou nenhuma iluminação natural, como regiões remotas ou de vegetação densa.
- Solução: As câmeras com visão termográfica e iluminadores IR permitem a detecção e o monitoramento de atividades em áreas de baixa luminosidade, ampliando a cobertura de segurança.

4. Resposta a Incidentes em Condições Adversas:

- Desafio: Manter a eficácia da vigilância e a capacidade de resposta a incidentes, mesmo em situações de pouca visibilidade, como neblina, chuva ou escuridão.
- Solução: As câmeras com recursos avançados de visão noturna e termográfica garantem a continuidade do monitoramento e a identificação de ameaças, mesmo em condições climáticas desfavoráveis.

5. Integração com Sistemas de Segurança:

- Desafio: Promover a interoperabilidade entre os sistemas de vigilância e os demais componentes do sistema de segurança aeroportuária.
- Solução: A integração das câmeras de alta resolução com a plataforma de gerenciamento de segurança unificada permite a correlação de dados, a geração de alertas e a coordenação de respostas a incidentes.

6. Otimização de Recursos Humanos:

- Desafio: Maximizar a eficiência da equipe de segurança, reduzindo a sobrecarga de trabalho e a necessidade de monitoramento manual constante.
- Solução: Os recursos de detecção e rastreamento automatizados das câmeras auxiliam na triagem de eventos, permitindo que a equipe de segurança se concentre nas ações prioritárias e responda a elas de forma mais ágil.

Ao enfrentar esses desafios por meio da implementação de câmeras de alta resolução com capacidades de visão noturna e termográfica, o setor aeroportuário poderá aprimorar a segurança do perímetro, aumentar a eficácia da vigilância e da resposta a incidentes, otimizando a utilização de recursos humanos e tecnológicos.

PLATAFORMA HABILITADORA EM QUE A TECNOLOGIA SE ENQUADRA:

As câmeras de alta resolução com capacidades de visão noturna e termográfica se enquadram na plataforma habilitadora de "Sensoriamento e Monitoramento Avançado" no contexto da segurança aeroportuária.

Essa plataforma habilitadora engloba soluções tecnológicas que aprimoram a capacidade de detecção, monitoramento e resposta a eventos e ameaças no perímetro e áreas críticas do aeroporto.

Algumas características-chave dessa plataforma habilitadora incluem:

1. Sensores Inteligentes:

- Câmeras de alta resolução com recursos avançados, como visão noturna e termográfica
- Sensores de movimento, de vibração, acústicos e outros para detecção de atividades suspeitas

2. Análise de Dados e Inteligência Artificial:

- Algoritmos de detecção e reconhecimento de padrões
- Capacidade de correlacionar dados de múltiplos sensores
- Geração de alertas e acionamento de respostas automatizadas

3. Integração de Sistemas:

- Interoperabilidade com a plataforma de gerenciamento de segurança unificada
- Conexão com sistemas de controle de acesso, iluminação e outros subsistemas

4. Visualização e Conscientização Situacional:

- Painéis de controle e *dashboards* para monitoramento em tempo real
- Recursos de mapeamento geoespacial e representação gráfica de eventos

5. Resiliência e Continuidade Operacional:

- Redundância e tolerância a falhas nos sistemas de sensoriamento
- Capacidade de operação em condições adversas de luminosidade e clima

Ao se enquadrar nessa plataforma habilitadora, as câmeras de alta resolução com visão noturna e termográfica contribuem para a criação de um ecossistema integrado de segurança, permitindo a detecção precoce de ameaças, a melhoria da conscientização situacional e a resposta ágil a incidentes no ambiente aeroportuário.

Essa abordagem holística, com a integração de múltiplos sensores e sistemas, é fundamental para fortalecer a segurança do perímetro e das áreas críticas do aeroporto, atendendo aos requisitos de vigilância, detecção e resposta a eventos adversos.

GRAU DE IMPACTO ESPERADO COM A IMPLANTAÇÃO DA TECNOLOGIA:

A implantação de câmeras de alta resolução com capacidades de visão noturna e termográfica em aeroportos pode gerar um impacto significativo em diversos aspectos da segurança e operação aeroportuárias. Alguns dos principais impactos esperados incluem:

1. Melhoria da Detecção e Monitoramento de Ameaças:

- Impacto: Alto
- Justificativa: As câmeras com recursos avançados de visão noturna e termográfica permitirão a detecção precoce de atividades suspeitas, movimentação de intrusos e objetos potencialmente perigosos ao longo do perímetro, mesmo em condições de baixa luminosidade.

2. Redução de Incidentes e Violações de Segurança:

- Impacto: Alto
- Justificativa: Com a melhoria da capacidade de detecção e a geração de alertas imediatos, espera-se uma redução significativa no número de incidentes e violações de segurança no perímetro do aeroporto, contribuindo para a mitigação de riscos.

3. Aumento da Eficiência Operacional:

- Impacto: Médio a Alto
- Justificativa: A integração das câmeras com a plataforma de gerenciamento de segurança unificada permitirá uma resposta a incidentes mais ágil e coordenada, otimizando os procedimentos operacionais e a utilização dos recursos de segurança.

4. Melhoria da Conscientização Situacional:

- Impacto: Alto
- Justificativa: As imagens e os dados fornecidos pelas câmeras, aliados à análise em tempo real, proporcionarão uma visão mais abrangente e precisa da situação de segurança no perímetro, permitindo uma tomada de decisão mais bem informada e eficaz.

5. Redução de Custos Operacionais:

- Impacto: Médio
- Justificativa: Embora o investimento inicial na implantação das câmeras possa ser significativo, a longo prazo, espera-se uma redução nos custos relacionados a incidentes, a danos e à necessidade de pessoal de segurança.

6. Conformidade Regulatória:

- Impacto: Alto
- Justificativa: O sistema de câmeras de alta resolução com visão noturna e termográfica contribuirá para o cumprimento dos requisitos de segurança estabelecidos pelas autoridades reguladoras, fortalecendo a conformidade do aeroporto com as normas vigentes.

7. Melhoria da Imagem e Confiança do Público:

- Impacto: Médio a Alto
- Justificativa: A implementação de tecnologias avançadas de segurança no perímetro do aeroporto pode transmitir uma imagem de maior segurança e confiança aos passageiros, colaboradores e comunidade local.

Destaca-se que a implantação de câmeras de alta resolução com capacidades de visão noturna e termográfica em aeroportos tem o potencial de gerar um impacto significativo na melhoria da segurança, na eficiência operacional e na conformidade regulatória, contribuindo para a mitigação de riscos e o fortalecimento da confiança dos *stakeholders*.

PRAZO PARA IMPLANTAÇÃO E DIFUSÃO DA TECNOLOGIA:

Considerando a adoção de câmeras de alta resolução com capacidades de visão noturna e termográfica nos aeroportos, é possível estimar o seguinte prazo para a implantação e difusão dessa tecnologia:

1. Curto Prazo (1-2 anos):

- Avaliação e planejamento da implementação:
 - » Realização de estudos de viabilidade e análise de requisitos
 - » Definição da arquitetura do sistema e seleção de tecnologias
 - » Desenvolvimento de planos de implementação e integração
- Implantação piloto em aeroportos selecionados:
 - » Instalação e configuração das câmeras em áreas críticas
 - » Integração com a plataforma de gerenciamento de segurança
 - » Testes e validação do desempenho do sistema

2. Médio Prazo (2-4 anos):

- Expansão gradual da adoção em outros aeroportos:
 - » Replicação do modelo de implementação em novos aeroportos
 - » Ajustes e otimizações com base na experiência adquirida
 - » Capacitação e treinamento da equipe de segurança
- Aprimoramento contínuo do sistema:
 - » Atualização de *firmware* e *software* das câmeras
 - » Integração com novos recursos e funcionalidades
 - » Expansão da cobertura e monitoramento do perímetro

3. Longo Prazo (4-6 anos):

- Adoção generalizada nos principais aeroportos do país:
 - » Implementação em todos os aeroportos de grande porte
 - » Integração com outros sistemas de segurança e operação
 - » Padronização de protocolos e procedimentos operacionais
- Evolução tecnológica e inovação contínua:
 - » Incorporação de novas tecnologias, como inteligência artificial
 - » Aprimoramento da análise de dados e geração de *insights*
 - » Melhoria da resiliência e continuidade operacional do sistema

Esse prazo estimado leva em consideração diversos fatores, como a complexidade da implementação, a necessidade de integração com sistemas existentes, a disponibilidade de recursos financeiros e a curva de adoção tecnológica no setor aeroportuário.

É importante ressaltar que a adoção dessa tecnologia pode variar entre os diferentes aeroportos, dependendo de suas prioridades, orçamentos e planos de investimento em segurança. Alguns aeroportos podem adotar essa solução de forma mais acelerada, enquanto outros podem seguir um ritmo mais gradual.

Independentemente do prazo, a implantação de câmeras de alta resolução com capacidades de visão noturna e termográfica nos aeroportos é uma tendência crescente, alinhada com os esforços de modernização e fortalecimento da segurança aeroportuária.

OBSTÁCULOS PARA IMPLANTAÇÃO, DIFUSÃO E/OU DESENVOLVIMENTO DA TECNOLOGIA:

Ao considerar a implantação, difusão e desenvolvimento de câmeras de alta resolução com capacidades de visão noturna e termográfica nos aeroportos, há alguns obstáculos importantes:

1. Investimento Inicial Elevado:

- Desafio: O custo de aquisição e implementação desse tipo de sistema de vigilância avançado pode ser significativo, especialmente para aeroportos de menor porte.
- Mitigação: Buscar soluções de financiamento, parcerias público-privadas e programas de incentivo governamental para viabilizar os investimentos necessários.

2. Integração com Sistemas Existentes:

- Desafio: Garantir a integração eficiente das câmeras com a plataforma de gerenciamento de segurança unificada e outros sistemas operacionais do aeroporto.
- Mitigação: Adotar padrões abertos e protocolos de comunicação que facilitem a interoperabilidade entre os diferentes sistemas.

3. Complexidade Técnica:

- Desafio: A implementação e a manutenção de um sistema de vigilância automatizado com recursos avançados requerem conhecimento técnico especializado.
- Mitigação: Investir em capacitação e treinamento da equipe de segurança, além de estabelecer parcerias com fornecedores e integradores de soluções.

4. Resistência à Mudança:

- Desafio: Alguns aeroportos podem apresentar relutância em adotar novas tecnologias, preferindo manter os métodos tradicionais de vigilância.
- Mitigação: Promover a conscientização sobre os benefícios e a importância estratégica da adoção de soluções de vigilância automatizadas.

5. Questões Regulatórias e de Privacidade:

- Desafio: Garantir o cumprimento de regulamentos e diretrizes relacionados à proteção de dados e à privacidade dos indivíduos.
- Mitigação: Desenvolver políticas e procedimentos claros para o uso responsável e ético das câmeras, em conformidade com a legislação vigente.

6. Manutenção e Atualização Contínua:

- Desafio: Assegurar a manutenção adequada e a atualização constante dos sistemas de vigilância, acompanhando a evolução tecnológica.
- Mitigação: Estabelecer planos de manutenção preventiva e programas de atualização de *firmware* e *software* das câmeras.

7. Disponibilidade de Infraestrutura:

- Desafio: Garantir a disponibilidade de infraestrutura adequada, como alimentação elétrica e comunicação de dados, para suportar a implementação das câmeras.
- Mitigação: Avaliar e investir na modernização da infraestrutura aeroportuária, de modo a atender aos requisitos dos sistemas de vigilância avançados.

Para superar esses obstáculos, é essencial uma abordagem holística que envolva o planejamento estratégico, a alocação de recursos, a capacitação da equipe, a integração com sistemas existentes e o estabelecimento de políticas e procedimentos claros. Essa abordagem permitirá uma implantação bem-sucedida e a difusão gradual das câmeras de alta resolução com capacidades de visão noturna e termográfica nos aeroportos.

CONSIDERAÇÕES FINAIS:

Frente ao exposto nesta sondagem tecnológica, observar-se que, para a disponibilização de câmeras de alta resolução com capacidades de visão noturna e termográfica nos aeroportos, é importante destacar os seguintes aspectos:

1. Alinhamento Estratégico:

- Garantir que a implementação dessas câmeras esteja alinhada com a estratégia geral de segurança e operação do aeroporto.
- Integrar o sistema de vigilância automatizado com os demais componentes da plataforma de segurança aeroportuária.

2. Análise de Custo-Benefício:

- Realizar uma avaliação detalhada dos custos de aquisição, implementação e manutenção das câmeras.
- Ponderar os benefícios em termos de melhoria da segurança, eficiência operacional e conformidade regulatória.
- Buscar soluções de financiamento e parcerias para viabilizar os investimentos necessários.

3. Planejamento e Implementação:

- Desenvolver um plano de implementação detalhado, com etapas claras de instalação, configuração e integração.
- Garantir a compatibilidade e a interoperabilidade das câmeras com os sistemas existentes no aeroporto.
- Estabelecer procedimentos operacionais e de manutenção para a utilização eficaz do sistema.

4. Capacitação e Treinamento:

- Investir na capacitação da equipe de segurança para a operação, o monitoramento e a manutenção das câmeras.
- Desenvolver programas de treinamento contínuo, acompanhando a evolução tecnológica.
- Promover a conscientização e a familiarização dos colaboradores com os recursos e funcionalidades do sistema.

5. Conformidade Regulatória e Privacidade:

- Garantir o cumprimento de todas as regulamentações e diretrizes relacionadas à proteção de dados e à privacidade.
- Estabelecer políticas claras e transparentes sobre o uso das câmeras, com relevância na ética e no respeito aos direitos individuais.
- Implementar medidas de segurança e criptografia para a proteção dos dados coletados.

6. Manutenção e Atualização Contínua:

- Desenvolver um plano de manutenção preventiva e corretiva para garantir o funcionamento ininterrupto do sistema.
- Acompanhar o desenvolvimento tecnológico e avaliar oportunidades de atualização e modernização das câmeras.
- Realizar testes periódicos e ajustes necessários para manter a eficácia do sistema de vigilância.

7. Comunicação e Engajamento das Partes Interessadas:

- Promover a comunicação transparente com os passageiros, colaboradores e comunidade local sobre a implementação das câmeras.
- Envolver as partes interessadas no processo de planejamento e implementação, buscando seu *feedback* e aceitação.
- Demonstrar os benefícios da adoção dessa tecnologia para a segurança e a experiência dos usuários do aeroporto.

Ao considerar esses pontos, os aeroportos poderão implementar um sistema de vigilância automatizado, com câmeras de alta resolução e capacidades avançadas, de forma estratégica, eficiente e alinhada com as melhores práticas de segurança, operação e conformidade regulatória.

ANEXO 2 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE DRONES DE PATRULHA PARA DETECÇÃO DE ANOMALIAS E PADRÕES DE COMPORTAMENTO SUSPEITO

CONSIDERAÇÕES INICIAIS:

É de conhecimento pacífico que, na aviação, os estudos e trabalhos de planejamento e de desenvolvimento de processos, a exemplo do projeto de novas aeronaves ou estruturas aeroportuárias, se realizam com o foco no seu emprego com segurança, por longo tempo, e com inúmeras condicionantes. Esse mesmo raciocínio é partilhado pelos que integram o Sistema *Aviation Security* (AVSEC) ou, porque não dizer, o Sistema de Gerenciamento da Segurança da Aviação Civil contra Atos de Interferência Ilícita (SGSE).

Os aeroportos, independentemente de suas categorias, realizam contínuos trabalhos de revisão de análises de risco, com atualização de informes, fontes utilizadas, bibliotecas de risco e medidas mitigadoras em curso. Com isso, empregam capital intelectual e meios diversos, bem como mantêm hipotecados profissionais e material para serem aplicados na proporcionalidade das mudanças de nível de ameaça local, nacional e/ou internacional. Não obstante, alguns processos e empregos de ferramentas necessitam estar sempre em condições vigentes e em constante atualização, com o máximo grau de excelência possível e à luz da realidade física e financeira de cada aeroporto, com o intento de propiciar a maior eficiência no gerenciamento das ações em uma situação de crise.

Frente ao breve exposto, é que os integrantes do Subgrupo 1 do BASeT (Ciclo 2024/2025), responsáveis pela coleta de dados sobre a operação de RPA em operações de AVSEC, trazem para análise os dados coletados sobre as possibilidades de se empregar esse equipamento como uma das novas ferramentas pelos sistemas de *Aviation Security*, particularmente, nas atividades de vistorias do perímetro operacional.

IDENTIFICAÇÃO DA TECNOLOGIA:

A essência da tecnologia nacional e internacional para o emprego de *Remotely Piloted Aircraft* (RPA), que será abordada no presente documento, já se encontra em estágio avançado de desenvolvimento, bem como os estudos para a melhoria contínua da regulamentação de seu emprego com segurança (*Safety*) junto ao tráfego aéreo de aeronaves que transportam pessoas ou carga.

A atividade finalística de RPA é bastante diversificada, seja pelas forças armadas, seja pelas instituições públicas, seja pela iniciativa privada.

No âmbito da aviação civil, o cerne da abordagem atual, ao se falar sobre *Remotely Piloted Aircraft* (RPA), é a preocupação com o emprego irregular desse equipamento, particularmente, nas proximidades de aeroportos ou heliportos, o que pode resultar em incidentes ou acidentes aéreos com consequências de elevado grau de severidade.

Como se observará mais a frente, operadores de aeródromos no Brasil e em outros países começam a vislumbrar as possibilidades do emprego seguro e coordenado com tráfego aéreo de RPA em atividades de manutenção, no gerenciamento de operações, no monitoramento de presença de aves nas proximidades de aeroporto, na fiscalização de instalações em pontos de difícil acesso; emprego esse, basicamente, focado em ações de segurança operacional. O emprego em AVSEC, essência do presente estudo, ainda é muito embrionário.

Com o propósito de tornar a leitura mais acessível, o *Remotely Piloted Aircraft* (RPA), doravante, passará a ser denominado somente como drone¹.

A aplicação de drones pode ser feita em atividades pré-programadas ou em situações de crise (emergências), mantendo-se as operações (voo dos drones) em níveis de risco dentro de limites considerados aceitáveis para a segurança operacional, por meio de planejamento prévio (ex: horário programado, voo sobre *waypoints*, etc.) e detalhado de coordenação de tráfego aéreo (por meio de TWR ou, se necessário, Controle APP).

Em pesquisas realizadas acerca do emprego de drones como ferramenta nos Sistemas de *Aviation Security* pelos aeroportos, observa-se, até o momento, que o tema é muito pouco abordado.

Provavelmente, e de maneira compreensível e plenamente justificável, um dos fatores condicionantes para que isso ocorra seja a elevada preocupação atual de órgãos reguladores internacionais e nacionais da aviação civil, com a necessidade de disseminar e fortalecer a cultura de *Safety*, diante da ameaça do emprego indevido de drones para as operações aéreas, em particular nas proximidades de aeroportos.

Instituições como a *Airports Council International* (ACI) (ACI, 2024) trazem amplo material de orientação sobre processos focados no combate ao uso indevido de drones nas proximidades de operações aeroportuárias, intituladas como: operações legais com drones; preparação e resposta do aeroporto, medidas de prevenção de drones, campanha de conscientização e soluções de tecnologia antidrone. Entretanto, nada focado, especificamente, no tema em estudo sobre emprego em AVSEC.

¹ No Brasil, as aeronaves não tripuladas ainda são amplamente conhecidas como drones (do inglês zangão, termo muito utilizado pelos órgãos de imprensa), Veículos Aéreos Não Tripulados (VANT), nomenclatura oriunda do termo Unmanned Aerial Vehicle (UAV) e considerado obsoleto na comunidade aeronáutica internacional, ou Aeronave Remotamente Pilotada (ARP)” (ICA 100-40, 2023).

Caso semelhante ocorre para as consultas feitas em material ostensivo, por meio de sites da IATA, EASA, FAA, ANAC e TSA. Em alguns, verificou-se o trato sobre *Security* relacionado a drones, mas sobre estudos para proteção contra atos de interferência ilícita que venham a ser praticados com esse instrumento.

Conforme se observará ao longo do presente documento, é possível a utilização dos drones em ações de AVSEC, quer de forma isolada na realização de patrulhamento rotineiro do perímetro do sítio aeroportuário (Lado Terra e Lado Ar), quer no trabalho em conjunto com outras tecnologias já em uso nos aeroportos (ex: trabalhos de verificação de pontos sensíveis do perímetro que tenham sido acionados por outras tecnologias já em uso, como Circuito Fechado de TV; sensores de movimento; etc.).

DESAFIOS DO SETOR QUE A TECNOLOGIA AUXILIARÁ:

Desafios que estão colocados para o setor e que podem ser enfrentados por meio das tecnologias: aumento da produtividade do setor, redução do impacto ambiental, geração de novos produtos ou serviços, melhoria de processos existentes, etc. Uma mesma tecnologia pode estar simultaneamente enfrentando mais de um problema.

A utilidade de drones e seus recursos agregados (câmeras termais, câmeras agregadas a sistemas de identificação facial e de dados, como placas de automóveis, identificação de condições meteorológicas, etc.) já são realidade no setor de Segurança Pública e Privada no Brasil.

Como é de conhecimento, o emprego geral de drones tem sua normatização primeira balizada pela ICA 100-40 (Aeronaves não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro), seguida pelos Manuais do Comando da Aeronáutica (MCA), Regulamentos Brasileiros da Aviação Civil (RBAC), entre outros.

Mesmo as normas específicas para o manuseio de drones pelos órgãos de segurança pública, que trazem maior flexibilidade quanto ao processo de autorização para o emprego dos drones, e os regulamentos que amarram os procedimentos para uso pela segurança privada partilham de uma diretiva maior e comum, qual seja: a plena preocupação com o aspecto da segurança operacional.

Este aspecto em *Safety* está sendo, novamente, repassado para que tenhamos sempre em mente que todas as sugestões apresentadas para análise quanto ao emprego de drones no Sistema AVSEC pelos operadores de aeródromo não poderão ser prioritárias à questão da segurança operacional, assim dizendo, o seu emprego, a todo momento, estará condicionado à preocupação de se evitarem incidentes ou acidentes aeronáuticos.

Dito isso, mesmo com uma gama já bastante diversificada de ferramentas utilizadas pelo Sistema AVSEC pelos operadores de aeródromos no Brasil, a mentalidade preventiva e preditiva do Sistema de Gerenciamento da Segurança da Aviação Civil contra Atos de Interferência Ilícita (SGSE) nos trouxe a

esse exato momento de busca pelo amadurecimento de como superar os desafios e utilizar, de forma contextualizada, essa valiosa ferramenta em prol de *Security* e com *Safety*, visto que a aplicação de drones em operações de *Security* de aeroportos, atualmente, está distante de ser uma prática comum.

Em conformidade com o relatado sobre a pouca literatura normativa e, até mesmo, acadêmica quanto ao emprego de drones em *Aviation Security* na atualidade, seria desaconselhável afirmar, categoricamente, quais as vantagens na aplicação de drones em AVSEC. Sendo assim, julga-se, salvo melhor juízo, utilizar a expressão: “potenciais benefícios que serão obtidos no uso de drones em AVSEC” (BALCI²). Consequentemente, é plausível apresentar e fazer um paralelo entre algumas das vantagens na serventia de drones na segurança privada (Grupo Premium, 2024) que venham a justificar os estudos para superar os desafios na sua aplicação em AVSEC, em virtude dos potenciais benefícios da utilização dessa ferramenta complementar na segurança dos sítios aeroportuários. Vejamos:

1. **Visão Aérea Abrangente:** os drones proporcionam uma perspectiva única, permitindo uma visão aérea abrangente das áreas monitoradas. Isso é especialmente útil para vigiar grandes propriedades, onde a visibilidade do chão pode ser limitada (ex: sítios aeroportuários que tenham grande área verde em torno de seu perímetro, com árvores de copas elevadas, mesmo dentro dos limites de *Safety*).
2. **Agilidade e Rapidez:** devido à sua mobilidade, os drones podem se deslocar rapidamente de um ponto a outro, cobrindo distâncias que seriam desafiadoras e demoradas para patrulhas terrestres (de moto ou carro). Eles serão capazes de alcançar, com maior facilidade dentro dos sítios aeroportuários, áreas de difícil acesso com eficiência e de fornecer respostas rápidas a alertas de segurança.
3. **Vigilância Discreta:** os drones podem operar de maneira relativamente discreta, especialmente os modelos menores. Isso os torna ideais para situações em que a vigilância não intrusiva é necessária e minimiza, ao máximo, a quebra prematura do fator surpresa da ação dissuasória das equipes AVSEC/Polícia Federal/Forças Auxiliares sobre praticantes de atos de interferência ilícita ou perpetradores que estejam atuando dentro do perímetro de responsabilidade dos aeroportos.
4. **Capacidade de Transmissão em Tempo Real:** com câmeras avançadas (visão termal, captação de imagem integrada a sistema de identificação facial, etc.) os drones podem transmitir imagens e vídeos em tempo real para as equipes de segurança. Isso permite uma avaliação imediata da situação e a tomada de decisões rápidas acerca das informações, como acionamento antecipado de equipes de AVSEC para averiguação e definição positiva ou negativa de pessoa ou objeto).

2 **BALCI**, Hüdaverdi. The Use of Drones in Airport Security Operations. 2023. Disponível em: (chrome-extension://oemmdcbldboiebfnladdacbfmadadm/https://www.theseus.fi/bitstream/handle/10024/808302/Balci_Hudaverdi.pdf?sequence=2&isAllowed=y).

5. **Flexibilidade em Diversos Ambientes:** os drones são versáteis e podem ser utilizados, desde que em perfeita coordenação com o controle de tráfego aéreo (TWR) do aeroporto. Mais à frente, será tratada, de forma um pouco mais pormenorizada, a questão desta coordenação para casos de usos em horários predeterminados ou em situações de emergência.
6. **Aprimoramento da Segurança da Equipe AVSEC:** ao utilizar drones para tarefas de alto risco (situações de crise ou não) ou em áreas mais sensíveis do sítio aeroportuário, as equipes AVSEC podem reduzir a exposição do seu pessoal a situações potencialmente prejudiciais, melhorando, assim, a segurança geral dos seus colaboradores.
7. **Capacidades Avançadas de Sensoriamento (atividade preventiva):** além das câmeras, alguns drones estão equipados com sensores avançados, como infravermelho ou sensores térmicos, que podem detectar movimentos ou atividades anormais (preventivamente) que não são visíveis a olho nu, especialmente durante a noite ou em condições atmosféricas degradadas, como nevoeiro.

É possível, também, empregar os drones em operações de AVSEC integrados a outras tecnologias:

1. **Sistemas de Câmeras de Vigilância:** a integração de drones com sistemas fixos de câmeras de vigilância permite uma cobertura de segurança mais ampla (ex: acionamento do emprego de drones mediante situação extraordinária plotada pelo sistema de câmeras de canal de acesso de veículos em ponto mais afastado do sítio aeroportuário e que não seja de uso diário; de sistema de vigilância em pátios de estacionamento de veículos do Lado Terra; de terminais logísticos).
2. **Análise de Dados e Inteligência Artificial:** a combinação com sistemas de análise de dados (Video Management System - VMS) e inteligência artificial potencializa a capacidade de identificar comportamentos suspeitos (veículos ou pessoas) e realizar análises preditivas. Isso resulta em uma resposta de segurança mais rápida e informada.
3. **Tecnologias de Reconhecimento Facial e de Placas de Veículos:** os drones equipados com tecnologias (algoritmos) de reconhecimento facial ou de placas de veículos, no entorno da cerca administrativa ou entre esta e a cerca operacional do aeroporto, podem ser usados em operações de segurança para identificar rapidamente indivíduos ou veículos suspeitos (ex: monitoramento de operações de transporte de valores a serem realizadas no aeroporto).
4. **Sistemas de Alarme e Sensores:** a integração com sistemas de alarme instalados em pontos externos (Lado Ar ou Terra), considerados mais vulneráveis do sítio aeroportuário, permite que os drones sejam despachados, mediante coordenação com tráfego aéreo, para investigar ativações de alarme. Isso proporciona uma visualização imediata da situação e possibilita uma resposta ainda mais rápida.
5. **Redes de Comunicação:** integrar drones com redes de comunicação avançadas garante que as informações coletadas sejam transmitidas em tempo real para as equipes de segurança (Sala AVSEC do aeroporto) e centros de comando em caso de crise (Centro de Emergência Operacional – COE) fixos ou móveis, o que facilita a coordenação eficaz das operações de segurança.

PLATAFORMA HABILITADORA EM QUE A TECNOLOGIA SE ENQUADRA:

Para se realizar a afirmação precisa da(s) plataforma(s) habilitadora(s) em que a tecnologia de emprego de drones se enquadra para a realização de operações de AVSEC em aeroportos, é necessária a consulta a profissional especializado. Entretanto, é notório o largo desenvolvimento de estudos de drones com a integração de tecnologias.

Destaca-se a evolução de estudos no emprego de drones com sistema de Inteligência Artificial, com sistemas de *Cyber Security*, com armazenamento de dados (em nuvem), gerando biblioteca de risco e realidade aumentada (aumento da percepção da atual realidade de imagem gerada e capturada pelo drone).

GRAU DE IMPACTO ESPERADO COM A IMPLANTAÇÃO DA TECNOLOGIA:

Visualiza-se que, como toda nova ferramenta, o impacto de seu emprego se dará de forma gradativa.

Como já fora comentado, por se tratar de uma ferramenta de uso ainda muito incipiente, vislumbra-se, em um primeiro momento (médio prazo – 5 a 15 anos), um **impacto elevado** (quando a tecnologia traz grandes mudanças e avanços na atividade) e, ao longo (longo prazo – mais de 15 anos) de seu amadurecimento, particularmente no que tange à concomitância segura (*Safety*) com o tráfego aéreo de aeronaves que transportam pessoas e carga, fluidez de seu emprego, um **impacto disruptivo** (quando a tecnologia é capaz de mudar paradigmas, introduzindo novas categorias de produtos e formas de produzir bem diferentes das vigentes).

A essência desta afirmação repousa nas sugestões de possíveis formas de se empregarem drones em operações de AVSEC em Operadores de Aeroportos, tendo por base as experiências já partilhadas pelas empresas de segurança privada. Dessa forma, é possível apresentar algumas propostas sobre a serventia de drones pelo Sistema AVSEC de operadores de aeródromos.

É oportuno sempre recordar que a aplicação fica condicionada a diversos fatores característicos de cada operador:

- estrutura física e características do terreno onde se encontra o aeroporto (vegetação, vizinhança, tamanho do aeroporto, etc.);
- intensidade da malha do tráfego aéreo do operador;
- condição financeira;
- histórico de ameaças e situações de crise vividas pelo aeroporto; e
- outros fatores julgados importantes pelo Operador.

Considerados esses aspectos, a operação do drone poderá ser realizada basicamente de duas formas:

- a) **Operação de drone cabeado** - em pontos pré-definidos no sítio aeroportuário (ex: local do sítio aeroportuário com histórico de maior incidência de tentativa de incursões não autorizadas, área de vegetação densa, etc.) ou em local de emergência, a equipe AVSEC estaciona um pequeno gerador em um pequeno automóvel ou mochila; o drone fica ligado via cabo de até 120m de altura; passa a transmitir imagem (360° e térmica, se necessário) por tempo indeterminado.

Dessa forma, o drone fica voando em local vertical limitado, possibilitando, em tempo real, informações para a ação das equipes em solo, na Sala AVSEC ou no COE.



Figura 1 - Exemplo de operação de drone cabeado. (Fonte: DroneShow Robotic e Aeroscan, 2024).

Inicialmente, apresenta-se como um fator facilitador para a segurança (*Safety*) mais favorável, pois o drone permanecerá em um ponto estacionário no espaço aéreo em relação ao solo, podendo subir até a altitude de 120m, sempre em coordenação com a TWR do aeroporto.

- b) **Operação via sinal de rádio (forma tradicional)** - o drone é operado por profissional homologado da equipe AVSEC, com coordenação prévia com a TWR do aeroporto (sempre) e Controle APP (se necessário), sob supervisão direta e em tempo real da Sala AVSEC do aeroporto e com rota pré-definida (automatizada, e não autônoma) sobre *waypoints* do perímetro do sítio aeroportuário (ex: sobrevoo de *waypoints* estabelecidos entre a cerca administrativa e a cerca operacional do perímetro do aeroporto).



Figura 2 – Exemplo de rota pré-definida sobre *waypoints* para voo automatizado e não autônomo em torno de complexo industrial.

(Fonte: DroneShow e AerOSCAN, 2024).

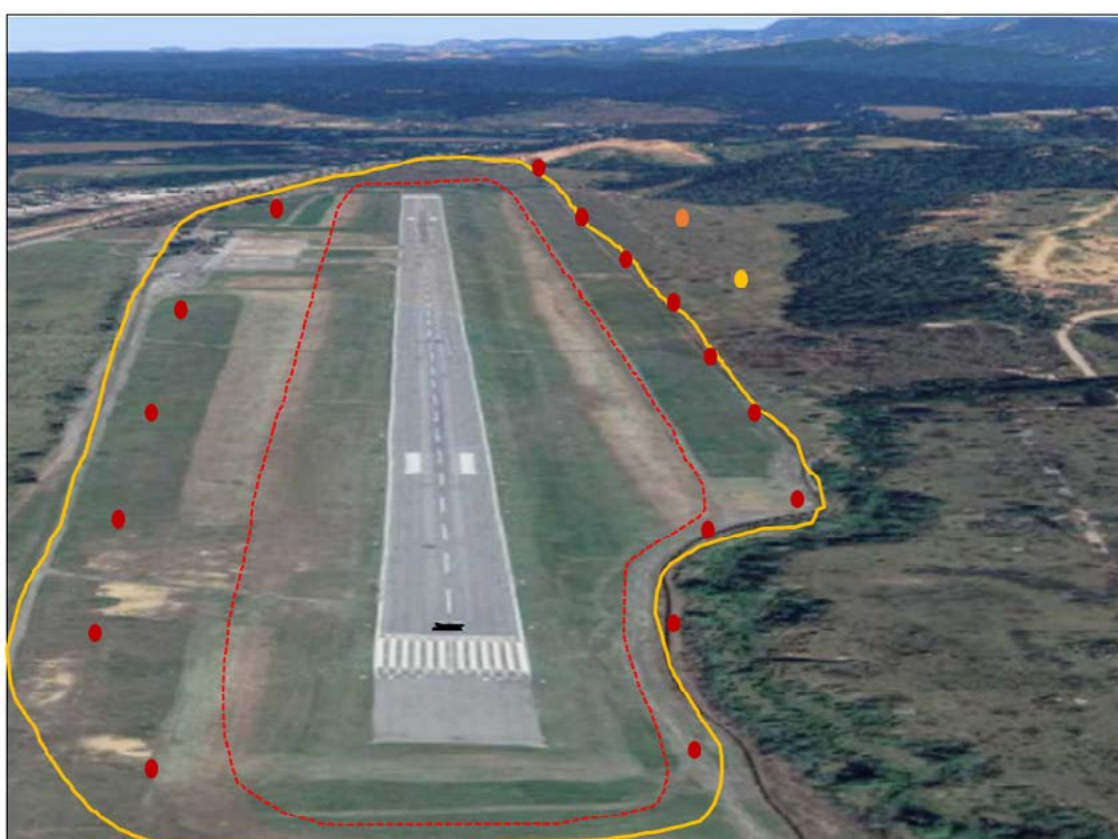


Figura 3 – Ilustração montada para visualizar uma simulação de *waypoints* para rota pré-definida em torno do perímetro de um aeroporto.

(Fonte: Google, 2024).

Com base na figura montada sobre a imagem ilustrativa de um aeroporto (linha amarela – cerca administrativa / linha vermelha – cerca operacional), poderão ser estabelecidos *waypoints* (pontos vermelhos e/ou laranjas) sem cruzar as cabeceiras ou cruzando-as, quando necessário, e mediante observação adicional na coordenação prévia com a TWR do aeroporto.

Nesse exemplo, seria possível conduzir em horários fora do “pico no tráfego aéreo” voos automatizados. No voo automatizado, o drone realiza o voo com rota já definida com monitoramento em tempo real do operador de drone para que este possa intervir, de imediato, a qualquer momento, em prol da segurança operacional. Esse tipo de voo é diferente do voo autônomo, o qual ainda não é autorizado no espaço aéreo brasileiro.

PRAZO PARA IMPLANTAÇÃO E DIFUSÃO DA TECNOLOGIA:

Por se tratar de uma ferramenta de uso ainda muito incipiente, vislumbra-se, em um primeiro momento, médio prazo (5 a 15 anos) para o desenvolvimento harmonioso do emprego de drones em operações de *Safety* e/ou AVSEC nos aeroportos, mesmo para operações de drones automatizados (com Piloto Remoto em Comando), quer sejam drones cabeados, quer sejam aqueles cuja operação é por sinal de rádio.

Se passarmos para a possibilidade de emprego de drones autônomos (sem Piloto Remoto em Comando), cujo voo é proibido pelas normas em vigor no Brasil, é muito pouco provável que isso se consolide com prazo inferior a 15 anos para o seu amadurecimento.

OBSTÁCULOS PARA IMPLANTAÇÃO, DIFUSÃO E/OU DESENVOLVIMENTO DA TECNOLOGIA:

O aumento da frota de drones em âmbito nacional levará, cada vez mais, a um natural entrelaçamento e a uma sobreposição dos dois sistemas ATM e UTM, sem contar que, muito em breve, será comum o emprego das aeronaves não tripuladas no transporte de passageiros (os eVTOL - *electric Vertical Take-Off And Landing* - vulgos carros voadores).

Mesmo em um ambiente mais reduzido, como a zona de proteção de aeródromo, de imediato, são observados obstáculos para a implantação da doutrina de uso de drones em operações de AVSEC:

1. **Controle de Tráfego Aéreo:** a óbvia necessidade de estreita e clara coordenação com o Controle de Tráfego Aéreo (TWR e, se necessário, Controle APP) para o emprego programado (horários pré-definidos) de drones ou para situações de emergência (crises), a fim de que se possa fazer o uso (pré-programado) dos drones durante os horários de menor tráfego (fora dos horários de pico) dos aeroportos ou em situações de emergência. Em se tratando destas últimas, procedimentos requerem que se mantenham, temporariamente, aeronaves em solo (suspensão temporária de pousos/decolagens); ações também aplicáveis em casos de elipses de espera pré-definidas no espaço aéreo, durante as operações com os drones.
2. **Faixas de Frequência:** coordenação (DECEA; ANATEL; operador de aeródromo) de utilização de faixas de frequência (infraestrutura técnica) para operações de drones dentro de bandas de frequência, sem conflito com as utilizadas pelos órgãos de controle de tráfego aéreo, serviços de AVSEC já em uso, empresas de apoio às operações de companhias aéreas (*catering*), etc.

Como fator motivacional para os estudos da utilização dessa valorosa ferramenta, o SGSE dos aeroportos poderá visualizar que um forte processo já se encontra em curso no Brasil para conciliar, também, os potenciais benefícios elencados e os desafios descritos nas operações com drones de interesse do Sistema AVSEC dos aeroportos.

ANEXO 3 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE SENSORES INTELIGENTES AO LONGO DO PERÍMETRO PARA DETECÇÃO DE ANOMALIAS, PROPORCIONANDO ALERTAS IMEDIATOS ÀS EQUIPES DE SEGURANÇA

CONSIDERAÇÕES INICIAIS:

Essa sondagem tecnológica fornece uma visão geral das principais características e funcionalidades desejáveis para um sistema de sensores inteligentes no perímetro aeroportuário, visando à detecção precoce de anomalias e à geração de alertas imediatos para as equipes de segurança. A implementação desse tipo de solução pode contribuir, significativamente, para a melhoria da segurança e da resposta a incidentes no perímetro operacional do aeroporto.

IDENTIFICAÇÃO DA TECNOLOGIA:

Com relação à ronda perimetral, é importante dizer que aspectos relacionados aos ambientes socioeconômicos e criminais em que os aeroportos brasileiros estão inseridos precisam ser considerados, pois essas questões podem influenciar na parametrização e no nível de aceitação à exposição de riscos, sobretudo, podem direcionar o investimento em recursos para questões mais aderentes à realidade local. Em contrapartida, empresas e organizações não arriscam macular sua imagem e reputação com questões advindas de delitos ou crimes. É nessa esteira que se pensa em uma solução mais aderente à realidade nacional. É sabido que apenas a realização de rondas em períodos pré-determinados ou visitas com cunho de imprevisibilidade não são suficientes para dissuadir ou denegar alguém mal-intencionado.

Outro aspecto importante que reforça a prática quanto às duas tecnologias somadas (barreira de proteção e ronda perimetral) é que elas se mostram ser mais eficazes, quando tais tecnologias têm como premissa evitar o confronto, trazendo, assim, o conceito de implementação de uma infraestrutura robusta capaz de repelir intrusões.

Para as barreiras perimetrais em aeroportos, os seguintes tipos de tecnologia e suas aplicações esperadas podem ser considerados:

1. **Sistemas de iluminação perimetral inteligente:** iluminação LED com sensores de movimento, controle remoto e integração com sistemas de segurança.

2. **Bastão de ronda:** sugestão para equipe de vigilância armada. Cabe ressaltar que o termo ronda refere-se à vistoria de instalações em tempo real, com o objetivo de prevenir riscos com o potencial de gerar situações indesejadas. Importante ressaltar que a segurança privada atua em várias localidades desde 1960. O bastão de ronda emite sinais sonoros e isso ajuda a orientar o vigilante, além disso, dispõe de outras funcionalidades de alerta, segurança e de resistência à queda.
3. **Ztrax:** equipamento de monitoramento contínuo em tempo real: apontamentos precisos; segurança; resistência e economia; bateria com mais de 30 horas de duração. São mais de 20 tipos de alertas, incluindo o 'botão de pânico'. Com ele, é possível sinalizar o centro de monitoramento de forma eficiente e eficaz. Sistema redundante, também sinaliza por meio de mensagens instantâneas, incluindo o envio de alerta via SMS. É acessível e não necessita de muito investimento, pode ser utilizado pelos vigilantes quando eles estiverem a pé. O monitoramento é contínuo e, se for de veículo, também registra as informações perimetrais assim como a velocidade do veículo. O aparelho é prático e o índice de ruído ou de falhas é baixo.



4. **Findme:** eficiência, gestão e controle, incluindo relatórios e diversas facilidades. Com ele, é possível programar as rondas com ou sem horários, rastreando, em tempo real, via GPS, QR Code e *Beacons*, vinculando *checklists* personalizados e fotos obrigatórias a cada ponto de ronda. Alguns pontos positivos: monitoramento em tempo real, rastreamento por GPS, registros automáticos de ponto de rondas, alerta e notificações imediatas, relatórios personalizados *online*, além disso, é fácil de usar.
5. **Sensores de infravermelhos:** a barreira de infravermelhos baseia a sua tecnologia na emissão e recepção de um sinal infravermelho – a célula da coluna emissora produz um raio diretivo de luz infravermelha, totalmente invisível a olho nu, que é captado pela célula receptora. Este sistema consiste em dois módulos: um emissor e um receptor que são instalados frente a frente sobre a linha a proteger, formando uma zona de detecção invisível que, se interrompida, gera um alarme. O sensor pode ser de feixe contínuo ou de feixe pulsatório. Em relação ao de feixe contínuo, a luz é facilmente interrompida e pode provocar falsos alarmes e, conseqüentemente, um baixo nível de segurança. O de feixe pulsatório emite luz em intervalos regulares, podendo a luz ser recebida por várias células e isso minimiza os falsos alarmes; oferece, portanto, um maior nível de segurança. Uma de suas vantagens é a utilização em canais multiplexados. Isso incrementa a imunidade de falsos alarmes e a segurança proporcionada.

6. **Sensores de micro-ondas:** as barreiras de micro-ondas são constituídas por emissores que geram ondas à frequência de 9900MHz e de receptores que analisam os sinais provenientes desses emissores. A zona de detecção é representada por um lobo que se desdobra desde a cabeça do emissor até a cabeça do receptor. Se um obstáculo em movimento atravessa o campo vigiado entre o emissor e o receptor, este é detectado pelo receptor, o qual envia imediatamente a informação.

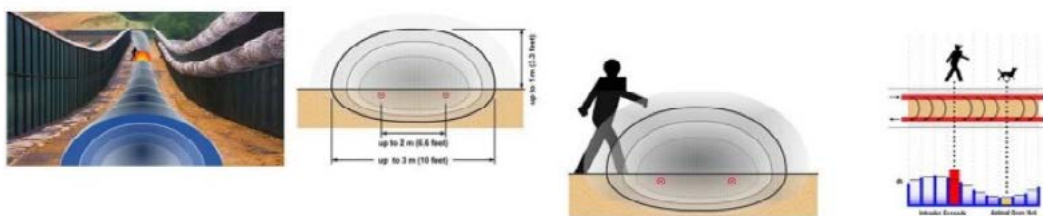
Na ausência de intrusão, o sinal de saída do receptor é estável. A penetração de um obstáculo no lobo de detecção origina uma variação da amplitude do sinal proporcional à sua dimensão. É a análise dessa variação que faz disparar o alarme de intrusão.



7. **Sensores de detecção com dupla tecnologia:** são sensores que combinam duas tecnologias para efetuar a detecção. As mais comumente utilizadas nesses tipos de equipamentos são as tecnologias de infravermelhos passivos e de micro-ondas. Infravermelhos passivos – qualquer objeto ou pessoa emite, naturalmente, uma radiação na gama de infravermelhos, que é o calor irradiado por cada um de nós. A principal diferença entre esta irradiação natural e o infravermelho ativo está no fato de a radiação não ser estimulada, mas de ser naturalmente emitida. Um sensor de infravermelhos passivos detecta movimentos por variação de temperaturas no campo de detecção. Micro-ondas – um sensor de micro-ondas combina as operações do emissor e do receptor em um único equipamento. O sinal de impulsos de micro-ondas emitido é refletido pelo meio ambiente do sensor e captado pelo receptor. O movimento na zona de detecção modifica o sinal refletido e a modificação é analisada e comparada com o sinal original. Os sensores de dupla tecnologia funcionam da seguinte forma: quando o aparelho detecta movimento, ativa o sensor de micro-ondas. Se este último também detectar movimento, o alarme é emitido. Ambas as tecnologias são sensíveis a diferentes fenômenos. O sensor de infravermelhos passivo é sensível aos movimentos de calor e o de micro-ondas, às condições meteorológicas (chuva, neve, nevoeiro, por exemplo.) ou a movimentos aleatórios não considerados como intrusão, como, por exemplo, os da vegetação ao vento. A combinação das duas tecnologias resulta em maior confiabilidade do sistema.

8. **Sensores de detecção de tripla tecnologia:** existem, ainda, sistemas de barreiras que utilizam e conjugam três tipos diferentes de tecnologias: infravermelhos ativos, micro-ondas e *doppler*. Devido a seus grandes poderes de detecção e eficiência, são equipamentos normalmente utilizados para proteção de perímetros de alta segurança, como sejam: prisões, instalações militares, nucleares e, de forma geral, todas as instalações de alto risco. A intrusão é detectada por interrupção dos feixes de infravermelhos e de uma das duas outras tecnologias (micro-ondas / *doppler*). A adição da hiperfrequência *doppler* elimina o ângulo morto que é criado por uma barreira de micro-ondas ao pé da coluna, não sendo preciso efetuar o cruzamento dos feixes das colunas para ter 100% de eficácia. Este tipo de barreira funciona em dupla direção, o que envolve menores custos.
9. **Sensor de detecção por impacto:** o seu princípio de funcionamento é o seguinte: a fibra óptica transporta um sinal luminoso. Quando há uma tentativa de intrusão (choque contra a parede), o sinal é deformado. Esta deformação do sinal é analisada pela Unidade Central, e a intrusão é detectada. Esse tipo de sistema é muito fiável, mas apresenta a desvantagem de ter de ser instalado na fase da construção do edifício ou quando da ocorrência de uma eventual remodelação. Outros destes sistemas e destinados para o mesmo fim utilizam um outro tipo de tecnologia que, embora baseada no mesmo princípio, isto é, análise de vibrações através de um cabo sensor, o faz de outra forma. O seu princípio de funcionamento é no cabo, a espaços definidos. São inseridos sensores detectores de vibrações, os quais transmitem, através do cabo, a informação de detecção à Unidade Central. Nesse tipo de instalação, o cabo é fixado sobre a parede interior do edifício, o que torna a sua instalação mais prática, facilitando a aplicação em edifícios existentes.
10. **Sistema de detecção para vedações:** o princípio de funcionamento é simples: a Unidade Central emite impulsos constantes ao longo do núcleo do cabo. Quando há um impacto brusco na vedação, o campo elétrico no interior do cabo é alterado e a detecção é efetuada. Os antigos sistemas de detecções utilizavam a detecção linear, ou seja, consideravam que o nível de ruído era constante ao longo da vedação, o que provocava inúmeros falsos alarmes, pois, como se sabe, ao longo de uma vedação, nem sempre esta tem a mesma tensão de instalação e, por vezes, é até constituída por diversos tipos de rede, malha ou material e até utiliza suportes com resistências e processos de assentamento muito diversos.

11. **Detecção por campo magnético (cabo enterrado):** tecnologia baseada na análise de alterações do campo magnético gerado entre dois cabos paralelos e equidistantes, enterrados ao longo do perímetro a proteger. O princípio de funcionamento é simples: a unidade central gera um campo magnético constante ao longo dos cabos e, quando o campo magnético é alterado, a detecção é efetuada. Além disso, esse tipo de sistema consegue fazer a detecção do ponto de intrusão com uma precisão inferior a 3 metros, sendo possível calibrar o limiar de detecção em função do tipo de solo em que o cabo é enterrado. Em caso de detecção, o campo magnético é modificado. Esta funcionalidade permite calibrar todo o comprimento do cabo em função do tipo de solo e, livremente, dimensionar as zonas de detecção, permitindo saber, com precisão, o ponto de intrusão e as zonas de detecção que podem ter o comprimento ajustado de acordo com quilometragem do local.



12. **Detecção telemétrica por laser infravermelho e Detecção por sensor de cabo microfônico:** sistema versátil que emite pulsos, recebe e analisa os impulsos através do tempo de retorno. Qualquer alteração causada por uma intrusão no tempo de varrimento do sensor ou qualquer modificação no ambiente de referência gera o sinal de alerta. Ressalta-se que apenas um detector a laser infravermelho dispõe da função do alcance de 360°, além disso, o dispositivo pode ser instalado de maneira vertical, horizontal ou até mesmo pode ser feita a combinação de ambos.
13. **Detecção por sensor de fibra óptica e algoritmos de inteligência artificial:** podem ser utilizados em qualquer ambiente. De fácil utilização e de alta potência, alguns detectores podem ser ajustados automaticamente em tempo real. Também dispõem de um *display* para facilitar a utilização e eliminar quaisquer suposições. É resistente a óleos e a produtos químicos. Além disso, geram economia de espaço. Também há disponível no mercado o sensor de fibra óptica digital, o qual oferece detecção estável em ambientes rígidos, manutenção automática e é de fácil utilização.

Essas tecnologias, quando implementadas de forma integrada e estratégica, podem contribuir, significativamente, para a segurança do perímetro aeroportuário, de forma que aumentam a detecção precoce de ameaças, podem dificultar a invasão e melhorar a resposta das equipes de segurança a incidentes.

É importante considerar a compatibilidade dessas soluções com os requisitos operacionais, a infraestrutura existente e as regulamentações aplicáveis, além disso, é recomendável realizar testes e avaliações para garantir a eficácia e a confiabilidade do sistema de barreiras perimetrais.

DESAFIOS DO SETOR QUE A TECNOLOGIA AUXILIARÁ:

Inicialmente, cabe salientar que a pesquisa foi realizada com um especialista em AVSEC e atual gestor da *Runway Solution*, com também que algumas análises foram realizadas com base na infraestrutura do Aeroporto Internacional de Brasília.

Portanto, seria crucial informatizar as guaritas, o controle de acessos para áreas controladas e áreas restritas, o que aumentaria a produtividade do serviço e a atuação efetiva de modo automatizado.

Além disso, um dos desafios do setor é a quilometragem, tendo em vista que alguns locais são demasiadamente extensos e alguns deles são de difícil acesso. Também, há outro ponto a ser mencionado: dependendo da localidade, o perímetro aeroportuário apresenta grandes índices de risco de fauna e similaridades nas proximidades. Nesses casos, com a inclusão de drones, poderia ser verificada a possibilidade da diminuição do impacto de CO2 emitido por veículos nas proximidades, assim como a utilização deles para situações flagrantes. Vale mencionar que, se se incluir outro tipo de detecção e se fizer um monitoramento à distância, também será possível posicionar os vigilantes nos perímetros de modo mais estratégico.

Por fim, os locais de rondas próximos das cercas perimetrais e operacionais devem estar sempre transitáveis. Por isso, o setor de manutenção deve ser informado, imediatamente, para fins de realizar as roçagens do mato, a poda das árvores próximas da cerca, a troca de mourões e manutenção das cercas (arame farpado ou concertina com 4,50 metros).

Quanto à fauna, recomenda-se implantar gaiolas para capturas de carcarás, raposas, tamanduás, entre outros, sem interferir no uso das demais tecnologias, em sensores de campo e alarmes.

PLATAFORMA HABILITADORA EM QUE A TECNOLOGIA SE ENQUADRA:

Tendo em vista que cada aeroporto tem limitações definidas e configurações diferentes, o modelo de gestão de pátio e o uso de plataformas de vigilância compartilhada é comumente utilizado em vários aeroportos pela SAAB³, mas, para confirmar a plataforma habilitadora e definir o *software* específico, uma vez que a maioria das plataformas são utilizadas *online*, é necessário que uma avaliação seja feita por um técnico especializado com precisão, a fim de realizar testes pilotos da implantação. Porém, ressalta-se que vários aeroportos do mundo utilizam a *Aerobahn Surface Manager* da SAAB, a qual proporciona um bom nível de consciência situacional, auxiliando não só nos voos, como também em terra, no Brasil, conforme o próprio site da empresa SAAB menciona. Dessa forma, a plataforma foi utilizada recentemente, no dia 4 de setembro de 2024, no Aeroporto Internacional Tom Jobim e no *Apron Control* da Concessionária para gerenciar não só os veículos na superfície, como também as movimentações de aeronaves, com o suporte de sensores de multilateração instalados na superfície do aeroporto. Este processo proporcionou agilidade, eficiência e previsibilidade, incluindo investigações de eventos críticos, incluindo relatórios estatísticos e prognósticos.

3 SAAB é uma empresa líder em defesa e segurança, está sediada na Suécia e estabelece ampla transferência de tecnologia ao Brasil, incluindo o programa Gripen Brasileiro.

GRAU DE IMPACTO ESPERADO COM A IMPLANTAÇÃO DA TECNOLOGIA:

O grau de impacto esperado com a implantação de sensores inteligentes no perímetro aeroportuário pode ser considerado alto e abrangente quanto a diversos aspectos da segurança e da operação do aeroporto. Alguns dos principais impactos esperados incluem:

1. Melhoria da Detecção de Ameaças e Intrusões:

- Impacto: Alto
- Justificativa: os sensores inteligentes, como detectores de movimento, por vibração e infravermelho, permitirão a detecção precoce de tentativas de invasão ou atividades suspeitas ao longo do perímetro, o que possibilita uma resposta rápida e eficaz das equipes de segurança.

2. Redução de Incidentes e Violações de Segurança:

- Impacto: Alto
- Justificativa: com a melhoria da detecção e a capacidade de gerar alertas imediatos, espera-se uma redução significativa no número de incidentes e violações de segurança no perímetro do aeroporto; fator que contribui para a mitigação de riscos.

3. Aumento da Eficiência Operacional:

- Impacto: Médio a Alto
- Justificativa: a integração dos sensores inteligentes com a plataforma de gerenciamento de segurança unificada permitirá uma resposta mais ágil e coordenada a incidentes; isso otimiza os procedimentos operacionais e a utilização dos recursos de segurança.

4. Melhoria da Conscientização Situacional:

- Impacto: Alto
- Justificativa: os dados fornecidos pelos sensores, aliados à análise em tempo real, proporcionarão uma visão mais abrangente e precisa da situação de segurança no perímetro, o que permite uma tomada de decisão mais informada e eficaz.

5. Redução de Custos Operacionais:

- Impacto: Médio
- Justificativa: embora o investimento inicial na implantação dos sensores possa ser significativo, a longo prazo, espera-se uma redução nos custos relacionados a incidentes, a danos e à necessidade de pessoal de segurança.

6. Conformidade Regulatória:

- Impacto: Alto
- Justificativa: o sistema de sensores inteligentes contribuirá para o cumprimento dos requisitos de segurança estabelecidos pelas autoridades reguladoras; fator que fortalece a conformidade do aeroporto com as normas vigentes.

7. Melhoria da Imagem e Confiança do Público:

- Impacto: Médio a Alto
- Justificativa: a implementação de tecnologias avançadas de segurança no perímetro do aeroporto pode transmitir uma imagem de maior segurança aos passageiros, aos colaboradores e à comunidade local e lhes proporcionar maior confiança.

Portanto, a implantação de sensores inteligentes no perímetro aeroportuário tem o potencial de gerar um impacto significativo na melhoria da segurança, na eficiência operacional e na conformidade regulatória, e isso contribui para a mitigação de riscos e o fortalecimento da confiança dos *stakeholders*.

Ademais, a combinação do campo magnético e dos sensores de micro-ondas, a princípio, seriam de impacto elevado, tendo em vista que já estão disponíveis no mercado. Além disso, há o fato de serem utilizados como ferramentas preditivas, em conjunto com outras ferramentas já existentes e com apoios locais, isto é, elementos que mitigariam riscos, o *inter-criminis* e auxiliaria nos objetivos principais: dissuasão, que seria a desistência pela parte do invasor; a deflexão, porque ele seria encaminhado para outros alvos; denegação; demora e detecção. Além disso, poderia ser evitado também o confronto, um dos objetivos principais das ferramentas tecnológicas.

PRAZO PARA IMPLANTAÇÃO E DIFUSÃO DA TECNOLOGIA:

Com base no Aeroporto Internacional de Brasília e no Aeroporto Internacional do Rio de Janeiro, pelo fato de a tecnologia ser existente, seria possível implantar com o prazo estimado de 5 anos. Tratando-se de um novo cabeamento, implantação de cabo enterrado em um raio aproximado, após o perímetro existente, seria de médio prazo entre 5 a 15 anos, tendo em vista que o aeroporto já apresenta uma praça nas proximidades, o que, também, gera risco e requer nova avaliação. Além disso, na iminência de haver projetos futuros ou em andamento, como, por exemplo, a construção de um *shopping* nas proximidades, seria necessário realizar uma avaliação mais precisa, incluindo, o estacionamento externo do Aeroporto, que, por vezes, permite a circulação de pessoas com facilidade, o que necessita de nova análise por um especialista habilitado em AVSEC.

OBSTÁCULOS PARA IMPLANTAÇÃO, DIFUSÃO E/OU DESENVOLVIMENTO DA TECNOLOGIA:

Responsabilidade ambiental e risco aviário nas proximidades, interferências ou qualquer extrapolação de limites nas proximidades e alcance de utilização com o uso dos drones no espaço aéreo, assim como verificação de qualquer interferência tecnológica seriam obstáculos para implantação da tecnologia.

Nesse caso, cabe mencionar que cada aeroporto tem suas facilidades e seria necessária uma abordagem minuciosa. Contudo, frisando como referência o Aeroporto Internacional de Brasília e suas facilidades, cogita-se ser possível implementar novas tecnologias complementares com as já existentes de maneira alcançável sem obstáculos e muitas interferências.

CONSIDERAÇÕES FINAIS:

No Aeroporto Internacional de Brasília, as vistorias mais comuns no perímetro são realizadas por meio de rondas motorizadas com vigilantes. No entanto, essa prática pode variar entre diferentes aeroportos, uma vez que, atualmente, também é comum o monitoramento em tempo real por câmeras de segurança.

No caso do Aeroporto Internacional de Brasília, o limite de afastamento do vigilante em relação ao seu posto de serviço (guarita) é de, no máximo, 50 metros. As rondas são realizadas com veículos, como carros ou motocicletas, o que torna a utilização de novas tecnologias, como a ztrax, uma opção complementar interessante. A ztrax dispõe de uma bateria com autonomia de até 30 horas, o que permite uma frequência de uso de, aproximadamente, 8 a 9 horas pelos vigilantes. Além disso, oferece mais de 20 funcionalidades e capacidade de enviar informações precisas em tempo real, elementos que fortalecem o suporte ao centro de monitoramento e aumentam a segurança.

Outra tecnologia complementar que pode ser empregada são os drones, que possibilitam a realização de buscas mais detalhadas em grandes áreas, inclusive próximo ao solo, o que permite a detecção de possíveis ameaças, como a presença de explosivos.

Para o sistema de detecção de intrusão, é recomendável a utilização de tecnologias combinadas, pois o emprego de elementos preditivos eleva os níveis de segurança. Nesse contexto, sugere-se a combinação de sensores de campo magnético e de micro-ondas. Isso proporciona uma abordagem mais abrangente e eficaz na detecção de atividades suspeitas no perímetro do aeroporto.

ANEXO 4 – SONDAGEM TECNOLÓGICA PARA UTILIZAÇÃO DE PLATAFORMAS DE GESTÃO CENTRALIZADA QUE PERMITEM MONITORAR, EM TEMPO REAL, O *STATUS* DAS PATRULHAS, INCIDENTES REPORTADOS E A LOCALIZAÇÃO DAS EQUIPES DE SEGURANÇA

IDENTIFICAÇÃO DA TECNOLOGIA:

Existem diferentes tipos de plataformas de gestão centralizada que permitem monitorar, em tempo real, o *status* das patrulhas, incidentes reportados e a localização das equipes de segurança em aeroportos. Algumas das principais opções incluem:

1. **Sistemas de Comando e Controle (C2):** plataformas integradas que centralizam o monitoramento, a coordenação e a resposta a incidentes de segurança.

Estes oferecem recursos como visualização geoespacial, despacho de equipes, registro de ocorrências e análise de dados.

- Exemplos: *Milestone XProtect Corporate*, *Genetec Security Center*, *Avigilon Control Center*.

2. **Soluções de Gerenciamento de Segurança Unificada (PSIM):** plataformas que integram diversos sistemas de segurança, como câmeras, sensores e controle de acesso.

Estes permitem o monitoramento centralizado, a correlação de eventos e a resposta coordenada a incidentes.

- Exemplos: *Verint Situational Awareness and Response*, *Qognify Situatoir*, *CNL Vidsys*.

3. **Aplicativos de Gerenciamento de Incidentes e Equipes:** soluções móveis e baseadas em nuvem para gerenciamento de equipes de segurança e resposta a incidentes.

Estes oferecem recursos como rastreamento de localização, despacho de equipes, registro de ocorrências e relatórios.

- Exemplos: *Omnigo Software*, *Omnisec*, *Trackforce Valiant*.

- 4. Plataformas de Gerenciamento de Operações de Segurança (SOMP):** soluções que integram diferentes sistemas de segurança e fornecem uma visão unificada das operações.

Estes permitem o monitoramento em tempo real, a análise de dados e a tomada de decisões informadas.

- Exemplos: *Lenel OnGuard, Honeywell Pro-Watch, Johnson Controls C•CURE 9000*.

- 5. Sistemas de Gerenciamento de Emergências (EMS):** plataformas voltadas para o planejamento, resposta e recuperação de emergências em aeroportos.

Estes incluem recursos de monitoramento, comunicação, coordenação de equipes e gestão de incidentes.

- Exemplos: *Everbridge, Veoci, Intermedix WebEOC*.

Ao avaliar essas diferentes opções, os aeroportos devem considerar fatores como integração com sistemas existentes, escalabilidade, usabilidade, suporte técnico e alinhamento com os requisitos de segurança e operação específicos do ambiente aeroportuário.

A escolha da plataforma de gestão centralizada adequada dependerá das necessidades, infraestrutura e recursos disponíveis em cada aeroporto, e deverá ter como fim aprimorar a eficácia da segurança, a coordenação de equipes e a resposta a incidentes.

DESAFIOS DO SETOR QUE A TECNOLOGIA AUXILIARÁ:

As plataformas de gestão centralizada que permitem monitorar, em tempo real, o *status* das patrulhas, incidentes reportados e a localização das equipes de segurança podem auxiliar o setor aeroportuário a enfrentar diversos desafios, incluindo:

1. Melhoria da Segurança Aeroportuária:

- Desafio: garantir a segurança de passageiros, colaboradores e infraestrutura aeroportuária e mitigar riscos de incidentes e ameaças.
- Contribuição: as plataformas de gestão centralizada proporcionam uma visão unificada e em tempo real das atividades de segurança e permitem uma resposta mais ágil e coordenada a ocorrências.

2. Eficiência Operacional:

- Desafio: otimizar os processos e recursos de segurança e minimizar interrupções e impactos nas operações aeroportuárias.
- Contribuição: essas plataformas permitem o gerenciamento eficiente das equipes de segurança, o despacho de recursos, a coordenação de respostas e melhoram a eficiência operacional.

3. Conformidade Regulatória:

- Desafio: cumprir as regulamentações e diretrizes de segurança estabelecidas pelas autoridades competentes.
- Contribuição: as plataformas de gestão centralizada auxiliam no registro, no monitoramento e na elaboração de relatório de incidentes, facilitando a comprovação do cumprimento dos requisitos regulatórios.

4. Conscientização Situacional:

- Desafio: obter uma visão abrangente e em tempo real da situação de segurança no aeroporto e apoiar a tomada de decisões.
- Contribuição: essas plataformas fornecem uma visualização centralizada de todas as atividades de segurança e permitem uma compreensão mais clara da situação operacional.

5. Coordenação e Comunicação:

- Desafio: garantir a comunicação eficaz e a coordenação entre as diferentes equipes e sistemas de segurança.
- Contribuição: as plataformas de gestão centralizada facilitam a comunicação, o despacho de equipes e a resposta coordenada a incidentes e melhoram a integração entre os diversos componentes de segurança.

6. Resiliência Operacional:

- Desafio: assegurar a continuidade das operações aeroportuárias, mesmo diante de interrupções ou incidentes de segurança.
- Contribuição: essas plataformas oferecem recursos de redundância, *backup* e recuperação de dados e aumentam a resiliência do sistema de segurança.

7. Análise de Dados e Melhoria Contínua:

- Desafio: coletar, analisar e utilizar os dados de segurança para identificar oportunidades de melhoria.
- Contribuição: as plataformas de gestão centralizada permitem a coleta, o armazenamento e a análise de dados de incidentes, patrulhas e desempenho e subsidiam a tomada de decisões e o aprimoramento contínuo das operações de segurança.

Ao adotar essas plataformas de gestão centralizada, os aeroportos poderão enfrentar, de forma mais eficaz, os desafios relacionados à segurança, à eficiência operacional, à conformidade regulatória e à resiliência, e elas contribuirão para a melhoria contínua de operações do aeroporto e para a experiência dos passageiros.

PRAZO PARA IMPLANTAÇÃO E DIFUSÃO DA TECNOLOGIA:

Considerando a adoção de plataformas de gestão centralizada que permitem monitorar, em tempo real, o *status* das patrulhas, incidentes reportados e a localização das equipes de segurança em aeroportos, é possível estimar o seguinte prazo para a implantação e difusão dessa tecnologia:

1. Curto Prazo (1-2 anos):

- Avaliação e planejamento da implementação:
 - » Realização de estudos de viabilidade e análise de requisitos;
 - » Definição da arquitetura do sistema e seleção da plataforma;
 - » Desenvolvimento de planos de implementação e integração;
- Implantação piloto em aeroportos selecionados:
 - » Instalação e configuração da plataforma de gestão centralizada;
 - » Integração com os sistemas de segurança e operações existentes;
 - » Testes e validação do desempenho do sistema.

2. Médio Prazo (2-4 anos):

- Expansão gradual da adoção em outros aeroportos:
 - » Replicação do modelo de implementação em novos aeroportos;
 - » Ajustes e otimizações com base na experiência adquirida;
 - » Capacitação e treinamento da equipe de segurança e operações;
- Aprimoramento contínuo da plataforma:
 - » Atualização de *software* e incorporação de novas funcionalidades;
 - » Integração com outros sistemas e sensores de segurança;
 - » Expansão da cobertura e monitoramento das atividades.

3. Longo Prazo (4-6 anos):

- Adoção generalizada nos principais aeroportos do país:
 - » Implementação em todos os aeroportos de grande porte;
 - » Integração com outros sistemas críticos de operação aeroportuária;
 - » Padronização de protocolos e procedimentos operacionais;
- Evolução tecnológica e inovação contínua:
 - » Incorporação de novas tecnologias, como inteligência artificial;
 - » Aprimoramento da análise de dados e geração de *insights*;
 - » Melhoria da resiliência e continuidade operacional do sistema.

Esse prazo estimado leva em consideração diversos fatores, como a complexidade da implementação, a necessidade de integração com sistemas existentes, a disponibilidade de recursos financeiros e a curva de adoção tecnológica no setor aeroportuário.

É importante ressaltar que a adoção dessas plataformas de gestão centralizada pode variar entre os diferentes aeroportos, dependendo de suas prioridades, orçamentos e planos de investimento em segurança. Alguns aeroportos podem adotar essa solução de forma mais acelerada, enquanto outros podem seguir um ritmo mais gradual.

Independentemente do prazo, a implementação de plataformas de gestão centralizada é uma tendência crescente no setor aeroportuário, alinhada com os esforços de modernização e fortalecimento da segurança operacional.

OBSTÁCULOS PARA IMPLANTAÇÃO, DIFUSÃO E/OU DESENVOLVIMENTO DA TECNOLOGIA:

Ao implementar plataformas de gestão centralizada para monitoramento em tempo real de patrulhas, incidentes e equipes de segurança em aeroportos, alguns obstáculos importantes a serem considerados incluem:

1. Integração com Sistemas Existentes:

- Desafio: garantir a integração eficiente da plataforma de gestão centralizada com os diversos sistemas de segurança, controle de acesso, monitoramento e de comunicação já existentes no aeroporto.
- Mitigação: adotar padrões abertos e API's que facilitem a interoperabilidade entre os diferentes sistemas.

2. Complexidade Técnica:

- Desafio: a implementação e a manutenção de uma plataforma de gestão centralizada requerem conhecimento técnico especializado em segurança, em TI e em operações aeroportuárias.
- Mitigação: investir em capacitação e em treinamento da equipe responsável, além de estabelecer parcerias com fornecedores e integradores de soluções.

3. Resistência à Mudança:

- Desafio: alguns aeroportos podem apresentar relutância em adotar novas tecnologias e preferirem manter os métodos tradicionais de gestão de segurança.
- Mitigação: promover a conscientização sobre os benefícios e a importância estratégica da adoção de plataformas de gestão centralizada.

4. Investimento Inicial Elevado:

- Desafio: o custo de aquisição, implementação e manutenção de uma plataforma de gestão centralizada pode ser significativo, especialmente para aeroportos de menor porte.
- Mitigação: buscar soluções de financiamento, parcerias público-privadas e programas de incentivo governamental para viabilizar os investimentos necessários.

5. Disponibilidade de Infraestrutura:

- Desafio: garantir a disponibilidade de infraestrutura adequada, como rede de comunicação de dados, servidores e dispositivos móveis, para suportar a implementação da plataforma.
- Mitigação: avaliar e investir na modernização da infraestrutura aeroportuária, de modo a atender aos requisitos da plataforma de gestão centralizada.

6. Questões Regulatórias e de Privacidade:

- Desafio: garantir o cumprimento de regulamentos e diretrizes relacionados à proteção de dados e à privacidade dos indivíduos monitorados.
- Mitigação: desenvolver políticas e procedimentos claros para o uso responsável e ético da plataforma, em conformidade com a legislação vigente.

7. Manutenção e Atualização Contínua:

- Desafio: assegurar a manutenção adequada e a atualização constante da plataforma de gestão centralizada e acompanhar a evolução tecnológica.
- Mitigação: estabelecer planos de manutenção preventiva e programas de atualização de *software* e *firmware* da plataforma.

Para superar esses obstáculos, é essencial uma abordagem holística que envolva o planejamento estratégico, a alocação de recursos, a capacitação da equipe, a integração com sistemas existentes e o estabelecimento de políticas e procedimentos claros. Essa abordagem permitirá uma implantação bem-sucedida e a difusão gradual das plataformas de gestão centralizada nos aeroportos.

