MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

SEGURANÇA

MCA 205-2

MANUAL DE SEGURANÇA DA AVIAÇÃO CIVIL DO SISCEAB

2019

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

SEGURANÇA

MCA 205-2

MANUAL DE SEGURANÇA DA AVIAÇÃO CIVIL DO SISCEAB

2019

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 65 /DGCEA, DE 24 DE MAIO DE 2019.

Aprova o Manual de Segurança da Aviação Civil do SISCEAB.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, de conformidade com o previsto no art. 19, inciso I, da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, e considerando o disposto no art.10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 1.668/GC3, de 16 de setembro de 2013, resolve:

Art. 1º Aprovar o MCA 205-2 "Manual de Segurança da Aviação Civil do SISCEAB", que com esta baixa.

Art. 2º Este Manual entra em vigor na data de sua publicação no Boletim do Comando da Aeronáutica.

Ten Brig Ar JEFERSON DOMINGUES DE FREITAS
Diretor-Geral do DECEA

(Publicado no BCA nº 090, de 28 de maio de 2019)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Estabelecer a aplicação das medidas de segurança destinadas a garantir a integridade de áreas, instalações e equipamentos dos órgãos do SISCEAB referentes à segurança da aviação civil contra atos de interferência ilícita.

1.2 ÂMBITO

Este manual aplica-se a todos os elos do SISCEAB nos limites de sua competência regulamentada e jurisdição técnico-operacional.

2 SIGLAS, ACRÔNIMOS E CONCEITUAÇÕES

2.1 SIGLAS E ACRÔNIMOS

ATS	Serviço de Tráfego Aéreo
ARS	Área Restrita de Segurança
ATCO	Controlador de Tráfego Aéreo
CINDACTA	Centro Integrado de Defesa Aérea e Controle do Tráfego Aéreo
DTCEA	Destacamento de Controle do Espaço Aéreo
ETD	Detector de Traços Explosivos (*Explosives Trace Detector*)
EPTA	Estação Prestadora de Serviços de Telecomunicações e de Tráfego Aéreo
LASER	Amplificação de luz por emissão estimulada de radiação (*Light Amplification by Stimulated Emission of Radiation*)
MANPAD	Sistema de Defesa Antiaéreo Portátil (*Man Portable Air-Defense System*)
MCA	Módulo de Controle de Acesso
MCI	Módulo de Contra incêndio
MCVE	Módulo de Central de Vigilância Eletrônica
MDI	Módulo de Detecção de Intrusão
MRE	Módulo de Reação
MRV	Módulo de Rastreamento de Veículo
MTI	Módulo de Tecnologia da Informação
MVE	Módulo de Vigilância Eletrônica
PSNA	Provedores de Serviços de Navegação Aérea
PNAVSECEA	Programa Nacional de Segurança para a Aviação Civil do Sistema de Controle do Espaço Aéreo Brasileiro
PES-AVSEC	Plano Específico de Segurança AVSEC
RFID	Identificação por Radiofrequência (*Radio Frequency Identification*)
SRPV-SP	Serviço Regional de Proteção ao Voo de São Paulo

2.2 CONCEITUAÇÕES

2.2.1 AERONAVE NÃO TRIPULADA

Qualquer aparelho que possa sustentar-se na atmosfera, a partir de reações do ar que não sejam as reações do ar contra a superfície.

2.2.2 AMEAÇA

É a intenção declarada de causar prejuízo, dano ou outra ação hostil a alguém, não se restringindo apenas a um evento isolado, podendo ser compreendida como circunstância ou tendência.

2.2.3 AMEAÇA INTERNA

Um ou mais indivíduos com acesso e/ou conhecimento do funcionamento do SISCEAB e intenção de causar prejuízos à operação deste, possibilitando a exploração das vulnerabilidades do Sistema.

2.2.4 ANÁLISE DE RISCO

Processo de compreensão da fonte e cenário do risco e a determinação do nível de risco inerente. Inclui a apreciação das causas, possíveis consequências, probabilidade e severidade.

2.2.5 ÁREA CONTROLADA

Área cujo acesso é permitido apenas após controle de acesso realizado pelo elo do SISCEAB. Pode abranger áreas administrativas, técnicas, operacionais, pontos sensíveis, ou outras áreas identificadas como de grau de risco não prioritário, dentro ou fora do perímetro patrimonial.

2.2.6 ÁREA DE ACESSO RESTRITO

Áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo elo do SISCEAB.

2.2.7 ÁREA RESTRITA DE SEGURANÇA

Área aeroportuária, identificada como área prioritária de risco, onde, além do controle de acesso, outros controles de segurança são aplicados. Tal área normalmente inclui as áreas do serviço aéreo público, de embarque de passageiros entre o ponto de inspeção e a aeronave, áreas de rampa e bagagens, inclusive as áreas nas quais as aeronaves são trazidas para operação e é realizada a inspeção de bagagem e carga, áreas de armazenagem de cargas, centros de tratamento de mala postal e instalações para os serviços de comissária, entre outras.

2.2.8 ARTIGO PERIGOSO

Todo artigo ou substância que pode constituir risco à segurança e à integridade das pessoas, instalações ou sistemas do SISCEAB, tais como: armas, explosivos e artefatos ou agentes químicos, biológicos, radioativos e nucleares.

2.2.9 ITENS PROIBIDOS

Artigos que comprometam a segurança da aviação civil, devendo ter seu acesso restrito à ARS e pontos sensíveis, exceto por pessoas autorizadas e quando necessários para realizar tarefas essenciais. Tais tarefas essenciais se referem à operação, manutenção, abastecimento ou segurança dos elos do SISCEAB.

2.2.10 LASER

Dispositivo que produz um feixe direcional intenso e coerente de radiação óptica, estimulando a emissão de fótons por transições eletrônicas ou moleculares para reduzir os níveis de energia.

2.2.11 MEDIDAS PREVENTIVAS DE SEGURANÇA

Ações de caráter permanente, aplicadas com a intensidade e periodicidade que se fizerem necessárias, no sentido de antecipar e mitigar causas de prováveis atos ilícitos que possam provocar interrupção ou afetar as atividades do elo do SISCEAB.

2.2.12 MEDIDAS ADICIONAIS DE SEGURANÇA

Conjunto de alterações em procedimentos, processos, equipamentos ou instalações, com o intuito de reforçar as medidas preventivas de segurança, a ser disponibilizado pelo PSNA, em virtude de elevação do nível de ameaça, evento com ameaça pontual, ativação de ações do plano de contingência ou devido à determinação específica do DECEA.

2.2.13 PONTO SENSÍVEL

Área, instalação, equipamento ou facilidade, dentro ou fora da organização, que se avariada ou destruída, prejudicará significativamente a operação do SISCEAB.

São considerados pontos sensíveis, dentre outros, os seguintes locais:

a) instalações de órgão de controle de trafego aéreo;

b) áreas de equipamento de auxílio à navegação aérea ou de comunicação aeronáutica;

c) transformadores de energia elétrica;

d) sistema de abastecimento de água;

e) linhas de suprimento de energia elétrica primária e secundaria; e

f) parque de abastecimento de combustíveis.

2.2.14 SEGURANÇA

Salvaguardar a aviação civil contra atos de interferência ilícita através de uma combinação de medidas e recursos humanos e materiais.

2.2.15 SÍTIO

Local ou ponto ocupado por instalações ou equipamentos do SISCEAB.

2.2.16 VARREDURA

Busca minuciosa implementada em um PSNA com o objetivo de identificar ou descartar a presença de objetos proibidos, os quais possam ser utilizados em atos de interferência ilícita.

3 SEGURANÇA DA AVIAÇÃO CIVIL NO SISCEAB

3.1 O Programa Nacional de Segurança para a Aviação Civil do Sistema de Controle do Espaço Aéreo (PNAVSECEA) segue as diretrizes estabelecidas em normas internacionais ratificadas pelo Brasil e nacionais que tratam sobre segurança da aviação civil contra atos de interferência ilícita e deve ser cumprido por todos os elos do SISCEAB.

3.2 As responsabilidades e diretrizes estabelecidas no PNAVSECEA devem ser incorporadas à regulamentação, aos planos e programas específicos AVSEC e aos procedimentos dos elos do SISCEAB, de acordo com suas características específicas, de forma a garantir nível adequado de proteção da aviação civil contra atos de interferência ilícita.

3.3 Este Manual define os requisitos mínimos para as medidas de segurança a serem estabelecidas e implementadas nos elos do SISCEAB, civis e militares, em coordenação com as respectivas administrações aeroportuárias e em consonância com as normas do COMAER.

3.4 Caso o elo do SISCEAB possua áreas localizadas dentro de instalações aeroportuárias civis, a segurança poderá ser realizada pela administração aeroportuária, mediante convênio, observando os requisitos mínimos estabelecidos nesse Manual.

3.5 Nos aeródromos compartilhados entre organizações militares da aeronáutica e aeroportos civis, as áreas operacionais destas organizações devem preservar, como mínimo, o nível de segurança existente nos respectivos aeroportos e adotar medidas de proteção para o acesso às áreas restritas de segurança dos aeroportos, tanto quanto possível, semelhantes.

3.6 A avaliação de risco determinará a necessidade de estabelecimento e implementação de medidas de segurança em sítios, instalações, equipamentos e auxílios à navegação aérea.

4 MEDIDAS DE SEGURANÇA

4.1 São as medidas aplicadas de acordo com o nível de ameaça ou por determinação específica do DECEA para a proteção de recursos humanos, equipamentos ou instalações dos elos do SISCEAB contra atos de interferência ilícita, podendo ser medidas preventivas de segurança ou medidas adicionais de segurança.

4.2 Devem ser estabelecidas e aplicadas medidas de segurança em sítios, instalações, equipamentos e auxílios à navegação aérea sob responsabilidade dos elos do SISCEAB.

NOTA: Caso o elo esteja localizado em aeródromo civil, as medidas de segurança devem ser coordenadas com a respectiva administração aeroportuária e devidamente documentadas.

4.3 As medidas de segurança das atividades de controle e gerenciamento de tráfego aéreo, de telecomunicações aeronáuticas, de inspeção em voo, de busca e salvamento, dos auxílios à navegação aérea, de meteorologia e informações aeronáuticas e de supervisão da manutenção e distribuição de equipamentos terrestres de auxílio à navegação aérea serão descritas nos Planos Específicos de Segurança (PES-AVSEC) de cada elo.

4.4 Independentemente da solução empregada, a eficácia das medidas de segurança resulta dos seguintes aspectos:

a) da aprovação dos procedimentos de segurança pela autoridade competente;

b) da correta orientação do emprego dos equipamentos;

c) do treinamento rotineiro do pessoal envolvido; e

d) da previsão, existência e adestramento da força de reação e do tempo para engajamento.

4.5 As salas operacionais dos órgãos ATC devem possuir, no mínimo: controle de acesso, vigilância eletrônica de sua porta de entrada e botão de pânico interligado com a equipe de segurança.

4.6 Caso o elo utilize Sistemas de Segurança Eletrônica (SSE), estes devem:

a) respeitar as peculiaridades de cada elo;

b) incrementar a eficácia das medidas de segurança;

c) reduzir a necessidade de recursos humanos; e

d) ser essencialmente proativos, buscando possibilitar à equipe de segurança antecipar-se às ameaças, dissuadindo, repelindo ou neutralizando-as, antes que essas alcancem o seu intuito.

4.7 Os equipamentos utilizados para segurança devem possuir adequada previsão de atualização, manutenção e reposição. Este aspecto, se não observado, acarreta na inoperância dos sistemas empregados, com impacto negativo sobre sua eficácia e confiabilidade, e consequente aumento da vulnerabilidade.

5 SEGURANÇA DO PESSOAL

A Segurança do Pessoal tem como objetivo confirmar a identidade, experiência de trabalho prévia, além de verificar o histórico criminal de pessoas que possuam envolvimento com as atividades de segurança dos PSNA ou sejam autorizadas a acessar a ARS e/ou os pontos sensíveis desacompanhadas.

É importante que sejam estabelecidas medidas relativas à seleção e avaliação do desempenho do pessoal que trabalha diretamente com AVSEC e do pessoal não pertencente à segurança que pode estar envolvido na implementação de medidas de segurança.

As medidas de seleção adotadas, de análise de desempenho e de desligamento da função visam garantir a salvaguarda das instalações, equipamentos e informações críticas do SISCEAB.

O pessoal não pertencente à segurança são os ATCO, técnicos, ou pessoas do efetivo que possuam atribuições relacionadas à operação do órgão ATS e podem estar envolvidos na aplicação de medidas de segurança, bem como acessar à ARS e/ou pontos sensíveis desacompanhados.

Devem ser submetidos aos procedimentos de segurança do pessoal os envolvidos com:

a) atividades de gerenciamento AVSEC;

b) controle de acesso;

c) vigilância e patrulhamento;

d) inspeção pessoal;

e) inspeção veicular;

f) condução de cursos e treinamentos AVSEC;

g) condução de atividades de controle de qualidade AVSEC;

h) condução de atividades de segurança do pessoal;

i) condução de atividades de segurança da informação e das telecomunicações; e

j) acesso desacompanhado à ARS e/ou aos pontos sensíveis.

5.1 SELEÇÃO

5.1.1 A seleção do pessoal que tenha responsabilidades, em todos os níveis, com funções de segurança, ou envolvimento na implementação das mesmas dos elos do SISCEAB, deve ser baseada em aspectos que garantam a sua idoneidade, adequação do perfil para a atividade e condição física e mental para o desempenho pleno das funções.

5.1.2 As medidas de segurança a serem aplicadas durante o processo seletivo de candidatos a ocuparem posições e funções citadas no item supracitado devem conter:

a) avaliação da sensibilidade da função: análise criteriosa das atividades a serem executadas, de acordo com o grau de importância e sensibilidade, correlacionando com as características pessoais dos candidatos;

b) investigação preliminar de segurança: levantamento dos dados biográficos e comportamentais de cada candidato, brasileiro ou estrangeiro, utilizando, como recurso, consultas a registros disponíveis junto aos órgãos competentes, nacionais ou estrangeiros, e verificação de antecedentes, no intuito de levantar fatos que os contraindiquem ao desempenho das funções. Deve ser verificada a documentação do candidato, analisada a experiência de trabalho prévia, histórico criminal, local de residência nos últimos 5 anos e se existem indícios de que o candidato possua envolvimento ou seja simpatizante de grupos suspeitos de atividades terroristas ou criminosas; e

c) entrevista seletiva: estabelecimento de procedimentos cautelares na fase da consulta e confirmação de dados biográficos obtidos.

5.1.3 Caso durante a investigação preliminar for verificado que o candidato foi condenado ou encontra-se em julgamento por algum dos seguintes motivos, definidos como critérios de desqualificação, será proibida a sua entrada nos pontos sensíveis e na ARS desacompanhado.

a) posse ou uso de drogas ilícitas;

b) tráfico de drogas ilícitas;

c) tráfico de armas ou posse ilegal de armas;

d) lesão corporal;

e) extorsão;

f) atos que ponham em risco a segurança pública, incluindo atos de interferência ilícita contra a aviação civil;

g) assédio sexual;

h) envolvimento com organizações criminosas;

i) furto ou roubo;

j) receptação de bens roubados;

k) fraude;

l) falsidade ideológica; e

m) outras situações que podem pôr em risco a segurança da aviação civil.

5.1.4 Deve ser mantido o registro da informação levantada acerca dos candidatos pelo prazo de 5 anos após o desligamento da função.

5.2 DESEMPENHO DA FUNÇÃO

5.2.1 Para o pessoal envolvido nas atividades citadas no *caput*, deverão ser observados os seguintes aspectos:

a) credenciamento de segurança: os elos do SISCEAB devem solicitar ao órgão competente o fornecimento de credencial de segurança de pessoa física, estabelecendo o grau de sigilo para o acesso de cada credenciado, de acordo com a necessidade de cada função ou atividade;

b) cultura da segurança: estabelecimento de processos contínuos de treinamento do pessoal em AVSEC, da admissão ao desligamento, por meio de orientações iniciais, específicas ou periódicas; e

c) controle periódico de segurança: acompanhamento contínuo do pessoal a fim de detectar indícios de ameaça interna, bem como comportamentos incompatíveis ao desempenho da função. A cada renovação da credencial de acesso permanente do pessoal citado no *caput*, deverá ser realizada uma investigação de segurança, apresentada no item 5.1.2, letra "b".

5.3 DESLIGAMENTO

5.3.1 O processo de desligamento do pessoal citado nos itens "a", "f", "g", "h" e "i" do *caput*, devem conter:

a) entrevista final: por ocasião do desligamento, deve-se ser comunicado ao desligado sobre a responsabilidade na manutenção do sigilo de conhecimentos e informações classificadas aos quais tenha tido acesso durante a permanência na função ou atividade, e incentivado para que o sigilo do conhecimento seja mantido. Deverá ser utilizado o Termo de Compromisso de Manutenção do Sigilo, conforme **Anexo A**.

b) controle após o desligamento: quando houver riscos, acompanhar ou, quando não for possível, solicitar ao DECEA o acompanhamento dos militares ou civis desligados de funções mais sensíveis.

5.4 AMEAÇA INTERNA

5.4.1 Ameaça interna é um potencial problema para a segurança da aviação civil e deve ser combatida diariamente.

5.4.2 As ameaças internas são causadas por fatores de risco específicos, sendo eles:

a) ignorância: falta de consciência das medidas de segurança;

b) complacência: abordagem relaxada das medidas de segurança; e

c) malícia: o infiltrado tem como objetivo realizar um ato que cause danos ao SISCEAB.

5.4.3 As principais motivações para que elementos do SISCEAB se tornem uma ameaça interna complacente ou maliciosa geralmente são: ego, vingança, ideologia, ganho material, coação ou chantagem.

5.4.4 Uma série de indicadores comportamentais podem ajudar a identificar um elemento infiltrado:

a) vida pregressa: histórico de problemas mentais, dificuldade no trato interpessoal, previa violação da lei ou dificuldade em se submeter à autoridade estabelecida;

b) comportamentos estranhos: conflitos não justificados com pares ou superiores, violação de regras incluindo os procedimentos de segurança, atrasos ou faltas recorrentes;

c) estressores organizacionais: rebaixamento de cargo, suspensão ou existência de punições e não promoção no tempo devido; e

d) estressores pessoais: problemas financeiros, problemas de relacionamento, casamento ou de família e problemas com a justiça.

5.4.5 Elementos infiltrados podem ter como objetivo os seguintes atos:

a) espionagem;

b) terrorismo;

c) comprometimento da segurança;

d) roubo de bens materiais;

e) sabotagem;

f) roubo de informações; e

g) atos que ponham em risco a vida e a saúde pública.

5.4.6 A abordagem para contrapor as ameaças internas se faz através da combinação da implementação de medidas regulatórias robustas e da promoção da cultura de segurança para todo o efetivo dos elos do SISCEAB.

5.4.7 A ameaça interna pode se apresentar tanto através de membros do efetivo quanto de pessoas interessadas em compô-lo, ambas com o objetivo de obter acesso e/ou vantagens para perpetrarem atos de interferência ilícita ou para facilitarem a realização destes atos.

5.4.8 As medidas de contraposição às ameaças internas devem apresentar uma abordagem em camadas e cada uma delas deve atuar em um tipo de ameaça interna, sendo elas:

a) ignorância: controle de acesso, medidas segurança existentes entre área externa do PSNA e os pontos sensíveis e o treinamento do efetivo na aplicação dessas medidas;

b) complacência: controle de acesso, medidas de segurança existentes entre a área externa do PSNA e os pontos sensíveis, aplicação das medidas de segurança; e

c) malícia: controle de acesso, medidas de segurança existentes entre a área externa do PSNA e os pontos sensíveis e identificação e acompanhamento dos indicadores comportamentais citados em **5.4.4**.

5.4.9 Os recursos para a contraposição às ameaças internas são as pessoas, processos e tecnologias que auxiliem na mitigação dos riscos e redução das vulnerabilidades, sendo eles:

a) existência de controles de acesso para todos aqueles que acessarem os PSNA e os pontos sensíveis;

b) efetivo e recorrente sistema de verificação de antecedentes a todo o pessoal autorizado a acessar as áreas controladas e os pontos sensíveis sem acompanhamento, incluindo aqueles que estiverem implementando medidas de segurança;

c) um processo de contratação que leve em conta o papel de cada função a ser desempenhada e o acesso às áreas controladas e pontos sensíveis que

necessitarem para essas funções, além dos potenciais riscos criados por esse acesso;

d) aplicação dos critérios de desqualificação;

e) realização de inspeções pessoais aleatórias e imprevisíveis no efetivo dos PSNA, em veículos e rondas aleatórias nos pontos sensíveis;

f) realização de palestras a todo o efetivo dos PSNA informando as formas de identificação de ameaças internas;

g) existência de um eficaz e bem divulgado sistema de reporte, que funcionará de maneira dissuasiva, reativa e em alguns casos preditiva, que será realizado através do preenchimento do RELSEC; e

h) permitir o acesso aos pontos sensíveis somente ao pessoal estritamente necessário.

5.4.9 O uso de processos de inspeção que não sejam completamente randômicos e imprevisíveis não é suficiente para deter as ameaças internas, pois os infiltrados podem aprender sobre a previsibilidade do sistema, através da exposição regular a estes e a explorar essas vulnerabilidades.

6 BARREIRAS PERIMETRAIS

6.1 DEFINIÇÃO

6.1.1 Barreira é o meio utilizado para definir os limites físicos de uma instalação ou área e para restringir, retardar ou impedir o acesso a esses locais, com o propósito de facilitar a detecção de intrusão e dissuadir física e psicologicamente a entrada não autorizada.

6.2 CLASSIFICAÇÃO

6.2.1 As barreiras perimetrais podem ser classificadas da seguinte forma:

a) naturais;

b) artificiais;

c) psicológicas;

d) eletrônicas; e

e) mistas.

6.2.1.1 Naturais: são acidentes no terreno que oferecem um grau de proteção semelhante a uma barreira artificial como rios, montanhas, penhascos, vegetação ou mata fechada, cercas-vivas entre outros.

6.2.1.2 Artificiais: são obstáculos construídos pelo homem para aumentar o grau de proteção de locais como muros, cercas, cones, cordões de isolamento, cancelas, dilaceradores de pneus, etc.

6.2.1.3 Psicológicas: são todos os meios ou métodos que gerem um aumento da proteção através de alertas ou avisos e que venham a produzir um ajustamento mental ou que atue como agente de inibição aos ilícitos.

6.2.1.4 Eletrônicas: podem ser definidas como todo e qualquer dispositivo baseado em um circuito eletrônico que visa barrar, impedir, canalizar, retardar, registrar ou detectar a entrada ou a saída de pessoas não autorizadas.

6.2.1.5 Mistas: são as barreiras em que se utilizam dois ou mais tipos, a exemplo de um muro de alvenaria com placas de aviso, monitoramento eletrônico e um sistema de detecção de intrusão.

6.2.2 As barreiras formam um elo da corrente de proteção e necessitam de monitoramento por uma equipe de segurança ou por um Sistema de Vigilância Eletrônica.

6.3 RECURSOS ADICIONAIS

Na configuração de um sistema de segurança e em função da percepção das ameaças no sítio e da classificação de risco, além de muros e cercas de proteção, poderão ser considerados os seguintes recursos adicionais:

a) emprego de cães;

b) concertinas;

c) obstáculos nas vias de acesso;

d) barreiras eletrônicas;

e) micro-ondas ou radiofrequência;

f) barreiras por sensor infravermelho ativo;

g) barreiras eletrificadas;

h) cabeamento sensoriado; e

i) sensores ativos de dupla tecnologia

6.3.1 Emprego de cães: podem ser empregados para detecção, alerta e proteção de locais, devido à maior capacidade olfativa e auditiva. Sua presença constitui, por si só, um fator de dissuasão para o invasor.

6.3.2 Concertinas: a proteção de cercas e muros pode ser melhorada com a utilização de concertinas, redes laminadas, arame farpado e espirais de aço, que têm como finalidade dificultar, impedir ou retardar o acesso a áreas proibidas.

6.3.3 Obstáculos nas vias de acesso: forçam a diminuição da velocidade dos veículos que se aproximam dos portões de acesso ao sítio. Poderão ser tonéis, cavalo de frisa, trilhos de trem, dilaceradores de pneus, cancelas e redutores de velocidade, entre outros.

6.3.4 Barreiras eletrônicas: protegem as instalações e equipamentos e diminuem o custo com a utilização de pessoal, bem como melhoram a eficácia do sistema de segurança mediante ao monitoramento ininterrupto. Para a utilização deste recurso, deverão ser observados os seguintes aspectos:

a) o ponto chave para a instalação de equipamentos eletrônicos é a infraestrutura dos sistemas elétricos;

b) deve ser considerado que todo o aparato eletrônico de segurança exigirá fornecimento de energia elétrica com qualidade e de maneira ininterrupta;

c) como os equipamentos de segurança são alimentados em baixa tensão, deverão ser verificadas as condições das instalações elétricas com respeito às normas técnicas vigentes, que tratem de instalações elétricas de baixa tensão;

d) em qualquer caso, deverá existir um sistema elétrico bem dimensionado, a fim de permitir o contínuo funcionamento dos equipamentos envolvidos, dotado de Sistema de Energia Ininterrupto (UPS); e

e) os cabos alimentadores deverão ser verificados com respeito às condições de isolamento e devem ser previstos sistemas de aterramento compatíveis, bem como a instalação de dispositivos de proteção contra descargas atmosféricas a fim de garantir tensões compatíveis no caso de curtos evitando, assim, a queima dos equipamentos de segurança.

6.3.4.1 Micro-ondas ou radiofrequência: meio eletrônico de detecção de intrusão de pessoas não autorizadas, dotado de transmissores e receptores, tendo baseada sua ação no efeito *doppler*, que pode estar ligado a um sistema de câmeras e monitoramento eletrônico. No emprego deste tipo de barreira, deve ser levada em conta a sua instalação em locais em que não haja a possibilidade de interferência em outros equipamentos eletrônicos, em especial em auxílios à navegação aérea.

6.3.4.2 Barreiras por sensor infravermelho ativo: baseado no princípio de transmissão e recepção de feixes infravermelho, bloqueados por objetos em movimento, que geram um contato seco (aberto ou fechado) para uma central de alarme. Caso o sensor infravermelho não possua dispositivo de regulagem de sensibilidade, seu emprego deve ser restrito a ambientes em que não haja interferência de pequenos animais, insetos ou vegetação, tendo em vista a sua grande sensibilidade para detectar movimento.

6.3.4.3 Barreiras eletrificadas: cerca composta por fios de baixa resistência, alimentada com altas tensões, pulsadas e de baixíssima amperagem. O equipamento instalado para energizar a cerca deverá prover choque pulsativo em corrente contínua, com amperagem que não seja mortal, em conformidade com as normas da Associação Brasileira de Normas Técnicas (ABNT). Deverão ser fixadas, em lugar visível, em ambos os lados da cerca eletrificada, placas de aviso que alertem sobre o perigo iminente de choque e que contenham símbolos que possibilitem a sua compreensão por pessoas analfabetas ou que não leiam português. O emprego deste meio deve ser restrito e deve levar em conta o especificado nas legislações federais, estaduais e/ou municipais.

6.3.4.4 Cabeamento sensoriado: sistema de alta confiabilidade e com elevado número de recursos que permite o gerenciamento, a criação e a supressão de zonas de sensibilidade. O princípio de funcionamento deste equipamento baseia-se na instalação de um cabo detector agregado a um meio (cercas, muros, alambrados, etc.) ou enterrado. Seu emprego deve ser limitado aos ambientes em que não haja interferência mecânica da natureza (raízes) ou condições adversas de temperatura e umidade no solo, que possibilita a detecção de entrada de pessoas não autorizadas, sendo os modelos principais de equipamentos:

a) sísmico: a vibração mecânica aciona o dispositivo de emissão de sinais da central de alarmes e monitoramento;

b) eletromagnético: detecta a variação no pulso elétrico inserido na rede (cabo sensor) e aciona o mecanismo de sinalização; e

c) por continuidade: percebe interrupção ou a quebra de um cabo detector de pequena espessura e aciona o sistema de sinalização.

6.3.4.5 Sensores ativos de dupla tecnologia: dispositivo eletrônico que usa o disparo conjugado de radiofrequência com a leitura do espectro de infravermelho para uma detecção com baixo índice de falsos alarmes. Este equipamento tem a capacidade de idealizar a exclusão de alvos pela massa por meio de regulagem interna e seu uso é recomendado para áreas externas e internas, além de poder ser exposto a intempéries.

6.4 EMPREGO

6.4.1 Os projetos de construção de barreiras perimetrais devem ser proporcionais à classificação obtida por intermédio da avaliação de risco.

6.4.2 O nível de proteção de uma barreira patrimonial dependerá de sua altura, método de construção, material utilizado e recursos adicionais utilizados para aumentar o desempenho ou eficácia.

6.4.3 Os muros e cercas devem ser submetidos a um contínuo processo de manutenção de forma a facilitar a substituição de seções danificadas ou inservíveis.

6.4.4 Nos locais em que a corrosão é mais provável, o uso de cercas revestidas em plástico ou feitas de aço galvanizado é recomendado.

6.4.5 Os muros e cercas devem, sempre que possível, ser construídos em linha reta para facilitar o monitoramento. As junções, onde os muros e cercas mudam de direção, geralmente são mais fáceis de escalar e devem ser minimizadas. As junções voltadas para fora da área patrimonial devem ser evitadas, pois são ainda mais fáceis de escalar.

6.4.6 Muros ou cercas que protegerem pontos sensíveis devem ser construídos no mínimo com as mesmas especificações técnicas que os que delimitam a área patrimonial do PSNA ou do aeroporto.

NOTA: Os auxílios à navegação instalados em locais protegidos pelas barreiras do aeroporto ou PSNA, nos quais a classificação do risco inerente seja baixa, não necessariamente deverão ser cercados.

6.4.7 Para garantir a segurança operacional e evitar interferência eletromagnética, conforme legislações e regulamentos específicos, as barreiras que protegerem os auxílios à navegação deverão ser:

a) frangíveis, caso instaladas próximas à pista de pouso; e/ou

b) não-metálicas, caso instaladas próximas ao auxílio.

6.4.8 As barreiras devem ser visíveis e sinalizadas para o público em geral.

6.4.9 Os muros e cercas devem possuir uma altura mínima de 2,44 metros.

6.4.10 Os muros e cercas devem ser reforçados por recursos adicionais, conforme **6.3**, consoante análise de risco local a ser protegido, em quantidade de acordo com a tabela abaixo:

Nível de Risco Inerente	Recursos Adicionais
baixo	-
médio-baixo	1
médio	2
médio-alto	3
alto	4

Tabela 1. Quantidade mínima de recursos adicionais

6.4.11 As barreiras devem ser suficientemente altas para impedir que sejam escaladas. Caso a altura mínima de 2,44 metros não seja suficiente para garantir este critério, devem ser aumentadas, conforme análise do especialista de segurança responsável pelo planejamento da construção. Devem ser levadas em consideração as características do terreno adjacente.

6.4.12 Os muros e cercas devem prevenir que uma pessoa passe por baixo dela rastejando ou cavando. Para atender este critério podem ser enterradas ou afixadas em uma base de concreto ou similar.

6.4.13 As barreiras adjacentes às áreas públicas deverão possuir uma zona de exclusão, ao longo de sua extensão, com no mínimo 3 metros de largura, para o lado interno, com a finalidade de permitir o monitoramento e o patrulhamento pela equipe de segurança.

NOTA 1: Pode ser criada uma zona de exclusão para o lado externo da barreira patrimonial, caso o elo julgue necessária.

NOTA 2: A zona de exclusão deve permitir a passagem dos veículos de patrulhamento utilizados pela equipe de segurança do elo.

6.4.14 As barreiras patrimoniais e os pontos sensíveis deverão possuir iluminação adequada ao seu monitoramento e patrulhamento.

6.4.15 As barreiras devem ser implantadas de tal forma que dificultem o arremesso de substâncias e objetos para o interior dos pontos sensíveis.

6.4.16 Os portões de acesso deverão proporcionar, quando fechados, a mesma segurança que as barreiras perimetrais.

6.4.17 O uso de barreiras psicológicas que identifiquem a criticidade de um ponto sensível para a operação do SISCEAB deve ser minimizado, devendo-se utilizar prioritariamente aquelas que exponham a proibição de acesso de maneira genérica, para evitar despertar o interesse de perpetradores.

7 CREDENCIAMENTO E CONTROLE DE ACESSO

7.1 PRINCÍPIOS GERAIS

7.1.1 O setor de segurança dos elos deverá estabelecer pontos de controle de acesso às áreas e instalações do SISCEAB, a fim de garantir que apenas o pessoal autorizado tenha acesso.

7.1.2 O elo deverá estabelecer o menor número possível de pontos de controle e de autorização de acesso às áreas controladas e restritas, objetivando melhor controle da segurança e redução dos custos associados.

7.1.3 Os postos de controle de acesso dos elos devem ser equipados com um sistema de comunicação, alarme ou botão de pânico interligado ao setor de segurança e à equipe de reação.

7.1.4 Deverá ser assegurado que as barreiras físicas dos postos de controle e credenciamento sejam mantidas em boas condições.

7.1.5 Todas as pessoas que acessam as instalações dos elos do SISCEAB devem ser identificadas, inclusive os passageiros e o motorista dos veículos.

NOTA: Os corredores de acesso de veículos e de pedestres deverão ser separados.

7.1.6 Deverá ser feita a identificação de todos os veículos particulares.

7.1.7 Os motociclistas devem retirar o capacete no momento da identificação.

7.1.8 Quando não houver sistemas eletrônicos para o controle de acesso, devem ser elaboradas fichas de controle padronizadas para todos os pontos de controle de veículos e de pedestres.

7.1.9 Os ciclistas devem se identificar da mesma forma que os pedestres. Caso necessário, o elo deverá desenvolver novos procedimentos para atender esse requisito.

7.1.10 O controle de acesso de pedestres aos ônibus que fazem o transporte do efetivo é de responsabilidade do motorista, o qual deve ser identificado na entrada e saída do elo.

7.1.12 O acesso às instalações definidas como pontos sensíveis está limitado a:

a) pessoas portadoras de credencial adequada ao nível de segurança estabelecido; e

b) visitantes e prestadores de serviço de natureza não permanente que, porventura, tenham de acessar ponto sensível, deverão ser devidamente identificados e acompanhados, devendo o responsável pela equipe de segurança e o Agente Local AVSEC estarem ciente da sua entrada.

7.1.13 O elo responsável pelo ponto sensível que autorizou a entrada de veículos e pessoas deve prover os meios para que o visitante seja continuamente acompanhado.

7.1.14 Os elos devem estabelecer procedimentos para controle de chaves de salas técnicas de órgãos ATC e de equipamentos de auxílio à navegação aérea, observando os seguintes requisitos:

a) lista contendo as pessoas autorizadas a retirar as chaves dos pontos sensíveis existentes no local de controle de chaves.

b) revistas periódicas pelo Agente Local AVSEC, verificando o correto funcionamento do controle de chaves.

7.1.15 Os elos devem, sempre que possível, estabelecer e implementar sistemas eletrônicos para controle de acesso de pessoas e veículos.

7.1.16 Os registros de controle de acesso e credenciamento de pessoas e veículos devem ser arquivados em local de acesso controlado, pelo elo emitente.

7.1.17 Os procedimentos para credenciamento e acesso de pessoas e viaturas e pertencentes aos elos do SISCEAB às ARS dos aeroportos devem ser coordenados com o operador aeroportuário.

7.2 CREDENCIAMENTO

7.2.1 O credenciamento de pessoas e veículos, desde a sua formalização, processamento e cancelamento, é um instrumento imprescindível para o controle de segurança dos elos. Deverá ser gerenciado por um setor específico, dotado de pessoal qualificado e instalado em área de acesso restrito.

7.2.2 O setor do elo que solicitar a emissão de credencial de acesso será responsável pela triagem e garantia da idoneidade da pessoa para a qual será emitida a autorização de acesso.

7.2.3 A emissão e o controle de credenciais para acesso devem seguir os seguintes critérios:

a) solicitadas por escrito e devidamente cadastradas no setor específico de credenciamento do elo;

b) verificadas quanto a sua necessidade, de acordo com a área ou setor de atuação, com base nas justificativas apresentadas;

c) concedidas para acesso limitado a determinadas áreas, setores e pelo tempo necessário ao desempenho de seu trabalho;

d) concedidas somente após análise do setor de segurança, com base nas justificativas apresentadas e resultado da investigação preliminar de segurança, para os casos citados no *caput* do Capítulo 5;

e) portadas de maneira visível, na altura do peito, durante todo tempo de permanência nas instalações;

f) adotadas providências administrativas de controle para evitar desvios e falsificações, bem como para reduzir o extravio ou a não devolução;

h) renovadas e emitidas, periodicamente, no máximo a cada dois anos, mantendo a integridade do documento;

i) expedidas em condições especiais e padronizadas, para os agentes envolvidos no gerenciamento de crise advinda de um ato de interferência ilícita; e

j) destruídas ou canceladas, mediante controle específico do setor de segurança, após o término da autorização de acesso.

7.2.4 As credenciais poderão ser eventuais, temporárias ou permanentes, de acordo com a necessidade de permanência nas instalações do elo, obedecendo os seguintes aspectos:

a) eventual: pessoas alheias à atividade do elo que necessitem de ingresso ocasional, tais como visitantes, civis e militares em serviço ou curso ou operação, funcionários de prestadoras de serviço, imprensa e estrangeiros, entre outras, que necessitem de ingresso por até 15 (quinze) dias;

b) temporária: pessoas alheias à atividade do elo que necessitem de ingresso regular, tais como militares ou civis em curso ou operação, funcionários de prestadoras de serviço, imprensa e estrangeiros, entre outras, que necessitem de ingresso acima de 15 (quinze) dias e menor que um ano.

c) permanente: pessoas que trabalhem no elo ou necessitem de acesso por mais de um ano. Deverão ser revalidadas a cada 2 (dois) anos.

7.2.5 A renovação de credencial deverá seguir as mesmas etapas realizadas para a emissão desta, conforme **7.2.2** e **7.2.3**.

7.2.6 As credenciais temporárias e permanentes devem conter, no mínimo:

a) nome do portador;

b) identificação do empregador, quando for o caso;

c) áreas as quais o acesso é permitido;

e) fotografia do portador; e

f) data de validade.

7.2.7 Caso haja tempo hábil, a credencial eventual seguirá o padrão supracitado. Caso negativo, a pessoa deverá estar acompanhada por pessoal com credencial permanente válida, durante todo o seu trânsito no interior do elo do SISCEAB.

7.2.8 As pessoas e veículos autorizados a acessar os pontos sensíveis deverão possuir esta autorização de acesso discriminada na credencial.

7.2.9 Somente será concedida credencial para as pessoas em exercício no elo ou no desempenho de atividade relacionada à operação desta.

7.2.10 A emissão de credencial será feita mediante a apresentação de documento legal de identidade expedido por órgão competente, considerando o nível de acesso inerente a sua presença e autorização específica do respectivo setor solicitante.

7.2.11 Devem ser indeferidas as solicitações de credenciamento de requerentes com antecedentes criminais que possam colocar em risco a segurança da aviação civil.

7.2.12 O estrangeiro ou o brasileiro que tenha morado fora do país e necessite entrar nos pontos sensíveis deve ser submetido ao processo de investigação preliminar de segurança.

7.3 ACESSO DE PESSOAS

7.3.1 O acesso de inspetores e investigadores da autoridade aeronáutica às ARS e áreas controladas, no exercício de suas obrigações funcionais, será permitido mediante o porte de credenciais oficiais e medidas de segurança estabelecidas pelo operador do aeródromo.

7.3.2 As pessoas que, intencionalmente, tentem ou consigam ultrapassar ou burlar os pontos de controle devem ser retidas e encaminhadas ao setor de segurança para as providências previstas em legislação pertinente.

7.3.3 A emissão de credencial para estrangeiro e membros da imprensa obedecerá à instrução específica, devendo estar acompanhados durante todo o seu trânsito no interior do PSNA.

7.4 ACESSO DE VEÍCULOS

7.4.1 Deverão ser estabelecidos meios para que os veículos que tenham acesso ao interior dos elos do SISCEAB sejam identificados com segurança e fluidez.

7.4.2 O controle dos pontos de acesso de veículos deverá ser prático, seguro e eficaz. As revistas veiculares devem ser realizadas somente quando houver suspeita da ocorrência de algum ilícito ou por ordem do responsável pela segurança do PSNA.

7.4.3 O setor de segurança do PSNA deverá estabelecer procedimentos padronizados para o controle de acesso de veículos utilizando os seguintes recursos:

a) portões equipados com comunicação, alarme, CFTV, dilaceradores de pneus, sistema de iluminação, espelho de verificação e outros dispositivos de segurança operados pela equipe de serviço de guarda;

b) guaritas construídas, sempre que possível, com paredes em concreto, visores blindados, seteira de tiro e com instalações de conforto adequadas para os seus ocupantes;

c) identificação, verificação de credenciais e inspeção de veículos, seus ocupantes e carga;

d) interdição do acesso a pedestres; e

e) medidas adicionais de segurança podem ser implementadas em função da especificidade do local e dos equipamentos instalados e da avaliação de risco.

7.4.4 A credencial de acesso do veículo deve ser portada em local visível e sem obstrução, e suas informações cadastrais devem conter:

a) marca, modelo e cor;

b) número da placa;

c) ano de fabricação;

d) número de registro da credencial fornecida pelo setor de segurança;

e) nome da empresa ou do empregador responsável, se for o caso;

f) data de expedição e validade; e

g) áreas restritas para a qual a credencial é válida.

7.4.5 Qualquer veículo abandonado e não identificado, tanto no interior quanto nas proximidades do PSNA, deve ser objeto de análise do setor de segurança, considerando a sua procedência e a possibilidade da existência de artigo perigoso ou proibido em seu interior. Após essa análise, caso haja suspeita de material explosivo, material com elementos QBRN, drogas ilícitas, armamentos ou qualquer outra situação anormal, deve ser acionado pessoal

especializado para cada tipo de ameaça identificada, tais como esquadrão antibombas, esquadrão antiterrorismo, hospitais e afins.

7.4.6 A credencial do veículo não autoriza o acesso irrestrito de seus ocupantes, devendo ser realizada a identificação de todos os ocupantes, simultaneamente à identificação do veículo.

7.4.7 Os veículos do próprio elo e de outros órgãos públicos, bem como os ocupantes, no exercício de suas funções, não estão isentos de serem identificados e inspecionados, conforme normas específicas.

NOTA: Para as organizações militares do DECEA aplica-se a NOSDE PRO 03, que determina que viaturas com autoridades civis e militares, devidamente identificadas, não serão alvo de revistas.

7.4.8 As câmeras instaladas nos controles de acesso de veículos devem ser instaladas de forma a filmar de maneira clara a placa dos veículos e o rosto dos motoristas.

8 INSPEÇÃO DE SEGURANÇA DA AVIAÇÃO CIVIL

8.1 O objetivo da inspeção de segurança da aviação civil é prevenir que artigos perigosos ou itens proibidos, conforme **Anexo B**, sejam introduzidos, sem autorização, ao elo do SISCEAB.

8.2 Em razão do nível de ameaça e de fatores de risco, os elos do SISCEAB poderão estabelecer e implementar procedimentos de inspeção de segurança para o efetivo ou visitantes, com a finalidade de identificar e detectar itens que possam ser utilizados para cometer ato de interferência ilícita no interior do PSNA.

8.3 A necessidade de realização da inspeção de segurança da aviação civil, em pessoas e pertences, para ingresso ao PSNA, bem como a lista de itens proibidos será definida pelo elo do SISCEAB com base nos resultados de avaliações de risco, podendo ser distintas para efetivo e para visitantes.

8.4 As informações específicas sobre procedimentos e responsabilidades pela inspeção de segurança da aviação civil devem ser incluídas no PES-AVSEC

8.5 A inspeção deve ser realizada prioritariamente com o uso de equipamentos de segurança (detector de metais, raios-x, ETD, etc.) e como alternativa ou complemento, de forma manual.

8.6 Quando ainda existir a suspeição sobre a pessoa que ingressa, adicionalmente pode ser realizada a busca pessoal ou inspeção manual de pertences, com a finalidade de identificar qualquer item proibido ou de natureza suspeita, observando os seguintes aspectos:

a) consistirá na procura material nas vestes, pastas, malas e outros objetos que estejam com a pessoa revistada e, quando necessário, no próprio corpo;

b) realizada preferencialmente por pessoa de mesmo sexo, se não importar retardamento ou prejuízo da diligência conforme legislações específicas;

c) caso a pessoa inspecionada solicite, a inspeção manual de pertences e a busca pessoal devem ser realizadas em local público ou em sala reservada;

d) deve ser acompanhada de testemunha pertencente ao efetivo do elo;

e) caso a pessoa se recusar a inspeção de si próprio ou de seus pertences ou na impossibilidade de assegurar que o passageiro não porta item proibido, o seu acesso ao interior do PSNA será negado.

8.7 Na hipótese de detecção de item proibido – definidos pelo elo – e que não constituam crime, a entrada da pessoa portando o item deve ser negada. O portador deve manter o item proibido fora da área patrimonial.

8.8 Caso seja detectada a presença de artigos perigosos ou a pessoa apresentar indícios de portar objetos, materiais ou substâncias cuja posse, em tese, constitua crime, deverá ser acionada a força de reação, equipe de segurança ou órgão de segurança pública, conforme legislação e regulamentos específicos.

8.9 Pode ser aplicada inspeção de segurança aleatória, incluindo a busca pessoal e a inspeção manual de pertences como forma de contrapor às ameaças internas.

8.10 A seleção de equipamentos de segurança a serem adquiridos pelos PSNA deve atender à especificação técnica mínima dos parâmetros de detecção, calibração e manutenção a serem utilizados nos equipamentos de controle de segurança, conforme regulamento específico, respeitando as recomendações dos fabricantes.

8.11 Deve ser mantida uma programação para testes, ensaios de aferição e de calibração de equipamentos e sistemas de suporte às medidas de segurança.

8.12 O pessoal responsável pelas inspeções de segurança da aviação civil deverá ser capacitado e treinado de acordo com regulamento específico.

9 SISTEMAS DE SEGURANÇA ELETRÔNICA

9.1 CONCEPÇÃO

9.1.1 A segurança das instalações do SISCEAB deve integrar três atividades básicas: o controle de acesso, a vigilância e a reação, que devem ser apoiadas por uma estrutura de comando e controle baseada na tecnologia da informação e por uma efetiva rede de comunicações.

9.1.2 A implantação de Sistema de Segurança Eletrônica (SSE) nos elos do SISCEAB tem a finalidade de:

a) aumento da eficácia das medidas de segurança das instalações;

b) redução dos recursos humanos empregados na segurança das instalações;

c) padronização e interoperabilidade dos SSE já instalados e dos que serão implantados nos elos; e

d) redução de inoperância dos SSE já implantados, aumentando a disponibilidade e a confiabilidade.

9.1.3 Os SSE devem respeitar as peculiaridades de cada elo, incrementar a eficácia das medidas de segurança existentes e reduzir a necessidade de recursos humanos.

9.1.4 Os SSE devem ser essencialmente proativos, buscando possibilitar à equipe de segurança do elo antecipar-se às ameaças, dissuadindo, repelindo ou neutralizando-as, antes que essas alcancem o seu intuito.

9.2 CATEGORIAS

9.2.1 Os SSE são categorizados por sua abrangência e pelo nível de interoperabilidade entre seus módulos, podendo ser: Básicos (SSEB) ou Complexos.

9.2.2 Os SSE Básicos devem ser constituídos pelos seguintes módulos:

a) Módulo de Vigilância Eletrônica (MVE);

b) Módulo de Detecção de Intrusão (MDI);

c) Módulo de Central de Vigilância Eletrônica (MCVE); e

d) Módulo de Reação (MRE).

9.2.3 O SSE Básico é a estrutura mínima necessária para propiciar algum auxílio à Segurança das Instalações. Neste sentido, deve-se considerar a existência de um Módulo de Vigilância Eletrônica (MVE), um Módulo de Detecção de Intrusão (MDI), um Módulo de Central de Vigilância Eletrônica (MCVE) e um Módulo de Reação (MRE), relacionando-se de acordo com a seguinte estrutura:

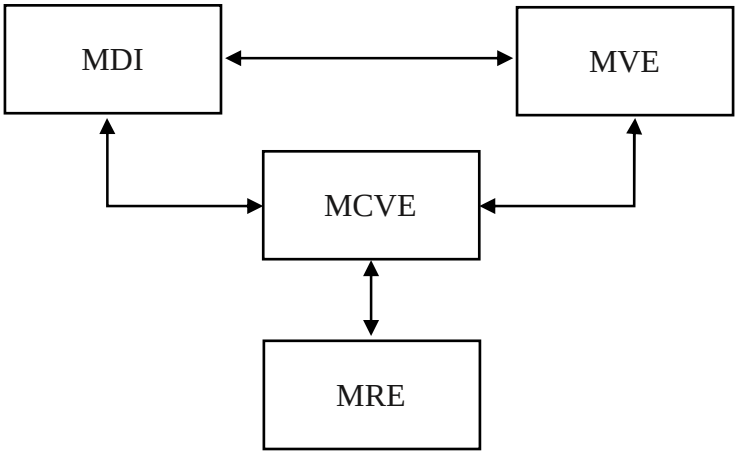

Figura 1: Estrutura esquemática de um SSE Básico

9.2.4 De acordo com o nível de risco, é imperioso que as três vertentes do SSE Básico sejam implementadas conforme a **Tabela 1**. As soluções aplicadas são cumulativas, ou seja, para o nível alto, além de suas implementações relacionadas, sugere-se a aplicação das abordagens dos níveis anteriores.

Nível de Risco	Sensores nas Áreas Restritas	Capacidade do CFTV
baixo	Perímetro externo	Nenhuma
médio-baixo	Perímetro externo e ambiente interno	Observar
médio	Perímetro externo, ambiente interno e alarme com ativação/desativação por intermédio de PIN	Reconhecer
médio-alto ou alto	Perímetro externo, Ambiente interno, Alarme com Ativação/Desativação por intermédio de PIN e Botão de pânico	Identificar

Tabela 1: Soluções de SSE Básicos

9.2.5 As capacidades do CFTV são definidas da seguinte maneira:

a) Observar: possibilita a verificação de detalhes característicos de um indivíduo, tais como roupas, permitindo monitorar as atividades em torno de um incidente;

b) Reconhecer: permite que o operador do MCVE verifique com alto grau de certeza o indivíduo visualizado; e

c) Identificar: possibilita a efetiva identificação do indivíduo.

9.2.6 A implantação do SSE Complexo será definida através de resultado da avaliação de risco.

NOTA: É obrigatória a implementação de SSE Complexo para o acesso ao interior dos Órgãos ATC.

9.2.7 Os SSE Complexos devem ser constituídos pelos seguintes módulos, além dos módulos dos SSE Básicos:

a) Módulo de Controle de Acesso (MCA); e

b) Módulo de Tecnologia da Informação (MTI).

9.2.8 Módulos opcionais podem ser agregados aos SSE Complexos, como:

a) Módulo de Contraincêndio (MCI); e

b) Módulo de Rastreamento de Veículos (MRV).

9.2.9 Os SSE Complexos serão constituídos por todos os módulos necessários para propiciar o adequado auxílio às operações de Segurança das Instalações. Neste sentido, deve-se considerar a existência de um Módulo de Vigilância Eletrônica (MVE), um Módulo de Controle de Acesso (MCA), um Módulo de Detecção de Intrusão (MDI), um Módulo de Tecnologia da Informação (MTI), um Módulo de Central de Vigilância Eletrônica (MCVE) e um Módulo de Reação (MRE).

9.2.10 O SSE Complexo possui o MCA, o MDI e o MVE integrados por intermédio do MTI, que possibilitará o monitoramento do Sistema pelos operadores do MCVE, os quais poderão acionar o MRE. Relacionam-se de acordo com a seguinte estrutura:

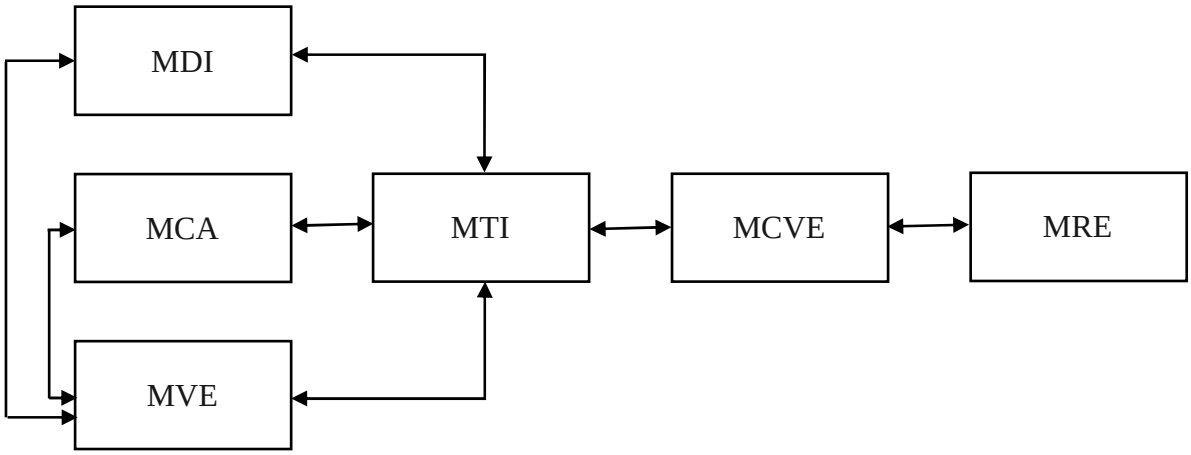

Figura 2: Estrutura esquemática de um SSE Complexo

9.2.11 De acordo com o nível de risco, é imperioso que as três vertentes do SSE Complexo sejam implementadas conforme a **Tabela 2**. As soluções aplicadas são cumulativas, ou seja, para o nível alto, além de suas implementações relacionadas, sugere-se a aplicação das abordagens dos níveis anteriores.

Nível de Risco	Sensor nas Áreas Restritas	Capacidade do CFTV	Nº de equipamentos de Controle de Acesso (por PCA)
baixo	Perímetro externo	-	1
médio-baixo	Perímetro externo e ambiente interno	Observar	1, sendo PIN ou Token
médio	Perímetro externo, ambiente interno e alarme com ativação/desativação por intermédio de PIN	Reconhecer	2, sendo um Biométrico
médio-alto ou alto	Perímetro externo, ambiente interno, alarme com ativação/desativação por intermédio de PIN e botão de pânico	Identificar	3, sendo um Biométrico

Tabela 2: Soluções de SSE Complexos

9.2.12 Para o acesso ao interior de Órgãos ATC deverá ser adotada os sensores referentes ao nível médio-alto ou alto da **Tabela 2**.

9.3 DESCRIÇÃO DOS MÓDULOS

9.3.1 Os softwares e hardwares dos diversos Módulos do SSE devem possuir interoperabilidade entre si, de modo a permitir um emprego integrado e, sempre que possível, permitir a efetiva integração com os sistemas já em funcionamento nos elos do SISCEAB.

9.3.2 Módulo de Detecção de Intrusão (MDI)

9.3.2.1 É o conjunto de equipamentos e aplicativos, dedicados à detecção de presenças humanas e ao monitoramento de portas e janelas, acionando alarmes sonoros ou silenciosos, possibilitando a utilização de senhas de coação e botões de pânico, inclusive sinalizando tentativas de fraudes em seus equipamentos, conforme descrito no **Anexo E**.

9.3.2.2 O MDI deverá ser integrado ao CFTV para possibilitar, com eficiência, a coordenação das atividades de verificação e interceptação realizadas pelas Forças de Reação.

9.3.2.3 No escopo dos SSE Complexos, o MDI possui basicamente as mesmas funcionalidades e especificidades existentes no SSE Básico. Entretanto, deverá possuir conexão com o MCA e com o MVE, por intermédio do MTI. O MDI deverá se comunicar com o MTI, enviando informações de detecção de intrusão que permitirão o efetivo monitoramento por intermédio dos integrantes do MCVE e o consequente acionamento do MRE, quando necessário.

9.3.3 Módulo de Central de Vigilância Eletrônica (MCVE)

9.3.3.1 É o local onde ocorrerá a efetiva visualização e controle das imagens do MVE, bem como o gerenciamento dos dispositivos do MDI. Os operadores do MCVE devem ser treinados para a utilização do sistema de comunicações e do CFTV, a fim de orientar a atuação das Forças de Reação.

9.3.3.2 O MCVE do SSE Complexo deverá ser constituído do MTI que irá possibilitar a integração dos módulos do Sistema por intermédio da infraestrutura de intranet do elo, por meio da implementação de uma VLAN (*Virtual Local Area Network*), conforme descrito no **Anexo H.**

9.3.4 Módulo de Vigilância Eletrônica (MVE)

9.3.4.1 É composto pelo CFTV. No escopo de SSE Básico, o MVE deverá possuir conexão com o MDI, pois os dois módulos irão possibilitar o efetivo monitoramento por intermédio dos operadores do MCVE e o consequente acionamento do MRE, quando necessário. Os equipamentos serão instalados em áreas internas e externas, dedicados ao monitoramento e gravação de vídeo dos ambientes, mesmo sob as condições adversas de meteorologia e luminosidade.

9.3.4.2 O MVE constitui-se de um dispositivo de gerenciamento das imagens (DVR, NVR ou similar), tela(s) para monitoramento, câmeras e demais itens relacionados; sendo o MCVE a central de monitoramento de tal sistema, conforme descrito no **Anexo C.**

9.3.4.3 O CFTV destina-se, prioritariamente, ao registro de ocorrências, ao acompanhamento de alvos e a identificação de objetos estranhos ao ambiente monitorado. O uso de câmeras com a função de detecção de movimento poderá ser implementado por intermédio de software de CFTV, contudo a aplicação dessa função ficará sob a incumbência do MDI.

Os dados e informações do CFTV deverão ser gravados para:

a) análise das ocorrências;

b) avaliação e aprimoramento das operações de Segurança das Instalações; e

c) apoio a investigações.

9.3.4.4 Como regra geral, o monitoramento por CFTV de ambientes internos só se justifica quando for fundamental à Segurança das Instalações, e o monitoramento de barreiras perimetrais, por CFTV ou sensores de intrusão, só se justifica em áreas restritas. O monitoramento deve ser direcionado às vias de acesso aos pontos críticos da instalação. Todos os pontos sensíveis e críticos à operação do SISCEAB do elo devem ser monitorados.

9.3.4.5 Conforme o grau de segurança necessário, pode-se utilizar o MVE combinado com recursos do MCA, tais como reconhecimento facial e reconhecimento de placas de veículos, os quais podem, ainda, ser confrontados com a leitura dos dispositivos de identificação individuais ou veiculares.

9.3.4.6 De acordo com a extensão física e área construída, cada instalação do elo pode possuir todos os módulos do SSE integrados e convergindo para um MCVE remoto que irá possibilitar a visualização das imagens dos MCVE primários, bem como de suas imagens locais. A finalidade do MCVE remoto é de orientar e suportar com informações oportunas à ação de resposta da equipe de segurança do PSNA ou da Força de Reação, no caso seja uma OM.

9.3.4.7 Instalações que podem ser trancadas não necessitam de sentinelas, devendo ser monitoradas pelo MCVE por meio do MDI e, se for o caso, do MVE.

9.3.4.8 Será priorizada a instalação de câmeras de vigilância nos seguintes locais:

a) vias de acesso ao elo, focalizando-se as entradas e as saídas;

b) depósitos de armas e munições, quando aplicável, tanto nos acessos quanto nas partes internas;

c) interior ou exterior de pontos sensíveis e julgados essenciais à operação do SISCEAB, tais como de Órgãos ATC, radares, equipamentos de auxílio à navegação, entre outros.

d) demais pontos sensíveis do elo, levando-se em consideração o preconizado em regulamentos específicos.

9.3.4.9 No escopo de SSE Complexo, o MVE possui basicamente as mesmas funcionalidades e especificidades existentes no SSE Básico. No entanto, deverá possuir conexão com o Módulo de Detecção de Intrusão (MDI) e com o Módulo de Controle de Acesso (MCA), por intermédio do Módulo de Tecnologia da Informação (MTI), que possibilitará o efetivo monitoramento por parte dos operadores do Módulo de Central de Vigilância Eletrônica (MCVE) e o consequente acionamento do Módulo de Reação (MRE), quando necessário.

9.3.5 Módulo de Reação (MRE)

9.3.5.1 Este Módulo diz respeito ao conjunto de ações que o sistema deverá realizar para acionamento da equipe de segurança do elo, em caso de ocorrência de eventos identificados pelos demais módulos do SSE, conforme descrito no **Anexo F.**

9.3.5.2 Para que o MRE seja acionado pelo sistema, é necessário o correto funcionamento dos demais módulos.

9.3.5.3 A eficácia do MRE é diretamente proporcional à capacidade de comunicação entre o Módulo Central de Vigilância Eletrônica (MCVE), os Postos de Controle de Acesso (PCA) e a Equipe de Serviço de Segurança das Instalações. Essa comunicação pode ser viabilizada por via rádio, telefonia convencional móvel ou fixa.

9.3.5.4 Outro fator importante para a eficácia do MRE é a mobilidade e a capacidade de resposta da equipe de segurança do PSNA.

9.3.5.5 Cada SSE deve ter, no mínimo, uma Equipe de Resposta com a mobilidade adequada à extensão coberta pelo SSE.

9.3.5.6 Os complexos de organizações, com mais de um SSE ativado, devem possuir uma Patrulha da Guarnição. Nos elos isolados, a Patrulha desempenhará, também, a função de Patrulha da Guarnição.

9.3.6 Módulo de Controle de Acesso (MCA)

9.3.6.1 É o conjunto de equipamentos e aplicativos que controlam a entrada/saída de pessoas e veículos por meio de dispositivos de bloqueio e de autenticação, autorização e auditoria, que possibilitam a execução de rotinas e procedimentos automáticos nos elos do SISCEAB.

9.3.6.2 O MCA é composto por software específico, servidor de aplicação e de banco de dados de usuários, monitor(es), placa controladora, leitores de dispositivos de identificação individual ou veicular (*tokens*, PIN ou biometria); bem como os itens correlatos que viabilizam as conexões, conforme descrito no **Anexo D.**

9.3.6.3 A parte física do MCA funciona pelo bloqueio de acesso a áreas controladas por barreiras perimetrais (cercas e muros) e postos de controle de acesso (PCA), que regulam o fluxo de entrada e saída por meio de dispositivos de bloqueio de acesso (portas, catracas, portões, cancelas e barreiras hidráulicas) e por leitores de dispositivos de identificação individual e veicular.

9.3.6.4 A abertura de portas e portões com dispositivos de identificação individual ou veicular, em locais de alto e médio fluxo de acessos, possibilita que mais de uma pessoa ou veículo entre ou saia por vez. Isso gera um descontrole dos acessos ao elo ou à área restrita. O uso de catracas e cancelas é mais eficaz para essa situação. No entanto, o uso de catracas e cancelas requer uma sentinela para coibir ultrapassagens proibidas e solucionar situações inopinadas. Em locais de baixo fluxo de acessos o uso de portas e portões é aplicável.

9.3.6.5 As viaturas militares devem utilizar etiquetas RFID para facilitar o controle de saída e entrada no elo.

9.3.6.6 O MCA deve integrar o controle de acesso de todos os PCA, permitindo a identificação do itinerário de uma pessoa ou veículo pelos postos os quais passou. Os *tokens* entregues a pessoas e veículos visitantes, terceirizados, prestadores de serviços, dentre outros, devem ser programados para não permitirem a saída da área controlada, a fim de impedir o extravio do material de identificação.

9.3.6.7 Os complexos de instalações ou os elos isolados, durante o expediente, devem manter aberto o menor número de PCA necessários à sua operacionalidade e, fora do expediente, preferencialmente, um só PCA de acesso ao complexo ou ao elo.

9.3.7 Módulo de Tecnologia da Informação (MTI)

9.3.7.1 É um elemento crítico em um SSE Complexo, pois possibilita a integração de todos os módulos. O MTI transmite as informações provenientes dos sensores, dos dispositivos de controle de acesso e dos componentes de vídeo, permitindo o efetivo monitoramento das áreas críticas pelos integrantes do MCVE que poderão acionar o MRE, conforme descrito no **Anexo G**.

9.3.7.2 O *link* do MTI, preferencialmente, deverá ser implementado utilizando a infraestrutura de enlaces da rede intranet, por intermédio da configuração de exclusiva para este fim. Uma conexão MTI eficaz garante uma transmissão rápida e confiável de dados. O MTI propiciará rápida detecção de falhas e reparação do SSE.

9.3.7.3 O diferencial na configuração do MTI como suporte ao SSE é a interoperabilidade entre os módulos do Sistema, bem como a flexibilidade no que se refere à disponibilização de pontos de visualização das imagens e a rápida possibilidade de rastreabilidade no controle de acesso.

9.3.8 Módulo de Contraincêndio (MCI)

9.3.8.1 É o conjunto de equipamentos e de aplicativos que monitoram, constantemente, as condições do ambiente, visando à detecção, ao processamento, ao aviso automático de focos de incêndio e o seu efetivo combate.

9.3.9 Módulo de Rastreamento de Veículos (MRV)

9.3.9.1 O MRV possibilita a instalação de câmeras de visualização no interior e exterior de veículos, bem como a inserção de sistema de posicionamento global (GPS), que possibilitam sua localização e monitoramento em tempo real.

10 AÇÕES COORDENADAS COM ÓRGÃOS DE SEGURANÇA

O decreto-lei nº 2.848, de 7 de dezembro de 1940, cita no Art. 261 que pôr a perigo aeronave, própria ou alheia, ou praticar qualquer ato tendente a impedir ou dificultar navegação aérea pode ser penalizado com reclusão, de dois a cinco anos.

Para que os atos supracitados sejam combatidos com eficácia, devem ser criados procedimentos para a comunicação célere e eficaz entre órgãos ATS e órgãos de segurança pública ou autoridade competente para contrapor a ameaça.

Visando preparar o SISCEAB para enfrentar os riscos emergentes no contexto mundial da aviação civil, quatro tipos de ameaças se destacam:

a) utilização de ponteiras de raio laser contra aeronaves e torres de controle;

b) utilização indevida de aeronave não tripulada (RPAS ou *drones*) na imediação de trajetória de rota de aeronave;

c) o uso de Sistemas de Defesa Antiaéreos Portáteis (MANPAD) por grupos terroristas; e

d) identificação de objeto suspeito.

10.1 LASER

10.1.1 Feixes laser podem causar cegueira temporária ou dano permanente aos tecidos humanos, especialmente a retina. A faixa de distância acima da qual as ponteiras de raio laser podem ser utilizadas variam de 2.000 pés até 20.000 milhas.

10.1.2 Quando apontada, diretamente ou indiretamente, para o piloto ou para o controlador de tráfego aéreo podem causar danos ou prejuízos à visão, como cegueira temporária e distração, podendo contribuir para a ocorrência de acidentes aeronáuticos.

10.1.4 Ao receber o reporte do piloto, o órgão ATS deve envidar esforços para que as seguintes informações essenciais sejam registradas:

a) data e hora do evento;

b) posição/localização da aeronave;

c) altitude;

d) direção da aeronave durante o incidente;

e) posição do laser em relação à aeronave; e

f) distância estimada do emissor.

10.1.5 Quando disponíveis, as seguintes informações deverão ser registradas:

a) identificação da aeronave;

b) modelo da aeronave;

c) cor do laser;

d) cabine iluminada ou não;

e) tripulação ferida;

f) efeitos visuais que afetaram a tripulação;

g) intenção da tripulação (prosseguir ou arremeter);

h) descrição resumida do evento; e

i) demais informações julgadas pertinentes.

10.1.6 O órgão ATS deve estabelecer procedimentos coordenados com o órgão de segurança pública de sua localidade para a comunicação de uso indevido de ponteiras de raio laser.

10.1.7 O ATCO que receber as informações do piloto deve estimar a uma posição do emissor no terreno, com a finalidade de favorecer as ações do órgão de segurança pública.

10.1.8 O órgão de segurança pública deve ser informado com brevidade, para contribuir na repressão do ato.

10.1.10 O órgão ATS deve registrar, no Livro de Registro de Ocorrência, o relato realizado ao órgão de segurança pública, bem como o nome de quem recebeu as informações, a hora da ligação e o telefone de contato.

10.2 AERONAVE NÃO TRIPULADA

10.2.1 Ao ser reportado o avistamento de aeronave não tripulada nas proximidades de aeroportos, independente da fonte, o nível de atenção deve ser elevado.

10.2.2 Deve ser verificado o exato local do avistamento, a fim de preparar as equipes para uma possível intervenção nas operações de pouso e/ou decolagens**.**

10.2.3 O administrador aeroportuário e o órgão de segurança pública responsável pelas atividades de polícia no aeroporto devem ser notificados, a fim de somar esforços para uma identificação positiva da aeronave não tripulada.

10.2.4 Todos os meios disponíveis para a confirmação da presença da aeronave não tripulada devem ser utilizados, tais como: câmeras, lunetas e binóculos, viaturas e apoio de outras aeronaves.

10.2.5 Sendo confirmada a presença da aeronave não tripulada, sua localização influencia diretamente a operação do órgão ATS, principalmente as operações de pouso, decolagem e arremetidas.

10.2.6 O órgão de segurança pública local deve ser informado, a fim de que sejam envidados os esforços necessários para a localização do piloto da aeronave não tripulada, a fim de possibilitar a extinção da ameaça e demais medidas cabíveis, criminais e administrativas.

10.2.7 Sendo julgado cabível e adequado, as operações poderão ser interrompidas parcialmente, não sendo necessária a interdição total do sítio aeroportuário, conforme procedimentos específicos estabelecidos no modelo operacional do órgão ATS.

10.2.8 Imediatamente, deve-se informar as ações que serão tomadas à célula de gerenciamento de fluxo (FMC) do Órgão Regional responsável pela área, e desta para o CGNA.

10.2.9 Nos casos em que tenha sido feita a identificação da aeronave não tripulada e seja verificado o afastamento do equipamento, caberá ao órgão ATS envolvido retomar a normalidade das operações, devendo informar a decisão ao Órgão Regional responsável, ao

administrador aeroportuário, ao órgão de segurança pública responsável pelas atividades de polícia no aeroporto, à FMC e ao CGNA.

10.2.10 O modelo operacional do órgão ATS deve estabelecer o membro da equipe de serviço responsável por executar ações supracitadas.

10.2.11 Caso seja identificada a localização do piloto da aeronave não tripulada, esta deve ser informada ao órgão de segurança pública responsável pelas atividades de polícia no aeroporto para que sejam tomadas as medidas cabíveis.

10.2.12 O Agente Local AVSEC do órgão envolvido deverá encaminhar uma cópia do procedimento lavrado (Boletim de Ocorrência, Termo Circunstanciado de Ocorrência, LRO, etc.) ao Gerente Regional AVSEC responsável para que as medidas administrativas sejam tomadas.

10.2.13 Caso o aeroporto disponha de equipamento de identificação e monitoramento de aeronave não tripulada, o alarme de detecção deve ser considerado como identificação positiva.

NOTA: Deve-se ainda buscar a identificação visual e caso não obtida, a identificação por meio do equipamento deve ser entendida como positiva.

10.3 SISTEMAS DE DEFESA ANTIAÉREOS PORTÁTEIS (MANPAD)

10.3.1 Os MANPAD representam ameaça significativa para a aviação. Por sua portabilidade e sofisticação, são de difícil detecção e capazes de causar um dano catastrófico, inclusive para aeronaves civis de grande porte.

10.3.2 Muitos MANPAD são letais a aproximadamente 15.000 pés e a uma distância de 5 milhas ou mais. Os tópicos a seguir definirão os níveis de alerta para ameaça MANPAD e os procedimentos para reportar este evento.

10.3.3 As ameaças MANPADS podem ser classificadas usando níveis de alerta.

a) nível 1: atenção aumentada, operação normal;

b) nível 2: ameaça plausível a um aeroporto específico, operador aéreo ou região de voo. Deve-se preparar a aplicação dos planos de contingência e degradação, além de aplicar as medidas adicionais de segurança previstas;

c) nível 3: lançamento observado ou reportado. Deve-se aplicar os planos de contingência e degradação.

10.3.4 As informações de ameaça MANPADS também deve ser comunicada para:

a) a TWR do aeródromo afetado;

b) o administrador aeroportuário envolvido;

c) órgão de segurança pública responsável pelas atividades de polícia no aeroporto;

d) o órgão ATC que controla o voo sob ameaça; e

e) ao ACC responsável pela área.

10.3.4.1 Resposta ao nível 1: representa o menor nível de alerta. Aumento da atenção e da vigilância pelo órgão ATS é um ponto chave para a prevenção ou limitação de um ataque. O ATCO que suspeite da iminência da ameaça deve notificar o supervisor ou chefe de equipe do órgão ATS, para que as ações necessárias sejam tomadas.

10.3.4.2 Resposta ao nível 2: deve ser implementado após o recebimento de informações confiáveis que indiquem a existência da ameaça nas imediações de um aeroporto, empresa aérea ou região de voo. A elevação do nível deve ser repassada aos órgãos citados em **10.3.4**.

10.3.4.3 Resposta ao nível 3: deve ser implementado após um ataque observado ou reportado. Após o lançamento, o Órgão ATS envolvido deve registrar as seguintes informações:

a) código de chamada da aeronave (se conhecido);

b) tipo de aeronave (se conhecido);

c) horário do ataque (UTC);

d) posição/localização estimada;

e) altitude da aeronave; e

f) outras informações pertinentes.

10.3.5 O supervisor ou chefe de equipe do Órgão ATS que receber o reporte ou testemunhar o ataque deve assegurar que a informação seja repassada aos órgãos citados em **10.3.4**.

10.3.6 As informações relativas a ameaças MANPAD devem ser transmitidas no ATIS do aeroporto envolvido.

10.4 IDENTIFICAÇÃO DE OBJETO SUSPEITO

10.4.1 O efetivo do elo deve ser orientado a comunicar imediatamente ao responsável pela segurança sobre a existência de qualquer objeto suspeito abandonado em sua área patrimonial.

10.4.2 A equipe de segurança do elo possui um papel crucial na identificação de objetos suspeitos e deve estar atenta para a existência de objetos dessa natureza.

10.4.3 A partir da identificação de um objeto suspeito, as ações elencadas nesse tópico deverão ser adotadas imediatamente.

10.4.4 O contato de pessoal não especializado com objeto suspeito é terminantemente proibido.

10.4.5 O PSNA deve designar uma área isolada para objetos suspeitos, na qual especialistas possam desarmar ou descartar o objeto suspeito.

10.4.6 Nos PSNA compartilhados, a área isolada para objetos suspeitos deverá preferencialmente estar situada próxima, mas a não menos de 100 m, do ponto remoto do aeroporto.

10.4.7 O itinerário a ser realizado pelo objeto suspeito até a área isolada deverá ser evacuado, podendo ser novamente utilizado após a passagem do objeto suspeito.

10.4.8 Deve-se definir, no mínimo duas rotas de transporte de objetos suspeitos de todos os pontos sensíveis até a área isolada, com o objetivo de estabelecer as rotas mais seguras, evitando, sempre que possível, passar próximo a outros pontos sensíveis e em locais com grande concentração de pessoas.

10.4.9 O PSNA deve estabelecer procedimentos coordenados previamente com o órgão de segurança pública ou unidade militar, para acionamento deste, identificação, desarme e descarte do objeto suspeito.

11 MEDIDAS ADICIONAIS DE SEGURANÇA

As medidas adicionais de segurança serão adotadas em virtude de elevação do nível de ameaça, indícios de ameaça iminente ou ocorrência de atos de interferência ilícita ou devido à determinação específica do DECEA.

São alterações realizadas com o intuito de elevar o nível de segurança do elo, mantendo as medidas preventivas existentes. A seguir são apresentados exemplos a serem adotados pelo elo. Ressalta-se que estes exemplos não esgotam as possibilidades, pois dependem do cenário da ameaça enfrentada.

11.1 BARREIRAS PERIMETRAIS

a) incremento das barreiras patrimoniais, usando concertina, arame farpado, cercas eletrificadas ou outras conforme melhor julgamento do Agente AVSEC, priorizando pontos sensíveis e vulneráveis do PSNA;

b) utilização de dilacerador de pneus, “jacaré” ou “ouriço” nas vias de acesso;

c) uso de veículos como barreiras temporárias;

d) instalação de grades de isolamento em pontos sensíveis e vulneráveis;

e) manter fechados os portões de acesso de veículos, somente sendo abertos após identificação de seus ocupantes (caso não possua portão para veículos, implementar meios de dificultar invasão de veículos, como cavaletes, cones com peso ou tonéis); e

f) utilização de cavaletes para “ziguezague”, antes do portão de acesso, forçando a redução da velocidade dos veículos.

11.2 CREDENCIAMENTO E CONTROLE DE ACESSO

a) restringir o acesso às salas técnicas e/ou operacionais do PSNA;

b) restringir o acesso ou a saída do efetivo do PSNA;

c) restringir o acesso ou a saída de visitantes;

d) autorização especial do comandante ou responsável pela segurança do PSNA para acesso de visitantes às instalações;

e) restringir, ao mínimo possível, o número de pontos de acesso ao PSNA e pontos sensíveis;

f) inspeção (revista) de volumes (bolsas, mochilas, etc.) nos pontos de controle de acesso às instalações, durante entrada e/ou saída do PSNA;

g) uso de cães para a realização de faro nas inspeções de visitantes e do efetivo;

h) inspeção (revista) de todos os compartimentos dos veículos; e

i) utilização de espelho de inspeção veicular, para inspeção da parte inferior do veículo.

j) estabelecimento de senha de coação;

k) solicitação de documentos adicionais para acesso de visitantes às instalações, em complemento à credencial; e

l) manter portões de acesso de veículos fechados abrindo-os somente após identificação de todos os ocupantes;

11.3 SISTEMA DE SEGURANÇA ELETRÔNICA

a) aumento do nível de sensibilidade das grades de detecção de movimento aplicadas nos sistemas de vigilância eletrônica;

b) instalação de equipamentos de segurança eletrônica de caráter temporário em locais julgados pertinentes; e

c) alteração da programação de gravação semanal dos sistemas de vigilância eletrônica, conforme necessário.

11.4 EQUIPE DE SEGURANÇA

a) orientar as equipes de segurança do PSNA, quanto à elevação do Nível de Ameaça AVSEC do SISCEAB e às medidas adicionais de segurança a serem adotadas pelo PSNA;

b) intensificar a frequência das rondas e/ou imprevisibilidade destas;

c) reforçar os pontos de acesso e de vigilância, prioritariamente nos pontos sensíveis e/ou vulneráveis do PSNA;

d) empregar efetivo para realizar rondas e varreduras em apoio ao patrulhamento, com objetivo de esterilizar o PSNA afetado (evitando desmobilizar os postos existentes);

e) realizar rendições com acompanhamento;

f) manter veículos afastados (tráfego e estacionamento), o quanto possível, dos pontos sensíveis; e

g) acionar os órgãos de segurança pública e/ou unidades militares, quando necessário ou por iminente esgotamento das capacidades de resposta do PSNA.

11.5 PATRULHAMENTO

a) intensificação da frequência das rondas e/ou imprevisibilidade destas, prioritariamente nos pontos sensíveis e/ou vulneráveis;

b) realizar varreduras durante as rondas, com objetivo de esterilizar área patrimonial que dê acesso aos pontos sensíveis; e

c) intensificação do patrulhamento nos pontos de barreiras patrimoniais que estejam danificados ou em más condições.

12 INSTALAÇÃO DE SÍTIO

12.1 ORIENTAÇÕES GERAIS:

12.1.1 Na escolha do sítio para a implantação de novas unidades do SISCEAB, no que concerne à segurança, deverão ser observados os seguintes aspectos:

a) operacionais;
b) técnicos;
c) logísticos;
d) patrimoniais;
e) ambientais;
f) econômicos; e
g) sociais.

12.1.2 O Gerente Regional AVSEC, em estreita coordenação com os demais responsáveis, deverá estar envolvido em todas as etapas do projeto que sejam pertinentes a sua área de atuação, desde a escolha do sítio até o recebimento em campo do empreendimento, de modo a especificar, acompanhar e aceitar os recursos de segurança implantados.

12.1.3 O elo responsável pela implantação de novas unidades do SISCEAB deverá designar o Agente Local AVSEC para realizar uma avaliação de risco do sítio, conforme regulamento específico.

12.1.4 Além dos critérios estabelecidos para cada aspecto, a escolha do sítio e posteriores planejamentos, execuções, fiscalizações, recebimentos e manutenções deverão atender à legislação e regulamentos nacionais vigentes e, quando aplicável, às normas internacionais, correspondentes das quais o Brasil seja signatário.

12.1.5 O Agente Local AVSEC do elo envolvido deve participar da definição dos requisitos de segurança para a instalação ou modernização de suas instalações, sistemas e equipamentos.

12.2 ORIENTAÇÕES ESPECÍFICAS

12.2.1 Depósitos de combustíveis devem ser construídos, sempre que possível, com no mínimo 35 metros de distância de pontos sensíveis.

12.2.2 Depósitos de lixo devem ser construídos o mais distante possível dos pontos sensíveis.

12.2.3 Durante a fase de planejamento de um novo sítio, evitar a instalação próxima a locais que possam representar uma ameaça a operação do SISCEAB, tais como: usinas nucleares, fábricas e depósitos de produtos químicos tóxicos, complexos prisionais, locais sob controle de facções criminosas, dentre outras.

12.2.4 Pontos sensíveis devem ser instalados o mais distante possível dos pontos de acesso externo, das principais vias de circulação de veículos e de estacionamentos.

12.2.5 A construção de barreiras perimetrais deve seguir o capítulo 6 deste manual.

12.2.6 Quando possível, evitar a construção de estacionamento sob ou dentro de edificações.

12.2.7 Quando possível, os pontos de acesso externo devem ser construídos com um ângulo em relação às vias de acesso, dificultando a entrada de veículos em alta velocidade.

12.2.8 Os pontos de acesso de veículos devem ser construídos com barreiras veiculares.

12.2.9 As portas de pontos sensíveis ou as portas que dão acesso ao exterior do PSNA devem ser reforçadas e construídas com abertura para fora.

12.2.10 As portas de emergência somente devem facilitar a saída de pessoas, não a entrada.

12.2.11 Os pontos de acesso do PSNA e de pontos sensíveis devem ser construídos prevendo uma boa iluminação.

12.2.12 Muros devem ser construídas, preferencialmente, em concreto armado.

13 REQUISITOS DE SEGURANÇA

13.1 ORIENTAÇÕES GERAIS

13.1.1 No caso de instalações onde haja a presença constante de pessoas, deve-se congregar os esforços para garantir a integridade das instalações com a segurança e fluidez das pessoas que ali transitam.

13.1.2 O profissional de segurança deve ser treinado regularmente para enfrentar situações de perigo diversas e agir ao perceber atividades suspeitas no local, ingresso de pessoas estranhas ou presença de objetos suspeitos, bem como lançar mão de técnicas de abordagem e proteção de patrimônio, de acordo com requisitos e normas específicas.

13.1.3 Os pontos sensíveis devem ser monitorados ininterruptamente, seja por meio de SSE, seja por meio de vigilantes ou sentinelas. Nos casos em que se julgar necessário, devido ao nível de risco, pode-se aplicar ambos.

13.1.4 O PSNA deverá estabelecer patrulhamentos de rotina, em horários não padronizados, que contemplem todos os pontos sensíveis e vulneráveis do PSNA, com o objetivo de identificar pessoas suspeitas e objetos suspeitos.

13.2 ORIENTAÇÕES ESPECÍFICAS

13.2.1 Devem ser mantidas vias de serviço que permitam a realização de patrulhamento sistemático e frequente por toda a área patrimonial, em especial nos pontos de controle de acesso mantidos fora de operação, pontos sensíveis e no entorno destes.

13.2.2 No caso de acesso indevido ou tentativa deste, o PSNA deve aplicar medidas de pronta-resposta que sejam suficientes para impedir a continuidade do acesso e mitigar os possíveis efeitos negativos. Quando aplicável, comunicar ao setor de segurança aeroportuária e/ou ao órgão de segurança pública responsável pelas atividades de polícia no aeroporto, especialmente no sentido de proteger a área restrita de segurança.

13.2.3 Todos os acessos aos equipamentos de auxílio à navegação aérea, sala técnica ou órgão operacional devem ser protegidos. Caso estes estejam localizados no térreo, as janelas e os dutos de ventilação devem estar protegidas com grades ou telas, impossibilitando a passagem de objetos ou pessoas que possam colocar em risco a operação do elo do SISCEAB.

13.2.4 Sempre que houver acesso indevido ou indício deste as equipes de segurança devem realizar uma verificação minuciosa no local, certificando-se de que não existem pessoas não autorizadas, nem a presença de objetos estranhos ao local.

13.2.5 Os depósitos e/ou latas de lixo devem ser posicionados o mais distante possível dos pontos sensíveis.

13.2.6 Deve ser retirada a vegetação na proximidade dos pontos sensíveis que possa encobrir a presença de pessoa ou objeto, levando-se em consideração as legislações ambientais nacionais, estaduais e municipais.

13.2.7 As valas de drenagem e demais infraestruturas que cruzem as áreas controladas do PSNA devem ser lacradas, e ser alvo de rondas, com objetivo de identificar violações.

13.2.8 As portas de saídas em emergência que permitirem o acesso a áreas restritas de segurança de aeroportos compartilhados ou aos pontos sensíveis do PSNA devem ser mantidas lacradas e possuir sensores e alarmes que indiquem a sua abertura para a equipe de segurança, bem como baterias que alimentem esses sensores em caso de interrupção no fornecimento de energia elétrica.

13.2.9 As portas de saídas de emergência devem possuir iluminação adequada e serem submetidas a rondas frequentes.

14 DISPOSIÇÕES FINAIS

14.1 Este Manual deverá estar completamente implementado e operacionalizado em até doze meses, a partir de sua entrada em vigor.

14.2 Os casos não previstos nesta Instrução serão submetidos à apreciação do Diretor-Geral do DECEA.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Ações de Segurança e Defesa no SISCEAB: ICA 205-40. Rio de Janeiro, 2018.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Política de Segurança da Aviação Civil do Sistema de Controle do Espaço Aéreo Brasileiro: ICA 205-7. Rio de Janeiro, 2017.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Programa de Capacitação AVSEC do Sistema de Controle do Espaço Aéreo Brasileiro: ICA 37-733. Rio de Janeiro, 2017.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Programa Nacional para a Segurança da Aviação Civil do Sistema de Controle do Espaço Aéreo Brasileiro: ICA 205-48. Rio de Janeiro, 2017.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Manual de Gerenciamento de Risco AVSEC no SISCEAB: ICA 205-51. Rio de Janeiro, 2019.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Procedimentos para os órgãos de SISCEAB em caso de atos de interferência ilícita contra a Aviação Civil: ICA 63-12. Rio de Janeiro, 2019.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Coleta, Tratamento e Difusão de Informações sobre Atos de Interferência Ilícita Contra a Aviação Civil no SISCEAB: CIRCEA 100-84. Rio de Janeiro, 2019.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Sistema de Controle do Espaço Aéreo Brasileiro: NSCA 351-1. Brasília, 2010.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante. Visitas às Organizações Militares do Comando da Aeronáutica. ICA 205-22. Brasília – DF, 2016.

BRASIL. Comando da Aeronáutica. Comando-Geral de Operações Aéreas. Identificação de Veículos Particulares: NOSDE PRO-01A. Brasília, 2015.

BRASIL. Comando da Aeronáutica. Comando-Geral de Operações Aéreas. Identificação de Pessoal: NOSDE PRO-02B. Brasília, 2015.

BRASIL. Presidência da República. Decreto nº 7.168, de 5 de maio de 2010. Dispõe sobre o Programa Nacional de Segurança de Aviação Civil Contra Atos de Interferência Ilícita (PNAVSEC), Brasília, 2010.

BRASIL. Presidência da República. Lei nº 13.477, de 30 de agosto de 2017. Instalação de Cerca Eletrificada ou Energizada em Zonas Urbana e Rural. Brasília, 2017.

BRASIL. Presidência da República. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código de Penal. Rio de Janeiro, 1940.

BRASIL. Presidência da República. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Rio de Janeiro, 1941.

OACI. Anexo 17 - Segurança. Proteção da Aviação Civil Internacional Contra Atos de Interferência Ilícita. 10ª edição. 2017.

OACI. DOC 8973 - Manual de Segurança para a Proteção da Aviação Civil Contra Atos de Interferência Ilícita. 10ª edição. 2017.

OACI. DOC 9815 – Manual de Emissores de Laser e Segurança de Voo. 1ª edição. 2003.

OACI. DOC 9985 - Manual de Segurança para o Gerenciamento do Tráfego Aéreo. 1ª edição. 2012.

OACI. Guia de Avaliação de Sistema de Defesa Antiaéreo Portátil. 1ª edição. 2015.

Anexo A - Termo de Compromisso de Manutenção do Sigilo

Eu, NOME COMPLETO brasileiro/a, CPF nº (N º, data e local de expedição do CPF), filiação e endereço, (PRESTADOR DE SERVIÇO NA – CITAR EMPRESA) ou (MILITAR SERVINDO NO – CITAR OM) perante ao CITAR O ÓRGÃO declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada ou sob restrição de acesso cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011 e a:

a) tratar as informações ou materiais classificados ou sob restrição de acesso que me forem fornecidos pelo _____e preservar o seu sigilo, de acordo com a legislação vigente;
b) preservar o conteúdo das informações ou materiais classificados ou sob restrição de acesso, sem divulgá-los a terceiros;
c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações ou materiais classificados ou sob restrição de acesso, ou dos materiais; e
d) não copiar ou reproduzir, por qualquer meio ou modo:

   (1) informações classificadas ou sob restrição de acesso;

   (2) informações relativas aos materiais de acesso restrito do _____, salvo autorização da autoridade competente.

Declaro que (RECEBI) ou (TIVE ACESSO) ao (à) (DOCUMENTO OU MATERIAL ENTREGUE OU EXIBIDO AO SIGNATÁRIO), e por estar de acordo com o presente Termo, assino na presença das testemunhas abaixo identificadas.

_____, _____de _____de_____

(Local e Data)

_____

(Nome completo, Posto, Identidade e Função)

Testemunhas:

_____

(Nome completo, Posto, Identidade e Função)

Anexo B – Lista de Itens Passíveis de Proibição

A lista de itens passíveis de proibição não é exaustiva, e poderá ser atualizada pelo DECEA conforme necessário.

Para garantir a segurança da aviação civil, o elo do SISCEAB pode determinar que um item que não conste expressamente na lista é proibido, desde que se enquadre nas definições de uma das categorias descritas, representando um risco à segurança e à integridade das pessoas, instalações ou sistemas do SISCEAB.

Sem prejuízo das normas de segurança aplicáveis, são itens passíveis de proibição:

a) dispositivos que podem ou aparentam poder ser utilizados para causar ferimentos graves através do disparo de um projétil, incluindo:
   - armas de fogo de qualquer tipo, tais como pistolas, revólveres, carabinas, espingardas;
   - armas de brinquedo, réplicas ou imitações de armas de fogo que podem ser confundidas com armas verdadeiras;
   - componentes de armas de fogo, excluindo miras telescópicas;
   - armas de pressão por ação de ar e gás comprimido ou por ação de mola, tais como armas de *paintball*, *airsoft*, pistolas e espingardas de tiro a chumbo ou outros materiais;
   - pistolas de sinalização e pistolas de partida esportiva;
   - bestas, arcos e flechas; e
   - armas de caça submarina, tais como arpões e lanças;

b) dispositivos neutralizantes destinados especificamente a atordoar ou a imobilizar, incluindo:
   - armas e bastões de choque elétrico;
   - dispositivos para atordoar e abater animais; e
   - químicos, gases e aerossóis neutralizantes ou incapacitantes, tais como spray de pimenta, gás lacrimogêneo, sprays de ácidos e aerossóis repelentes de animais;

c) objetos pontiagudos ou cortantes que, devido à sua ponta afiada ou às suas arestas cortantes, podem ser utilizados para causar ferimentos graves, incluindo:
   - objetos concebidos para cortar, tais como machados, machadinhas e cutelos;
   - *piolets* e picadores de gelo;
   - estiletes, navalhas e lâminas de barbear, excluindo aparelho de barbear em cartucho;
   - facas e canivetes com lâminas de comprimento superior a 6 cm;
   - tesouras com lâminas de comprimento superior a 6 cm medidos a partir do eixo;
   - equipamentos de artes marciais pontiagudos ou cortantes;
   - espadas e sabres; e
   - instrumentos multifuncionais com lâminas de comprimento superior a 6 cm;

d) ferramentas de trabalho que podem ser utilizadas para causar ferimentos graves ou para ameaçar a segurança da aeronave, incluindo:
   - pés-de-cabra e alavancas similares;
   - furadeiras e brocas, incluindo furadeiras elétricas portáteis sem fios;
   - ferramentas com lâmina ou haste de comprimento superior a 6 cm que podem ser utilizadas como arma, tais como chaves de fendas e cinzéis;
   - serras, incluindo serras elétricas portáteis sem fios;
   - maçaricos;
   - pistolas de cavilhas, pistolas de pregos e pistolas industriais; e
   - martelos e marretas;

e) instrumentos contundentes que podem causar ferimentos graves se utilizados para agredir alguém fisicamente, incluindo:
   - tacos de beisebol, pólo, golfe ou hockey;
   - cassetetes, porretes e bastões retráteis;
   - equipamentos de artes marciais contundentes; e
   - soco-inglês;

f) substâncias e dispositivos explosivos ou incendiários que podem ou aparentam poder ser utilizados para causar ferimentos graves ou para ameaçar a segurança do elo, incluindo:
   - munições;
   - espoletas e fusíveis;
   - detonadores e estopins;
   - réplicas ou imitações de dispositivos explosivos;
   - minas, granadas e outros explosivos militares;
   - fogos de artifício e outros artigos pirotécnicos;
   - botijões ou cartuchos geradores de fumaça;
   - dinamite, pólvora e explosivos plásticos;
   - substâncias sujeitas a combustão espontânea;
   - sólidos inflamáveis, considerados aqueles facilmente combustíveis e aqueles que, por atrito, podem causar fogo ou contribuir para ele, tais como pós metálicos e pós de ligas metálicas;
   - líquidos inflamáveis, tais como gasolina, etanol, metanol, óleo diesel e fluido de isqueiro;
   - gases inflamáveis, tais como metano, butano, propano e GLP;
   - substâncias que, em contato com a água, emitem gases inflamáveis;
   - cilindros de gás comprimido, inflamável ou não, tais como cilindros de oxigênio e extintores de incêndio; e
   - isqueiros do tipo maçarico;

g) substâncias químicas, tóxicas e outros itens perigosos capazes de ameaçar a saúde das pessoas ou integridade das instalações do elo, incluindo:
   - baterias com líquidos corrosivos derramáveis;
   - mercúrio, exceto em pequena quantidade presentes no interior de instrumentos de medição térmica (termômetro);
   - substâncias oxidantes, tais como pó de cal, descorante químico e peróxidos;
   - substâncias corrosivas, tais como ácidos e alcalóides;
   - substâncias venenosas (tóxicas) e infecciosas, tais como arsênio, cianetos, inseticidas e desfolhantes;

- materiais infecciosos, ou biologicamente perigosos, tais como amostras de sangue infectado, bactérias ou vírus; e
- materiais radioativos (isótopos medicinais e comerciais);

h) outros itens proibidos que não se enquadram nas categorias anteriores:
- materiais que possam interferir eletromagneticamente nos equipamentos e sistemas ATM dos elos do SISCEAB;

Anexo C - Descrição do desempenho do Módulo de Vigilância Eletrônica (MVE)

1 REQUISITOS MANDATÓRIOS

1.1 Permitir a integração com os demais módulos do SSE;

1.2 Permitir a exibição de imagens ao vivo/gravado;

1.3 Permitir a exibição e gravação em diferentes streamings de vídeo, possibilitando a configuração de transmissão em diversos padrões de quadros por segundo;

1.4 Permitir o ajuste do modo de gravação para cada câmera individualmente, com base em detecção de movimentos, entrada de alarmes e/ou instantes programados de gravação;

1.5 Permitir a visualização das imagens, gravadas e ao vivo, de todas as câmeras, em todas as estações de trabalho simultaneamente, possibilitando ao operador estabelecer o layout da imagem, observado as credenciais de acesso do usuário;

1.6 Possibilitar trabalhar, preferencialmente, com equipamentos analógicos; Suportar diversos modelos de câmeras analógicas e gerenciadores de vídeo;

1.7 Permitir acesso remoto, possibilitando várias conexões por gerenciadores de vídeo;

1.8 Permitir visualização de câmeras de diversos gerenciadores de vídeo na mesma tela;

1.9 Permitir operações simultâneas como gravação, reprodução e exportação de vídeo, configuração do sistema, monitoramento ao vivo, consulta de eventos, pesquisa de imagens de monitoramento nos gerenciadores de vídeo;

1.10 Permitir a busca de imagens por câmera, através de data e hora com exportação de vídeos, com velocidade configurável em sentido normal ou inverso, através de barra de tempo, possibilitando selecionar uma faixa de vídeo;

1.11 Exibir imagens de câmeras quando houver um alarme de controle de acesso ou de intrusão, permitindo visualizar, além da imagem, no mínimo:

a) se houve ou não alarme de coação;

c) tempo excedido de porta/portão aberto;

d) usuário responsável pelo *token*, PIN ou biometria utilizado; e

e) rastreamento de uso do *token*, PIN ou biometria.

1.12 Visualizar em mapa a localização de cada câmera/tipo, identificando aquelas cujas imagens estão sendo exibidas;

1.13 Possibilitar que seja inserido e visualizado no mapa o setor e o alcance de visualização de cada câmera;

1.14 Dependendo das capacidades de cada câmera, permitir focar em um ponto determinado, de forma manual (clique do mouse) ou automática (programada), a partir de indicação na tela da estação de trabalho do operador do MCVE;

1.15 Permitir focar uma câmera no alvo e fazê-la acompanhar sua trajetória de forma manual ou automática;

1.16 Mediante clique na posição de uma câmera no mapa, visualizar a sua imagem na tela de controle do MVE;

1.17 Possibilitar seguir um rastreamento de um intruso na tela de controle do MVE;

Continuação do Anexo C - Descrição do Desempenho do Módulo de Vigilância Eletrônica (MVE)

1.18 Efetuar o direcionamento das câmeras, com recursos de *Pan*, *Tilt* e *Zoom*, via interface do próprio sistema;

1.19 Permitir a detecção de movimento, em área determinada, por meio da alteração da imagem das câmeras, com capacidade de calibração do tamanho da alteração;

1.20 Permitir o controle total de câmeras móveis ou câmeras com *zoom* óptico;

1.21 Permitir ao operador armar e desarmar por câmera ou área os recursos de detecção de movimento;

1.22 Ser flexível e possibilitar o uso de gerenciadores de vídeo padrões de mercado para processamento, transmissão, gerenciamento, armazenamento e visualização de imagens de vídeo capturadas por câmeras analógicas;

1.23 Os sinais de vídeo deverão ser codificados em formato digital, quando possível, utilizando tecnologia de compressão e gravados simultaneamente em tempo real;

1.24 Possibilitar de qualquer gerenciador de vídeo do Sistema:

a) controle das câmeras com *zoom* ótico e das câmeras móveis;

b) apresentação ao vivo de câmeras ou sequências de câmeras; e

c) recuperação e reprodução de vídeos arquivados.

1.25 Possibilitar, a partir de qualquer gerenciador de vídeo do Sistema, recuperar e/ou reproduzir dados, para fins de pós-avaliação e análise, sendo o intervalo de tempo da reprodução de dados facilmente selecionável;

1.26 As imagens vídeo das câmeras devem ser gravadas no disco rígido do gerenciador de vídeo, utilizando-se as soluções necessárias para armazenamento e recuperação dos dados;

1.27 Permitir que a reprodução dos vídeos seja feita de forma a não interromper, ou comprometer, a operação geral do MVE, ou a efetividade dos operadores no serviço;

1.28 Possuir *leds* de infravermelho que iluminem a imagem captada no período noturno; e

1.29 Possibilitar o emprego de Ronda Virtual Eletrônica.

2 REQUISITOS DESEJÁVEIS

2.1 Possibilitar trabalhar com câmeras de alta resolução que possibilite a identificação facial mesmo durante à noite;

2.2 O gerenciador de imagens deve permitir acesso remoto, preferencialmente, por interface web http/https;

2.3 As câmeras das entradas principais do PSNA devem permitir o reconhecimento de caracteres de placas veiculares;

2.4 O Sistema deve possuir, em locais de alta criticidade, câmeras que possam permitir a compensação da luz, mantendo a nitidez da imagem;

2.5 O Sistema deve possuir, em locais de elevada restrição de acesso, câmeras que possam permitir o reconhecimento facial; e

2.6 Possibilitar utilização de Sistema de Alta Voz.

Anexo D - Descrição do desempenho do Módulo de Controle de Acesso (MCA)

1 REQUISITOS MANDATÓRIOS

1.1 Possibilitar a capacidade de identificação por meio de *token* e/ou *PIN* e/ou biometria, cujos dados dos usuários deverão estar armazenados em um banco de dados;

1.2 As informações básicas do banco de dados devem incluir:

a) nome completo;

b) foto;

c) dados pessoais (data de nascimento, nacionalidade, naturalidade, CPF, tipo, órgão emissor, número e datas de emissão e validade do documento de identificação, endereço);

d) dados do *token*;

e) nível de autorização de acesso;

f) validade da autorização (data e hora);

g) categoria do usuário;

h) setor de trabalho ou de destino;

i) dados biométricos;

j) dados da etiqueta *RFID*;

k) dados do *PIN*;

l) responsável pela recepção (quando não do efetivo);

m) responsável pelo credenciamento; e

n) outros campos editáveis pelo administrador do sistema.

1.3 Utilizar, como dispositivos de bloqueio de fluxo, catracas e portas para pessoal e cancelas e barreiras hidráulicas para viaturas;

1.4 Fornecer uma interface de importação e exportação, em formatos padrões de mercado, que permita importar os registros de um usuário, de um banco de dados padrão de mercado ou de um sistema de terceiro;

1.5 Fornecer uma interface de pesquisa dos dados dos usuários e veículos com a disponibilização de filtros comuns ao banco de dados e aos campos existentes;

1.6 Permitir o controle de acesso por área agrupada;

1.7 Permitir a contagem de usuários e veículos dentro de determinada área, por meio de leitores de entrada e saída, fornecendo em caso de emergência ou a critério do operador, uma lista de pessoas no local/área em determinadas data e hora;

1.8 Apresentar em painéis gerenciais, os alertas provenientes de tentativas de acesso em áreas/zonas não autorizadas;

1.9 Permitir a utilização de *PIN* e/ou biometria para alarme de coação;

Continuação do Anexo D - Descrição do Desempenho do Módulo de Controle de Acesso (MCA)

1.10 Permitir o bloqueio de usuários ou veículos por uma janela de tempo específica ou indefinidamente;

1.11 Permitir a administração de visitantes em um único banco de dados integrado ao sistema de controle de acesso, cadastrando visitantes, terceirizados, servidores, prestadores de serviços, dentre outros casos de necessidade de acesso;

1.12 Possibilitar a emissão e impressão de relatórios por pessoal ou veículos do efetivo, visitantes, locais acessados, datas, tipos de alarmes, duração, tentativas de acesso, quantidade de acesso entre outras;

1.13 Os relatórios deverão ser gerados tanto de forma alfanumérica quanto apresentado em mapas com simbologia adequada;

1.14 Permitir, no mínimo, os seguintes alarmes e status:

a) *token*, PIN ou biometria desconhecidos;
b) *token*, PIN ou biometria não autorizados, expirado ou em “quarentena”;
c) *token*, PIN ou biometria fora do período de uso;
d) *token*, PIN ou biometria tentativa de acessos sucessivos;
e) abertura de porta ou portão não autorizada;
f) entrada e saída não autorizada;
g) alarme de PIN ou biometria de coação;
h) *token*, PIN ou biometria fora de rota;
i) tempo de porta/portão aberta(o) excedido;
j) outros tipos de alarme programáveis.

1.15 Possibilitar edição e impressão de mapas e relatórios por período de tempo, mostrando as regiões de maior acesso, tipo de usuário, de incidentes e tentativas de acesso, bem como a análise por períodos diferentes de tempo, comparando, visualmente em mapa, os diferentes resultados para a identificação de locais que estão sendo acessados;

1.16 Possibilitar ao operador habilitar e desabilitar camadas de informações;

1.17 Permitir a busca de uma camada, através do seu nome;

1.18 Permitir a navegação no mapa com ferramentas de Mover e *Zoom* (Mais, Menos, Anterior, Posterior e Completo);

1.19 Habilitar e desabilitar diversos *templates* (mapas);

1.20 Permitir imprimir e ou gerar um PDF a partir da captura da visualização atual do mapa em um modelo padrão de impressão;

1.21 Possuir captura de imagem do visitante;

Continuação do Anexo D - Descrição do Desempenho do Módulo de Controle de Acesso (MCA)

1.22 Possuir captura de imagem do documento do visitante;

1.23 Permitir a geração de gráficos dinâmicos (formato pizza ou barra) que irão possibilitar análises estatísticas de soma ou contagem, em tempo real, sobre as informações geradas;

1.24 Permitir a interligação de dados, em tempo real, entre os PCA e a CVE;

1.25 Possuir recurso que viabilize a coleta a inserção de fotos no banco de dados do sistema;

1.26 O MVE e o MCA devem ser totalmente integrados, de modo que, ao ocorrer um alarme de Controle de Acesso, o *streaming* da câmera de TV mais próxima deverá ser exibido pelo MVE;

1.27 Os dispositivos de bloqueio de fluxo (portas, portões, catracas, cancelas e barreiras hidráulicas) e os leitores de dispositivos de identificação individual e veicular devem ser compatíveis com o fluxo de pessoas e veículos nos horários de maior movimento;

1.28 Permitir a evacuação rápida dos ambientes em casos de emergências (ameaça de bomba, incêndio, dentre outros); e

1.29 Permitir o controle de material carga, utilizando-se de etiquetas *RFID* fixado a esse material.

2 REQUISITOS DESEJÁVEIS

2.1 Possuir ferramentas para ajuda de utilização;

2.2 Permitir encaminhamento para documentação oficial;

2.3 Possuir registro ágil de visitantes;

2.4 Permitir a impressão de cartão e etiquetas;

2.5 Possibilitar o uso de três fatores de controle de acesso simultâneos ou em sequência deve servir para aumentar a velocidade do fluxo;

2.6 Permitir o rastreamento de um ou mais usuários ou veículos dentro de determinada área, por meio de leitores de entrada e saída instalados nos dispositivos de bloqueio de fluxo, fornecendo a localização em determinadas data e hora;

2.7 Permitir adicionar *PIN*, *tokens* ou biometrias a uma lista de “quarentena”, com programação de alarme automático em caso de sua utilização, alarmes estes que deverão ser visualizados em mapas no painel gerencial;

2.8 Possuir ferramenta de desenho para anotações diversas no mapa, além de ferramentas de medições de distâncias entre dois ou mais pontos, medições da área de um polígono ou tamanho de uma linha desenhada sobre o mapa em diversas unidades de medida. As informações sobre distância ou área deverão ser automaticamente recalculadas ao se editar a forma geométrica do desenho em questão; e

Continuação do Anexo D - Descrição do Desempenho do Módulo de Controle de Acesso (MCA)

2.9 Permitir a identificação e visualização dos atributos de cada ponto, linha ou polígono selecionado, e ainda, definir se o usuário quer identificar uma camada visível ou selecionar a partir de uma lista quais camadas ele quer identificar.

Anexo E – Descrição do desempenho do Módulo de Detecção de Intrusão (MDI)

1 REQUISITOS MANDATÓRIOS

1.1 Exibir em mapas a localização dos sensores de intrusão, podendo exibi-los por camadas de tipo;

1.2 Possuir a funcionalidade de exibição por meio de mapas da localização da intrusão, de modo a facilitar o vetoramento da Equipe de Resposta ou da Força de Reação;

1.3 Os mapas devem possuir a função *zoom*, de modo a detalhar os ambientes do sensor alarmado;

1.4 Permitir que operadores autorizados, de sua estação de trabalho, ativem ou desativem os sensores de áreas e zonas previamente definidas;

1.5 Os equipamentos que irão compor o MDI deverão ter capacidade de integração com os demais módulos do SSE;

1.6 Possibilitar resposta imediata às diversas ocorrências com alarmes de intrusão que possam afetar ou ameaçar da Segurança das Instalações;

1.7 Possibilitar a exibição, em mapa, alarmes para alvos em aproximação de áreas restritas;

1.8 Permitir a configuração dos parâmetros de exibição e aceitação das mensagens de alarme;

1.9 Permitir a definição de alarmes padrão para qualquer evento e/ou alarme individual para cada evento;

1.10 Permitir que quaisquer alarmes de eventos associados a Segurança das Instalações sejam igualmente apresentados no painel gerencial;

1.11 Possibilitar que seja inserido e visualizado no mapa o setor e o alcance do sensor de intrusão;

1.12 Permitir o disparo de alarme manual por um operador ou usuário;

1.13 Possibilitar a emissão de relatórios por tipo de alarme, local acionado, data/hora, duração e tentativas de acesso;

1.14 Possibilitar o gerenciamento de alarmes visualizando-os no mapa e podendo classifica-los por data/hora, local, gravidade, prioridade e tipo de alarme, associando-os aos vídeos relacionados;

1.15 Permitir a inclusão de novos sensores de intrusão;

1.16 Possibilitar a análise, em períodos diferentes de tempo, da incidência de alarmes, por regiões e por tipo;

1.17 Permitir que o operador do MCVE, por meio do MVE, visualize o ambiente e avalie os alarmes consultando as informações de segurança relacionadas;

Continuação do Anexo E - Descrição do Desempenho do Módulo de Detecção de Intrusão (MDI)

1.18 Os MVE e MDI devem ser totalmente integrados, de modo que, ao ocorrer um alarme de intrusão, o *streaming* câmera de TV mais próxima deverá ser exibido pelo MVE;

1.19 Permitir simulação de alarmes para treinamentos;

1.20 Possibilitar de exibição de estatísticas de alarmes por meio de gráficos (colunas, linhas, pizza), os quais devem ser configuráveis e exportáveis como relatório; e

1.21 Permitir a exibição de todas as demais atividades enquanto o alarme estiver aberto e após a confirmação ou fechamento do mesmo.

2 REQUISITOS DESEJÁVEIS

2.1 Permitir a configuração do módulo de alarme por intermédio de rede Protocolo de Controle de Transmissão - Protocolo de Rede (*TCP-IP - Transmission Control Protocol - Internet Protocol*), sendo preferencialmente o ambiente segregado logicamente na estrutura da rede do elo;

2.2 Possibilitar o suporte aos diversos tipos de sensores/equipamentos, a exemplo de:

a) detectores de movimento infravermelho passivos;

b) barreiras de infravermelho ativas;

c) contatos magnéticos;

d) barreiras de microondas;

e) barreiras magnéticas;

f) sensores sísmicos;

g) sensores de movimento; e

h) radares de vigilância terrestre.

2.3 Possibilitar a exibição de vídeos digitais, ao vivo e gravados, relacionados aos alarmes.

Anexo F – Descrição do desempenho do Módulo de Reação (MRE)

1 REQUISITOS MANDATÓRIOS

1.1 Permitir o acionamento do efetivo específico de acordo com tipo de natureza do evento acionado pelos sensores/leitores/equipamentos/câmeras;

1.2 Permitir o gerenciamento do efetivo despachado para o atendimento de eventos;

1.3 Permitir o acionamento e o gerenciamento do efetivo despachado para o atendimento de eventos por meio de radiocomunicadores em UHF e por dispositivos de telefonia móveis; e

1.4 Possuir total disponibilidade de comunicação com o MCVE.

2 REQUISITOS DESEJÁVEIS

2.1 Manter o máximo de proximidade com o MCVE para fins de acionamento.

Anexo G – Descrição do desempenho do Módulo de Tecnologia da Informação (MTI)

1 REQUISITOS MANDATÓRIOS

1.1 Utilizar a estrutura física da intranet, sendo segregado por intermédio de *VLAN*.

2 REQUISITOS DESEJÁVEIS

2.1 Configurar os *IP* da *VLAN* com faixa diferente dos endereços da rede local da OM.

Anexo H – Descrição do desempenho do Módulo de Central de Vigilância Eletrônica (MCVE)

1 REQUISITOS MANDATÓRIOS

1.1 Permitir limitar a visualização de câmeras e alarmes e a orientação das Equipe de Resposta ou Forças de Reação aos operadores do MCVE;

1.2 Permitir acesso à CVE somente para pessoal autorizado;

1.3 Possuir efetividade de comunicação com o MRE; e

1.4 Permitir a verificação da operacionalidade dos dispositivos de todos os módulos do SSE.

2 REQUISITOS DESEJÁVEIS

2.1 Manter o máximo de proximidade com o MRE para fins de acionamento.