MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

SEGURANÇA

MCA 205-4

MANUAL DE GERENCIAMENTO DE RISCO AVSEC NO SISCEAB

2019

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

SEGURANÇA

MCA 205-4

MANUAL DE GERENCIAMENTO DE RISCO AVSEC NO SISCEAB

2019

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

PORTARIA DECEA Nº 64 /DGCEA, DE 24 DE MAIO DE 2019.

Aprova a edição do MCA 205-4 “Manual de Gerenciamento de Risco AVSEC no 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 e o item 3.2 da DCA 205-7, de 25 de janeiro de 2017, resolve:

Art. 1º Aprovar a edição do MCA 205-4 “Manual de Gerenciamento de Risco AVSEC no SISCEAB”.

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

Este manual tem a finalidade de estabelecer a metodologia de gerenciamento de risco à segurança da aviação civil contra atos de interferência ilícita (AVSEC), prevista nos regulamentos do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB).

1.2 ÂMBITO

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

2 SIGLAS, ACRÔNIMOS E DEFINIÇÕES

2.1 SIGLAS E ACRÔNIMOS

ATC	Controle de Tráfego Aéreo
ATS	Serviço de Tráfego Aéreo
PSNA	Provedor de Serviço de Navegação Aérea
SISCEAB	Sistema de Controle do Espaço Aéreo Brasileiro

2.2 DEFINIÇÕES

As definições desta Instrução são complementadas pelas estabelecidas nos demais regulamentos AVSEC do SISCEAB.

2.2.1 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.

2.2.2 IMPACTO

Reflete a severidade dos efeitos da ocorrência do risco nos objetivos da organização.

2.2.3 INCERTEZA

Incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

3 GERENCIAMENTO DE RISCO AVSEC

Este manual apresenta o processo pormenorizado de gerenciamento de risco e a metodologia de avaliação de risco, fundamentais para a eficiência das atividades decorrentes e eficácia da gestão do risco AVSEC do SISCEAB.

Para que a metodologia de avaliação de risco seja compreendida, faz-se necessário explicitar o processo de gerenciamento de riscos AVSEC do SISCEAB, estabelecido na DCA 205-8, que serão explicitados ao longo deste manual, conforme a figura abaixo:

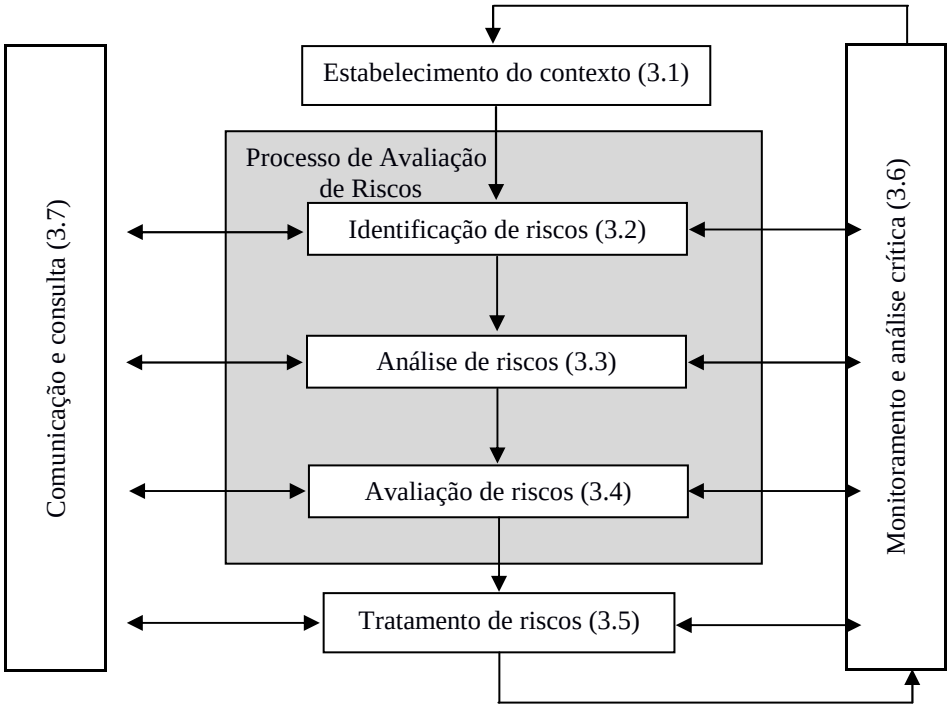

Figura 1. Processo de gerenciamento de risco AVSEC.

3.1 ESTABELECIMENTO DO CONTEXTO

As leituras de cenário atual, através do levantamento dos contextos interno e externo, deverão ser realizadas anteriormente à etapa de identificação de riscos. O contexto delimita o escopo do processo, no que se refere à abrangência e aos critérios gerais para as atividades da gestão de riscos, podendo ser externos ou internos.

O contexto externo é o ambiente alheio ao controle do DECEA. Entender o contexto externo é importante para assegurar que a segurança da navegação aérea e as preocupações das partes interessadas sejam consideradas no desenvolvimento dos critérios de risco. É baseado no contexto de todo o SISCEAB, porém com detalhes específicos sobre requisitos legais e regulatórios, percepções de partes interessadas e outros aspectos dos riscos específicos para o escopo do processo de gerenciamento de riscos.

O contexto interno é o ambiente intrínseco no qual o DECEA busca garantir a segurança da navegação aérea. É algo interior à organização que pode influenciar a maneira pela qual ela gerenciará os riscos.

A identificação dos objetivos estratégicos e operacionais não é parte integrante do processo de gerenciamento de riscos, mas eles são parte do processo de planejamento estratégico e são de vital importância para que a atividade de identificação de riscos seja bem-sucedida.

3.1.1 OBJETIVOS ESTRATÉGICOS

Objetivos estratégicos viabilizam a missão estabelecida pelo DECEA. Em sentido mais amplo, é aquilo que se deseja alcançar. É importante que a alta administração estabeleça e comunique os motivos da existência do SISCEAB. A partir desses motivos, é possível fixar objetivos estratégicos, formular estratégias e estabelecer os objetivos operacionais. Embora a missão e os objetivos estratégicos de uma organização sejam estáveis, a sua estratégia e muitos de seus objetivos operacionais são dinâmicos e ajustam-se às condições internas e externas presentes. Na medida em que essas condições se modificam, as estratégias e os objetivos operacionais são realinhados aos objetivos estratégicos.

Conforme consolidado em diretriz específica, o planejamento estratégico do DECEA estabelece:

a) missão: “contribuir para a garantia da soberania nacional, por meio do gerenciamento do Sistema de Controle do Espaço Aéreo Brasileiro”; e

b) visão: “ser reconhecido como referência global em segurança, fluidez e eficiência no gerenciamento e controle integrado do espaço aéreo.

Dentro do escopo do planejamento estratégico do DECEA, o objetivo estratégico definido para o gerenciamento de risco AVSEC é a “segurança da navegação aérea”.

3.1.2 OBJETIVOS OPERACIONAIS

Os objetivos operacionais são mais concretos, dão suporte, são alinhados com a estratégia selecionada e estão associados a todas as atividades específicas do SISCEAB.

Ao orientar o seu enfoque para o objetivo estratégico, ou seja a segurança da navegação aérea, o Órgão Regional Executivo está pronto para definir os objetivos operacionais. Ao fixar objetivos nos âmbitos da organização e de atividades, pode-se identificar os riscos associados. Os riscos podem estar presentes em uma organização, função, órgão, local, sistema, órgão ATS, pessoa física, entre outros, relacionados ao contexto interno ou externo. Os objetivos operacionais devem ser definidos e explicitados ao envolvidos com as atividades AVSEC das organizações do SISCEAB.

Ao considerar as alternativas para alcançar os objetivos estratégico e operacionais, os comandantes identificam os riscos associados com uma ampla gama de escolhas e analisa as suas implicações no funcionamento das organizações.

Sendo assim, existe uma hierarquia entre os objetivos estratégico e operacionais, conforme demonstra a **Figura 2**. É de suma importância que todos os objetivos sejam identificados e relacionados entre si, pois servirão de base para a próxima etapa do processo, a identificação dos riscos.

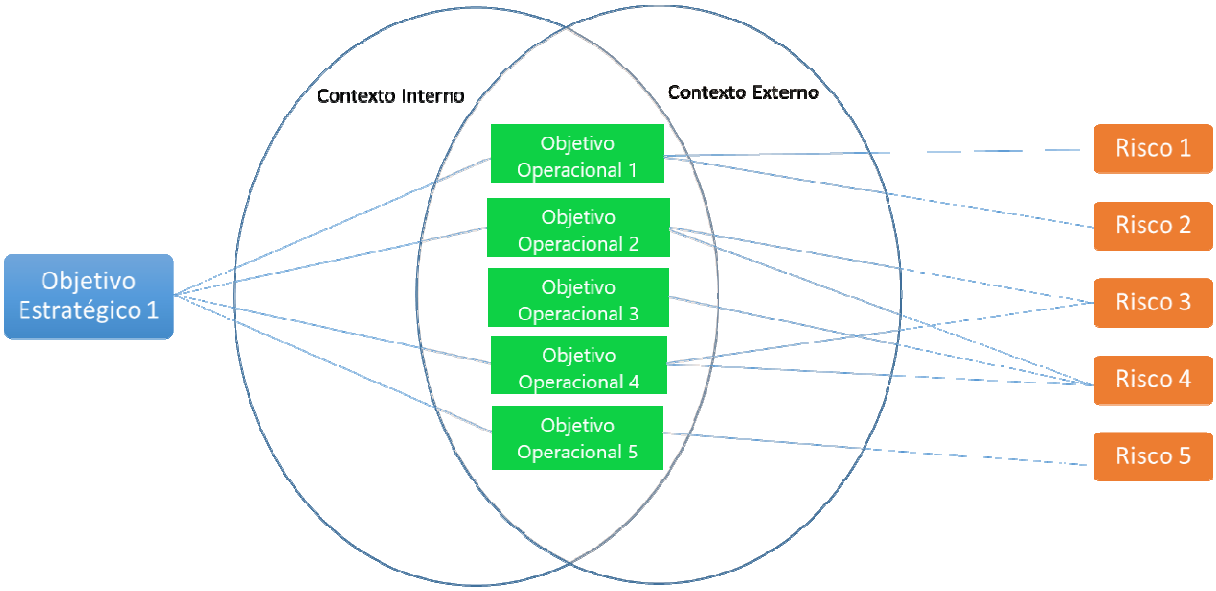

Figura 2. Hierarquização de Objetivos

3.2 IDENTIFICAÇÃO DE RISCOS

Riscos são incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos. Os riscos podem provocar impacto positivo, negativo ou ambos. O foco do gerenciamento de risco AVSEC do SISCEAB será apenas os riscos com impactos negativos.

Ao identificar os riscos, deve-se reconhecer que existem determinadas incertezas. Não é possível afirmar se ou quando o risco ocorrerá, nem o impacto deste. Inicialmente, deve-se considerar uma faixa de eventos em potencial, originada de fontes internas e externas.

Os riscos variam do óbvio ao obscuro, e vão de insignificantes a significativos. Para evitar que um risco deixe de ser percebido, recomenda-se identificá-lo de forma independente à da avaliação de sua probabilidade de ocorrência e de seu impacto. Ressalta-se que mesmo os riscos com possibilidade de ocorrência baixa não devem ser ignorados se o impacto da sua ocorrência for elevado.

A identificação de riscos emprega uma combinação de técnicas como ferramentas de apoio. Por exemplo, a administração do DECEA e de cada PSNA poderá utilizar recursos interativos em grupo como parte de seu método de identificação de riscos, com um facilitador, utilizando ferramentas para assessorar os participantes. As técnicas de identificação de eventos examinam tanto o passado quanto o futuro e apresentam grande variação em relação à sofisticação; enquanto muitas técnicas são específicas ao próprio ramo de atividades das organizações, outras técnicas identificam eventos mediante uma abordagem simples.

As organizações mais avançadas em termos de gerenciamento de riscos utilizam uma combinação de técnicas que aliam eventos passados e potenciais eventos futuros. As técnicas também variam de acordo com o nível onde são utilizadas na organização.

A **Figura 3** demonstra o fluxo e o relacionamento entre as atividades de reconhecimento de objetivo estratégico e operacionais (entradas), a aplicação das técnicas de identificação de eventos e os riscos observados.

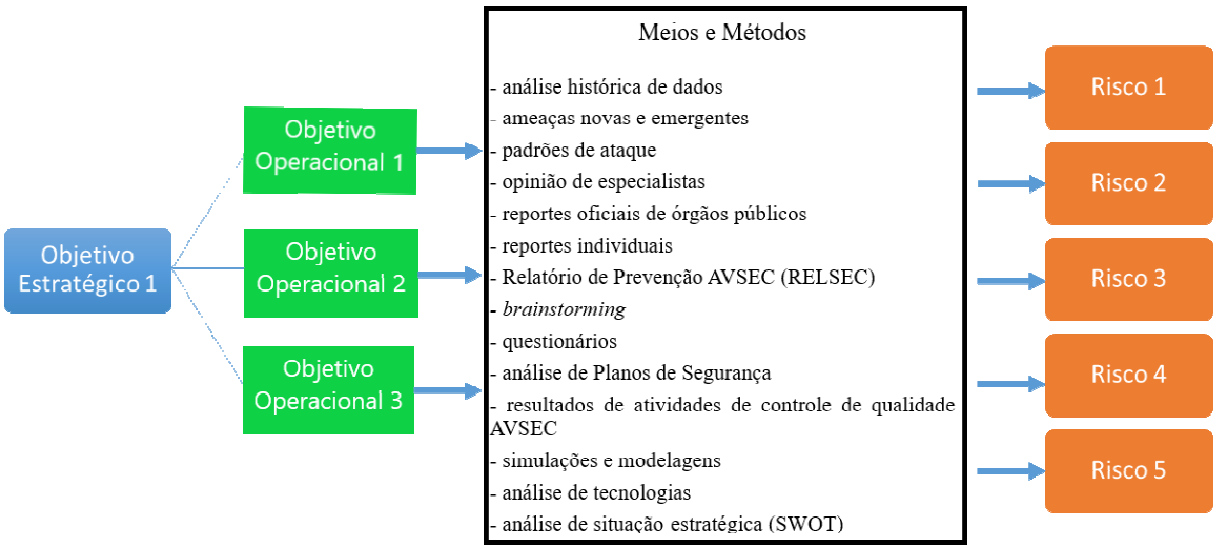

Figura 3. Fluxo das técnicas de identificação de risco AVSEC

Portanto, o grau de profundidade, de amplitude e de disciplina na identificação de eventos pode variar de uma organização para outra. A administração seleciona os meios e métodos compatíveis com a sua filosofia de gerenciamento de riscos – não necessariamente todas ou somente os demonstrados acima – e assegura que as funcionalidades necessárias de identificação de riscos e que as ferramentas de apoio estão implementadas. De um modo geral, a identificação necessita ser eficaz pelo fato de ser a base dos componentes da avaliação de riscos e da resposta a estes.

Independente do meio ou método empregado, após a identificação do risco este deve ser transcrito em um Relatório de Prevenção AVSEC (RELSEC), para que seja registrado e gerenciado. O **Anexo A** demonstra um exemplo de preenchimento de RELSEC.

3.3 ANÁLISE DE RISCOS

Uma vez que os riscos são identificados, uma minuciosa análise da ameaça deve ser feita utilizando-se as escalas de probabilidade e severidade. A análise definirá o Nível de Risco Inerente que corresponde ao nível da ameaça por si, sem que sejam analisadas as medidas de segurança existentes para contrapor à ameaça ou as ações para o tratamento do risco.

Probabilidade x Severidade = Nível de Risco Inerente

Alguma forma de mensuração do risco se faz necessária. Sem um padrão de comparação, não é possível comparar riscos ao longo de toda uma organização. Muitas delas definem escalas para graduar os riscos em termos de severidade, probabilidade e outras dimensões. Estas escalas facilitam uma interpretação consistente dos níveis de riscos.

O quanto mais descritivas forem as escalas, mais consistente será a sua interpretação por aqueles que as utilizam. O ponto chave é achar o equilíbrio certo entre simplicidade e compreensibilidade. Escalas devem promover diferenciação clara para propósitos de seleção e priorização. Escalas de cinco níveis possibilitam uma dispersão

melhor do que escalas de três níveis. Por outro lado, escalas de dez níveis levam a imprecisões na análise qualitativa e perda de tempo na análise e qualificação do nível do risco, sabendo-se que a diferença entre o nível seis ou sete é muito sutil.

Os critérios de riscos AVSEC seguirão as seguintes escalas de probabilidade e severidade definidas na ICA 205-51. A probabilidade deve ser realizada considerando o levantamento de todas as informações de situação do cenário. Quando assinalamos um nível de severidade a um risco, devemos assinalar o nível mais alto entre todos os aspectos analisados. Por exemplo, se qualquer dos aspectos analisados tiver sido considerado como nível "Alto", então o nível de severidade assinalado ao risco deverá ser "Alto".

3.4 AVALIAÇÃO DE RISCOS

Após a análise do risco inerente, será realizada a avaliação deste, levando em consideração a sua vulnerabilidade, de modo a obtermos o Nível de Risco Residual.

Nível de Risco Inerente x Vulnerabilidade = Nível de Risco Residual

O critério de avaliação de vulnerabilidade, definido da ICA 205-51, leva em conta a avaliação das medidas de segurança existentes para cada cenário de ameaça a que a organização estiver submetida.

O **Apêndice** deste manual apresenta exemplos de tabelas de apoio para a avaliação das medidas de segurança existentes. Caso a organização enfrente um cenário diferente ou possua medidas de segurança distintas das apresentadas, o avaliador poderá criar uma tabela de apoio específica para realizar a avaliação da vulnerabilidade, devendo citá-la e anexá-la no Formulário de Avaliação de Risco AVSEC.

Após a avaliação do risco, este deve ser adicionado na composição do mapa de risco AVSEC. O mapa é uma ferramenta útil para demonstrar a quantidade de reportes e a média dos níveis de riscos inerentes e residuais, podendo ser acessado de acordo com a amplitude e temporalidade necessárias para o gerenciamento de risco específico do Agente Local, Gerente Regional ou Nacional, conforme exemplo demonstrado no **Anexo C**.

A elaboração e constante atualização do mapa de riscos é essencial para uma compreensão rápida dos perigos ao qual o SISCEAB está exposto, auxiliando na tomada de decisões gerenciais de comandantes e na avaliação dos Comitês AVSEC.

3.5 TRATAMENTO DE RISCOS

Depois de identificados, avaliados e mensurados, deve-se definir qual tratamento que deve ser dado aos riscos. Determinar a solução mais adequada de tratamento envolve balancear os custos e os esforços de implementação com os benefícios obtidos e atendimento de requisitos legais, regulatórios, técnicos, operacionais, dentre outros. As decisões também devem levar em consideração os riscos que demandam um tratamento economicamente não justificável, como por exemplo, riscos com custo de tratamento mais alto do que o custo dos impactos gerados.

As ações necessárias para o tratamento devem constar no Plano de Tratamento do Risco, conforme exemplo no **Anexo D.**

Em uma primeira abordagem da elaboração do Plano de Tratamento, deve ser avaliada a necessidade de melhorar ou substituir as medidas de segurança já existentes. Após essa avaliação, e se ainda identificada a necessidade de redução do nível do risco, devem ser propostos novos controles, observados os critérios de eficiência e eficácia da sua implementação.

A organização proprietária do risco deve ser assessorada pelo respectivo Comitê de Risco. É importante também ressaltar que o tratamento a ser implementado pode ser uma nova fonte de risco e deve ser tratado em conjunto com sua implementação.

Caso o tratamento esteja fora da competência ou capacidade da organização e a propriedade do risco seja transferida, a organização que receber a propriedade deste deverá elaborar um novo Plano de Tratamento do Risco, a ser controlado, monitorado e atualizado por esta.

Cada risco deve ser relacionado a uma opção de tratamento. Conforme já definido na ICA 205-51, a escolha da opção depende do nível do risco residual, do contexto do SISCEAB ou do seu custo, conforme abaixo:

a) aceitar: quando seu nível está nas faixas de apetite a risco. Nenhum novo controle precisa ser implementado, apenas manter o monitoramento.

   – Exemplo 1: A EPTA decide não investir em melhorias da área de controle de acesso, assumindo que as perdas e erros atualmente sabidos e esperados de informações internas para o processo de decisão e de gestão são impactos toleráveis.

   – Exemplo 2: um DTCEA identificou e avaliou o risco de um ponto do muro não possuir vigilância eletrônica. Como não há eventos registrados no histórico de ocorrências e o entorno do prédio do PSNA está totalmente coberto pelas câmeras de vigilância, o risco foi aceito.

b) evitar: quando a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação. Significa encerrar a atividade relacionada. Nesse caso, essa opção deve ser adotada pelo Comandante do Órgão Regional Executivo.

   – Exemplo: uma organização decide se desfazer de um auxílio à navegação pelo fato de estar localizado em área de alta criminalidade e possuir histórico de frequentes furtos de cabos de energia, ar condicionado e equipamentos de informática. Bem como ser de alta periculosidade o acesso de militares que realizam a manutenção do auxílio à navegação ao bairro.

c) mitigar: quando a implementação de medidas de controle apresenta um custo/benefício tolerável. Significa implementar controles que possam reduzir a probabilidade, a severidade ou a vulnerabilidade avaliada, a um nível aceitável.

   – Exemplo: O ACC verifica que a probabilidade de um ataque cibernético aos seus sistemas ATM está aumentando. Desta forma, decide-se investir na redundância dos equipamentos que processam os dados mais críticos para o controle do tráfego aéreo. Caso aconteça o ataque cibernético em algum desses equipamentos, a redundância

implementada asseguraria a continuidade da operação dos respectivos sistemas, mitigando o impacto nas atividades críticas do órgão.

d) compartilhar: quando a implementação de controles não apresenta um custo/benefício tolerável. Pode-se compartilhar o risco por meio de terceirização do serviço, por exemplo.

– Exemplo: a EPTA identificou e avaliou os custos administrativos e riscos de falhas e desgaste natural dos portões de acesso ao prédio da Torre de Controle. Após analisar a melhor estratégia a ser adotada referentes aos riscos e despesas com o treinamento de pessoal, manutenção corretiva e preventiva, certificações e verificar que o aeroporto (operado por empresa distinta) ao qual está sediado possui uma estrutura eficiente e eficaz de controle de acesso, a EPTA decide terceirizar o serviço para o aeroporto, de forma que a estrutura de seleção e capacitação de pessoal, bem como a manutenção e garantia de disponibilidade dos portões sejam de responsabilidade de um fornecedor externo (no caso, o aeroporto).

Após a implementação da estratégia de tratamento selecionada, a efetividade dos controles postos em prática deve ser avaliada no devido tempo necessário e, em seguida, uma nova avaliação do risco a eles relacionados deve ser realizada, obtendo-se assim uma nova medida de índice de risco residual.

A **Figura 4** apresenta o fluxo básico do gerenciamento de riscos, desde o estabelecimento dos objetivos estratégicos até o tratamento, para uma melhor compreensão de como as atividades estão relacionadas.

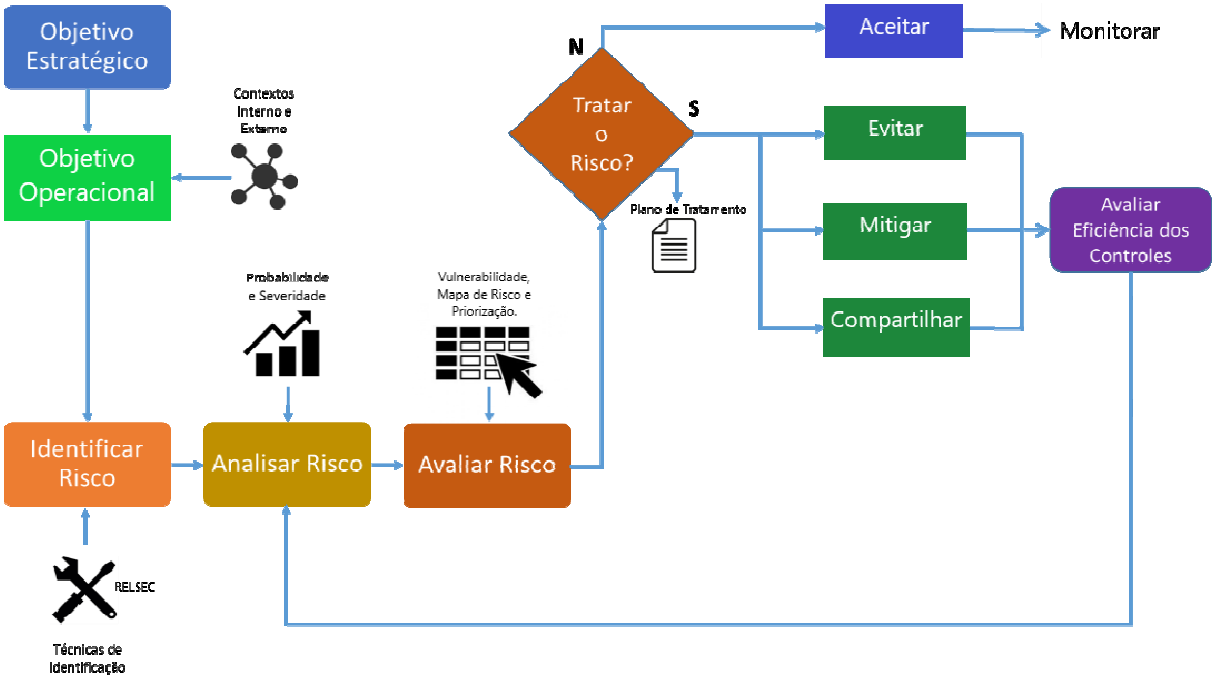

Figura 4. Fluxo Básico do Gerenciamento do Risco

Após a implementação de controles para o tratamento do risco, a eficácia desses controles deve ser avaliada e uma nova avaliação dos critérios de probabilidade, severidade e vulnerabilidade deve ser realizada. Esta nova medida de Nível de Risco Residual deverá estar dentro dos critérios de apetite ao risco definidos na ICA 205-51, caso não se

enquadre, o proprietário do risco deve realizar novas ações de controle, até que o risco residual seja aceito, evitado ou compartilhado.

As medidas de risco, inerente e residual, devem ser mantidas documentadas a cada ciclo de tratamento, com o objetivo de avaliar se os resultados esperados com as ações de tratamento estão sendo alcançados.

Outros fatores podem influenciar a tomada de decisão quanto a tratamento de um dado risco. Limitações orçamentárias, inviabilidade técnica e outros podem ser determinantes. Nesse caso, todos os riscos que pertencem à faixa dos que devem ser tratados, e que em função dessas circunstâncias, foram aceitos, devem possuir justificativas que suportem a sua aceitação e a respectiva aprovação do proprietário do risco.

3.6 MONITORAMENTO E ANÁLISE CRÍTICA

O gerenciamento de riscos é um processo que se modifica com o passar do tempo. As respostas aos riscos que se mostravam eficazes podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de serem executadas; ou os objetivos podem mudar. Essas modificações podem ser causadas pela chegada de novos profissionais, pelas mudanças na estrutura ou no direcionamento da organização ou, ainda, pela introdução de novos processos. Diante dessas mudanças, a alta administração do DECEA necessita determinar se o funcionamento do gerenciamento de riscos AVSEC permanece eficaz.

O monitoramento deve ser conduzido mediante avaliação periódica de indicadores e de mapas de risco.

Os indicadores de riscos AVSEC são estruturados para fazer o próprio monitoramento de forma contínua. A adoção de indicadores é essencial para representar, de maneira padronizada e consistente, os resultados obtidos pelo processo, viabilizando assim o monitoramento do desempenho das práticas de gerenciamento de riscos por meio da coleta, análise e divulgação das informações aos envolvidos no processo, além de facilitar a tomada de decisão da alta administração do DECEA.

Os mapas de risco complementam os indicadores e devem ser utilizados de acordo com a amplitude e a temporalidade que se pretenda analisar. A amplitude será definida com a jurisdição da organização responsável. Por exemplo, uma EPTA somente poderá visualizar o mapa dos riscos registrados pela sua organização. Um Órgão Regional poderá visualizar os riscos de um ou mais PSNA específicos na sua área de jurisdição. A AVSECCEA poderá visualizar todos os riscos registrados no SISCEAB, podendo selecionar os riscos de organizações, regionais ou nacional. A temporalidade é o período a ser monitorado, podendo ser dias, meses ou anos.

A análise crítica será realizada pelos Comitês AVSEC, que devem levar em consideração todos os resultados obtidos no processo de gerenciamento AVSEC e demais atividades AVSEC realizadas na organização. Os riscos registrados e avaliados, planos de tratamento, mapas e indicadores de risco são os elementos básicos que devem ser analisados durante as reuniões dos Comitês.

As ferramentas de monitoramento e de análise crítica tem o objetivo de garantir que os mesmos auxiliem na compreensão de como o processo de gerenciamento de

riscos está sendo executado, permitindo realizar ajustes nos procedimentos, processos e normas.

Ao longo do ciclo, os critérios de riscos poderão ser alterados e novas ocorrências poderão incrementar o mapa de riscos. Os contextos interno e externo podem sofrer alterações e a organização pode aprender com seus sucessos e falhas, amadurecendo internamente o processo. Poderão ser criados novos indicadores para o processo de gerenciamento de riscos e identificados pontos de melhoria a cada medição.

Cabe ao Comitês AVSEC reunir, organizar e preparar as proposições de melhoria contínua, monitorar as ações decorrentes dos planos de tratamento e registrá-las nas atas de reunião. Seguem abaixo exemplos de mecanismos para captura de proposições de melhoria contínua:

a) acompanhamento de atividades e consultas: em todas as reuniões dos Comitês AVSEC deve-se realizar a busca de oportunidades de melhoria que, uma vez identificadas, devem ser avaliadas e registradas. Também devem ser feitas consultas periódicas aos demais participantes do processo em busca de sugestões que possam melhorá-lo.

b) recebimento de sugestões de melhoria espontâneas: é comum que os participantes do processo encaminhem, formal ou informalmente, sugestões de melhorias aos processos. Todos devem ser encorajados a fazê-lo.

A melhoria contínua tem por escopo o desempenho do modelo em relação ao processo alvo, não obstante, a possibilidade de ajustes no modelo em si. O objetivo é de cunho prático e devem ser questionados, no mínimo, os seguintes aspectos:

a) Todos os atores estão em sintonia quanto ao processo de Gerenciamento de Riscos?

b) O processo atual tem conseguido antecipar-se aos riscos?

c) O processo de melhoria contínua e o aprendizado têm sido efetivos?

d) Ocorreu alguma mudança no contexto não registrada?

e) Os planos de tratamentos estão sendo executados dentro dos prazos?

f) Contribui para a consecução dos objetivos institucionais?

g) Agrega valor aos processos?

h) É percebida melhoria nos processos?

Ao final das reuniões dos Comitês AVSEC, será elaborada uma Ata de Reunião contendo os itens previstos na ICA 205-51. Ressalta-se que as informações a serem inseridas na ata devem possuir qualidade contextual e de representação como base nos critérios a seguir:

a) relevância: a informação deve ser útil para o objetivo do trabalho;

b) integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;

c) adequação: volume de informação adequado e suficiente;

d) concisão: informação deve ser apresentada de forma compacta;

e) consistência: as informações apresentadas devem ser compatíveis;

f) clareza: informação deve ser compreensível;

g) padronização: informação deve ser apresentada conforme prevista.

3.7 COMUNIÇÃO E CONSULTA

Como acontece em qualquer processo de gestão, a comunicação é atividade chave para a obtenção dos resultados esperados. É importante ressaltar que o processo de comunicação deve permear toda a estrutura organizacional do SISCEAB, desde a alta administração até a ponta da linha, onde os riscos serão identificados e tratados.

Sendo assim, a tabela abaixo apresenta as principais ferramentas de comunicação que são geradas pelo processo de gerenciamento de riscos, seus responsáveis, público alvo, suas descrições e frequência sugerida. À medida que o processo de gestão de riscos ganha maturidade, esta tabela deve ser alvo de análise crítica com o objetivo de assegurar que as comunicações permanecem satisfazendo todas as partes envolvidas no que diz respeito à sua forma, conteúdo e frequência.

Ferramenta	Descrição	Responsável	Público Alvo	Frequência
RELSEC	Listagem abrangente de eventos que possam afetar a realização dos objetivos, incluindo suas causas e consequências, reações em cadeia provocadas por consequências específicas e efeitos cumulativos e em cascata.	Público Interno e/ou Externo do SISCEAB	Agente Local e Gerente Regional	A cada risco identificado
Mapa de Risco	Compreensão rápida dos riscos a que a organização está exposta, auxiliando na tomada de decisões gerenciais dos comandantes e na avaliação dos Comitês AVSEC.	Proprietário do Risco	Comitê AVSEC e Comandante	Trimestral
Avaliação de Risco	Processo de compreensão da fonte e cenário do risco e comparação com a eficácia das medidas de controle existentes para a determinação do nível de risco inerente. Inclui a apreciação das causas, possíveis consequências, probabilidade, severidade e vulnerabilidade.	Proprietário de Risco	Comitê AVSEC	A cada risco identificado
Plano de Tratamento de Risco	Descrição detalhada das ações de tratamento dos riscos, com responsáveis, custos estimados, prazos de conclusão e situação atualizada da implementação.	Proprietário de Risco	Comitê AVSEC e Comandante	Mensal
Ata de Reunião	Quantidade de riscos, indicadores de riscos, planos de tratamento em curso e concluídos, custos de ações de tratamento, mapa de riscos e sugestões de melhorias.	Comitê AVSEC	Comandante	Anual
Ficha de Difusão de Ameaça	Processo de disseminação de informações relativas a evento AVSEC aos destinatários que possuam necessidade de conhecer	Agente Local, Gerente Regional e Gerente Nacional	Entidades de Aviação Civil, Gerentes Regionais e Agentes Locais	A cada ameaça identificada

Tabela 1. Comunicação de Riscos e Ameaças AVSEC no SISCEAB

4 METODOLOGIA DE AVALIAÇÃO DE RISCO

Com a finalidade de facilitar a compreensão do gerenciamento de risco, a aplicação da metodologia de avaliação de riscos pelos Agentes Locais, Gerentes Regionais e Gerente Nacional será detalhada neste capítulo, devendo seguir o fluxograma abaixo:

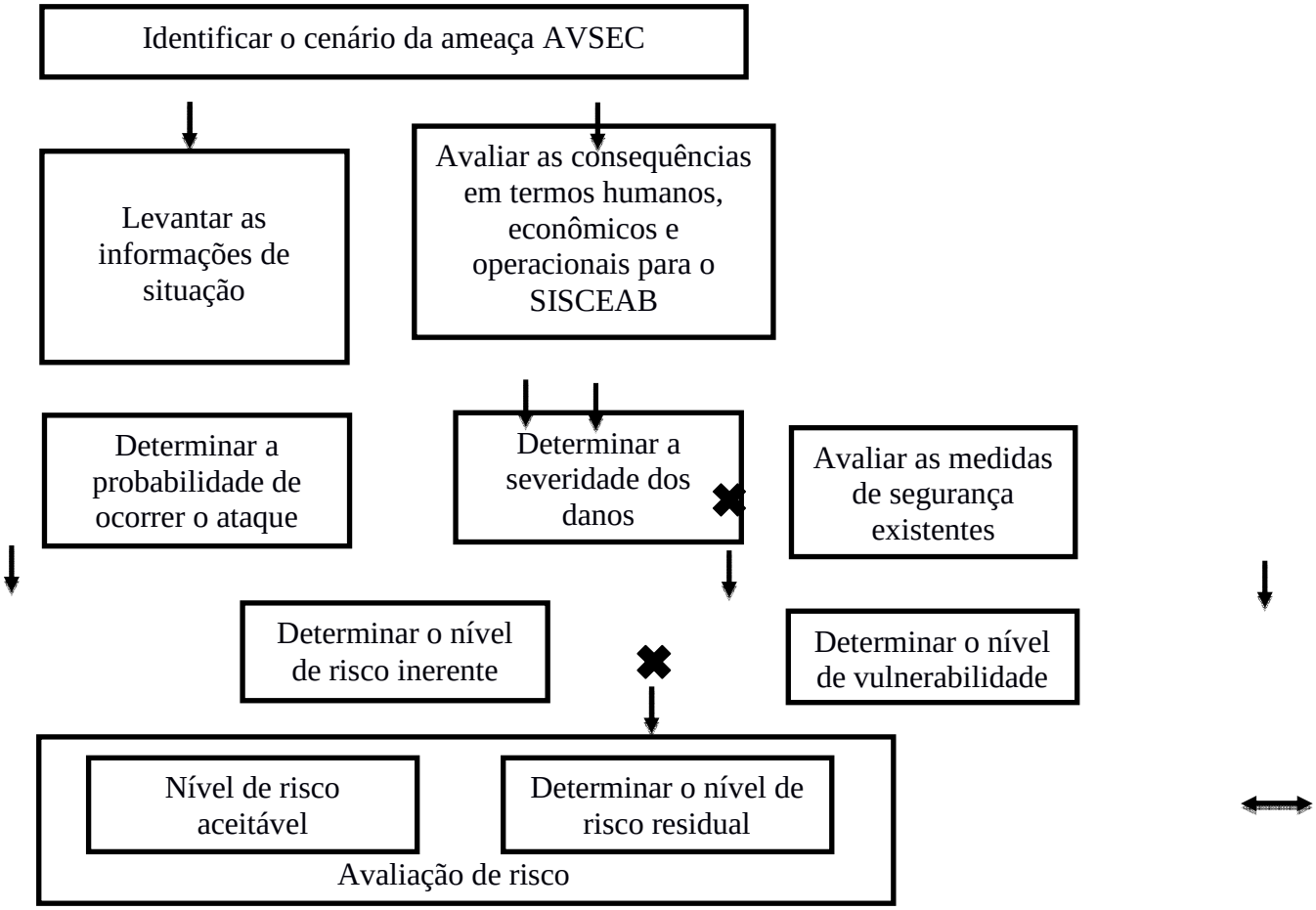

Figura 1. Fluxograma da Avaliação do Risco

Os **Anexos A, B, C** e **D** deste manual apresentam exemplos de um ciclo completo do Processo de Gerenciamento de Risco AVSEC, desde a sua identificação até o tratamento, a partir dos relatórios e formulários definidos na DCA 205-8 e na ICA 205-51.

O **Anexo E** deste manual apresenta um exemplo de aplicação da metodologia de avaliação de risco, com a finalidade de explicitar e elucidar as etapas do Processo.

4.1 IDENTIFICAÇÃO DOS CENÁRIOS DA AMEAÇA AVSEC

Ameaça AVSEC é a intenção declarada de causar prejuízo, dano ou outra ação hostil a alguém, a aeronave ou a instalação aeronáutica, não se restringindo apenas a um evento isolado, podendo ser compreendida como circunstância ou tendência. A identificação de cenários de ameaça consiste em relacionar quais são as atitudes que podem ser adotadas por um indivíduo ou grupo com o propósito de causar um evento adverso e consequências indesejáveis.

É importante que a avaliação de risco identifique os cenários de ameaça e considere todas as possibilidades de ataque, que podem, por exemplo, serem dirigidos a uma

instalação aeronáutica específica, a um equipamento de infraestrutura, às áreas de armazenamento de combustíveis, aos órgãos e equipamentos de controle de tráfego aéreo ou de navegação aérea.

As avaliações de risco no SISCEAB serão realizadas a partir da identificação do cenário de ameaça (**Etapa 1**) ou de situações que demandem a análise de risco, tais como (relação não exaustiva):

a) introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo, nos pertences de mão ou em veículo;

b) introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por funcionário, no próprio corpo, nos pertences de mão ou em veículo;

c) invasão física de organização do SISCEAB visando, através dessa, obter acesso à área restrita de segurança (ARS) de aeródromo;

d) invasão física de PSNA visando controlar, impedir ou degradar a operacionalidade do SISCEAB;

e) ataque ou perturbação no exterior do PSNA;

f) ataque cibernético aos Sistemas ATM visando controlar, impedir ou degradar a operacionalidade do SISCEAB;

g) utilização de dispositivos (MANPAD, aeronaves não tripuladas ou de raios laser) que impeçam ou degradem a navegação aérea;

h) segurança dos pontos sensíveis; e

i) instalação de novos sítios do SISCEAB.

4.2 LEVANTAMENTO DE INFORMAÇÕES DE SITUAÇÃO

As informações de situação são aquelas que explicitam a realidade atual em termos sociais, econômicos, políticos, criminais e de logística da localidade da organização.

O levantamento de informações de situação da localidade onde se encontra a organização, tem a função de subsidiar o responsável pela avaliação de riscos AVSEC com dados suficientes para determinar a probabilidade de ocorrer cada um dos atos de interferência ilícita contra a segurança da aviação civil.

O responsável pela elaboração da avaliação de risco poderá utilizar todas as informações que estiverem à sua disposição, no intuito de determinar a probabilidade de ocorrer um possível ato de interferência ilícita contra a aviação civil. De forma exemplificativa e não exaustiva, e explicitada na **Etapa 2** do **Anexo E,** as seguintes informações que poderão ser observadas nessa etapa:

a) presença conhecida de organização criminosa na região, com potencial para conduzir ato de interferência ilícita contra a aviação civil;

b) histórico de ações violentas no entorno e nas dependências da organização ou aeródromo nos últimos anos, inclusive atos de interferência ilícita;

c) histórico de manifestações ou greves nas dependências ou imediações da

organização ou aeródromo nos últimos anos;

d) volume de tráfego de voos regulares domésticos e internacionais em operação no(s) aeródromo(s) ao qual o órgão ATS proporciona serviços de tráfego aéreo;

e) voos que possam ser considerados alvos potenciais como, por exemplo, aqueles com ligação a localidades sujeitas a atos de interferência ilícita;

f) realização de eventos de grande visibilidade e repercussão na mídia nacional ou internacional na região de influência da organização ou aeródromo;

g) presença de dignitários, autoridades nacionais e internacionais ou de pessoas que sejam potencialmente sujeitas a ataques individuais;

h) existência de crise interna;

i) existência de problemas econômicos; e

j) informações específicas acerca da possibilidade de ocorrer um ataque.

O responsável pelo levantamento das informações de situação utilizadas na elaboração da avaliação de risco deve considerar que, quanto maior a quantidade de informações, maior a confiabilidade da fonte e melhor a qualidade da informação, melhor também será a precisão da definição da probabilidade de concretização dos cenários de ameaça avaliados.

4.3 PROBABILIDADE DE OCORRER O ATAQUE

A probabilidade de ocorrer um determinado ato de interferência ilícita baseia-se na intenção de grupo ou indivíduo e na sua capacidade real de concretizar o referido ato, considerando também o histórico de ocorrências de cada tipo de evento.

Nesse manual, a probabilidade de ocorrer um ataque à aviação civil será determinada por meio de perguntas que deverão ser respondidas com base nas informações de situação levantadas na etapa anterior, bem como na eventual existência de informações específicas acerca do planejamento, intenção e capacidade de um grupo ou indivíduo concretizar tal ataque.

Cada uma das perguntas será respondida com nota graduada de zero a cinco, atribuindo cinco pontos quando a resposta for totalmente negativa, zero ponto quando a resposta for totalmente positiva e valores intermediários quando ocorrer uma situação nem totalmente positiva nem totalmente negativa, conforme **Etapa 2** do **Anexo E**.

A pontuação final será obtida pela média simples das pontuações de todas as respostas, arredondando-se para um número inteiro, para posterior classificação da probabilidade de ocorrer o ataque na tabela abaixo:

Probabilidade	alta (5)	cenário muito plausível, com forte evidência de capacidade, intenção e planejamento
	média-alta (4)	cenário claramente plausível, com evidências de início de planejamento do ataque ou hostilidade
	média (3)	cenário plausível, com alguma evidência de intenção e capacidade, mas nenhuma evidência de planejamento de ataque
	média-baixa (2)	cenário com alguma evidência de intenções, ainda que com método aparentemente não suficientemente desenvolvido
	baixa (1)	cenário teoricamente plausível, com intenção teórica, mas sem capacidade ou sinais de planejamento

Tabela 2. Classificação da probabilidade de ocorrer um ataque

A critério do responsável pela realização da avaliação de riscos, cada pergunta pode receber um peso que a diferencie das demais, que corresponde ao grau de relevância da pergunta para a medida da probabilidade de ocorrer o ato ilícito, ou seja, a pergunta que tiver peso maior é aquela vista como mais relevante para indicar probabilidade maior de ocorrer um ataque. A pontuação final será obtida pela média ponderada das pontuações de todas as respostas, arredondando-se para um número inteiro, para posterior classificação da probabilidade de ocorrer o ataque no quadro mencionado. Caso sejam determinados pesos diferentes, estes deverão ser detalhados e justificados no Formulário de Avaliação de Risco AVSEC.

NOTA: No exemplo apresentado na **Etapa 2** do **Anexo E** optou-se por não adotar pesos diferentes para as perguntas para simplificar o entendimento do método.

A quantidade de perguntas relacionadas e os seus conteúdos, bem como os pesos, caso sejam estabelecidos, são fruto da percepção e experiência do responsável pela execução da avaliação de risco AVSEC e da maturidade do processo de gerenciamento de risco na organização, que podem variar de acordo com cada localidade.

4.4 SEVERIDADE DOS DANOS CAUSADOS PELO ATAQUE

A severidade dos danos causados por um ataque é função da natureza e da escala das consequências em termos humanos, econômicos e operacionais para o SISCEAB.

Dessa forma, conforme já estabelecida na ICA 205-51 e exemplificada na **Etapa 4** do **Anexo E** a severidade dos danos deve ser classificada por meio da escala que varia de 1 (baixa) a 5 (alta), segundo os critérios abaixo, para cada um dos cenários de ameaça identificados:

		Termos humanos	**Termos econômicos**	**Termos operacionais**
Severidade	alta (5)	centenas de mortos	bilhões de dólares	interrupção severa dos serviços
	média-alta (4)	alguns, mas não todos os itens acima com alta severidade		
	média (3)	dezenas de mortos	milhões de dólares	interrupção moderada dos serviços
	média-baixa (2)	alguns, mas não todos os itens acima com média severidade		
	baixa (1)	feridos e eventualmente algum morto	pouco impacto econômico	pouca interrupção dos serviços

Tabela 3. Classificação da severidade dos danos causados por um ataque

4.5 DETERMINAÇÃO DO NÍVEL DE RISCO INERENTE

O nível de risco inerente representa o nível de ameaça em si, independente das medidas de segurança existentes. É a relação entre a probabilidade de ocorrer um ato de interferência ilícita contra a aviação civil e a severidade dos danos causados pelo ataque. Conforme já estabelecida na ICA 205-51 e exemplificada na **Etapa 5** do **Anexo E**, para cada um dos cenários de ameaça identificados deve ser determinado o respectivo nível do risco inerente a partir da seguinte tabela:

Nível de Risco Inerente		**Severidade**				
		baixa (1)	média-baixa (2)	média (3)	média-alta (4)	alta (5)
Probabilidade	alta (5)	médio-baixo (5)	médio (10)	médio-alto (15)	alto (20)	alto (25)
	média-alta (4)	baixo (4)	médio-baixo (8)	médio (12)	médio-alto (16)	alto (20)
	média (3)	baixo (3)	médio-baixo (6)	médio-baixo (9)	médio (12)	médio-alto (15)
	média-baixa (2)	baixo (2)	baixo (4)	médio-baixo (6)	médio-baixo (8)	médio (10)
	baixa (1)	baixo (1)	baixo (2)	baixo (3)	baixo (4)	médio-baixo (5)

Tabela 4. Quadro para determinação do nível de risco inerente

4.6 MEDIDAS DE SEGURANÇA EXISTENTES

As medidas de segurança existentes na organização que impeçam ou mitiguem a concretização de um ato de interferência ilícita devem ser avaliadas. Da mesma forma, devem ser observadas as eventuais vulnerabilidades, que acabam facilitando a perpetração do ato ou dificultando a adoção de contramedidas.

Essa atividade está relacionada às atribuições do Agente Local AVSEC da organização e pode ser realizada utilizando-se das informações obtidas através das atividades de controle de qualidade AVSEC.

A identificação de medidas de segurança e de vulnerabilidades existentes será determinada por meio de perguntas que abordam os principais aspectos de recursos humanos, recursos tecnológicos e procedimentos de segurança relacionados a cada um dos cenários de ameaça identificados. As perguntas deverão ser respondidas com base nos relatórios das atividades de controle de qualidade AVSEC.

Os exemplos no **Apêndice** demonstram modelos de apoio para a avaliação dos cenários mais prováveis de ataques ao SISCEAB. Caso a organização enfrente ameaça específica e não listadas neste Manual, o avaliador deverá listar as medidas de segurança existentes e aplicáveis à situação em uma tabela de apoio, aos moldes das tabelas apresentadas.

O peso das questões referente ao levantamento de informações de situação e das medidas de segurança existentes, constantes na **Etapa 6** do **Anexo E** e no **Apêndice**, poderá ser alterado conforme citado em **4.3**.

4.7 DETERMINAÇÃO DO NÍVEL DE VULNERABILIDADE

A determinação do nível de vulnerabilidade é a localização, em escala estabelecida, que explicite quão vulnerável a organização está em relação a um cenário de ameaça.

Para tanto, cada uma das perguntas listadas na etapa anterior (**Apêndice**) será respondida com nota graduada de 0 a 5, atribuindo 5 pontos quando a resposta for totalmente negativa, 0 pontos quando a resposta for totalmente positiva e valores intermediários quando ocorrer uma situação nem totalmente positiva nem totalmente negativa. Caso a pergunta não se aplique à situação, esta não será avaliada e não entrará no cálculo da média.

A pontuação final será obtida pela média simples das pontuações de todas as respostas, arredondando-se para um número inteiro, para posterior classificação do nível de vulnerabilidade, conforme já estabelecida na ICA 205-51, exemplificada na **Etapa 7** do **Anexo E**, conforme abaixo:

Vulnerabilidade	alta (5)	não há procedimentos de segurança sendo realizados adequadamente para mitigar o risco
	média-alta (4)	procedimentos de segurança realizados tem um alcance limitado para mitigar o risco, ou áreas importantes não são abrangidos pelo efeito das medidas mitigadoras
	média (3)	características das vulnerabilidades média-alta e média-baixa estão presentes
	média-baixa (2)	procedimentos de segurança estão em vigor, mas são parcialmente efetivos
	Baixa (1)	existem requisitos claros para mitigar o risco e os procedimentos de segurança estão sendo efetivamente realizados de forma adequada

Tabela 5. Quadro para determinação do nível de vulnerabilidade

A critério do responsável pela realização da avaliação de riscos AVSEC, cada pergunta pode receber um peso que a diferencie das demais, que corresponde ao grau de importância da pergunta para a mitigação do risco relacionado a um cenário de ameaça, ou seja, a pergunta que tiver peso maior é aquela vista como mais importante para a segurança

contra o cenário de ameaça identificado, devendo ser seguido o procedimento para alteração de peso citado em **4.3**. Nesse caso, a pontuação final será obtida pela média ponderada das pontuações de todas as respostas, arredondando-se para um número inteiro, para posterior classificação do nível de vulnerabilidade no quadro mencionado.

4.8 DETERMINAÇÃO DO NÍVEL DE RISCO RESIDUAL

O nível de risco residual ou nível de exposição ao risco de um cenário de ameaça determinado é a relação entre o nível de risco inerente (probabilidade x severidade) e o nível de vulnerabilidade dos procedimentos de segurança, conforme já estabelecido na ICA 205-51 e exemplificado na **Etapa 8** do **Anexo E**, deve ser determinado através dos critérios abaixo:

Nível de Risco Residual		**Nível de Risco Inerente (Severidade x Probabilidade)**				
		baixa (5)	média-baixa (10)	média (15)	média-alta (20)	alta (25)
Vulnerabilidade	alta (5)	médio-baixo (25)	médio (50)	médio-alto (75)	alto (100)	alto (125)
	média-alta (4)	baixo (20)	médio-baixo (40)	médio (60)	médio-alto (80)	alto (100)
	média (3)	baixo (15)	médio-baixo (30)	médio-baixo (45)	médio (60)	médio-alto (75)
	média-baixa (2)	baixo (10)	baixo (20)	médio-baixo (30)	médio-baixo (40)	médio (50)
	baixa (1)	baixo (5)	baixo (10)	baixo (15)	baixo (20)	médio-baixo (25)

Tabela 5. Quadro para determinação do Nível de Exposição ao Risco

Quando o nível de risco residual foi classificado como aceitável, há evidências de que as medidas de segurança existentes são adequadas para evitar ou mitigar a perpetração do ato de interferência ilícita de que trata o cenário de ameaça considerado.

Por outro lado, quando o nível de risco residual é maior que o nível de risco aceitável, é necessário que o responsável pela AVSEC da organização adote as providências para reduzir os índices aos níveis aceitáveis, utilizando as informações que embasaram a análise de risco, bem como sua percepção e experiência. Poderá, por exemplo, promover a adequação dos recursos humanos, dos recursos tecnológicos ou dos procedimentos estabelecidos ou, ainda, adotar medidas mitigadoras ou medidas adicionais de segurança.

5 DISPOSIÇÕES FINAIS

5.1 As sugestões para o contínuo aperfeiçoamento desta publicação deverão ser enviadas por intermédio dos endereços eletrônicos http://publicacoes.decea.intraer/ ou http://publicacoes.decea.gov.br/, acessando o link específico da publicação.

5.2 Os casos não previstos neste Programa serão submetidos ao Senhor Diretor-Geral do DECEA.

REFERÊNCIAS

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

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.

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.

Anexo A – Exemplo de Relatório de Prevenção AVSEC

nº: **001/DTCEA-SP**

RELSEC

De acordo com os regulamentos do DECEA, este relato **será usado para a prevenção de atos de interferência ilícita**, a fim de aumentar a segurança da aviação civil. Este relatório não precisa ser identificado. Caso o relator se identifique, a resolução da situação reportada será comunicada ao autor, ao término do processo.

LOCAL	**TWR-SP**		
DATA	**01/ABR/2019**	**HORA**	**12:00 Z**
PESSOAL ENVOLVIDO	**Chefe de Sala, Controlador da posição TWR e GOL 1944**		

DADOS GERAIS DA OCORRÊNCIA

SITUAÇÃO:

A aeronave B737, GOL1944, ao aproximar para pouso no perfil do ILS 17R, reportou a visualização de drone de pequeno porte no seu través direito, a 0,5 NM da sua aeronave, a 2 NM da cabeceira e altitude aproximada de 1500 Ft.

DADOS PARA CONTATO (opcional):

NOME: 3 Sgt Fulano .

E-MAIL: fulanodetal@decea.gov.br .

TELEFONE: (11) 1234-56789 .

Avaliação de Risco AVSEC								nº 001/DTCEA-SP
Fonte do risco	**Causas**	**Consequências**	**Probabilidade**	**Severidade**	**Risco Inerente**	**Vulnerabilidade**	**Risco Residual**	**Mitigações adicionais**
Pessoas e Tecnologia	Não foi possível determinar a causa da utilização indevida do drone.	As aproximações ficaram suspensas por 20 minutos, sendo necessário que 10 aeronaves alternassem o pouso para SBGR e SBKP. Além disso, o índice de atrasos do dia subiu de 30 min para 3h.	**média-baixa**	**baixa**	**baixo**	**alta**	**médio-baixo**	A definição de procedimentos específicos, aliado com a aquisição de equipamentos para a captura, interferência de aeronaves não tripuladas contribui para a redução da vulnerabilidade da navegação aérea no cenário analisado.
Cenário relacionado			A aeronave não tripulada reportada no RELSEC não foi confirmada visualmente pela equipe de serviço da TWR presente no momento do ocorrido. Pelo fato do objeto ter sido avistado apenas uma vez e sendo essa uma aparição isolada, foi atribuída a probabilidade média-baixa.	O reporte indicou que a aeronave não tripulada era de pequeno porte, sendo a severidade avaliada como baixa.	Através dos valores encontrados de probabilidade, severidade, o risco inerente avaliado como baixo.	Não existem equipamentos ou procedimentos adequados para contrapor a ameaça reportada na localidade. A vulnerabilidade foi considerada alta.	Através das tabelas de apoio, o risco residual foi considerado médio-baixo.	
7. Utilização de dispositivos (Sistemas de Aeronaves Remotamente Pilotadas ou raios laser) que impeçam ou degradem a navegação aérea.								

Anexo C – Exemplo de Mapa de Riscos AVSEC

Organização	**DTCEA-SP**	**Período**	de 01/01/2018 a 31/12/2018

Cenário	**Quantidade de Reportes**	**Risco Inerente**	**Risco Residual**
1. Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo, nos pertences de mão ou em veículo.	**2**	**médio (30)**	**médio-baixo (27,50)**
2. Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por funcionário, no próprio corpo, nos pertences de mão ou em veículo.	**4**	**médio-baixo (32,5)**	**baixo (22,50)**
3. Invasão física de organização do SISCEAB visando, através dessa, obter acesso à área restrita de segurança (ARS) de aeródromo.	**20**	**médio-alto (76,25)**	**médio (53,40)**
4. Invasão física de PSNA visando controlar, impedir ou degradar a operacionalidade do SISCEAB.	**5**	**baixo (22)**	**baixo (20,25)**
5. Ataque ou perturbação no exterior do PSNA.	**20**	**médio (51,25)**	**baixo (18,50)**
6. Ataque cibernético aos Sistemas ATM visando controlar, impedir ou degradar a operacionalidade do SISCEAB.	**80**	**baixo (20)**	**baixo (18,87)**
7. Utilização de dispositivos (MANPAD, aeronaves não tripuladas ou raios laser) que impeçam ou degradem a navegação aérea.	**3**	**alto (103,3)**	**médio-alto (78,33)**

Plano de Tratamento de Risco AVSEC								☐ evitar ☒ mitigar ☐ compartilhar ☐ aceitar	**nº 001/DTCEA-SP**
Iniciativa	Ação de Tratamento	Organização responsável	Organizações ou entidades corresponsáveis	Responsável pela implementação	Breve descrição da implementação	Custo previsto	Data prevista para início da implementação	Data prevista para o término da implementação	situação
1	modificação de procedimentos entre a TWR e os órgãos de segurança pública	DTCEA-SP	INFRAERO e Polícia Federal – Aeroporto de Congonhas	Responsável AVSEC do Aeroporto e Polícia Militar	Definição de procedimentos específicos para a coordenação entre TWR e Central 190 da Polícia Militar	não há	01 MAIO 2019	01 JUL 2019	sendo coordenado com os responsáveis da Polícia e Comandante da TWR-SP
2	Aquisição de sistema para identificação de drones	DTCEA-SP	CISCEA e INFRAERO	Gerente Regional do SRPV-SP	Definição de critérios e requisitos para a aquisição de sistema de identificação de RPAS	3 milhões de reais	01 JUL 2020	01 JUL 2021	Sendo coordenado com o SDOP e CISCEA

Anexo E – Exemplo de Avaliação de Risco

ETAPA 1 – Cenário de Ameaça: Introdução de arma, artefato ou material perigoso, com intenções criminais em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo ou nos pertences de mão ou em veículo.

ETAPA 2 – Levantamento das informações de situação:

Essa tabela deverá ser utilizada para todos os cenários ou situações a serem avaliados.

Informações de situação		5 pontos	de 1 a 4 pontos	0 pontos	Pontos	Peso
Q1	Há presença conhecida de organização criminosa na região, com potencial para conduzir ato de interferência ilícita contra a aviação civil?	alto potencial	baixo potencial	ausência	**2**	**1**
Q2	Há histórico de ações violentas no entorno e nas dependências da organização ou aeródromo no último ano, inclusive atos de interferência ilícita?	mais que 3 alto	de 1 a 3 médio	0 baixo	**1**	**1**
Q3	Há histórico de manifestações ou greves nas dependências ou imediações do aeródromo no último ano?	mais que 3 alto	de 1 a 3 médio	0 baixo	**1**	**1**
Q4	Qual é o volume de tráfego semanal de voos regulares em operação no(s) aeródromo(s) ao qual o órgão ATS proporciona serviços de tráfego aéreo?	mais que 49 alto	de 20 a 49 médio	0 a 19 baixo	**5**	**1**
Q5	Há voos que possam ser considerados alvos potenciais como, por exemplo, aqueles com ligação a localidades potencialmente sujeitas a atos de interferência ilícita?	presença de 1 ou mais empresas aéreas	-	ausência	**0**	**1**
Q6	Há histórico de realização de eventos de grande visibilidade e repercussão na mídia nacional ou internacional na região de influência do aeródromo?	histórico de mais de 2 eventos nos últimos 5 anos	histórico de até 2 eventos nos últimos 5 anos	sem histórico nos últimos 5 anos	**5**	**1**
Q7	Há presença de dignitários, celebridades ou pessoas que sejam potencialmente sujeitas a ataques individuais (custodiados de alta periculosidade, pessoas incluídas em programa de proteção à testemunha, etc)?	frequência acima de 1 embarque ou desembarque por semana	frequência de 1 embarque ou desembarque por semana	frequência de uso do aeródromo irrelevante	**5**	**1**
Q8	Existe de crise interna (revolta, distúrbio ou comoção interna, tais como guerra civil iminente ou em andamento ou qualquer outra instabilidade política) na região de influência do aeródromo?	guerra civil iminente ou em andamento; vigência de estado de sítio, defesa ou intervenção federal	presença de manifestação de grande vulto organizada	cenário de estabilidade sociopolítica	**0**	**1**
Q9	Existe problemas econômicos (qualquer estado de crise econômica capaz de resultar em severos cortes orçamentários, que possam impactar na manutenção das medidas de segurança da aviação civil)?	declaração de default financeiro; grave desabastecimento de bens de consumo e primeira necessidade; situação de desemprego grave e generalizada;	Quadro de recessão financeira; situação de desequilíbrio financeiro do Estado; atraso reiterado no pagamento dos servidores públicos gerando insatisfação e desencadeando movimentos grevistas;	Cenário de estabilidade econômica	**1**	**1**
Q10	Há informações específicas acerca da possibilidade de ocorrer um ataque através desse cenário de ameaça?	há informações específicas de planejamento, intenção e capacidade de ataque	há alguma evidência de intenção e capacidade, mas nenhuma evidência de planejamento de ataque real	não há informações específicas ou sinais de possibilidade ou planejamento de ataque; ou há uma intenção teórica, mas sem capacidade aparente	**0**	**1**
MÉDIA (PROBABILIDADE DE ATAQUE):					2	

Continuação do Anexo E – Exemplo de Avaliação de Risco

ETAPA 3 – Probabilidade de ocorrer o ataque:

	alta (5)	cenário muito plausível, com forte evidência de capacidade, intenção e planejamento
	média-alta (4)	cenário claramente plausível, com evidências de início de planejamento do ataque ou hostilidade
	média (3)	cenário plausível, com alguma evidência de intenção e capacidade, mas nenhuma evidência de planejamento de ataque
	média-baixa (2)	cenário com alguma evidência de intenções, ainda que com método aparentemente não suficientemente desenvolvido
	baixa (1)	cenário teoricamente plausível, com intenção teórica, mas sem capacidade ou sinais de planejamento

ETAPA 4 – Severidade dos danos causados pelo ataque:

		Termos humanos	**Termos econômicos**	**Para o SISCEAB**
Severidade	alta (5)	centenas de mortos	bilhões de dólares	interrupção severa dos serviços
	média-alta (4)	alguns, mas não todos os itens acima com alta severidade		
	média (3)	dezenas de mortos	milhões de dólares	interrupção moderada dos serviços
	média-baixa (2)	alguns, mas não todos os itens acima com média severidade		
	baixa (1)	feridos e eventualmente algum morto	pouco impacto econômico	pouca interrupção dos serviços

Continuação do Anexo E – Exemplo de Avaliação de Risco

ETAPA 5 – Determinação do nível do risco inerente:

Nível de Risco Inerente		Severidade				
		baixa (1)	média-baixa (2)	média (3)	média-alta (4)	alta (5)
Probabilidade	alta (5)	média-baixa (5)	média (10)	média-alta (15)	alta (20)	alta (25)
	média-alta (4)	baixa (4)	média-baixa (8)	média (12)	média-alta (16)	alta (20)
	média (3)	baixa (3)	média-baixa (6)	média-baixa (9)	média (12)	média-alta (15)
	média-baixa (2)	baixa (2)	baixa (4)	média-baixa (6)	média-baixa (8)	média (10)
	baixa (1)	baixa (1)	baixa (2)	baixa (3)	baixa (4)	média-baixa (5)

ETAPA 6 – Medidas de segurança existentes:

Para cada cenário ou situação prevista na Etapa 1, será aplicada uma tabela específica. As tabelas de apoio para os demais cenários e situações encontram-se no **Apêndice**.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	É realizada a inspeção de segurança nos visitantes no acesso ao PSNA?	não	sim, sem procedimentos formalizado ou profissional treinado	sim, com procedimento formalizado e profissional treinado	**5**	**1**
Q2	Há força de segurança pública atuando em apoio às medidas de inspeção de segurança?	não	sim, mas sem pronta resposta	sim, com base fixa no local e pronta resposta	**0**	**1**
Q3	Há equipamentos de segurança para inspeção de visitantes no acesso ao PSNA?	não	sim, através de busca pessoal	sim, com equipamento detector de metais	**5**	**1**
Q4	Há equipamentos de segurança para inspeção de bagagens de mão no acesso ao PSNA?	não	sim, apenas com raio-x	sim, com ETD e raio x	**5**	**1**
Q5	As equipes de segurança do PSNA possuem treinamento específico para a realização de inspeção de segurança em visitantes?	não	Sim, porém não regulamentado	Sim, sistemático e regulamentado	**5**	**1**
Q6	Os equipamentos de inspeção de segurança são submetidos a manutenções preventivas e corretivas?	não	sim, somente manutenção corretiva	sim, manut. corretiva e preventiva	**0**	**1**
Q7	Há monitoramento eletrônico dos locais de acesso ao PSNA onde são realizadas as inspeções de segurança?	não	sim, sem procedimentos formalizado ou profissional treinado	sim, com procedimento formalizado e profissionais treinados	**0**	**1**
Q8	Há procedimento padronizado de avaliação das equipes de serviço que desenvolvem atividade de inspeção de segurança?	não	-	sim	**0**	**1**
Q9	O procedimento de inspeção de segurança está livre de interferências de tempo de fila e fatores externos?	não, há interferências ambientais e de gestão	não, há apenas a pressão pelo tempo de processamento	sim	**1**	**1**
Q10	As portas de emergência com acesso à área operacional são lacradas ou possuem sistema de alarme/monitoramento?	não	Somente lacre	Sim, lacre e sistema de alarme/ monitoramento	**5**	**1**
MÉDIA (NÍVEL DE VULNERABILIDADE):					**2,6**	

Continuação do Anexo E – Exemplo de Avaliação de Risco

ETAPA 7 – Determinação do nível de vulnerabilidade:

Vulnerabilidade		
	alta (5)	não há procedimentos de segurança sendo realizados adequadamente para mitigar o risco
	média-alta (4)	procedimentos de segurança realizados tem um alcance limitado para mitigar o risco, ou áreas importantes não são abrangidos pelo efeito das medidas mitigadoras
	média (3)	características das vulnerabilidades média-alta e média-baixa estão presentes
	média-baixa (2)	procedimentos de segurança estão em vigor, mas são parcialmente efetivos
	Baixa (1)	existem requisitos claros para mitigar o risco e os procedimentos de segurança estão sendo efetivamente realizados de forma adequada

NOTA: O valor encontrado na Etapa 6 deverá ser arredondado para cima durante a determinação do nível de vulnerabilidade, na Etapa 7. No exemplo acima, o valor encontrado foi “2,6”, sendo então arredondado para “3” (média).

ETAPA 8 – Determinação do nível de risco residual:

Nível de Risco Residual		**Severidade x Probabilidade**				
		baixa (5)	média-baixa (10)	média (15)	média-alta (20)	alta (25)
Vulnerabilidade	alta (5)	média-baixo (25)	médio (50)	médio-alto (75)	alto (100)	alto (125)
	média-alta (4)	baixo (20)	médio-baixo (40)	médio (60)	médio-alto (80)	alto (100)
	média (3)	baixo (15)	médio-baixo (30)	médio-baixo (35)	médio (60)	médio-alto (75)
	média-baixa (2)	baixo (10)	baixo (20)	médio-baixo (30)	médio-baixo (40)	médio (50)
	baixa (1)	baixo (5)	baixo (10)	baixo (15)	baixo (20)	médio-baixo (25)

Continuação do Anexo E – Exemplo de Avaliação de Risco

ETAPA 9 – Avaliação do risco:

Para essa etapa, serão consideradas duas hipóteses:

1. Observa-se no exemplo que o **nível de risco residual** para o cenário de ameaça "Introdução de arma, artefato ou material perigoso, com intenções criminais em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo ou nos pertences de mão" é **médio-baixo**, estando então **dentro dos níveis aceitáveis**; ou
2. Caso o **nível de risco residual** para o cenário de ameaça "Introdução de arma, artefato ou material perigoso, com intenções criminais em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo ou nos pertences de mão" fosse classificado como **médio-alto**, estaria **fora dos níveis aceitáveis**. Assim, seria necessário adotar medidas para incrementar as medidas de segurança existentes e reduzir as vulnerabilidades, mitigando assim a ameaça.

ETAPA 10 – Medidas mitigadoras e medidas adicionais de segurança:

Para essa etapa e considerando as hipóteses citadas na Etapa 9, serão consideradas as possíveis conclusões:

1. Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da organização na manutenção de respostas e controles para manter o risco nesse nível ou reduzi-lo a critério do comandante da organização; ou
2. Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado aos comandantes envolvidos e ser tratado em período determinado. Postergação de medidas só com autorização do Comandante do Órgão Regional Executivo. Através da tabela preenchida na Etapa 6, é possível observar, por exemplo, que as questões Q1, Q3, Q4 e Q10 possuem alta relevância no cálculo do nível de vulnerabilidade e ambas receberam avaliação negativa, ou seja, nota 5. Sendo assim, para que o risco residual seja reduzido ao nível aceitável, essas quatro questões precisam ser trabalhadas pela organização.

Q1	É realizada a inspeção de segurança nos visitantes no acesso ao PSNA?	não	sim, sem procedimentos formalizado ou profissional treinado	sim, com procedimento formalizado e profissional treinado	**5**	**1**

A questão Q1 trata da realizada a inspeção de segurança nos visitantes no acesso ao PSNA. Portanto, conclui-se que é necessário o estabelecimento de procedimentos para a inspeção de visitantes, a ser determinado conforme regulamentos e legislações específicos.

Q3	Há equipamentos de segurança para inspeção de visitantes no acesso ao PSNA?	não	sim, através de busca pessoal	sim, com equipamento detector de metais	**5**	**1**

A questão Q3 trata da existência de equipamentos de segurança para inspeção de visitantes no acesso ao PSNA. Portanto, conclui-se que é necessário adquirir equipamentos para a inspeção de visitantes.

Continuação do Anexo E – Exemplos de Avaliação de Risco

Q4	Há equipamentos de segurança para inspeção de bagagens de mão no acesso ao PSNA?	não	sim, apenas com raio-x	sim, com ETD e raio x	**5**	**1**

A questão Q4 trata dos equipamentos de segurança para inspeção de bagagens de mão no acesso ao PSNA. Assim, concluímos que é necessário a aquisição de tais equipamentos.

Q5	As equipes de segurança do PSNA possuem treinamento específico para a realização de inspeção de segurança em visitantes?	não	Sim, porém não regulamentado	Sim, sistemático e regulamentado	**5**	**1**

A questão Q5 trata do treinamentos específico das equipes de segurança do PSNA para a realização de inspeção de segurança em visitantes. Assim, concluímos que é necessário estabelecer tais treinamentos.

Q10	As portas de emergência com acesso à área operacional são lacradas ou possuem sistema de alarme/monitoramento?	não	Somente lacre	Sim, lacre e sistema de alarme/ monitoramento	**5**	**1**

A questão Q10 trata de lacres e sistema de alarme/monitoramento de portas de emergência com acesso à área operacional. Assim, concluímos que é necessário instalar lacres e sistema de alarme/monitoramento de portas de emergência com acesso à área operacional.

Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Durante a Etapa 6, descrita no **Anexo E**, serão utilizadas tabelas de apoio para analisar as medidas de segurança existentes, visando simplificar a avaliação da vulnerabilidade. A seguir serão apresentados exemplos de tabelas de apoio a serem utilizadas nos cenários de ameaça ou em situações, citadas em **4.1**, sendo definidas como **Etapa 1** do processo e abaixo listados:

1. Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo, nos pertences de mão ou em veículo;

2. Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por funcionário, no próprio corpo, nos pertences de mão ou em veículo;

3. Invasão física de organização do SISCEAB visando, através dessa, obter acesso à área restrita de segurança (ARS) de aeródromo;

4. Invasão física de PSNA visando controlar, impedir ou degradar a operacionalidade do SISCEAB;

5. Ataque ou perturbação no exterior do PSNA;

6. Ataque cibernético aos Sistemas ATM visando controlar, impedir ou degradar a operacionalidade do SISCEAB;

7. Utilização de dispositivos (MANPAD, aeronaves não tripuladas ou de raios laser) que impeçam ou degradem a navegação aérea;

8. Segurança dos pontos sensíveis do PSNA; e

9. Instalação de novos sítios do SISCEAB.

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 1: Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por visitante, no próprio corpo, nos pertences de mão ou em veículo.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Há barreiras patrimoniais capazes de dissuadir o acesso indevido ao PSNA e aos pontos sensíveis?	não	sim, porém existem pontos vulneráveis na barreira	sim e não existem pontos vulneráveis na barreira		
Q2	Há portões de acesso que proporcionem o mesmo nível de segurança, quando fechados, que as barreiras perimetrais?	não	sim, mas não todos	sim		
Q3	Os portões de emergência dos Órgãos Operacionais possuem iluminação, monitoramento, permanecem lacrados e são submetidos a rondas frequentes?	não	sim, com infraestrutura parcial ou rondas	sim, com infraestrutura completa e rondas		
Q4	As valas de drenagem, dutos e demais infraestruturas que cruzem as áreas controladas possuem proteção contra acesso indevido e são submetidas a rondas frequentes, com objetivo de identificar violações, pessoas suspeitas e objetos suspeitos abandonados?	não	sim, apenas com bloqueios ou apenas rondas	sim, com bloqueios e rondas		
Q5	A unidade possui equipamento, em condições de pronto emprego, que possa ser utilizado na aplicação de medidas adicionais de segurança visando a dificultar a invasão de veículos? (dilacerador de pneus, ouriço...)	não	sim, mas insuficiente para todos os pontos de acesso ou sem condições de pronto emprego	sim, disponíveis para todos os pontos de acesso e com condições de pronto emprego		
Q6	Há sistema de credenciamento para acesso de visitantes?	não	sim, mas não é distribuído o crachá de visitantes, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá de visitante		
Q7	É realizada a verificação de antecedentes dos visitantes no momento do credenciamento?	não	-	sim		
Q8	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q9	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de visitantes, suas credenciais e autorizações de acesso ao PSNA e aos pontos sensíveis?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q10	Há procedimento de inspeção dos visitantes e seus pertences antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		
Q11	Há procedimento de inspeção de veículos de visitantes antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q12	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos e vias de acesso, pontos sensíveis e demais áreas de risco da Unidade, conforme regulamento específico?	não	sim, mas não existem câmeras em todos os pontos em que o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é a determinada	sim e a instalação das câmeras está de acordo com o nível de risco		
Q13	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos em que o nível de risco determina que sejam instaladas	sim e todos os pontos possuem sensores conforme o nível de risco		
Q14	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregad, conforme regulamento específico?	não existe uma central de vigilância eletrônica	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q15	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q16	O Módulo de Controle de Acesso (MCE), nas situações em que couber, foi implementado e está sendo empregado nos pontos de acesso para visitantes e seus veículos, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos em que o nível de risco determina que sejam instalados, ou a capacidade dos instalados não é a determinada	sim e todos os pontos em que o nível de risco determina que sejam instalados possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q17	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q18	Existem postos de serviço que monitorem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar pessoas suspeitas e objetos suspeitos abandonados?	não	sim, mas não em todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		
Q19	São realizadas rondas em trajetos e horários aleatórios que contemplem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar pessoas suspeitas e objetos suspeitos abandonados?	não	sim, mas não contemplam todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q20	Há procedimento de acionamento de apoio em caso de identificação de pessoa ou objeto suspeito?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q21	O resultado do último teste de falso credenciamento foi satisfatório?	não	-	sim		
Q22	O resultado do último teste de intrusão de instalações foi satisfatório?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 2: Introdução de arma, artefato ou material perigoso, com intenções criminosas em PSNA ou auxílio à navegação aérea por funcionário, no próprio corpo, nos pertences de mão ou em veículo.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Os portões de emergência dos Órgãos Operacionais possuem iluminação, monitoramento, permanecem lacrados e são submetidos a rondas frequentes?	não	sim, com infraestrutura parcial ou rondas	sim, com infraestrutura completa e rondas		
Q2	As valas de drenagem, dutos e demais infraestruturas que cruzem as áreas controladas possuem proteção contra acesso indevido e são submetidas a rondas frequentes, com objetivo de identificar violações, pessoas suspeitas e objetos suspeitos abandonados?	não	sim, apenas com bloqueios ou apenas rondas	sim, com bloqueios e rondas		
Q3	Há sistema de credenciamento para acesso de funcionários (militares ou civis)?	não	sim, mas não é distribuído o crachá, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá		
Q4	É realizada a verificação de antecedentes dos funcionários previamente ao credenciamento?	não	-	sim		
Q5	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q6	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de credenciais e autorizações de acesso ao PSNA e aos pontos sensíveis?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q7	Há procedimento de inspeção aleatória dos funcionários e de seus pertences antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim		
Q8	Há procedimento de inspeção aleatória de veículos de funcionários antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim		
Q9	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos e vias de acesso, pontos sensíveis e demais áreas de risco da Unidade, conforme regulamento específico?	não	sim, mas não existem câmeras em todos os pontos em que o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é a determinada	sim e a instalação das câmeras está de acordo com o nível de risco		
Q10	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos em que o nível de risco determina que sejam instaladas	sim e todos os pontos possuem sensores conforme o nível de risco		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q11	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregado, conforme regulamento específico?	não	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q12	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q13	O Módulo de Controle de Acesso (MCE), nas situações em que couber, foi implementado e está sendo empregado nos pontos de acesso para funcionários e seus veículos, conforme MCA 205-2?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos em que o nível de risco determina que sejam instalados, ou a capacidade dos instalados não é a determinada	sim e todos os pontos em que o nível de risco determina que sejam instalados possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q14	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q15	Existem postos de serviço que monitorem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar funcionários em atitudes suspeitas e objetos suspeitos abandonados?	não	sim, mas não em todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		
Q16	São realizadas rondas em trajetos e horários aleatórios que contemplem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar funcionários em atitudes suspeitas e objetos suspeitos abandonados?	não	sim, mas não contemplam todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		
Q17	Há procedimento de acionamento de apoio em caso de identificação de funcionários em atitudes suspeitas ou objetos suspeitos?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q18	Existe um canal de comunicações confidencial para a denúncia de funcionários que apresentem comportamento suspeito?	não	existe, mas este canal não é divulgado, ou é divulgado e	existe e a maior parte do efetivo tem conhecimento de		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

			poucas pessoas tem conhecimento de sua existência	sua existência		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 3: Invasão física de organização do SISCEAB visando, através dessa, obter acesso à área restrita de segurança (ARS) de aeródromo.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Há barreiras patrimoniais capazes de dissuadir o acesso indevido ao PSNA?	não	sim, porém existem pontos vulneráveis na barreira	sim e não existem pontos vulneráveis na barreira		
Q2	O limite entre o PSNA e à ARS é protegido por barreiras patrimoniais?	não	sim, porém existem pontos vulneráveis na barreira, ou ela não contempla toda a extensão do limite entre o PSNA e a ARS	sim e não existem pontos vulneráveis na barreira		
Q3	Há portões de acesso no PSNA e nos limites entre este e à ARS, que quando fechados, proporcionem o mesmo nível de segurança que as barreiras perimetrais?	não	sim, mas não todos	sim, todos		
Q4	Os pontos de acesso à ARS fora de uso permanecem lacrados?	não	sim, mas não são verificados regularmente, ou nem todos são lacrados	sim, todos são lacrados e verificados regularmente		
Q5	As valas de drenagem, dutos e demais infraestruturas que cruzem as áreas controladas possuem proteção contra acesso indevido e são submetidas a rondas frequentes, com objetivo de identificar violações, pessoas suspeitas e objetos suspeitos abandonados?	não	sim, apenas com bloqueios ou apenas rondas	sim, com bloqueios e rondas		
Q6	A unidade possui equipamento, em condições de pronto emprego, que possa ser utilizado na aplicação de medidas adicionais de segurança visando a dificultar a invasão de veículos? (dilacerador de pneus, ouriço...)	não	sim, mas insuficiente para todos os pontos de acesso ou sem condições de pronto emprego	sim, disponíveis para todos os pontos de acesso e com condições de pronto emprego		
Q7	Há sistema de credenciamento para acesso de visitantes?	não	sim, mas não é distribuído o crachá de visitantes, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá de visitante		
Q8	É realizada a verificação de antecedentes dos visitantes previamente ao credenciamento?	não	-	sim		
Q9	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q10	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de credenciais e autorizações de acesso ao PSNA e a ARS?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q11	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos de acesso à ARS, conforme regulamento específico?	não	sim, mas não existem câmeras em todos os pontos de acesso à ARS nos quais o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é a determinada	sim e a instalação das câmeras está de acordo com o nível de risco		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q12	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos da barreira que divide o PSNA e a ARS nos quais o nível de risco determina que sejam instalados	sim e foram instalados em todos os pontos da barreira que divide o PSNA e a ARS nos quais o nível de risco determina		
Q13	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregado, conforme regulamento específico?	não	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q14	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q15	O Módulo de Controle de Acesso (MCE), nas situações em que couber, conforme MCA 205-2, foi implementado e está sendo empregado, nos pontos de acesso à ARS do aeródromo?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos de acesso à ARS do aerodromo, ou a capacidade dos instalados não é a determinada	sim e todos os pontos de acesso à ARS do aerodromo possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q16	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme MCA 205-2?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q17	O Sistema de Segurança Eletrônica contempla os pontos de acesso à ARS?	não	sim, mas não todos	sim		
Q18	Há procedimento de acionamento de apoio em caso de tentativa de invasão à ARS?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q19	O resultado do último teste de falso credenciamento foi satisfatório?	não	-	sim		
Q20	O resultado do último teste de intrusão de instalações foi satisfatório?	não	-	sim		
Q21	São realizadas rondas em trajetos e horários aleatórios que contemplem os pontos de acesso entre o PSNA e o aeródromo, com objetivo de identificar pessoas suspeitas?	não	sim, mas não contemplam todos os pontos, ou não existe previsão desta atividade na norma interna do PSNA	sim e existe a previsão desta atividade na norma interna do PSNA		
Q22	O Agente Local AVSEC têm participação regular na CSA?	não	-	sim		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q23	Há procedimento de comunicação ao Administrador Aeroportuário Local em caso de invasão?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 4: Invasão física de PSNA visando controlar, impedir ou degradar a operacionalidade do SISCEAB.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Há barreiras de segurança capazes de dissuadir o acesso indevido ao PSNA e aos pontos sensíveis?	não	sim, porém existem pontos vulneráveis na barreira	sim e não existem pontos vulneráveis na barreira		
Q2	Há portões de acesso que quando fechados, proporcionem mesmo nível de segurança que as barreiras patrimoniais?	não	sim, mas não todos	sim, todos		
Q3	Os portões de emergência dos Órgãos Operacionais possuem iluminação, monitoramento, permanecem lacrados e são submetidos a rondas frequentes?	não	sim, com infraestrutura parcial ou rondas	sim, com infraestrutura completa e rondas		
Q4	As valas de drenagem, dutos e demais infraestruturas que cruzem as áreas controladas possuem proteção contra acesso indevido e são submetidas a rondas frequentes, com objetivo de identificar violações, pessoas suspeitas e objetos suspeitos abandonados?	não	sim, apenas com bloqueios ou apenas rondas	sim, com bloqueios e rondas		
Q5	A unidade possui equipamento, em condições de pronto emprego, que possa ser utilizado na aplicação de medidas adicionais de segurança visando a dificultar a invasão de veículos? (dilacerador de pneus, ouriço...)	não	sim, mas insuficiente para todos os pontos de acesso ou sem condições de pronto emprego	sim, disponíveis para todos os pontos de acesso e com condições de pronto emprego		
Q6	Há sistema de credenciamento para acesso de visitantes?	não	sim, mas não é distribuído o crachá de visitantes, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá de visitante		
Q7	É realizada a verificação de antecedentes dos visitantes previamente ao credenciamento?	não	-	sim		
Q8	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q9	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de credenciais e autorizações de acesso ao PSNA e aos pontos sensíveis?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q10	Há procedimento de inspeção dos visitantes e seus pertences antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		
Q11	Há procedimento de inspeção de veículos antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q12	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos e vias de acesso, ponstos sensíveis e demais áreas de risco da Unidade, conforme regulemento específico?	não	sim, mas não existem câmeras em todos os pontos em que o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é a determinada	sim e a instalação das câmeras está de acordo com o nível de risco		
Q13	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos em que o nível de risco determina que sejam instaladas	sim e todos os pontos possuem sensores conforme o nível de risco		
Q14	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregado, conforme regulamento específico?	não	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q15	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q16	O Módulo de Controle de Acesso (MCE), nas situações em que couber, foi implementado e está sendo empregado nos pontos de acesso para pessoas e veículos, pontos sensíveis e demais áreas de risco da Unidade, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos em que o nível de risco determina que sejam instalados, ou a capacidade dos instalados não é a determinada	sim e todos os pontos em que o nível de risco determina que sejam instalados possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q17	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q18	Existem postos de serviço que monitorem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar pessoas suspeitas e objetos suspeitos abandonados?	não	sim, mas não em todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		
Q19	São realizadas rondas em trajetos e horários aleatórios que contemplem os pontos sensíveis e vulneráveis do PSNA, com objetivo de identificar pessoas suspeitas e objetos suspeitos abandonados?	não	sim, mas não contemplam todos os pontos, ou não possuem instrução sobre a identificação desse tipo de objeto e das ações a se adotar, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q20	Há procedimento de acionamento de apoio em caso de invasão ou identificação de pessoa suspeita ou objeto suspeito?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q21	O resultado do último teste de falso credenciamento foi satisfatório?	não	-	sim		
Q22	O resultado do último teste de intrusão de instalações foi satisfatório?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 5: Ataque ou perturbação no exterior do PSNA.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Há barreiras de segurança capazes de dissuadir o acesso indevido ao PSNA e aos pontos sensíveis?	não	sim, porém existem pontos vulneráveis na barreira	sim e não existem pontos vulneráveis na barreira		
Q2	Há portões de acesso que quando fechados, proporcionem mesmo nível de segurança que as barreiras patrimoniais	não	sim, mas não todos	sim, todos		
Q3	A unidade possui equipamento, em condições de pronto emprego, que possa ser utilizado na aplicação de medidas adicionais de segurança visando a dificultar a invasão de veículos? (dilacerador de pneus, ouriço...)	não	sim, mas insuficiente para todos os pontos de acesso ou sem condições de pronto emprego	sim, disponíveis para todos os pontos de acesso e com condições de pronto emprego		
Q4	Há sistema de credenciamento para acesso de visitantes?	não	sim, mas não é distribuído o crachá de visitantes, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá de visitante		
Q5	É realizada a verificação de antecedentes dos visitantes previamente ao credenciamento?	não	-	sim		
Q6	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q7	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de credenciais e autorizações de acesso ao PSNA e aos pontos sensíveis?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q8	Existe procedimento, previsto nas normas internas do PSNA, para reforçar o efetivo de segurança dos pontos de acesso em caso de perturbação no exterior do PSNA?	não	sim, mas o procedimento não é de conhecimento do efetivo	sim		
Q9	Há procedimento de inspeção dos visitantes e seus pertences antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		
Q10	Há procedimento de inspeção de veículos antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		
Q11	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos e vias de acesso, no perímetro da Unidade e demais áreas de risco da Unidade, conforme conforme regulamento específico?	não	sim, mas não existem câmeras em todos os pontos em que o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é	sim e a instalação das câmeras está de acordo com o nível de risco		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

			a determinada			
Q12	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos em que o nível de risco determina que sejam instaladas	sim e todos os pontos possuem sensores conforme o nível de risco		
Q13	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregado, conforme regulamento específico?	não	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q14	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q15	O Módulo de Controle de Acesso (MCE), nas situações em que couber, foi implementado e está sendo empregado nos pontos de acesso para pessoas e veículos, pontos sensíveis ou qualquer outra área do perímetro onde haja fluxo de pessoas, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos em que o nível de risco determina que sejam instalados, ou a capacidade dos instalados não é a determinada	sim e todos os pontos em que o nível de risco determina que sejam instalados possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q16	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q17	Há procedimento de acionamento de apoio em caso de ataque ou perturbação no perímetro externo do PSNA?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q18	Há monitoramento, via sentinela ou vigilância eletrônica, no perímetro do PSNA?	não	sim, mas não em todo o perímetro	sim, em todo o perímetro		
Q19	Existe um canal de comunicações confidencial para a denúncia de situações suspeitas?	não	existe, mas este canal não é divulgado, ou é divulgado e poucas pessoas tem conhecimento de sua existência	existe e a maior parte do efetivo tem conhecimento de sua existência		
Q20	O Órgão de Segurança Pública responsável pelo policiamento da região do PSNA realiza rondas periódicas no perímetro do PSNA?	não	sim, mas não existe coordenação para a realização de tal ronda, ou existe coordenação e as rondas são escassas	sim, existe coordenação e as rondas são realizadas rotineiramente		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q21	O resultado do último teste de intrusão de instalações foi satisfatório?	não	-	sim		
Q22	O resultado do último teste de falso credenciamento foi satisfatório?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 6: Ataque cibernético aos Sistemas ATM visando controlar, impedir ou degradar a operacionalidade do SISCEAB

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Existe controle de inventário de dispositivos objetivando identificar os equipamentos que pertencem a unidade e os que são de terceiros?	não	Sim, porém o controle não é automático e o processo não está definido	sim		
Q2	Existe um local para armazenamento e publicação dos documentos normativos de segurança da Informação?	não	Sim, porém não é de conhecimento do usuário	sim		
Q3	Existem controles de segurança para acesso à rede interna e sistemas de TI ?	não	Sim, porém o controle de acesso não existe granularidade para o perfl de usuário	sim		
Q4	Os usuários da rede são validados periodicamente de forma a verificar se existem usuários ativos que não fazem mais parte da OM ?	não	sim, mas não todos	sim		
Q5	Existe controle para os usuários de rede objetivando verificar se os perfis de acesso estão de acordo com as atuais funções dos usuários?	não	sim, mas o processo não está definido	sim		
Q6	Existem controles de segurança para segregação de perfis de usuários objetivando mapear as funções dos usuários?	não	sim, mas o processo não está definido	sim		
Q7	Existem controles de segurança para verificar se os perfis de acesso estão vigentes?	não	sim, mas o processo não está definido	sim		
Q8	Os arquivos de cópia de segurança da informação contendo informações confidenciais são armazenados em local específico?	não	sim, mas não atende as normas de segurança para guarda de informações	sim		
Q9	Há procedimento específico estabelecido para controle de senhas e proteção adequada (criptografia, cofre, dupla custódia e etc.)?	não	sim, mas o processo não está definido	sim		
Q10	Existe monitoramento dos ativos de segurança?	não	sim, mas não cobre todos os ativos	sim		
Q11	Existe monitoramento dos logs de segurança?	não	sim, mas não cobre todos os ativos	sim		
Q12	Existe armazenamento adequado de acordo com as normas vigentes para a retenção de logs?	até 50% de resultados positivos	sim, mas não cobre todos os ativos	sim		
Q13	O acesso aos arquivos de cópia de segurança da informação classificadas como confidenciais ou reservadas são controladas, registradas e formalmente autorizado pelo comandante ou similar da organização?	não	sim, sem procedimento formalizado	sim		
Q14	Os serviços de rede da INTRAER e da Internet, disponibilizados pelas Organizações, são utilizados somente para apoio às atividades de interesse do SISCEAB?	não	sim, mas sem procedimento formalizado	sim		
Q15	A utilização de computadores portáteis é precedida de medidas que visem à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados, respeitando normativas gerenciais e técnicas existentes no SISCEAB?	não	sim, com adoção de medidas mitigadoras	sim		
Q16	Os processos de desenvolvimento e manutenção de sistemas aplicativos são acompanhados pelo setor da Organização envolvida, responsável pela segurança das informações, o qual realizará os testes necessários para detectar vulnerabilidades nos sistemas?	não	sim, sem procedimento formalizado	sim		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q17	Os sistemas de TI considerados críticos estão protegidos por um Plano de Continuidade de Negócios?	não	sim, sem procedimento formalizado	sim		
Q18	Os recursos computacionais utilizados pelos usuários possuem um software antivírus homologado e atualizado?	não	sim, mas não existe uma gerência e o processo é manual	sim		
Q19	A Equipe de TI local mantém um controle rígido sobre os usuários e os equipamentos que estão conectados às suas respectivas Redes de Comunicação de Dados Locais, de forma a impedir qualquer conexão de recursos computacionais não autorizados àquelas rede?	não	sim, mas não existe processo e regras bem definidas	sim		
Q20	A Equipe de TI local mantém um controle rígido sobre a forma de utilização da Rede acesso à Internet, de forma a impedir qualquer conexão não autorizada àquelas redes?	não	sim, mas não existe processo e regras bem definidas	sim		
Q21	A Equipe de TI local mantém cópias de segurança dos sistemas da Organização?	não	sim, mas o processo não está definido	sim		
Q22	As cópias de segurança são guardadas em local seguro com controle de acesso específico?	não	sim, mas o processo não está definido	sim		
Q23	Existem ferramentas para controle de acesso a rede e internet?	não	sim, mas o processo não está definido	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 7: Utilização de dispositivos (MANPAD, aeronaves não tripuladas ou de raios laser) que impeçam ou degradem a navegação aérea.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	O efetivo do órgão ATS é orientado a recolher as informações sobre reportes de MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não antes de cada serviço	sim, diariamente no briefing do serviço		
Q2	Foi estabelecida coordenação do órgão ATS com os órgãos de segurança pública para a comunicação e o acionamento em caso de detecção ou reporte de MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequencia		
Q3	Em caso de reporte, o ATCO é orientado sobre como levantar as informações necessárias de modo a obter uma posição estimada do MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequência		
Q4	Existe procedimento padronizado pelo órgão ATS para elevação no nível de alerta, conforme MCA 205-2, em caso de avistamento ou reporte de MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequência		
Q5	Existe procedimento para interrupção das operações caso o MANPAD, aeronaves não tripuladas ou de raios laser deteriore consideravelmente a segurança da aviação civil?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequência		
Q6	Existe procedimento de comunicação para as entidades aeroportuárias envolvidas, em caso de detecção de MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequencia		
Q7	O Órgão ATS possui equipamentos para confirmar a existência de aeronaves não tripuladas, em caso de suspeita?	não	existe, mas não são adequados	sim e são adequados		
Q8	Existe procedimento padronizado de comunicação com o APP, ACC e ao CGNA para informar a ocorrência de MANPAD, aeronaves não tripuladas ou de raios laser?	não	sim, mas não é treinado	sim, o procedimento é treinado com frequencia		
Q9	Existe procedimento padronizado para inserção de ameaça reportada e confirmada de MANPAD, aeronaves não tripuladas ou de raios laser na informação ATIS ou NOTAM?	não	-	sim		
Q10	Existe previsão, nos documentos do órgão, dos níveis de alerta MANPAD, aeronaves não tripuladas ou de raios laser?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 8: Segurança dos pontos sensíveis do PSNA.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Há barreiras de segurança capazes de dissuadir o acesso indevido aos pontos sensíveis do PSNA?	não	sim, porém existem pontos vulneráveis na barreira	sim e não existem pontos vulneráveis na barreira		
Q2	Há portões/portas de acesso aos pontos sensíveis que quando fechados, proporcionem o mesmo nível de segurança, que as barreiras perimetrais?	não	sim, mas não todos	sim, todos		
Q3	Os portões de emergência dos Órgãos Operacionais possuem iluminação, monitoramento, permanecem lacrados e são submetidos a rondas frequentes?	não	sim, com infraestrutura parcial ou rondas	sim, com infraestrutura completa e rondas		
Q4	As valas de drenagem, dutos e demais infraestruturas que cruzem as áreas controladas possuem proteção contra acesso indevido e são submetidas a rondas frequentes, com objetivo de identificar violações, pessoas suspeitas e objetos suspeitos abandonados?	não	sim, apenas com bloqueios ou apenas rondas	sim, com bloqueios e rondas		
Q5	A unidade possui equipamento, em condições de pronto emprego, que possa ser utilizado na aplicação de medidas adicionais de segurança visando a dificultar a invasão de veículos? (dilacerador de pneus, ouriço...)	não	sim, mas insuficiente para todos os pontos de acesso ou sem condições de pronto emprego	sim, disponíveis para todos os pontos de acesso e com condições de pronto emprego		
Q6	Há sistema de credenciamento para acesso de visitantes?	não	sim, mas não é distribuído o crachá de visitantes, ou é parcialmente distribuído, ou nem todos são credenciados	sim, todos são credenciados e recebem o crachá de visitante		
Q7	É realizada a verificação de antecedentes dos visitantes previamente ao credenciamento?	não	-	sim		
Q8	Há controle das credenciais emitidas, devolvidas e extraviadas?	não	-	sim		
Q9	Existem recursos humanos, sistemas automatizados de controle de acesso e procedimentos suficientes para realizar identificação de credenciais e autorizações de acesso aos pontos sensíveis?	não	sim, mas o funcionamento não está adequado, ou o equipamento está apresentando defeitos, ou não são suficientes em todos os pontos de acesso	sim		
Q10	Existe equipamento, procedimento ou efetivo realizando controle de acesso específico para cada ponto sensível?	não	sim, mas o equipamento não é adequado ou não está funcionando bem, ou procedimento não foi formalizado ou não é de conhecimento do efetivo, ou o efetivo não possui treinamento para realizar controle de acesso	sim		
Q11	Há procedimento de inspeção dos visitantes e seus pertences antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

			realizar a inspeção			
Q12	Há procedimento de inspeção de veículos antes de acessar o PSNA e/ou pontos sensíveis?	não	sim, mas o equipamento não é adequado, ou não está funcionando bem, ou o efetivo não possui treinamento para realizar a inspeção	sim e o equipamento está funcional e o efetivo está treinado para realizar as inspeções		
Q13	O Módulo de Vigilância Eletrônica (MVE), foi implementado e está sendo empregado nos pontos sensíveis, conforme regulamento específico?	não	sim, mas não existem câmeras em todos os pontos em que o nível de risco determina que sejam instaladas, ou a capacidade das câmeras não é a determinada	sim e a instalação das câmeras está de acordo com o nível de risco		
Q14	O Módulo de Detecção de Intrusão (MDI), foi implementado e está sendo empregado vinculado ao MVE, conforme regulamento específico?	não	sim, mas não existem sensores em todos os pontos em que o nível de risco determina que sejam instaladas	sim e todos os pontos possuem sensores conforme o nível de risco		
Q15	O Módulo Central de Vigilância Eletrônica (MCVE), foi implementado e está sendo empregado, conforme regulamento específico?	não	sim, mas não está em boas condições, ou não possui capacidade de comunicação com o Módulo de Reação	sim, está em boas condições e possui capacidade de comunicação com o Módulo de Reação		
Q16	O Módulo Reação (MRE), foi implementado e está sendo empregado com mobilidade para chegar nos pontos sensíveis e capacidade de resposta, conforme regulamento específico?	não	sim, mas o efetivo está mal equipado, mal treinado, ou não possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações	sim, o efetivo está bem equipado, bem treinado e possui boa capacidade de comunicação com o MCVE e com a equipe de serviço de segurança das instalações		
Q17	O Módulo de Controle de Acesso (MCE), nas situações em que couber, foi implementado e está sendo empregado nos pontos sensíveis, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas não existem controle de acesso eletrônico em todos os pontos em que o nível de risco determina que sejam instalados, ou a capacidade dos instalados não é a determinada	sim e todos os pontos em que o nível de risco determina que sejam instalados possuem controles de acesso eletrônico com as capacidades determinadas, ou não se aplica		
Q18	O Módulo de Tecnologia da Informação (MTI), nas situações em que couber, foi implementado e está sendo empregado, conforme regulamento específico?	se aplica, porém não está sendo empregado	sim, mas a integração entre os sistemas é parcial	sim e a integração entre os sistemas é plena, ou não se aplica		
Q19	Todos os pontos sensíveis do PSNA são monitorados por postos de serviço ou câmeras?	não	sim, mas não todos	sim		
Q20	São realizadas rondas em trajetos e horários aleatórios que contemplem os pontos sensíveis e vulneráveis do PSNA?	não	sim, mas não contemplam todos os pontos, ou não existe previsão desta atividade na norma interna do PSNA	sim e possuem instrução para tal atividade que está prevista na norma interna do PSNA		

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Q21	Há procedimento de acionamento de apoio em caso de ameaça a ponto sensível do PSNA?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q22	O resultado do último teste de falso credenciamento foi satisfatório?	não	-	sim		
Q23	O resultado do último teste de intrusão de instalações foi satisfatório?	não	-	sim		
MÉDIA (NÍVEL DE VULNERABILIDADE):						

Continuação do Apêndice – Exemplos de Tabelas para Análise das Medidas de Segurança

Tabela 9: Instalação de novos sítios do SISCEAB.

Medidas de segurança existentes		5 pontos	de 1 a 4 pontos	0 pontos	pontos	peso
Q1	Foi realizada avaliação de risco prévia à escolha do local de instalação do novo sítio?	não	-	sim		
Q2	Há barreira natural ou artificial que delimite a área patrimonial do novo sítio?	não	sim, mas não em todo o perímetro, ou existem pontos vulneráveis	sim, em todo o perímetro		
Q3	Existe controle de acesso, para veículos e pessoas, à área patrimonial do novo sítio?	não	sim, mas não foram emitidas credenciais, ou não existe uma relação atualizada de quem está autorizado a entrar	sim e existe um sistema de emissão de credenciais estabelecido		
Q4	Há sistema de vigilância eletrônica no novo sítio?	não	sim, mas não contempla todo o perímetro ou pontos sensíveis em construção	sim e contempla todo o perímetro e pontos sensíveis em construção		
Q5	Há equipe de segurança disponível 24h para proteger o novo sítio?	não	sim, mas o efetivo não é suficiente	sim e o efetivo é suficiente		
Q6	Há apoio de unidade militar ou órgão de segurança pública nas proximidades do novo sítio?	não	-	sim		
Q7	Existe procedimento de acionamento de apoio em caso de ameaça ao novo sítio?	não	sim, mas a comunicação com a equipe que prestará o apoio não é boa, ou o apoio será prestado por Órgão de Segurança Pública e não existe uma coordenação prévia com este	sim, o procedimento está estabelecido, as comunicações são boas e as coordenações de apoio já foram realizadas		
Q7	O efetivo que está trabalhando na construção do novo sítio foi orientado quanto aos procedimentos que deve adotar quanto à segurança?	não	sim, mas parcialmente	não		
MÉDIA (NÍVEL DE VULNERABILIDADE):						