

Segurança da Informação na Navegação Aérea: estudo de caso de uma sala de informações aeronáutica

Resumo: O transporte Aéreo é essencial em um mercado competitivo e em constante evolução, além de ser considerado estratégico para o desenvolvimento do país. Nos últimos anos, um aumento expressivo das atividades aéreas foi registrado, por isso, deve-se pensar em como manter os níveis de segurança na navegação aérea. Dados do CENIPA – Centro de Investigação e Prevenção de Acidentes Aeronáuticos indicam que o planejamento do voo é fator contribuinte em 47,7% dos acidentes aeronáuticos. A sala de informações aeronáuticas (AIS) é o órgão responsável pela disponibilização das informações associadas a navegação aérea e indispensáveis para o planejamento do voo. Desta forma, os três princípios básicos da informação: confidencialidade, integridade e disponibilidade devem ser garantidos neste órgão. O objetivo deste trabalho foi identificar as vulnerabilidades existentes na segurança da informação em uma sala AIS e propor recomendações para melhoria. O uso de diagramas de causa e efeito permitiu associar as vulnerabilidades detectadas, através de observação direta, pesquisa documental e questionário semi-estruturado, aos princípios da informação violados. A ferramenta 5W2H foi utilizada para propor medidas de segurança com o objetivo de minimizar o risco de ameaças aos ativos da informação.

Palavras-chave: Segurança da Informação; Sala de informações aeronáuticas; Transporte Aéreo.

1. Introdução

O transporte aéreo constitui-se em um dos meios de locomoção mais importantes de um mercado competitivo, dinâmico e em constante evolução. Segundo dados da IATA (Associação Internacional de Transporte Aéreo), o setor aéreo registrou em 2010, um lucro de cerca de US\$ 16 bilhões. Ainda conforme a entidade, a previsão para 2014 é que aproximadamente, 3,3 bilhões de pessoas viajarão de avião. No Brasil, este crescimento também é perceptível. A INFRAERO, empresa que administra 66 aeroportos do país, registrou um aumento de mais de 100% no número de passageiros entre 2003 e 2010.

Nos últimos dez anos, de acordo com dados do CENIPA (2010), foram registrados mais de setecentos acidentes e novecentas mortes, sendo o planejamento fator contribuinte em 47,7% das ocorrências. É necessário, portanto, preocupar-se com a segurança dos vãos, principalmente no início de seu planejamento que começa dentro de uma sala de informações aeronáuticas (AIS), pois um dado incorreto transmitido a um piloto ou o desrespeito ao plano de voo elaborado pode provocar graves acidentes como a colisão em voo de duas aeronaves ocorrido, no Brasil, em 2006.

Este trabalho efetuou um estudo para a redução da vulnerabilidade da segurança da informação na navegação aérea, identificando e analisando as variáveis que afetam os princípios básicos da segurança da informação, que são: a confidencialidade, a integridade e a

disponibilidade, partindo da análise operacional de uma sala de informações aeronáuticas e possibilitando a proposta de melhorias.

2. Referencial Teórico

2.1 Segurança da informação

Para abordar este tema procura-se, anteriormente, estabelecer uma relação entre dados, informação e ativo. Dados são simples observações sobre um estado, facilmente armazenados e obtidos de máquinas, enquanto que informação é um dado acrescido de contexto, relevância e propósito (SIQUEIRA, 2005). Sêmola (2003) define ativo como todo elemento que compõe os sistemas que manipulam e processam a informação, a contar a própria informação em todo seu ciclo de vida, que inclui o armazenamento, manuseio, transporte e descarte. Dessa forma, o autor determina que segurança da informação é uma área do conhecimento que visa à proteção de ativos da informação.

Sobre o assunto, Campos (2007) sugere um sistema de segurança da informação baseado em três princípios básicos: a confidencialidade, que visa garantir que a informação seja acessada apenas por pessoas autorizadas; a integridade, que assegura que a informação esteja completa e a disponibilidade, a qual permite acessibilidade à informação por pessoas autorizadas, sempre que necessário.

Para que os princípios anteriormente citados sejam respeitados, é necessário agir no sentido de descobrir quais são os pontos vulneráveis e a partir daí, avaliar os riscos e impactos.

2.2 Vulnerabilidades e Ameaças

Vulnerabilidades são as fragilidades nos ativos da informação que poderiam ser explorados, intencionalmente ou não, resultando na quebra de um ou mais princípios de segurança da informação (CAMPOS 2007). Segundo Sêmola (2003), as vulnerabilidades podem ser distribuídas conforme a seguir:

Vulnerabilidades	Exemplos
Físicas	Instalações fora do padrão, falta de recursos de combate a incêndio e falta de barreiras físicas para a segurança patrimonial.
Naturais	Incêndios, enchentes, terremotos, tempestades, falta de energia, acúmulo de poeira, aumento de umidade e de temperatura.
Hardware	Falha nos recursos tecnológicos (desgaste, obsolescência e má utilização) ou erros durante instalação.
Mídias	Perdas e danos à CDs, fitas, pen drives, relatórios e impressos.
Comunicação	Interferência ou perda de comunicação.
Humanas	Falta de treinamento, compartilhamento de informações confidenciais, não execução das rotinas de segurança, erros ou omissões.
Software	Erros na instalação ou na configuração de programas operacionais.

Quadro 1- Classificação das vulnerabilidades. Fonte: Adaptado de Sêmola (2003).

As vulnerabilidades são potencialmente exploradas por ameaças que, quando bem sucedidas, interrompem o fluxo de informações e põe em risco todos os envolvidos. De acordo com Campos (2007), ameaça é um agente externo ao ativo da informação, que se aproveitando de suas vulnerabilidades, poderá quebrar a confidencialidade, integridade ou a disponibilidade da informação.

Diante das vulnerabilidades e conseqüentes ameaças de um sistema de informação, medidas de seguranças devem ser adotadas a fim de evitar ou minimizar os impactos causados. Para Sêmola (2003) é importante criar barreiras a fim de desencorajar, dificultar, discriminar, detectar, deter e/ou diagnosticar os riscos existentes nos sistemas de informação.

Após identificar as vulnerabilidades, é necessário iniciar uma análise das causas potenciais das mesmas. Para isso, neste trabalho, foi utilizada a ferramenta da qualidade conhecida como diagrama de causa e efeito ou diagrama de Ishikawa. Para Slack, Chambers e Johnston (2002) os procedimentos para se desenhar este diagrama são: colocar o problema na caixa de “efeito”, identificar e registrar as principais categorias para causas possíveis do problema e discutir em grupos cada item.

Encontradas as causas e seus efeitos, um plano de ação 5W2H foi executado. Aguiar (2002) afirma que esta ferramenta é eficiente no auxílio, na análise e no conhecimento de um determinado problema. O termo pode ser definido como: Why (por quê?), motivo pelo qual será realizada a tarefa; What (o quê?), o que deve ser feito; Who (quem?), identifica a pessoa que será responsável; When (quando?), prazo para a realização das tarefas; Where (onde?), indica o local no qual a tarefa será realizada; How (como?); define os métodos que serão utilizados em cada etapa e How much (quanto custa?), quanto será investido.

2.3 Segurança da Informação e a Navegação Aérea

Realizar o controle de tráfego aéreo, assim como prestar o serviço de informações aeronáuticas, não são tarefas simples em um país de dimensões continentais. De acordo com o CENIPA (2010), nos últimos dez anos, a aviação civil totalizou 757 acidentes, com perda de 312 aeronaves e de 984 vidas em 245 acidentes com fatalidades. E a incidência dos fatores contribuintes, pode ser visualizada no gráfico a seguir:

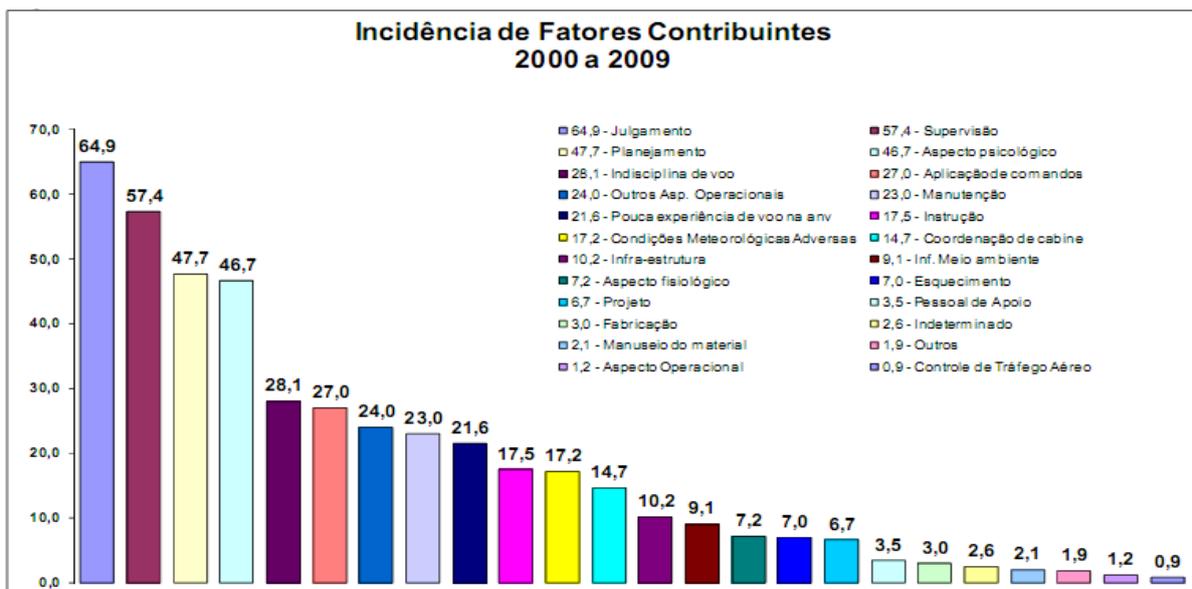


FIGURA 1- Incidência de Fatores Contribuintes Fonte: CENIPA (2010).

Conforme os dados acima, observa-se que planejamento é responsável por 47,7% da incidência de fatores contribuintes para ocorrências de acidentes aéreos. Este fato, de acordo com o CENIPA (MCA 3-6, 2008), está relacionado, principalmente, com a inadequação nos trabalhos de preparação para o voo. Por isso, para auxiliar a navegação aérea, existe um órgão do SISCEAB (Sistema de Controle do Espaço Aéreo), denominado sala de informações aeronáuticas ou sala AIS (Aeronautical Information Service), que tem “o objetivo de prestar o serviço de informação prévia ao voo e receber os planos de voo que se apresentam antes da saída das aeronaves, bem como os informes referentes ao serviço de tráfego aéreo” (DECEA, ICA 53-2, 2009, p.12).

A disposição da informação dentro de uma sala AIS deve estar de acordo com as normas do DECEA (ICA 53-2, 2009) que dentre outras determinações estabelece: O material informativo será disposto em uma ordem lógica, de maneira a facilitar a auto-informação, de modo que o usuário tenha de se locomover o mínimo possível; As informações operacionais deverão ser expostas em painéis, exemplo: as horas do nascer e do pôr-do-sol no aeródromo, condições meteorológicas, frequências de rádio de comunicação disponíveis e outras informações que se façam necessárias; Quanto aos sistemas automatizados, são obrigatórios o SAIS, para preenchimento do plano e o SISNOTAM para consulta de NOTAM (Notice to airmen, informação aeronáutica de interesse direto e imediato para a segurança e regularidade da navegação aérea).

É importante ressaltar que a sala AIS é o principal suporte ao serviço de controle de tráfego aéreo, pois recebe da mesma todos os dados dos voos que trafegam sob sua responsabilidade.

3. Estudo de caso

3.1 Descrição da organização

A organização estudada é uma sala de informações aeronáuticas, localizada em um aeroporto da cidade de Belo Horizonte que atende aos voos não-regulares de empresas de táxi aéreo, de aviação geral e de escolas de aviação, além de dispor de empresas de manutenção, hangaragem e construção de ultraleves. Suas operações estão restritas entre os horários do nascer ao pôr-do-sol. Conforme dados divulgados pela INFRAERO, no ano de 2010, o órgão apresentou um movimento operacional superior a 25 mil pousos e decolagens.

O órgão em estudo possui dois tipos de profissionais: Operador de Estação Aeronáutica (OEA) e Operador AIS. Suas funções, assim como a rotina de trabalho do órgão, foram analisadas com o objetivo de detectar possíveis vulnerabilidades aplicadas ao sistema de informação. O responsável pelo órgão tratado neste estudo de caso é o coordenador de navegação aérea, que tem a formação de OEA e é assistido pelo supervisor AIS. Ambos têm a função de manter o funcionamento da sala AIS dentro das normas estabelecidas pelo DECEA.

3.2 Vulnerabilidades e Ameaças

A sala AIS estudada apresentou vulnerabilidades que afetam a segurança da informação. Quanto à estrutura física, constatou-se que o acesso ao órgão é irrestrito, há procedimentos para identificação de estranhos, assim como o uso de detector de metais apenas no setor de embarque.

A área da sala AIS (27m²), não atende o mínimo requerido pelo o DECEA (ICA 53-2, 2009), e não permite a auto-informação por parte do piloto devido dificuldades para disposição das publicações técnicas, sendo necessário o envolvimento do operador AIS para consultar as cartas de rota. A localização da estação de telecomunicações também

compromete a área da sala AIS, além de gerar bastante ruído no ambiente, o que interfere na comunicação oral entre os usuários, afetando diretamente a integridade da informação.

Outro problema é a falta de treinamento para os funcionários atuarem em caso da ameaça natural de um incêndio, apesar da disponibilidade de extintores. Esse fato põe em risco a integridade e a disponibilidade de equipamentos, sistemas e impressos que podem ser danificados pela fumaça e pelo fogo.

Os principais softwares utilizados na sala AIS, no auxílio ao planejamento de um voo, foram analisados e as vulnerabilidades e ameaças identificadas. Logo abaixo, estão as descrições de cada programa examinado:

O SAIS (Sistema Automatizado de Sala AIS) surgiu pela necessidade de adaptar-se à velocidade exigida para que o processo de gerenciamento de tráfego aéreo não fosse prejudicado no seu início, além de substituir os formulários manuais para preenchimento de plano de voo (DECEA, SAIS: Guia do usuário, 2007). Para utilizar o sistema é necessário digitar uma senha que é comum a todos os operadores, isto dificulta a identificação do responsável pela aceitação e confecção do FPL para análises posteriores.

Os dados como matrícula da aeronave, número do registro do piloto, aeródromo de partida e destino, nível, rota e tempo estimado do voo são inseridos no programa. Nesta sala AIS analisada, o SAIS apenas tem a função de confeccionar planos de voo, ou seja, não transmite os mesmos para os órgãos pertinentes. Dessa forma, o programa envia o FPL para outro computador que está integrado em rede e este, o transmite a partir do sistema de transmissão de mensagens aeronáuticas. Por isso, o SAIS aceita caracteres que não são codificados por esse sistema, o que pode ocasionar erros na transcrição. Logo abaixo, um exemplo deste problema:

FIGURA 2 – SAIS. Fonte: Próprios autores.

Conforme figura acima, uma aeronave de matrícula “TESTE” vai decolar do aeroporto Internacional Tancredo Neves/Confins para o aeroporto Carlos Drummond de Andrade/Belo Horizonte. No campo “outros dados”, onde é preenchido o nome do responsável pela aeronave (operador), observa-se que o programa aceitou os caracteres “~” e “”, porém, logo após a transmissão do FPL, a mensagem obtida é a seguinte:

```

FF SBBHZZTZ SBBHZZAZ SBCFZZTZ
101550 SBCF YOYX
(FPL-TESTE
-C150-S/C
-SBCF1800
-N0100A045 DCT
-SBBH0010 SBCF
-OPR/JO?O M?RCIO)
    
```

FIGURA 3 – FPL transcrito. Fonte: Próprios autores.

O nome “JOÃO MÁRCIO” não é transcrito corretamente pelo sistema, afetando a integridade da informação. Sendo assim, as torres de controle dos aeroportos de Belo Horizonte e de Confins que irão receber a mensagem, não compreenderão quem é o operador da aeronave.

O SISNOTAM (Sistema Gerenciador de NOTAM) foi concebido e desenvolvido com a finalidade de controlar todos os processos referentes aos NOTAM, os quais são acessados a partir de uma base de dados on-line (DECEA, SISNOTAM: Manual do usuário, 2002). NOTAM é toda informação relacionada à segurança e regularidade da navegação aérea, os assuntos podem estar relacionados com a indisponibilidade de algum serviço, pista fechada para manutenção, mudança do horário de funcionamento da sala AIS, exercício de paraquedismo, entre outros. Para utilizar o programa, basta digitar uma senha que é comum a todos os operadores. Posteriormente, a consulta é realizada inserindo o indicativo do aeródromo a ser pesquisado ou o nome do município onde fica localizado o mesmo. Uma “janela” será aberta, se houver algum dado que interfira na navegação aérea, aparecerá no sistema, caso contrário, uma mensagem com a expressão “NIL” (nada tenho a transmitir-lhe) será visualizada. Contudo, ao abrir a janela com os NOTAM dos referidos aeródromos, as informações podem ser alteradas ou excluídas involuntariamente violando o princípio da integridade da informação.

O Painel Informativo AIS facilita a consulta de informações relativas ao aeródromo e necessárias a preparação do plano de vôo. O órgão em estudo utiliza um monitor de 42 polegadas. As informações do painel devem estar dispostas conforme figura a seguir:

SALA AIS _____					
COMUNICAÇÕES		AUXÍLIOS À NAVEGAÇÃO		DADOS DA PISTA	
CLRD		NDB		RWY	
GNDC		VOR		DIMENSÕES	
TWR		DME		PCN	
APP		ILS		COND MET _____	
ACC		NASCER/PÔR-DO-SOL		CONDIÇÃO OPERACIONAL	
RECALADA		DATA: _____		VFR	DIURNA () NOTURNA ()
TEL/FAX FPL		_____ / _____		IFR	DIURNA () NOTURNA ()
OPERAÇÕES		ADVERTÊNCIAS À NAVEGAÇÃO AÉREA			
RÁDIO		LOCAL	PERÍODO	ASSUNTO	LIMITE
					INFERIOR

FIGURA 4 - Painel AIS. Fonte: DECEA (ICA 53-2, 2010, p. 58).

Apesar de facilitar a legibilidade dos dados fundamentais para o planejamento do vôo e de não haver ocorrências de inoperância, o painel AIS apresenta falhas de configuração como indisponibilidade das informações dos horários do nascer e pôr-do-sol nos dois últimos dias

de cada mês, além de não ser possível editar os dados dos NOTAM, que é feito através de um terminal de computador, sem ter que apagar todas as informações e inseri-las novamente.

O Fluxo de informações dentro de uma sala AIS, por muitas vezes, não atendem ao princípio da disponibilidade, o que pode ocasionar transtornos no ambiente de trabalho. As normas do DECEA e os acordos entre os órgãos locais são atualizados frequentemente, por isso, briefings operacionais, são repassados com frequência na organização. Essas informações são impressas pela supervisão e cada operador, depois de fazer a leitura do documento, assina-o para comprovar a ciência do seu conteúdo. Para facilitar a divulgação destas instruções, os briefings são colocados dentro do LRO (Livro de Registro de Ocorrências) da sala AIS. Porém, eles misturam-se com outros impressos com correspondências, escala de serviço e formulários para troca de turno. Essa significativa quantidade de papéis dificulta a visualização de um briefing com recomendações de extrema importância e com necessidade de um conhecimento imediato.

Na sala AIS, também existe o manual de operações, o qual fornece dados sobre equipamentos, atribuições dos funcionários, medidas a serem tomadas em caso inoperância de sistemas e recomendações sobre situações de acidente ou incidente aeronáutico. Este manual é atualizado anualmente ou quando necessário pelo coordenador de navegação aérea, ficando indisponível para consulta por vários dias. Não existe um lugar fixo para guardá-lo e por isso, pode ser colocado em diferentes locais da sala. Esse fato dificulta o trabalho dos operadores, pois este manual contém, de forma clara e resumida, instruções básicas para situações de emergência.

3.3 Diagrama de causa e efeito e Plano de Ação

Nesta seção, foi utilizado o diagrama de Ishikawa para identificar as causas raízes das vulnerabilidades detectadas, associadas ao princípio da informação violado:

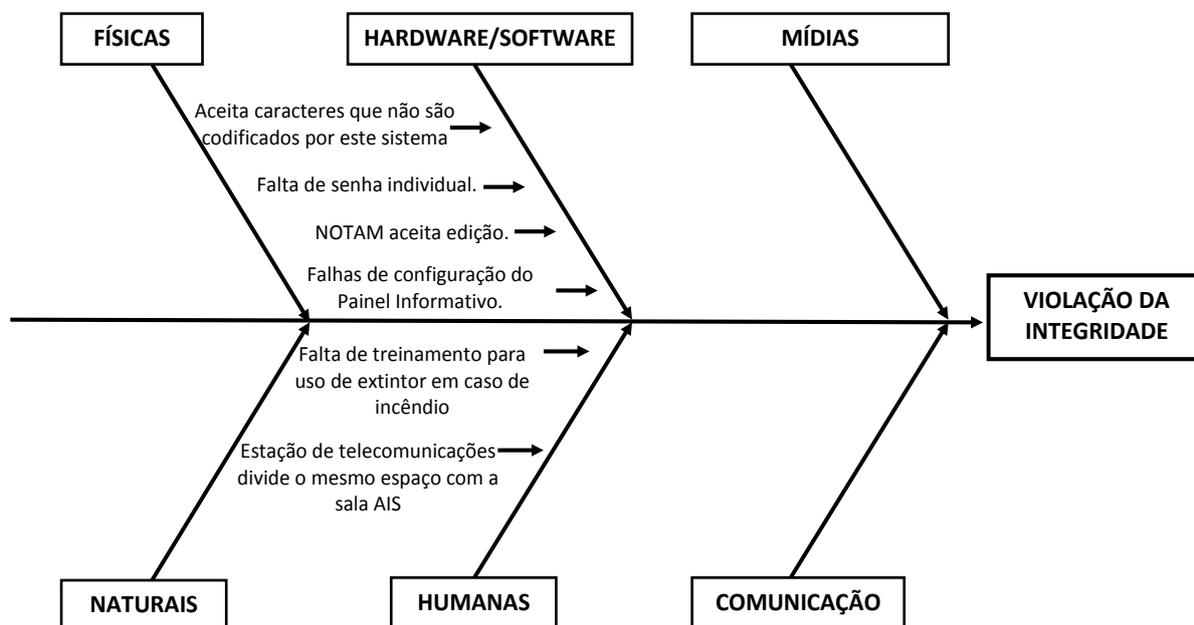


FIGURA 5 – Diagrama de causa e efeito. Fonte: Próprios autores.

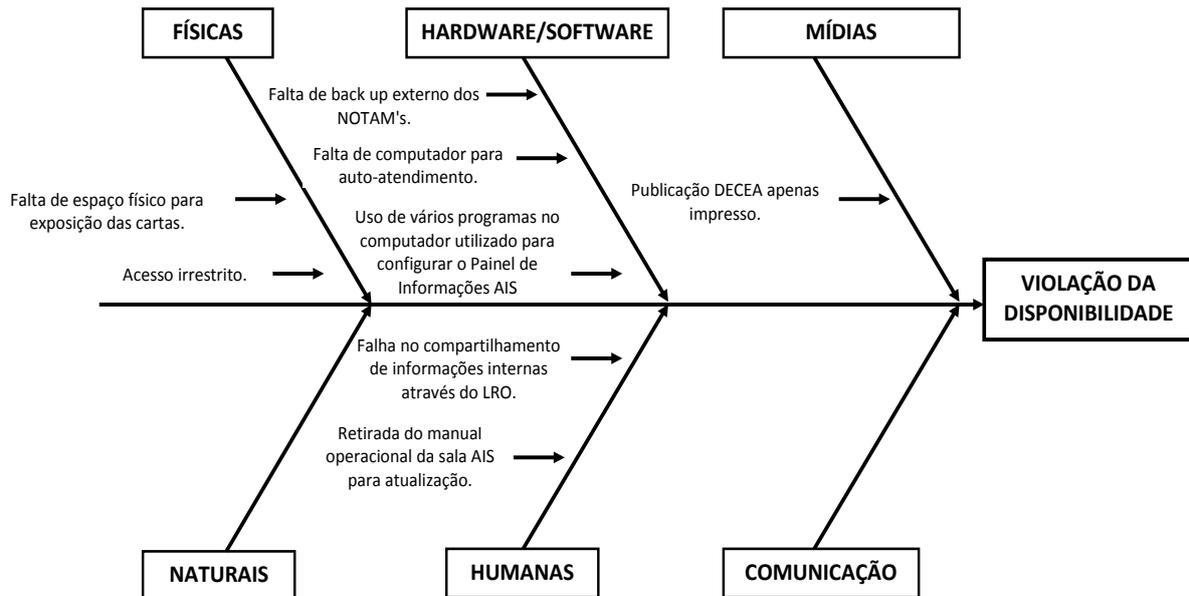


FIGURA 6 – Diagrama de causa e efeito. Fonte: Próprios autores.

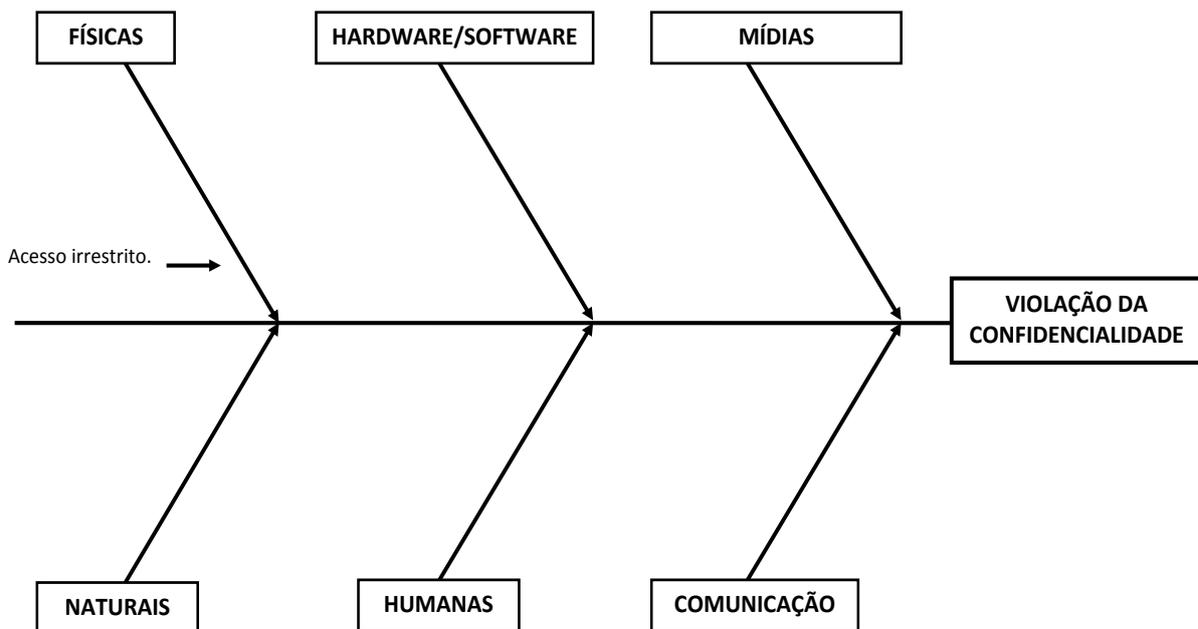


FIGURA 7 – Diagrama de causa e efeito. Fonte: Próprios autores.

Observa-se que as vulnerabilidades afetam principalmente os princípios da disponibilidade e integridade essenciais para a confiabilidade da elaboração do plano de vôo.

Após a associação das causas e efeitos, foi elaborado um plano de ação 5W2H (Tabela 1) para a proposta de medidas de segurança visando a redução da vulnerabilidade e proteção dos ativos da informação contra ameaças.

TABELA 1 – Plano de Ação 5W2H.

What?	Why?	How?	Where?	Who?
O quê?	Por quê?	Como?	Onde?	Quem?
Controlar acesso de pessoas	Evitar que o princípio da disponibilidade e confidencialidade seja violado	Alterar posição porta de acesso para área restrita do aeródromo	AIS	Superintendente
Ampliar sala AIS	Atender norma do DECEA e evitar intempéries na comunicação. Melhorará exposição das cartas.	Fazer projeto de ampliação utilizando área disponível do Aeroporto.	AIS	Superintendente
Disponibilizar computadores para usuários da sala AIS	Permitir auto-atendimento (norma DECEA) e evitar sobrecarga sobre operadores no horário de pico	Solicitar a superintendência regional	AIS	Superintendente
Disponibilizar back up	Evitar violação da disponibilidade	Efetuar back up em drive externo	AIS	Operador AIS
Melhorar o desempenho do computador associado ao painel de informação	Falha na configuração do painel de informação AIS	Desinstalar os programas não utilizados	AIS	Técnico de Informática
Disponibilizar publicação DECEA no formato eletrônico	Para agilizar consulta às normas no caso de indisponibilidade do impresso	Efetuar download dos arquivos do DECEA e INFRAERO	AIS	Supervisor
Disponibilizar uma caixa transparente para armazenamento de briefings operacionais	Melhorar a visualização de briefings	Instalar a caixa em local de fácil visualização.	AIS	Coordenador de navegação aérea
Disponibilizar versão eletrônica do manual operacional	Permitir acesso ao manual no formato eletrônico no caso de indisponibilidade do formato impresso durante período de atualização	Digitalizar manual	AIS	Coordenador de navegação aérea
Treinamento de combate a incêndio para funcionários	Permitir ação dos funcionários no caso de princípio de incêndio	Coordenar Treinamento	AIS	Superintendente
Solicitar senha individual para acessar SAIS	Facilitar a identificação do operador AIS responsável pela aceitação de confecção de FPL	Propor ao DECEA a criação de senhas individuais para aprovadores	AIS	Superintendência de Navegação Aérea
Impedir que SAIS aceite a inserção de caracteres não conhecidos	Evitar a violação do princípio da integridade na preparação/transmissão do FPL	Propor ao DECEA a correção do programa	AIS	Superintendência de Navegação Aérea
Impedir a edição do NOTAM no SISNOTAM	Evitar a violação do princípio de integridade na consulta e disponibilidade do NOTAM ao usuário	Propor ao DECEA a correção do programa	AIS	Superintendência de Navegação Aérea

Fonte: Próprios autores.

4. Discussão dos Resultados

Os dados apresentados neste trabalho basearam-se em instrumentos de coleta de dados realizados com os colaboradores da organização, tais como: entrevistas semi-estruturadas, observações diretas e análise de documentos cedidos pela empresa. Durante todo o estudo, foram considerados critérios como confidencialidade, integridade e disponibilidade das informações.

A utilização do diagrama de causa e efeito permitiu identificar as principais vulnerabilidades associadas aos princípios básicos da informação violados em uma sala de informação aeronáutica. Desta forma, serviu como uma eficiente ferramenta na localização e reparo dos problemas.

O plano de ação 5W2H aponta as medidas de segurança que podem ser adotadas para cada vulnerabilidade detectada. Este diagnóstico permitirá uma adequação dos futuros investimentos em segurança, reduzindo de forma significativa as ameaças aos ativos da informação.

5. Considerações finais

Este estudo de caso se justifica pelo crescimento da atividade aérea e seu valor estratégico para o país. Considerando ainda, sua importância em um mercado competitivo, dinâmico e em constante evolução, faz-se necessário manter os níveis de segurança das operações. O planejamento é fator contribuinte na metade dos acidentes aeronáuticos ocorridos nos últimos dez anos, e a sala AIS, responsável pela disponibilização das informações relativas à navegação aérea para a preparação do plano de voo. Sendo assim, é importante identificar as principais vulnerabilidades e adotar medidas de segurança minimizando a possibilidade de ameaças aos ativos da informação. Sem dúvidas, era extremamente necessário uma análise para identificação de falhas na segurança da informação que garantissem que os princípios da informação não fossem violados.

Todo o fluxo de informação foi mapeado e analisado. Utilizamos diagramas de causa e efeito para associar as diferentes classificações de vulnerabilidades aos princípios da informação: confidencialidade, integridade e disponibilidade, e identificar as causas raízes que levam a violação desses princípios.

No plano de ação foi possível propor medidas de segurança a fim de reduzir os riscos existentes em função das vulnerabilidades detectadas.

As ferramentas utilizadas contribuíram para a elucidação do problema de pesquisa e alcance dos objetivos propostos. Conclui-se então que medidas de segurança podem ser adotadas para minimizar as ameaças aos ativos de informação dentro de uma sala AIS, favorecendo a confiabilidade na preparação do plano de voo.

Referências

AGUIAR, S.. **Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma**. Belo Horizonte: Editora de Desenvolvimento Gerencial, 2002.

CAMPOS, André. **Sistema de Segurança da Informação: Controlando os Riscos**. 2 ed. Florianópolis: Visual Books, 2007.

CENTRO DE INVESTIGAÇÃO E PREVENÇÃO DE ACIDENTES AERONÁUTICOS – CENIPA. **Manual de Investigação do SIPAER – MCA 3-6**. Rio de Janeiro, 2008. Disponível em: <<http://www.cenipa.aer.mil.br/cenipa/paginas/normas/MCA3-6.pdf>>. Acesso em: 26 mar. 2011.

CENTRO DE INVESTIGAÇÃO E PREVENÇÃO DE ACIDENTES AERONÁUTICOS – CENIPA. **Panorama Estatístico da Aviação Civil Brasileira para 2000 a 2009**. Brasília, 2010. Disponível em:

<http://www.cenipa.aer.mil.br/cenipa/Anexos/article/19/PANORAMA_2000_2009.pdf>. Acesso em: 23 mar 2011.

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO – DECEA. **Manual do Especialista em Informação Aeronáutica – MCA 53-1**. Rio de Janeiro, 2008. Disponível em: <<http://publicacoes.decea.gov.br/?i=publicacao&id=2602>>. Acesso em: 26 mar. 2011.

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO – DECEA. **SAIS: Guia do Usuário**. Rio de Janeiro, 2007.

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO – DECEA. **Sala de Informações Aeronáuticas de Aeródromos (Sala AIS) – ICA 53-2**. Rio de Janeiro, 2009. Disponível em: <<http://publicacoes.decea.gov.br/?i=publicacao&id=2522>>. Acesso em: 26 mar. 2011.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão executiva**. 9º ed. Rio de Janeiro: Editora Campus, 2003.

SIQUEIRA, Marcelo Costa. **Gestão Estratégica da Informação**. 1º ed. Rio de Janeiro: Brasport, 2005.

SLACK, N.; CHAMBERS, S.; JOHNSTON, R.; **Administração da Produção**. 2º ed. São Paulo: Editora Atlas, 2002.