UNIVERSIDADE FEDERAL DE PERNAMBUCO

DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

CURSO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

AUDITORIA E SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: BREVE ANÁLISE EM UM ÓRGÃO DE CONTROLE DE TRÁFEGO AÉREO

TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO

POR

RAFAEL MARINHO DE ALBUQUERQUE

Orientadora: Prof[a]. Ana Paula Cabral, DSc.

RECIFE, JUNHO/2010

UNIVERSIDADE FEDERAL DE PERNAMBUCO

DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

CURSO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

AUDITORIA E SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: BREVE ANÁLISE EM UM ÓRGÃO DE CONTROLE DE TRÁFEGO AÉREO

Trabalho de conclusão de curso apresentado ao departamento de Engenharia de Produção da Universidade Federal de Pernam buco- UFPE - como requisito parcial para obtenção de Grau em Engenharia de Produção

RECIFE, JUNHO/2010

A345a **Albuquerque, Rafael Marinho de**

Auditoria e segurança em sistemas de informação: breve análise em um órgão de controle de tráfego aéreo / Rafael Marinho de Albuquerque. – Recife: O Autor, 2010.

viii, 42 f.; il., figs., tabs.

TCC (Graduação) – Universidade Federal de Pernambuco. CTG. Curso de Engenharia de Produção, 2010.

Inclui Referências Bibliográficas.

1. Engenharia de Produção. 2. Sistemas de Informação. 3. Auditoria e Segurança. 4. Controle de Tráfego Aéreo. I. Título.

UFPE

658.5 **BCTG/2010-120**

“Seja fiel nas pequenas coisas, porque é nelas que reside a sua força”.

Madre Teresa de Calcutá

Agradecimentos

A Deus, que é o meu maior porto seguro, com a ajuda dele tive coragem e forças chegar até o fim dessa pequena jornada.

A meus pais, pelo exemplo de honestidade, amor, compreensão e perseverança. É através de seus puxões de orelha e conselhos que tento progredir. Obrigado por participarem comigo dessa caminhada e acreditarem em mim.

A minha irmã que me ensinou a dividir e conviver com o próximo.

Aos meus avôs, tios, primos, minha grande família.

Aos meus amigos, que desde sempre me ajudaram. A Franci, Jafé, Cayo, Marília, Mari, Gabi, Regina, Rebeca, Jefferson, Thiago...

Aos companheiros de trabalho, por todo o incentivo, pela amizade e também pelas trocas de serviço...

À Profª. Ana Paula, por todo o apoio, compreensão e orientação.

A todos do GPSID, sobretudo a Rodrigo, pelo aprendizado e iniciação acadêmica.

Aos Professores do Curso de Engenharia de Produção pelos conhecimentos proporcionados. Quero agradecer em particular à Profa. Gisele, de quem pude colher ensinamentos ainda no ensino fundamental, quando formava as bases que me possibilitaram chegar aqui.

Aos colegas de curso, por todos os anos de crescimento conjunto. Em especial a estas grandes pessoas, das quais foi indispensável o apoio nos últimos anos: Tarcila, Paula, Kakuta, Ayana, Japa, Yuri, Roberta, Nathália Cavalcanti, Petra, Eugênia, Eduardo, Guilherme, Danilo, Paulino, Luís, Gustavo, Jonathan, Gil, Paulo Roma, Thiago Henrique... a todos enfim.

E aos funcionários que fazem a UFPE.

Resumo

O uso de sistemas de informação está totalmente disseminado nas organizações hoje em dia. Eles tornaram-se indispensáveis para garantir a eficiência das operações mais fundamentais e mesmo para alavancar a competitividade das empresas. Para este trabalho, busca-se avaliar a problemática da segurança e da auditoria em sistemas de informação (SI) em um setor onde a tecnologia da informação e comunicação (TIC) é aspecto crítico: o controle de tráfego aéreo. Em um contexto em que se projeta cada vez mais aumento da demanda no setor, a eficácia do serviço de controle de tráfego aéreo é um dos gargalos que precisam ser considerados para suportar esse crescimento. Para tanto dependerá da disponibilidade e do desempenho dos meios de comunicação, de navegação e de vigilância, bem como da adequação dos demais recursos técnicos instalados nos órgãos de controle e da qualificação dos recursos humanos. Dessa forma, garantir a eficiência dos SIs, sua segurança e auditorias para acompanhar seu planejamento e utilização, são fatores primordiais para alcançar os objetivos estratégicos evitando que os sistemas acabem se tornando mais um limitante da eficiência na prestação de serviço de controle de tráfego aéreo.

Palavras Chaves: Sistemas de informação, Auditoria e Segurança, Controle de tráfego Aéreo.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

INTRODUÇÃO

O uso de sistemas de informação está totalmente disseminado nas organizações hoje em dia. Eles tornaram -se indispensáveis para garantir a eficiência das operações m ais fundamentais e mesmo para alavancar a competitividade das empresas.

Para este trabalho, busca-se avaliar a prob lemática da segurança e da auditoria em sistemas de inform ação (SI) em um setor ond e a tecno logia da inform ação e comunicação (TIC) é aspecto crítico: o controle de tráfego aéreo.

O setor de aviação, passada a fase crítica da crise econômica mais recente, já demonstra sinais de recuperação e tendê ncia de crescim ento. Segundo da dos da Agência Nacional de Aviação Civil, os primeiros quatro meses 2010 acumulam alta de 32,22% no tráfego de vôos domésticos e de 9,54% no de vôos internaciona is operados por com panhias brasileiras em comparação ao mesmo período de 2009 (ANAC, 2010b).

Ainda segundo informações da ANAC (2010a), "no Brasil, a aviação regular apresenta expressivo crescimento e novas empresas estão surgindo. Em setembro de 2009, a Sol Linhas Aéreas, do Paraná, iniciou suas atividades co m vôos na região Sul do País. Quase um ano antes, em dezembro de 2008, a Azul lançou suas operações".

No dia 14 de maio deste ano, a mesma agência aprovou a concessão para a Noar Linhas Aéreas, empresa aérea pernam bucana, explo rar por 10 anos o serviço de transporte aéreo público regular de passageiro, carga e m ala postal. E além do surgim ento de novas companhias, as empresas de menor porte também avançam (ANAC, 2010a).

Em contrapartida, o setor de controle de tráfego, que deveria suportar esse desenvolvimento, vem se destacando negativamente, sobretudo por problem as gerenciais, de forma que se viu em ergir inúmeros prejuízos para as atividades econôm icas e para o cidadão comum nos últim os anos. Existe u m gargalo n esse se tor que engloba inúm eros fatores. Por essa razão, buscar melhorias e gerenciamento mais eficientes para a área é fundamental.

Como esclarece Siewerdt (2008, pág. lviii), "a eficácia do serviço de controle de tráfego aéreo dependerá da disponibilidade e do de sempenho dos m eios de com unicação, de navegação e de vigilância, bem como da adequação dos d emais recursos técn icos [...] e da qualificação dos recursos humanos".

Vê-se que garantir a eficiência dos SIs, é fa tor prim ordial para alcançar os objetivos estratégicos e atendim ento da de manda no cont role de tráfego aéreo, para evitar que os sistemas acabem se tornando mais um limitante da eficiência na prestação de serviço.

Este trabalho busca, portanto, fazer um estudo sobre o ciclo operacional em um órgão de controle de tráfego aéreo para avaliar como a segurança da informação e auditoria em SI estão sendo tratados: aspecto importante para garantir a eficiência do serviço de controle de tráfego aéreo. E ainda propor recomendações para direcionar melhorias para a organização.

1.1 Justificativa

"Uma análise do cenário atual demonstra que o crescimento e o sucesso das organizações atualmente estão diretamente relacionados à necessidade de se manter uma infra-estrutura de Tecnologia da Informação e Comunicação (TIC) segura e confiável" (BERNARDES; MOREIRA, 2005).

Como afirma Cascarino (2007, pag. xix, tradução nossa), "atualmente torna-se impossível uma empresa de qualquer porte ou ramo de atividade manter seus negócios sem o suporte da TIC para suas operações. O velho adágio de que 'sempre é possível voltar às operações manuais' hoje não passa de uma falácia".

Um fato recente exemplifica o que disse Cascarino: vinte e cinco unidades da Agência do Trabalho em Pernambuco passaram mais de uma semana sem prestar atendimento ao público, devido à indisponibilidade do seu SI ocasionada pela invasão de dois vírus (JC ONLINE, 2009a).

No caso anterior, a parada das atividades realmente não pôde ser evitada, mas o que o autor quis dizer, na verdade, não é que nunca se possam realizar algumas atividades de forma manual quando ocorrem problemas com o SI ou falhas em algum recurso de TIC. O grande problema são os custos e as perdas por essa indisponibilidade. Mesmo quando existem formas alternativas de fazer as coisas sem os sistemas, a eficiência e a eficácia dos processos ficam comprometidas de tal forma que voltar às atividades manuais não deveria figurar como uma opção para os gestores.

No setor de transporte aéreo, totalmente apoiado em TIC, esse comprometimento é evidente. Há exemplos recentes, como no caso de problemas no sistema de *check-in* da TAM que obrigou os funcionários a realizar os procedimentos manualmente, fazendo com que os atrasos nos vôos da empresa representassem quase metade dos vôos atrasados no País naquele dia (JC ONLINE, 2009b).

Nos EUA, falhas no sistema de processamento de planos de vôo da *Federal Aviation Administration* (FAA) obrigaram os controladores de tráfego aéreo a tratarem manualmente as informações, por esse motivo vários aeroportos sofreram com atrasos que se propagaram

durante todo um dia. E há pouco mais de um ano problemas semelhantes já haviam ocorrido nos sistemas da FAA (WALD, 2009).

Ainda sobre fatos recentes, a notícia a seguir ilustra outro exemplo:

> No dia 10 de novembro, 18 estados brasileiros e parte do Paraguai ficaram seis horas às escuras. O caos que se viu é um ensaio do que pode acontecer a um país atacado por hackers. Aliás, o Brasil já viveu isso. Em janeiro de 2005, um apagão atingiu o Rio de Janeiro. Em setembro de 2007, um incidente ainda maior deixou três milhões de pessoas sem luz no Espírito Santo. Em Vitória, o blecaute resultou em lojas saqueadas, celulares mudos, caos no trânsito e hospitais em pane. O governo brasileiro nega, mas o serviço de inteligência dos EUA atribui a ação a ciberterroristas. (SALVADORI, 2009)

Quando se fala do tráfego aéreo, especialistas repetem: "'um avião só é derrubado por uma cadeia de falhas, [...] destruir um Boeing usando o laptop não é uma a tarefa das mais fáceis. Mas é possível. Sistemas de controle do tráfego aéreo podem ser invadidos'" (SALVADORI, 2010).

Mesmo em hipóteses menos catastróficas, prejuízos como o de informações erradas sendo transmitidas podem também comprometer a segurança ou ocasionar grandes transtornos ao fluxo de aeronaves.

Percebe-se que, "ao passo que se tornam fundamentais para a sobrevivência das organizações, as informações trazem consigo preocupações acerca da sua segurança e da forma como devem ser organizadas. Acontece que para configurar apoio, as informações precisam ser aplicáveis ao contexto, confiáveis e de fácil acesso" (MENDONÇA, 2009, pág. iv).

Diante de toda essa conjuntura, o presente trabalho demonstra sua relevância ao se propor a diagnosticar e estabelecer recomendações relacionadas à segurança da informação e a auditoria de SI em um ciclo de operações de um órgão de controle de tráfego aéreo. Por meio do que perdas e prejuízos possam ser evitados em um setor totalmente dependente da TIC e de grande representatividade para as atividades econômicas do país.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo deste trabalho é fazer um estudo sobre o ciclo operacional em um órgão

de controle de tráfego aéreo para avaliar como a segurança da informação e auditoria em SI estão sendo tratados nesse ambiente, de forma que se possam propor recomendações de melhorias.

1.2.2 Objetivos Específicos

Mais especificamente, busca-se:

- Estudar os conceitos de segurança da informação e auditoria em SI;
- Analisar algumas metodologias existentes nessa área;
- Descrever o ciclo operacional do órgão tratado e ratificar a necessidade de tratar a segurança da informação e fazer auditoria nos seus SIs;
- Analisar SIs no órgão para obter um diagnóstico e propor melhorias para a organização;

1.3 Metodologia

Este trabalho foi constituído de pesquisa exploratória e para a sua execução realizou as atividades de pesquisa bibliográfica e documental, e de observação assistemática da organização. Essas etapas foram distribuídas basicamente como segue:

- Etapa 1: Fundamentação teórica sobre os conceitos de segurança e auditoria em SI e análise de metodologias relevantes nessa área.
- Etapa 2: Descrição do ciclo operacional e verificação da necessidade de tratar da segurança da informação e de se fazer auditoria em SI no órgão de controle de tráfego aéreo estudado.
- Etapa 3: Análise para diagnóstico e recomendações no órgão tratado.

1.4 Estrutura do Trabalho

Este trabalho está dividido em cinco capítulos. Neste primeiro capítulo são apresentados a justificativa, os objetivos gerais e específicos e a metodologia para sua realização.

O segundo capítulo é composto por dados teóricos que fundamentam o trabalho. Nele é apresentado conceitos e termos utilizados no estudo do controle e auditoria de sistemas de informação.

O terceiro capítulo faz uma explanação básica sobre o serviço de controle de tráfego aéreo, contextualiza o uso de SIs nesse ambiente e traz alguns novos conceitos que vêm se

desenvolvendo nesse setor e implicam mudanças a serem feitas.

O quarto capítulo reporta o estudo de caso, as observações e conclusões a respeito do órgão em análise.

Por fim , o quinto capítulo traz as cons iderações fi nais e sugestões para o desenvolvimento de trabalhos futuros.

BASE CONCEITUAL

Neste capítulo são apresentados alguns conceitos teóricos para um melhor entendimento do estudo de caso proposto neste trabalho. Sistemas de informação, auditoria e segurança da informação, objetivos e importância são alguns dos assuntos apresentados.

1.5 Sistemas de Informação

Um sistema de informação é um tipo de sistema, ou seja, um conjunto de partes que interagem para alcançar um objetivo, cujas entradas e saídas são dados e informações. (STAIR, 1996 apud COSTA; ALMEIDA, 2002)

Segundo Almeida et al (2002), dados são fatos sobre um objeto ou conceito, enquanto informações são dados que foram organizados, refinados e se apresentam de uma forma tal que podem ser usados para facilitar o processo de tomada de decisão presente ou futura.

Podem-se estabelecer então três atividades que levam o sistema a produzir as informações que as organizações precisam para tomar decisões, controlar operações, analisar problemas, criar novos produtos ou serviços. Essas atividades são: a entrada de dados brutos da organização ou do ambiente externo, o processamento que converte esses dados para formas que tenham utilidade e significado, e a saída das informações para os fins a que se destinam. Um SI também necessita de realimentação, que são saídas que servem para avaliar ou corrigir algum estágio durante a entrada de dados. A figura 2.1 apresenta um modelo básico do funcionamento de um SI genérico (LAUDON; LAUDON, 2007).

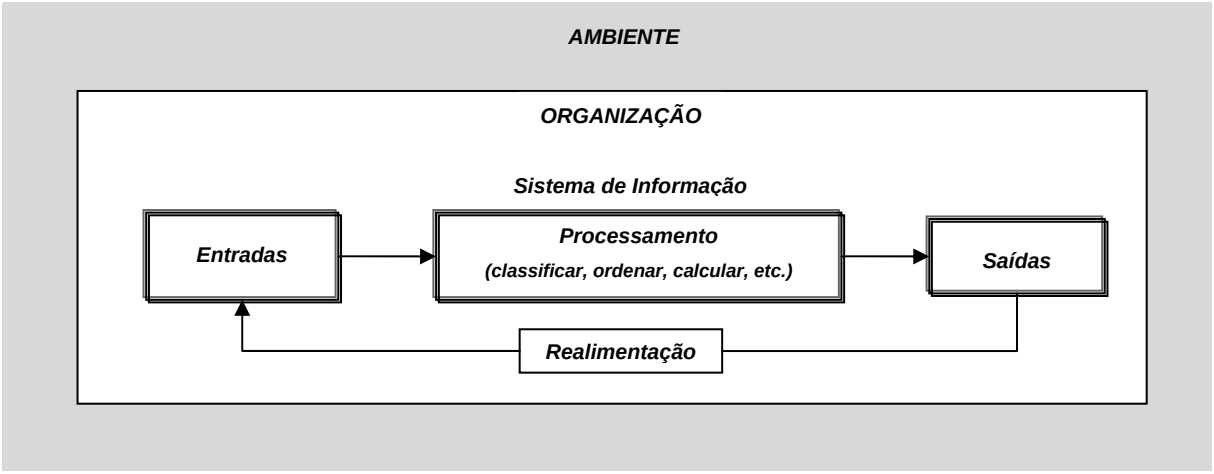

Figura 0.1- Atividades dos sistemas de informação: entrada, processamento e saídas.

Fonte: adaptado de Laudon e Laudon (2007)

Outro aspecto importante no contexto de qualquer sistema é o ambiente em que ele está inserido. Há fatores que não pertencem ao sistema, mas que têm influência sobre ele. O que separa um sistema do seu ambiente e de outros sistemas é a sua fronteira. Vários sistemas podem compartilhar um mesmo ambiente e estabelecer comunicação, se conectando entre si através de um limite compartilhado, ou interface. Se um sistema for componente de um sistema maior ele é um subsistema, e o sistema maior é o seu ambiente. (COSTA; ALMEIDA, 2002; O'BRIEN, 2002).

Um sistema de informação tem por finalidade coletar, processar, armazenar, analisar e disseminar informações para uma finalidade específica. O SI é um conjunto de componentes inter-relacionados trabalhando juntos para facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório das organizações. Basicamente, fazem parte de um SI: (TURBAN et al., 2005; LAUDON; LAUDON, 2007)

- *Hardware* – conjunto de dispositivos como o processador, monitor, teclado impressora, etc. Juntos, esses dispositivos aceitam dados e informações, os processam e os apresentam.
- *Software* – conjunto de programas que permitem que o hardware processe dados.
- Banco de dados – coleção de arquivos relacionados, tabelas, relações e assim por diante, que armazena dados e associações entre eles.
- Rede – sistema de conexão (com ou sem fio) que permite o compartilhamento de recursos por diferentes computadores.
- Procedimentos – conjuntos de instruções sobre como combinar os componentes anteriores a fim de processar informações e gerar a saída desejada.
- Pessoas - indivíduos que trabalham com o sistema de informação, interagem com ele ou utilizam sua saída.

Dentro das organizações os SIs desempenham papel fundamental. Sistemas eficazes contribuem significativamente para a estratégia corporativa, visto que, dentre outras coisas, disponibilizam com maior precisão e agilidade a informação, cada vez mais valiosa. O uso dos SIs permite o fornecimento de melhores bens e serviços, maior eficiência, maior produtividade, suporte mais preciso no processo de avaliação de desempenho e tomada de decisão (COSTA; ALMEIDA, 2002).

De fato, como ressalta Costa e Almeida (2002), uma organização "não consegue alcançar seus objetivos se não tiver um processo de tomada de decisão eficaz e se não tiver como garantir a eficiência de seus processos".

Algumas vezes "o termo *tecnologia da informação* [TI] é usado para indicar a mesma coisa que *sistema de informação"*. No entanto, o termo TI, em seu sentido mais amplo, refere-se à "coleção de recursos de informação da organização, seus usuários e a gerência que os supervisiona, ou seja, a tecnologia da informação inclui a infra-estrutura da TI e todos os outros sistemas de informação da organização" (TURBAN et al., 2005, grifos do autor).

1.6 Auditoria e Segurança de Sistemas de Informação

Os SI, como foi visto, são constituídos de inúmeros componentes que podem estar localizados em mais de um lugar. Dessa forma, esses sistemas são bastante vulneráveis a diversos riscos e ameaças que podem comprometer o seu funcionamento. (TURBAN et al., 2005).

Conforme explica Laudon e Laudon (2007, pág. 210), "quando grandes quantidades de dados são armazenadas sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual".

Os mesmos autores acrescentam que "sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicação. Logo, o potencial para acesso não autorizado, uso indevido ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede" (LAUDON; LAUDON, 2007, pág. 210).

Nesse sentido, para assegurar "a qualidade, o desempenho dos sistemas de informação e das atividades que os mesmos suportam, as organizações podem fazer uso de métodos e dispositivos que envolvem aspectos de segurança de *hardware*, *software* e procedimentos". (COSTA; ALMEIDA, 2002)

1.6.1 Ameaças aos sistemas de informação

As vulnerabilidades dos sistemas de informação citadas na lista anterior são classificadas por Turban et al. (2005) em ameaças intencionais e ameaças não intencionais.

Estas últim as, por sua vez, podem ser didatica mente divididas em : erros hum anos, riscos ambientais e falhas de sistema.

Ameaças in tencionais incluem roubo de dado s; uso inad equado de dados; roub o de equipamentos ou program as; m anipulação deliberad a no m anuseio, fornecim ento, processamento, transferência ou pro gramação de dados; greves, manifestações ou sabotagem; danos maliciosos aos recursos de TI e fraudes (TURBAN et al., 2005).

Problemas por erro hum ano podem ocorrer desde o projeto dos sistem as até a programação, testes, coleta de dados, entr ada de dados, autorização ou instruções. Especialistas em SI també m pode m com eter um erro ao fazer a m anutenção dos sistem as existentes (TURBAN et al., 2005).

Estudos apontam ainda que erros hum anos contribuem para a grande parte dos problemas relacionados ao controle e seguran ça em muitas organizações. Muitas oco rrências indesejadas partem de dentro dos próprios am bientes internos ao negócio, resultante m uitas vezes da in observância dos usuários aos proc edimentos de segurança. Além disso, pessoas externas podem enganar funcionários fingindo serem ent es legítim os; assim conseguem informações importantes ou privilégios de acesso não autorizados. Essa prática é denominada engenharia social (TURBAN et al., 2005; LAUDON; LAUDON, 2007; MENEZES, 2008).

Os riscos am bientais incluem eventos com o terrem otos, f urações, tem pestades, inundações, falhas ou forte v ariação no fornecim ento de energia elétrica, incênd ios, defeitos de condicionadores de ar, explosões, vazamento radioativo, falhas de sistemas de refrigeração de água. Essas am eaças podem interrom per as operações n ormais e resultar em inúm eras perdas, incluindo longos períodos de espera e custos de recuperação do s recursos de TI e dos sistemas (TURBAN et al., 2005)

As falhas de sistem a podem ocorrer com o resultado de problem as de problem as de fabricação ou materiais defeituosos. Maus func ionamentos não intencion ais também ocorrem por motivos como a falta de exp eriência até a realização incorreta de testes (TURBAN et al., 2005).

Como se vê, há três fontes principais de ri scos aos SIs: cau sas naturais, tecnológicas e fatores humanos. O que se percebe é que nos dias de hoje a segurança do s sistemas está mais relacionada às pessoas e aos pr ocessos do que à tecnologia. De ssa forma deve-se dar ênfase no controle não apenas tecnológico, mas dos recursos humanos e de procedimentos. É preciso

ainda fomentar uma cultura organizacional preocupada com essa segurança. Nesse sentido, além de treinamento adequado aos funcionários, é importante, dentre outras coisas, se adequar às legislações e normas existentes (XUEMEI et al, 2009).

Laudon e Laudon (2007) corroboram a percepção anterior ao estabelecer que "quando se fala em controle e segurança dos sistemas de informação, tecnologia não é a peça-chave. Tecnologia é o que dá base, mas na ausência de políticas de gerenciamento inteligentes, até as mais avançadas tecnologias são facilmente vencidas".

1.6.2 Controles e Auditorias

Vê-se que é incorreto tratar a segurança apenas sob uma perspectiva técnica. Para melhor proteger a infra-estrutura de TIC e os SIs, é preciso incorporar as questões de segurança nas ações de governança corporativa das organizações (CGTRF, 2004 apud MAIA, 2009)

Pode-se afirmar que a segurança nesse caso é multidimensional. Ela está relacionada à tecnologia, às pessoas e aos processos. O problema é que muitas organizações têm dificuldade em lidar com um conceito que é multidisciplinar por natureza. Todos esses aspectos devem ser considerados de maneira estruturada e holística (XUEMEI et al, 2009).

A proteção dos recursos de informação é obtida principalmente inserindo controles, que se destinam a proteger de danos acidentais, deter atos intencionais, solucionar problemas o mais cedo possível, melhorar a recuperação de danos e corrigir problemas. Deve-se enfatizar, sobretudo, a prevenção, visto que a defesa não tem sentido após o incidente.

A tabela a 2.1 mostra os vários tipos de controles, divididos em duas categorias: controles gerais e controles de aplicação (TURBAL et al., 2005).

Tabela 0.1-Controles gerais e controles de aplicação para a proteção dos sistemas de informação

TIPO DE CONTROLE	**FINALIDADE**
Controles gerais	
Controles físicos	Proteger fisicamente os recursos de TI
Controles de acesso	Restringir o acesso de usuários não-autorizados aos recursos de TI; ênfase na identificação do usuário. Pode usar qualquer um dos seguintes identificadores:

	algo que o usuário saiba (por exemplo, senha), algo que o usuário tenha (por exemplo, cartão inteligente, ficha), algo que o usuário seja (biometria – fotografia do rosto, impressões digitais, leitura da íris, leitura da retina, análise da voz).
Controles de segurança de dados	Proteger os dados contra a exposição acidental ou intencional para pessoas não autorizadas, ou contra modificação ou destruição não autorizadas.
Controles administrativos	Emitir e monitorar diretrizes de segurança
Controles de comunicações (rede)	
- Segurança de fronteira	O principal objetivo é o controle de acesso.
- *Firewalls*	Sistema que impõe política de controle de acesso entre duas redes.
- Controle de vírus	*Software* antivírus, restrição de uso de mídias de armazenamento removíveis.
- Detecção de intrusão	O principal é detectar acesso não autorizado à rede.
- Rede privada virtual	Usa a internet para transportar informações dentro de uma empresa e entre parceiros comerciais, mas com segurança reforçada pelo uso de criptografia, autenticação e controle de acesso.
Autenticação	O principal objetivo é a prova de identidade.
Autorização	Permissão concedida a pessoas e grupos para certas atividades com recursos de informação, com base na identidade verificada.
Controle de aplicação	
Controles de entrada	Previnem a alteração ou perda de dados.
Controles de processamento	Assegura que dados estejam completos, válidos e exatos quando estiverem sendo processados e que os programas estejam sendo corretamente executados.
Controles de saída	Assegura que os resultados do processamento sejam exatos, válidos, completos e consistentes.

Fonte: adaptado de Turban et al. (2005, p.452)

Segundo Weber (1998, apud COSTA; ALMEIDA, 2002), uma forma checar se os controles utilizados pela organização estão adequados é a auditoria de sistemas de informação. Ela consiste em uma declaração de opiniões relacionadas às atividades de uma empresa obtidas por meio de coleta e análise isenta e objetivas, ou seja, os observadores que realizam essa tarefa devem ser independentes e imparciais.

A auditoria irá verificar se os controles foram instalados adequadamente, se eles são eficazes, se não há brechas de segurança e determinar quais ações podem ser feitas para melhoria. Uma auditoria é basicamente um exame dos sistemas de informação, suas entradas, saídas e processamento (TURBAN et al., 2005).

Weber (1998, apud COSTA; ALMEIDA, 2002) afirma que a auditoria visa ajudar a organização a atingir de forma eficiente seus objetivos. Essa importância se deve a fatores como:

- aumento da importância dos SIs nas organizações;
- aumento rápido da utilização de SIs;
- conflito na busca de eficiência através dos SIs;
- aumento nos custos dos sistemas;
- problemas causados por redes, etc.;
- diminuição da eficiência dos SIs;
- aumento da fragilidade e dos riscos dos SIs falharem;
- desastre natural;
- desastre artificial;
- erro de entrada de dados;
- crimes, etc.;
- diminuição da confiabilidade e segurança dos SIs.

É importante lembrar que a auditoria pode e deve ser realizada em todas as fases do ciclo de desenvolvimento dos SIs. Desde o planejamento até depois que o sistema já está implementado e estável, as auditorias devem continuar periodicamente (COSTA; ALMEIDA, 2002).

As técnicas usadas em auditoria para outras áreas podem ser aplicadas no caso dos SIs, como por exemplo: entrevistas, observação, comparação, inspeção técnica, etc. Porém também é usual fazer teste no sistema para verificar se as saídas estão adequadas às entradas fornecidas para o sistema, ou seja, faz-se a comparação do sistema em operação com as especificações de projeto. Pode-se ainda introduzir a auditoria com o um módulo usuário do sistema e fazer simulações (COSTA; ALMEIDA, 2002).

Para garantir o bom desempenho dos SI, os cuidados de auditoria devem envolver ainda questões éticas e sociais em termos de seu impacto no emprego, individualidade, condições de trabalho, privacidade, saúde e crimes com o uso de sistemas e tecnologias (O'BRIEN, 2002).

Dentro da preocupação que deve existir com a eficiência e com os recursos humanos, diretamente afetados e envolvidos com a utilização dos SIs, algumas medidas precisam basear-se na Ergonomia, para criar um ambiente de trabalho saudável, seguro, confortável e agradável para as pessoas. Além de todos os benefícios para o usuário, isso resultará em aumento da produtividade para a organização. A auditoria deve, portanto, verificar essas questões desde o início do projeto de sistema de informação (COSTA; ALMEIDA, 2002).

A figura 2.2 ilustra os aspectos importantes das dimensões de segurança, éticas e sociais nos SIs. Sobre cada uma das áreas apresentadas, as tecnologias de informação podem possuir tanto efeitos benéficos quanto prejudiciais, e tudo isso deve ser considerado para um bom gerenciamento (O'BRIEN, 2002).

Figura 0.2 – Aspectos importantes das dimensões de segurança, éticas e sociais de sistemas de informação. Fonte: adaptado de O'BRIEN (2002)

1.6.3 Norteadores da auditoria e segurança em SI

Dado o número significativo de falhas graves ocorridas em grandes empresas na última década, autoridades reguladoras têm elaborado conjuntos complexos de novas leis e normas com o intuito de forçar a melhoria da governança, segurança, controle e transparência organizacionais (ITGI, 2006 apud MAIA, 2009).

Como relata Martins e Santos (2005), a preocupação com a segurança dos sistemas remonta à década de 60, quando o processo de definição de regras e padrões de segurança iniciou-se impulsionado pela Guerra Fria.

O *British Standards Institute* (BSI), na década de 80, deu origem a uma das primeiras normas sobre o assunto, denominada BS7799 – *Code of Practice for Information Security Management*, para atender às necessidades das organizações, agências governamentais e instituições internacionais em relação ao estabelecimento de padrões e normas que refletisse as melhores práticas de mercado relacionadas à segurança dos sistemas e informações (Maia, 2009).

Esse esforço culminou com a publicação da Norma Internacional de Segurança da Informação (ISO/IEC-17799) em 2000, baseada na BS7799, após um intenso trabalho de consulta pública e internacionalização. A ISO/IEC-17799 possui uma versão aplicada aos países de língua portuguesa: a NBR ISO/IEC-17799:2001.

Em 2005, foi publicada uma segunda edição tecnicamente revisada da ISO/IEC 17799, que passou a se chamar ISO/IEC 27002 a partir de 2007. Ela passou a fazer parte de uma nova família de normas relacionadas aos temas de requerimentos de segurança para gerenciamento de sistemas, gerenciamento de riscos, indicadores e suas medições, e guias de implementação (ISO/IEC 27002, 2005 apud MAIA, 2009).

Segundo Cunha (2008):

> A norma ISO/IEC 27002 tem como principal objetivo garantir a continuidade dos negócios de uma organização, através da preservação dos três componentes básicos de uma informação: confidencialidade, integridade e disponibilidade. É obtida através da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software. Estes controles precisam ser

> estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

Ainda de acordo com a norma ISO/IEC 27002, muitos sistemas de informação não foram projetados para serem seguros. A segurança, que pode ser alcançada por meios técnicos, é limitada e convém que seja apoiada por gestão e procedimentos apropriados. As identificações de quais controles convêm que sejam implantados requer planejamento cuidados e atenção aos detalhes (CUNHA, 2008).

Um ponto a se destacar para a gestão da segurança é a necessidade da participação de todos os funcionários da organização, fornecedores, clientes, acionistas bem como acesso ao conhecimento especializado através de consultorias (CUNHA, 2008).

1.7 Considerações sobre o capítulo

O controle e a segurança dos SI envolvem uma variedade de processos de negócio que combinados reduzem riscos de acidentes, crimes e uso ineficiente ou pouco produtivo. Segundo Alter (2001), pode-se estabelecer a seguinte ordem para o desenvolvimento do sistema, garantia da segurança, controle das operações e antecipação aos problemas:

- Em primeiro lugar, garantir que o sistema seja desenvolvido corretamente e controlar suas modificações;
- Treinar os usuários quanto a questões de segurança;
- Com o sistema já em operação, garantir a segurança física do mesmo;
- Estando ele seguro fisicamente, prevenir acesso não-autorizado a computadores, rede e dados;
- Tendo controle de acesso, garantir que as transações são realizadas corretamente;
- Mesmo com controles de transação em ordem, buscar a eficiência e eficácia da operação e meios de melhorá-la;
- Mesmo que o sistema pareça seguro, fazer auditorias;
- Mesmo com vigilância constante, estar preparado para desastres.

Nesse sentido, é importante que as organizações observem normas, legislações e

melhores práticas ex istentes na área para que p lanejem e au ditem seus s istemas de f orma a garantir os objetivos do negócio e a competitividade.

SISTEMAS DE INFORMAÇÃO E O CONTROLE DE TRÁFEGO AÉREO

Neste capítulo é apresentada uma visão básica do serviço de controle de tráfego aéreo, contextualiza o uso de SIs nesse ambiente e traz alguns novos conceitos que vêm se desenvolvendo nesse setor e implicam mudanças a serem feitas nos sistemas.

1.8 O serviço de controle de tráfego aéreo

O serviço de controle de tráfego aéreo de forma geral caracteriza-se pela "inter-relação entre o operador de um órgão de tráfego aéreo e o piloto da aeronave, por meio de recursos de comunicação, possibilitando que os objetivos sejam entendidos e atendidos. O nível da complexidade do cenário de tráfego aéreo determina o tipo de serviço a ser oferecido" (DECEA, 2010).

A aviação no mundo evoluiu muito nos últimos anos em termos tecnológicos, aeronaves cada vez maiores, mais pesadas e velozes cruzam os continentes. A prestação do serviço de controle de tráfego aéreo vem se desenvolvendo visando à promoção de uma atividade segura, ordenada e com a máxima fluidez (POGIANELO; MÜLLER, 2008).

No Brasil, foi estabelecido o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB). Envolve todos os órgãos civis e militares que executam atividades relacionadas aos Sistemas de Proteção ao Vôo, de Telecomunicações, de Busca e Salvamento, de Defesa Aérea e Controle de Tráfego Aéreo e os meios de Comunicações e Controle do Sistema de Controle Aerotático no Espaço Aéreo Brasileiro.

A gerência desse sistema fica a cargo do Departamento de Controle do Espaço Aéreo (DECEA), órgão ligado ao Comando da Aeronáutica.

O que se tem de uma forma geral é a dependência intensa do uso de informações por parte dos controladores e dos gestores do serviço de tráfego aéreo para estabelecer (DECEA, 2010):

- Ações adequadas para cada segmento do espaço aéreo
- As estruturas para o uso eficaz do espaço aéreo - aerovias, procedimentos de subida e descida, delimitação de áreas condicionadas que restringem, proíbem ou alertam sobre possíveis perigos aos aeronavegantes.

- As necessidades operacionais que irão balizar as diversas concepções de empreendimentos para a implantação de órgãos de controle do trafego aéreo, equipamentos-radar, auxílios à navegação aérea, equipamentos de telecomunicação, bem como o dimensionamento de pessoal operacional, dentre outros.
- Os espaços onde os controladores de tráfego poderão prover a separação das aeronaves.

1.9 Sistemas de informação e o tráfego aéreo

O sistema de informações que os controladores de tráfego aéreo usam para controlar aeronaves em vôo ou no solo é um sistema crítico, cujas falhas podem em último caso pôr em perigo a vida de centenas de pessoas. Os objetivos desses sistemas são a minimização dos atrasos, maximização da eficiência aeroportuária e a garantia de segurança dos passageiros e tripulantes (ALTER, 2001).

Segundo Pogianelo e Müller (2008),

> desde os primórdios do controle não-radar até o emprego de técnicas que utilizam a navegação por satélite, muitas fases foram consolidadas no controle de tráfego aéreo. Porém, o gerenciamento e a aplicação de novas tecnologias no espaço aéreo devem ser feitos com embasamento científico, procurando minimizar a possibilidade de falhas no Sistema.

Infelizmente, alguns desses sistemas ainda usam muitas vezes computadores e estações de trabalho (*workstations*) obsoletas e fornecem aos controladores apenas uma parte de todo o potencial de informações que se poderia utilizar em situações normais ou emergenciais. Falhas ocorrem ocasionalmente, fazendo com que os controladores tenham poucas alternativas além de estimar e fazer projeções a partir das últimas informações conhecidas (ALTER, 2001).

De modo geral, porém, a estrutura de serviços de navegação aérea e de controle do tráfego aéreo evoluiu e ficou bem mais complexa, pois, assim como as aeronaves evoluíram ao longo das décadas, também o controle de tráfego aéreo tornou-se uma atividade sofisticada e altamente dependente de tecnologia. Outrora apenas dotados de algumas facilidades automatizadas para melhorar a informação sobre os planos de vôos e das imagens fornecidas

por equipamentos de vigilância radar, os sistemas de controle de tráfego aéreo atuais, sejam de controle de área ou de aproximação, incorporam sistemas com funcionalidades avançadas de tratamento de dados de vôo e de dados de vigilância, comunicações digitais e comutação automática de mensagens, rotinas de identificação de riscos à segurança operacional e de apoio à decisão, entre muitas outras (SIEWERDT, 2008).

1.9.1 Novos Conceitos

Houve uma época, não muito distante, em que se afirmava que para aumentar a capacidade ATC, seriam suficientes novas tecnologias. Nada poderia ser mais enganoso, pois ficou evidente que não é a tecnologia em si, mas o grau em que se a utiliza, que proporciona os ganhos de capacidade com a qualidade requerida. No passado, os avanços tecnológicos davam impulso às operações. Agora as necessidades operacionais devem guiar os desenvolvimentos tecnológicos e deve haver uma decisiva migração dos antigos conceitos de controle de tráfego aéreo (ATC, do inglês *air traffic control service*) para um sistema global e harmonizado de gerenciamento do tráfego aéreo (ATM, do inglês *air traffic management*), com uma inerente transição dos processos decisórios unilaterais para os de tomada de decisão colaborativa e a ampla utilização de recursos automatizados em todos os órgãos operacionais (SIEWERDT, 2008).

Como explica Miyamaru (2008), o termo Controle de Tráfego Aéreo exprimia a noção de uma tarefa necessária e suficiente para proporcionar segurança e eficiência para a operação de aeronaves em nosso espaço aéreo e em nossos aeroportos. Contudo, observou-se nos últimos anos, no Brasil e no mundo, que o aumento do volume de tráfego diminuiu a eficiência das operações, decorrente do descompasso da ampliação da infra-estrutura aeroportuária.

Segundo dados da ANAC, a velocidade média de vôo diminuiu 12% entre 1997 e 2007, mesmo com a utilização de aeronaves mais modernas, e isso está associado a atrasos e aumento de custos, que são prejudiciais aos passageiros e para toda a economia do país (MIYAMARU, 2008).

Já prevendo essa dissonância, a OACI - Organização de Aviação Civil Internacional (OACI), agência especializada das Nações Unidas, da qual o Brasil é um dos países-membros, promulgou em 1998 o documento denominado Plano Global de Navegação Aérea para os Sistemas CNS/ATM, Doc. 9750. Dessa forma, os atores do transporte aéreo civil passaram a

se conscientizar de que o conceito de ATC não era mais suficiente para proporcionar segurança e eficiência e, mais do que isso, é preciso planejar e executar um processo de Gerenciamento de Tráfego Aéreo (*Air Traffic Management* – ATM), onde imprevistos passam a ser mais bem administrados, e procura-se um aumento contínuo da eficiência de utilização dos recursos existentes (MIYAMARU, 2008; SIEWERDT, 2008).

As novas tecnologias CNS e o mencionado Conceito Operacional ATM Global ensejam alterações marcantes na tradicional forma de prover os serviços de navegação aérea. A transição e implementação do novo sistema, visando à segurança e à eficácia das operações, requerem, entre outras, a disponibilidade de avançadas funções automatizadas e a aplicação de considerações e conhecimentos em matéria de princípios de fatores humanos.

Nesse contexto de melhorias, outro conceito que vem se estabelecendo é o de *Aeronautical Informations Management* (AIM). Segundo Silva (2009),

> esse termos refere ao fornecimento de informações aeronáuticas com qualidade assegurada, de forma a atender as necessidades dos sistemas de gerenciamento de tráfego aéreo. O AIM é uma abordagem global para prover informações aeronáuticas. É referenciado como um ambiente de rede (*network-centered*) ou ainda *information centered* (centrado na informação).

O objetivo estratégico desse ambiente é disponibilizar uma estrutura lógica de compartilhamento de informações uniforme e eficiente, de forma a suportar todas as fases de vôo. O AIM se diferencia do atual Serviço de Informações Aeronáuticas (AIS) na medida em que se afasta da mera gestão e disponibilização de produtos obtidos de forma semi-automática e busca, através da interoperabilidade digital de informações, abranger todas as fases do vôo, inclusive entre entidades internacionais (SILVA, 2009).

Esta interoperabilidade é buscada através de novos padrões para normalizar o modelo de troca de informações aeronáuticas para integrar informações de diversos sistemas, como o sistema de informações aeronáuticas (AIS), MET (serviço de meteorologia), Informação Civil, Informação Militar e ATFM (*Air Traffic Flow Management*) (SILVA, 2009).

Além da preocupação com a interoperabilidade, deve-se assegurar a persistência e a entrega da informação aos usuários corretos. Isto pode ser feito através de servidores e canais de comunicação redundantes, funções de validação e através de mecanismos de controle de acesso, por exemplo. A informação aeronáutica é um componente crítico para a evolução dos sistemas de gerenciamento do trafego aéreo. O acesso a informações aeronáuticas de alta

qualidade e no m omento certo são fatores funda mentais para o sucesso destes sistem as (SILVA, 2009).

Pode-se dizer, então, q ue a im plementação do AIM atin girá os seg uintes ob jetivos (SILVA, 2009):

- Digitalizar todo o fluxo de inform ação entre fonte e usuários, en tregando informação 100% dig ital em tem po real den tro de um padrão in ternacional d e troca de informações aeronáuticas;
- Manter um sistema de gestão de qualidad e certificado p ara dados e inform ações aeronáuticas;
- Estabelecer um processo de auditoria, que garanta a integridade das informações desde a fonte até a distribuição;
- Atender às expectativ as do clien te no que se refere ao fornecimento de informações aeronáuticas;
- Cumprir os requisitos inte rnos do Estado, concernentes aos produtos de dados e informações aeronáuticas.

1.10 Considerações sobre o capítulo

É indiscutível que o uso de SI no am biente de contro le de tráfego aéreo to rna-se essencial para atender à de manda crescente. Nesse sentido é preciso investir não só e m tecnologia, mas em formas e conceitos para m elhorar o sistem a de controle do tráfego aéreo. Essas mudanças já vêm sendo estudadas e precisam ser incorporadas nos sistem as, mas o fato é que só estarão plenamente estabelecidas em médio prazo.

O que não se pode é negligenciar os atuais sistemas e admitir seus prejuízos até que a transição para novos padrões seja feita. Al ém disso, a preocupação com a segurança e eficiências dos sis temas deverá s er acen tuada num contexto de in tegração global e automatismo que se pretende. As deficiências de gerenciam ento atua is, portanto, devem ser verificadas para que não se perpetuem as ineficiências e perdas.

ESTUDO DE CASO

Este capítulo apresenta uma descrição da organização estudada, considerações sobre os SIs presentes, bem como resultados da análise sobre a auditoria e segurança de sistemas de informação no ciclo operacional do órgão em questão.

1.11 Descrição da Organização

A organização estudada é uma torre de controle de tráfego aéreo. Como todas as torres,

> fornece o serviço de controle de aeródromo às aeronaves nas fases de manobra, decolagem, pouso ou sobrevôo de aeródromo. Visa principalmente evitar colisões com outras aeronaves, obstáculos e veículos movimentando-se no solo. A área de jurisdição abrange o circuito de tráfego e a área de manobras do aeródromo (DECEA, 2010).

Presta o serviço de controle de aeródromo para um aeroporto de 1ª categoria do Nordeste, em se tratando de movimentação operacional, segundo classificação da INFRAERO. Segundo dados divulgados pela INFRAERO, o número de pousos e decolagens (sem contar os vôos militares) ultrapassou 66 mil no ano de 2009.

Vale salientar que se trata de um órgão que não presta serviço de vigilância radar pela própria característica do local sob o qual tem responsabilidade: o aeródromo e seu entorno, área em que a visualização das aeronaves deve ser direta.

Para a prestação do serviço, faz interação com outros dois órgãos que também prestam o serviço de tráfego aéreo:

- Centro de Controle de Aproximação (APP): Provê o Serviço de Controle de Aproximação às aeronaves que estejam executando procedimentos para chegar ou partir do aeródromo. Visa, sobretudo, a separação de outras aeronaves ou obstáculos geográficos. A área de jurisdição do APP é o espaço aéreo denominado Área de Controle de Terminal (TMA) ou Zona de Controle (CTR).
- Centro de Controle de Área (ACC): Fornece o Serviço de Controle de Área às aeronaves quando elas já estão no vôo em rota, a fim de garantir a separação entre as mesmas com segurança. A área de jurisdição do ACC é o espaço denominado Região de Informação de Vôo (FIR). Essas regiões são estabelecidas abrangendo diversas Áreas de Controle de Terminal (TMA) e rotas de vôo, denominadas aerovias.

O órgão em estudo tem três posições operacionais, cujas atribuições dos operadores estão descritas a seguir:

- Operador da posição "torre" (TWR):
  - prestar os serviços de controle de tráfego aéreo, de informação de vôo e de alerta aos tráfegos de aeródromo, bem como prestar os serviços de informação de vôo e de alerta a todas as aeronaves que houverem dado conhecimento do seu vôo;
  - dar início ao plano de emergência do aeródromo e coordenar as ações necessárias em cada situação de emergência.
- Operador da posição "solo" (GND)
  - acumular as funções de controle solo (GND) com as de autorização de tráfego (CLR);
  - obter do ACC-RF e do APP-RF, conforme o caso, as autorizações de plano de vôo;
  - coordenar com o APP-RF as saídas de aeronaves com plano de vôo VFR;
  - manter controle sobre as viaturas e pessoas na área de manobras;
- Operador da posição "assistente" de TWR
  - manter o ACC, o APP, o Supervisor do Aeroporto e as salas de informação aeronáutica (salas AIS) permanentemente informados das condições meteorológicas e operacionais do aeródromo;
  - fazer as coordenações necessárias com o APP e/ou com o ACC, conforme o caso, para se conseguir o maior número de pousos e decolagens com o menor tempo possível de espera para as aeronaves;
  - atender as ligações telefônicas externas, internas e operacionais;
  - manter o APP-RF informado da seqüência para decolagens e das aeronaves que estejam prestes a decolar;
  - informar os horários reais de decolagem das aeronaves aos órgãos envolvidos

A rotina operacional do órgão em estudo pode ser resumida de forma simples como descrita a seguir:

- Para tráfegos que chegam.
  - O APP tendo previamente feito a transferência de controle, transfere as comunicações e a aeronave faz o primeiro contato com a TWR.
  - A TWR, tendo feita a devida coordenação com o APP, autoriza a aeronave para o pouso direto, ou para o circuito de tráfego.
  - Após o pouso, a TWR transfere o controle da aeronave para o GND para instruções de táxi.
  - O "solo" autoriza o táxi da aeronave até o pátio.
  - O assistente coordena com fiscal de pátio a posição do estacionamento da aeronave, quando não houver informação automática do SGTC.
- Para tráfegos que saem
  - Se o piloto da aeronave fizer contato com o GND a mais de 5 min. para início de acionamento, será informado do *take-off data*, caso não tenha acusado o recebimento da mensagem ATIS atual, procedimento de saída previsto (SID), e será instruído a informar quando a 5 min. para o acionamento e *push-back*.
  - Quando a 5 minutos para o *push-back* e acionamento, o controlador do GND faz a solicitação de autorização do plano de vôo (FPL) ao APP-RF ou ACC-RF conforme o caso;
  - É transmitida a autorização ao piloto, que é instruído, após o cotejamento, a informar quando pronto para o *push-back* e acionamento.
  - Quando o piloto informa pronto para o *push-back* e acionamento, o controlador do GND autoriza, tão logo seja possível, o *push-back* em coordenação com os balizadores e o acionamento dos motores.
  - O piloto informa pronto para início de táxi e o GND autoriza o táxi e o assistente procede à coordenação da seqüência de decolagem com o APP ratificando a SID, o nível de vôo (FL) autorizado e o limite de

autorização.

- A TWR autoriza a decolagem, tão logo seja possível.
- O assistente informa a decolagem ao ACC-RF ou APP-RF, conforme o caso.

Será considerado nesse caso apenas o ciclo operacional do órgão e os SIs envolvidos. Dessa forma, SIs relacionados a outras áreas, como o setor administrativo ou serviço meteorológico, não serão contemplados nesse primeiro momento.

A seguir serão destacados os sistemas analisados nesse trabalho.

1.11.1 SGTC

O Sistema de Gerenciamento de Torre de Controle é um sistema desenvolvido para auxiliar os controladores de tráfego aéreo nas suas tarefas nos órgãos ATS, através de recursos de automação, reduzindo ou eliminando certas atividades manuais repetitivas e possibilitando o intercâmbio de dados entre os mesmos, seja através de fichas de progressão de vôo eletrônicas ou tabelas de dados, tornando as operações aéreas mais ágeis e seguras.

Algumas características do sistema:

- O sistema tem por objetivo permitir que o uso de comandos simplificados e menus inteligentes exigindo, portanto, pouca ação dos operadores para com o mesmo, liberando-os para o exercício de suas atividades-fim, além de proporcionar recursos adicionais, tais como: extração de dados para fins estatísticos, emissão de mensagens ATS automatizadas e geração de relatórios inclusive para cobrança de tarifas e pesquisa de movimento de aeronaves.
- Além de realizar transferências automáticas de fichas de progressão de vôo eletrônicas entre as posições operacionais do órgão, o SGTC permite facilidades como: tabela de nascer e pôr do sol, cronômetro regressivo, geração automática de mensagem ATS, preenchimento de livro de registro de ocorrências e tela de *briefings* operacionais, etc.
- O SGTC tem como interface, externamente, a Rede de Telecomunicações Fixas Aeronáutica (AFTN), por meio do aplicativo INFRAEROCOM, pelo qual

recebe as mensagens ATS endereçadas ao órgão usuário, g erando as ações de criação, modificação ou cancelam ento de fichas de progress ão de vô o eletrônicas apresentadas aos operado res. Para is so existe u m Receptor CCAM, que é a interface que recebe as m ensagens enviadas ao órgão ATS, por m eio do Centro de Com utação Autom ática de Mensagens (CCAM) e transform a em dados compatíveis com o SGTC, encam inhando-as, automaticamente, à posição operacional correspondente do sistem a do referido órgão. Os dados dos planos de vôos apresentados pelo s pilotos nas sala s AIS, por exem plo, são recebidos pelo recep tor CCAM. Além do tratam ento dos dados pelo INFRAEROCOM, ficam disponíveis para cons ulta textual através do SGTC os dados brutos caso seja necessário.

- A geração de um a ficha de progre ssão d e vôo eletrônica pode ocorrer automaticamente pelo recebimento das mensagens FPL, FPVD, FPVA ou FPVT ingressadas via CCAM. Pode també m ser originada de um Plano de Vôo Repetitivo, presente na base de da dos RPL l ocal e despertado no mom ento adequado ou, ainda, por uma criação manual, mediante ação do operador.
- Uma vez criada, a ficha de progressão de vôo eletrônica é tran sferida entre os módulos das posições operacionais do órgão ATS, ao com ando dos operadores, na m edida em que o tráfego em que stão evolua entre as áreas d e responsabilidade de cada posição.

1.11.2 ATIS

É um sistem a automatizado de infor mações de área term inal que transmite ininterruptamente em inglês e portuguê s, em freqüência VHF específica, mensagens gravadas que contêm as condições operacionais do ae ródromo, como pista em uso, temperatura, condições clim áticas, procedim ento de descida, restrições ope racionais, avisos, etc. A s mensagens são sempre verificadas e atualizadas:

a) quando há um a alteração em um dado si gnificativo, como, por exemplo, pista em uso, procedimento de descida ou ajuste de altímetro;

b) quando há um a mudança significativa em qualquer um dos parâm etros, como, por exemplo, visibilidade, intensidade do vento ou temperatura;

c) para inclusão ou exclusão de informações;

d) dentro de sessenta minutos a contar da última atualização.

1.11.3 Repetidora X-4000

É um equipamento de visualização do tipo *Bright Display* com capacidade de repetir as informações de radar de vig ilância com a finalidade de auxiliar o planejam ento e a coordenação referente aos tráf egos operando na área de res ponsabilidade de um órgão de serviço de tráfego aéreo (ATS).

O objetivo dessas inform ações radar é possibili tar ao controlador de tráfego aéreo em um órgão de controle que não presta serviço radar com o a Torre de Controle obter um a visão antecipada das aeronaves que lh e serão transferidas para o p lanejamento do tráfego aéreo do seu loca l d e jur isdição, bem como possibilita r a utilização de um recurso adicional nas coordenações de tráfeg o. Por coordenação de tráfego deve-se en tender o intercâm bio de informações entre órgãos ATS ou entre posições operacionais de um mesmo órgão ATS, com a finalidade de assegurar a continuidade da prestação dos serviços de tráfego aéreo.

Esses equipam entos de visualização repr oduzem a i magem dos dados radar de form a semelhante àquela apres entada n a console do órgão que presta serviço de vig ilância r adar, porém tal im agem não garante, para o órgã o que faz uso do equipam ento repetidor, os critérios de conf iabilidade, dispon ibilidade, ac uracidade e integ ridade necessá rios ao uso efetivo dessas inform ações radar no controle do tráfego aéreo. Isso quer dizer que serão utilizados s omente no planejam ento e nas c oordenações ATS pertinentes e não implicarão mudanças do tipo de serviço prestado no órgão us uário (ou seja, não deixa de ser um órgão não-radar).

1.12 Resultados observados

Neste ponto, são destacadas algum as observações e conclusões feitas a partir da análise dos sistem as. Para tanto, f oi observada a rotin a de utiliza ção dos sistem as, f oram colhidos relatos dos usuários, bem como os registros dos últimos 12 meses contidos no livro de registro de ocorrências do órgão (LRO) referentes aos sistemas analisados. Apenas para m elhor entendimento, as explicações es tão agrupada s por sistem a e ao fim são feitos outros comentários de caráter geral.

1.12.1 SGTC

Não são feitas auditorias nos sistem a de pois de im plementados para acom panhar seu funcionamento e verificar m udanças que sejam necessárias. Uma evidência disso está no fato de dados de planos de vôo sim plificado (tam bém conhecido com o notificação de vôo) não gerarem uma ficha de progressão de vôo eletrônica (*strips*) nas *workstations* do S GTC. Os operadores têm de fazer um a consulta ao s dados bru tos do CCAM e criar a ficha manualmente. O que os usuários perceberam na prática é que há um problema no sistema em que apenas dados inseridos para um plano de vôo com pleto geram a ficha corretam ente no SGTC.

Como não há previsão pra que modificações no software sejam feita, tem -se usado como alternativa o envio dos planos sim plificados com o planos com pletos para os tráfegos militares. N o entan to, p ara a avia ção civil, in serir d ados d essa f orma im plicaria tarif ação maior a ser cobrada das em presas, visto que para um a notificação de vôo as tarifas são menores que para um plano de vôo completo.

Por conta ainda desse problem a no tratam ento dos dados, muitas vezes havia demora em solicitar autorização e coor denar alguns tráfegos, já que os controladores só descobriam que faltava um plano quando os pilotos já chamavam prontos pela fonia. Diante disso a chefia instruiu os operadores de infor mação aeronáutica (AIS) a ligar para o órgão de controle assim que receberem as notificações de vô o para verificar se os dados já constam no CCAM e pedir que os controladores criem logo as fichas de vô o para fazer as coordenações com os dem ais órgãos. Houve, portanto, aumento na carga de trabalho por esse problema nos SIs.

Ainda com relação às *strips* eletrônicas, verifica-se que o tam anho de alguns campos destinados à exibição da rota de vôo não são m ais suficientes. Houve um a mudança nos procedimentos operacionais, mas os sistem as não foram revistos. Anteriorm ente o Centro de Controle apenas autorizava a rota do vôo até u m lim ite, que nem se mpre era o destino. Atualmente ele tem de autorizar até o destino e informar toda a rota mesmo depois de sua área de jurisdição. Além desse caso, há vôos cujas rotas são realmente longas (vôos de treinamento militar, circuitos de vôo fechado que passam por mais de um aeródromo, etc.). Dessa forma, o campo para rota, que anteriorm ente comportava a maioria das informações necessárias para o operador do órgão de controle em questão, não é m ais suficiente hoje. As fichas criadas n o SGTC apresentam a rota incom pleta e os ope radores sempre que preciso têm de consultar manualmente o CCAM para checar inform ações detalh adas e acrescentá-las nu m cam po

genérico que consta na *strip*.

Outras informações que também não aparecem automaticamente nas fichas eletrônicas e que os operadores necessitam constantemente consultar no CCAM incluem : tempo estimado de vôo, número de pessoas a bordo.

Não existem procedimentos de *backup* ou redundância de sistemas. Um dos bancos de dados do SGTC, o TABLES, por exemplo, não é armazenado para casos de danos aos arquivos originais. Caso ocorra um problema, informações de aeronaves, procedimentos de saída, e outros dados que são gravados para facilitar o uso diário do sistema não serão recuperados e o restabelecimento dessas informações será difícil.

Não se busca a eficiência no uso dos SIs disponíveis. Módulos de supervisão e gerenciamento são subutilizados ou nem sequer são usados. A melhoria e integração desses módulos evitariam, por exemplo, que operadores tivessem que, diariamente às 00:00Z, salvar relatórios de movimentação em formato de texto e copiar via disquete de um computador para outro para enviar aos órgãos de gerenciamento do DECEA. É uma tarefa improdutiva que evidencia a pouca preocupação com o uso pleno dos sistemas.

A ligação do SGTC com os módulos desse sistema que são utilizados pela administração do aeroporto é feita por rede sem fio (*wi-fi*). A distância da antena do órgão e a do receptor no aeroporto está muito próxima do limite de funcionalidade da tecnologia. Por vezes, verificaram-se quedas no sistema que são ocasionadas por esse uso próximo do máximo permitido. A alternativa de ligação por cabos, que minimizaria também problemas de quebra de segurança no acesso à rede sem fio, vem sendo postergada visto que dependeria de obra bastante dispendiosa.

De toda forma, essas e outras questões de infra-estrutura precisam ser mais bem acompanhadas, pois, pelo que se observa, não há um adequado planejamento da utilização dos recursos de TI.

Recomendações

Da análise desse sistema, recomenda-se que a organização:

- Implemente a auditoria de sistemas de informação para a avaliação do estado atual dos sistemas e análise de desempenho dos mesmos. Dessa forma poderá realizar melhorias para corrigir problemas que hoje afetam a eficiência dos SIs, bem como revisar requisitos de negócio decorrentes de mudanças nas rotinas

operacionais.

- Treinar demais funcionários para utilizar os módulos gerenciais do sistema que hoje estão subutilizados.
- Estabelecer procedimentos de salva-guarda de dados para os casos em que seja necessário recuperar-se de perdas ou danos ao sistema.
- Avaliar a infra-estrutura de TIC utilizada para garantir tempos de resposta e nível de disponibilidade adequados.

1.12.2 ATIS

Planejamento da manutenção e da continuidade dos processos é deficiente. Uma evidência disso ocorreu no início do ano. O ATIS (sistema automático de informações de terminal), que veicula via rádio as informações meteorológicas e de operação do aeródromo ficou inoperante por quase dois meses. A demora no restabelecimento se deu pela falta de equipamento com sistema operacional adequado para instalar o programa do ATIS novamente, já que a versão necessária não era mais comercializada e a organização não dispunha de equipamento com o sistema instalado de fácil acesso.

Mesmo após conseguir novo computador, detectou-se um problema no *hardware* que faz a interface entre a CPU e a transmissão rádio VHF. Não havia sobressalentes de fácil acesso. Também houve problema para configurar o programa novamente e recompor a base de dados dos arquivos de áudio referentes às informações do aeródromo específico.

Ainda sobre o ATIS, verificam-se possibilidades de melhoria caso sejam adotadas soluções mais modernas. O sistema utilizado é uma solução particular, feita por alguns controladores que tinham conhecimento de eletrônica e desenvolveram o sistema no final da década passada. Não existe, portanto, uma empresa que possa prestar suporte, nem fornecer *upgrades*.

No mercado já estão disponíveis soluções profissionais que fazem, por exemplo, a coleta automática de informações meteorológicas e se interligam com os demais sistemas do órgão de controle para permitir o uso de uma interface única e evitar a necessidade de intervenção manual constante dos operadores para atualizar as mensagens. Esse novo sistema já é usado em poucos aeroportos, como o Galeão e Fortaleza, mas não foi divulgado nada sobre qualquer plano de implementação disso outras torres em um horizonte próximo.

Recomendações

Das observações do sistema ATIS, sugere-se que a organização:

- Estabeleça planos de gerenciamento que garantam a continuidade dos sistemas.
- Identifique e implemente soluções automatizadas para aumentar a eficiência dos serviços

1.12.3 Repetidora X-4000

Não há preocupação com a interoperabilidade dos SIs internamente e nem mesmo entre os demais órgãos. Esse fato é ratificado por resultados de auditorias realizadas pelo TCU quando tratava do sistema de visualização radar X-4000 presente em outros órgãos de controle. Um dos fatos é que:

> com a implantação do SGTC, os operadores das torres de controle deixaram de realizar as entradas de dados nas consoles do sistema X-4000 lá localizadas. Como o SGTC não possui integração com o sistema X-4000, os controles de aproximação deixaram de receber informações importantes para o planejamento das saídas das aeronaves, o que gera retrabalho e aumento das coordenações entre a torre de controle e o respectivo centro de controle de aproximação (TCU, 2008).

Dessa falta de integração, percebe-se um prejuízo no órgão em estudo. Ligado à repetidora do X-4000 utilizada no órgão estudado, existe uma impressora de fichas de progressão de vôo (conhecida como 'stripadeira'), da qual não se faz uso normalmente, visto que a fichas são manuseadas por meio eletrônico. Sua função, em verdade, é possibilitar diante de falhas do sistema eletrônico, a impressão automática das fichas das aeronaves que estavam sob controle. Para o órgão em questão, contudo, como as informações colhidas para impressão vêm do X-4000 e não estarão sincronizadas com as do SGTC, as fichas impressas serão inúteis. Os operadores terão de recriar então as fichas em formulários de papel à caneta, ficando inadequada essa função de contingência do sistema para o órgão em estudo.

Recomendações

Verificando os aspectos relacionados à repetidora X-4000, percebe-se que a organização precisa, por meio da alta administração:

- Gerenciar melhor os investimentos em TIC e os projetos de SI para garantir que todos os recursos adquiridos sejam plenamente utilizáveis e que todos os equipamentos e sistemas estejam integrados de forma adequada.
- Gerenciar as mudanças.

1.12.4 Comentários gerais

Não há controle de acesso efetivo e formalmente estabelecido no órgão. As ações são isoladas e não refletem uma política de segurança instituída. Computadores da *workstation* do SGTC estão vulneráveis a infecções, visto que os antivírus instalados há muito não recebem atualização. O uso de mídias de armazenamento externo não é controlado.

Percebe-se uma atitude reativa às falhas. O DECEA, por meio de instrução do comando da aeronáutica - ICA 66-22: Gerenciamento de Inoperâncias no SISCEAB - assume uma posição apenas reativas às falhas. No documento existe a preocupação apenas com a manutenção corretiva do sistema e não há de plano de contingência formal para os ativos de informática e continuidade dos serviços, pois não descrevem procedimentos a serem adotados para restauração do sistema que garanta o restabelecimento das atividades de pronto e reduza as conseqüências e danos em caso de incidentes (DECEA, 2009; TCU, 2008).

Essa postura pode ser verificada em um dos fatos ocorridos quando a rede interna (INTRAER) que faz a intercomunicação de uma das *workstation*s presentes no órgão esteve fora por um período de quase 20 dias. Ficam comprometidos às consultas a informações aeronáuticas veiculadas pela AISWEB, que são feitas usando-se essa intranet. A comunicação interna por e mail com outros setores também ficou indisponível, dessa forma, a versão eletrônica do livro de registro de ocorrências (LRO) que é enviada diariamente à chefia do órgão não estava sendo encaminhada, diminuindo a presteza com que providências pudessem ser tomadas diante das necessidades. Não havia uma alternativa, e teve-se de esperar a manutenção corretiva. Percebe-se a falta de uma rede paralela ou redundante para assegurar a continuidade dos processos.

Ainda sobre manutenção e preocupação com a integridade e continuidade dos serviços, verifica-se que não há controle de acesso, sobretudo com relação a funcionários terceirizados, para evitar, por exemplo, danos aos recursos de TI inadvertidamente. Um problema desse tipo foi registrado quando operários que estavam executando reparos na edificação fizeram uso

incorreto de um ponto de fornecimento de energia elétrica. O ponto utilizado não suportava a intensidade de corrente elétrica da ferramenta que os trabalhadores queriam utilizar e pertencia a um ramo que alimentava roteadores do sistema de informações. Houve uma queda temporária no fornecimento para os equipamentos ligados àquele ramo e paralisação do sistema até que todos os equipamentos tivessem sido ligados em outro ramo.

Publicações aeronáuticas presentes apenas em formato eletrônico não tem uma versão impressa disponível para consulta em caso de danos a esses arquivos ou indisponibilidade de acesso ao meio eletrônico. Também não há controle de atualização dessas informações. Grande parte desses arquivos é copiada da rede AISWEB, mas não há uma prática de verificação de mudanças e atualizações dos arquivos para disseminar as informações mais atuais para as estações de trabalho dos operadores.

O órgão conta com ao menos três linhas telefônica de acesso externo, cujas comunicações e informações transmitidas não são devidamente controladas. Do relato dos operadores do órgão, observa-se que muitas das ligações recebidas não são relacionadas com o serviço de controle de tráfego aéreo diretamente. Essas chamadas poderiam ser filtradas inicialmente por um profissional adjunto que verificaria o teor das chamadas.

E, como uso de linhas externa não pode ser evitado, é importante também haver um treinamento adequado dos operadores para identificar possíveis golpes de engenharia social. Indivíduos mal intencionados podem usar esses canais de comunicação fazendo se passar por pessoas legítimas e, por meio da enganação ou exploração da confiança dos usuários, fornecerem informações falsas, que de alguma forma comprometam o serviço, ou realizar algum outro tipo ação enganosa para obter acesso a informações importantes ou sigilosas da organização e dos sistemas.

As comunicações com trabalhadores de solo e outros setores da administração do aeroporto é feito via rádio analógico. Essas mensagens podem ser facilmente interceptadas devido às próprias brechas tecnológicas do sistema. Não há controle, nem gravação das mensagens, caso seja necessário em alguma investigação futura.

A própria comunicação rádio aeronáutica por ser transmitida abertamente via rádio VHF, deve ser levada em consideração na avaliação de requisitos de segurança. Há relatos de ações criminosas que ocorrem na área de pátio de aviação geral, em que os assaltantes acompanhavam as informações repassadas a aeronaves que se sabia estar transportando valores. O pátio em que as aeronaves costumavam estacionar nesses casos tinha uma segurança deficiente e tudo contribui para o evento indesejado.

Desde então as aeronaves em transporte de valores são direcionadas ao pátio de aviação comercial, mais seguro, e as mensagens dos controladores e pilotos usam de termos para disfarçar o caráter da operação daquelas aeronaves.

A partir desse fato, pode-se observar que a falta de análise do caráter das informações veiculadas e a preservação da privacidade de determinados dados pode gerar prejuízos indesejados. Não se pode esperar que medidas sejam tomadas apenas após a ocorrência de problemas. Deve-se, portanto, fazer um estudo maior para contemplar outras situações que ainda não foram tratadas.

Recomendações

De forma geral, são resumidas a seguir outras recomendações que podem ser feitas:

- Avaliar e gerenciar melhor os riscos de TI e os requisitos de segurança de informação relacionados aos SI utilizados na organização.
- Controlar o acesso às instalações, estabelecer controles físicos e gerenciar o serviço prestado por terceiros para garantir a segurança dos recursos de TI e a operação dos sistemas.
- Estabelecer controles e correções para as vulnerabilidades dos sistemas e das plataformas em que eles funcionam.
- Avaliar aspectos relacionados ao ambiente externo (e gerenciar os canais de comunicações) que podem afetar o desempenho dos usuários ou comprometer a privacidade de informações (interferências na realização das atividades ou golpes de engenharia social).

1.13 Considerações sobre o capítulo

Neste capítulo foi apresentado o estudo de caso objeto desse trabalho. Inicialmente, descreveu-se a organização e o ciclo operacional desse órgão de controle de tráfego aéreo. Depois disso, a partir da análise dos SIs utilizados dentro do contexto em questão, percebeu-se a importância de tratar a segurança e a auditoria desses sistemas. Por fim, foram identificadas algumas oportunidades de melhoria.

Mesmo que de forma preliminar, dado o escopo restrito das observações feitas aqui, pode-se estabelecer que o nível de maturidade da organização nesse âmbito fica entre o inexistente e o inicial. Isso significa que os processos para assegurar a segurança e realizar

auditorias nos sistemas não foram implementados ou são realizados sem organização e de modo não planejado.

A partir desses resultados, é preciso que a organização realize as melhorias e que os gestores reconheçam que a segurança e eficiência dos sistemas de informação devem fazer parte da operação do negócio da organização.

CONSIDERAÇÕES FINAIS

Este capítulo apresenta as conclusões em relação ao desenvolvimento deste trabalho de conclusão de curso e as limitações e sugestões para o desenvolvimento de trabalhos futuros.

1.14 Conclusão

De uma maneira geral, a partir desse trabalho e da leitura de outros estudos e relatórios de outros países, conclui-se que é preciso maior nível de transparência e adoção de regras de governança para os sistemas utilizados no controle de tráfego aéreo brasileiro, nesse caso representado pelo órgão de controle alvo do estudo. (MCKINSEY & COMPANY, 2010; TCU, 2008; US GAO, 1998; US DOT, 2008, 2009)

Conforme se verificou nesse texto, legitimado pelas observações do TCU e m outros órgãos, o tratamento da segurança da informação é a área mais crítica no âmbito da governança de TI dentro da administração federal (TCU, 2009).

É um aspecto em que se precisa induzir o processo de aperfeiçoamento da governança de TI. Para isso o TCU, que já realizou algumas auditorias em outros órgãos do SISCEAB, figura como ente relevante para o papel (TCU, 2008).

No caso do controle de tráfego aéreo brasileiro, viu-se nesse estudo que não há nem mesmo indícios de que sejam feitas auditorias internas nos sistemas. Essa falta de preocupação com a transparência e com a exigência de melhor gestão, sem dúvida, compromete a eficiência e segurança dos SIs.

A análise inicial presente nesse texto deve servir para abrir caminhos para o entendimento do momento da Gestão de TI e busca pela Governança Corporativa num universo bem maior que o próprio órgão estudado.

Vem ao encontro da nova visão que vem sendo adotada em muitos outros órgãos do governo para tentar recuperar o tempo e investimentos perdidos por anos sem profissionalização e preocupação com resultados de seus sistemas. A reestruturação do ambiente de SI na organização se faz necessária e todas as entidades que compõem este complexo sistema de controle de tráfego aéreo e de informações aeronáuticas devem trabalhar juntos, buscando soluções otimizadas e agregando valor aos seus serviços (TCU, 2008; SILVA, 2009).

1.15 Limitações e sugestões para Trabalhos Futuros

Este trabalho teve o foco apenas no ciclo operacional de um órgão de controle. Como os sistemas de informações dessa organização fazem parte de um sistema maior que compõe todo o sistema de controle de tráfego aéreo brasileiro, devem-se desenvolver análises do ambiente como um todo.

O que se propõe é uma análise mais complexa que não caberia neste trabalho, mas da qual se pode esperar grande melhoria com a sua consecução. É preciso que a organização estruture um modelo de Governança da Segurança da Informação como parte do controle interno e políticas que façam parte da Governança Corporativa.

As observações contidas nesse texto foram em grande parte coletadas a partir de relatos e registros dos usuários. Foram poucos os testes com análise de entradas e saída, devido à limitação de acesso. Em trabalhos futuros, o engajamento e motivação da gerência permitirão verificações mais aprofundadas e o desenvolvimento de estudos mais completos.

Referências Bibliográficas

ALMEIDA, A. T.; COSTA, A. P. C. S.; DE MIRANDA, C. M. G. Inform ação e Gestão. In: ALMEIDA. A. T.; RAMOS, F. S. (Org.). **Gestão da Informação na Competitividade das Organizações.** 2ª ed. Recife: Ed. Universitária da UFPE, 2002.

ALTER, S. **Information systems: foundation of e-bussiness.** 4th ed. New Jersey: Prentice Hall, 2001.

ANAC. **ANAC aprova concessão para Noar Linhas Aéreas, de Pernambuco**. Assessoria de Im prensa. 17 de m aio de 2010a. Disponível em : <http://www.anac.gov.br/ imprensa/AnacAprova.asp> Acesso em 26 mai. 2010.

___. **Dados Comparativos Avançados**. Assessoria de Im prensa. Abril, 2010b. Di sponível em: <http://www.anac.gov.br/dadosComparativos/ABRIL%202010.xls> Acesso e m: 26 m ai. 2010.

BERNARDES, M. C.; MOREIRA, E. S. Um Modelo para Inclusão da Governança da Segurança da Inform ação no Escopo da G overnança Organizaciona l. In: SIMPÓSIO SEGURANÇA EM INFORMÁTI CA - SSI' 2005, 2005, São José dos Ca mpos. **Anais do Simpósio Segurança em Informática.** São José dos Ca mpos: Paulo Sergio Motta Pires e Clovis Fernandes Torres: CTA/ITA/IEC, 2005.

CASCARINO, R. E. **Auditor's Guide to Information Systems Auditing.** New Jersey: John Wiley & Sons, 2007. Disponível em : <http://www.wiley.com /WileyCDA/WileyTitle/ productCd-0470009896,descCd-google_preview.html> Acesso em: 19 nov. 2009

COSTA, A. P. C. S.; ALMEIDA, A. T. Sistem as de Inform ação. In: ALMEIDA. A. T.; RAMOS, F. S. (Org.). **Gestão da Informação na Competitividade das Organizações.** 2ª ed. Recife: Ed. Universitária da UFPE, 2002.

CUNHA, R . M. **Modelo de governança da segurança da informação no escopo da governança computacional.** 2008. 85 f. Dissertação (Mestrado em Engenharia de Produção). Programa de Pós-Graduação em Engenharia de Prod ução, Univ ersidade Federal de Pernambuco, Recife.

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO – DECEA. **Gerenciamento de Inoperâncias no SISCEAB – ICA 66-22.** Rio de Janeiro, 2009. Disponível em : <http://publicacoes.decea.gov.br/index.cfm?i=publicacao&id=2545> Acesso em : 10 abr. 2010.

___. **Gerenciamento do Tráfego Aéreo.** Rio de Janeiro, 2010. Disponível em : <http://www.decea.gov.br/espaco-aereo/gerenciamento-de-trafego-aereo/> Acesso em : 10 abr. 2010.

DUTRA, A. M. C. Sistemas de Informações Aeroportuárias no Brasil. In: SIMPÓSIO DE TRANSPORTE AÉREO – VII SITRAER, 2008, Rio de Janeiro. **Anais do VII SITRAER...** Rio de Janeiro: Sociedade Brasileira de Transporte Aéreo, 2008, p. 937-956. Disponível em : <http://www.tgl.ufrj.br/viisitraer/anais.html > Acesso em: 10 abr. 2010

JC ONLINE. Agências do Trabalho de Pernambuco só voltam a funcionar segunda. **Jornal do Commercio**, Recife, 19 nov. 2009a. Disponível em : <http://jc.uol.com.br/canal/cotidiano/pernambuco/noticia/2009/11/19/agencias-do-trabalho-de-pernambuco-so-voltam-a-funcionar-segunda-205959.php> Acesso em: 19 nov. 2009.

___. Falha da TAM é responsável por 45% dos voos atrasados no país. **Jornal do Commercio**, Recife, 19 nov. 2009b. Disponível em : <http://jc.uol.com.br/canal/cotidiano/nacional/noticia/2009/11/19/falha-da-tam-e-responsavel-por-45_porcento-dos-voos-atrasados-no-pais-205972.php> Acesso em: 19 nov. 2009.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais.** 7. ed. São Paulo: Prentice-Hall, 2007.

MAIA, G. Governança da Segurança da Informação: Uma proposta de uso combinado do COBIT e da ISO 27002 para sua implementação. 2009. 46 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Produção). Departamento de Engenharia de Produção, Universidade Federal de Pernambuco, Recife.

MARTINS, A. B.; SANTOS, C. A. S. Uma metodologia para implantação de um Sistema de gestão de segurança da informação. Revista de Gestão da Tecnologia e Sistemas de Informação, vol. 2, n. 2, p. 121-136, 2005. Disponível em : <http://www.jistem.fea.usp.br/index.php/jistem/article/viewFile/10.4301%252FS1807-17752005000200002/15> Acesso em: 19 nov. 2009

MCKINSEY & COMPANY. **Estudo do Setor de Transporte Aéreo do Brasil: Relatório consolidado.** Rio de Janeiro: McKinsey & Company, 2010. Disponível em : <http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Navegacao_Suplementar/Destaques/chamada_aereo.html> Acesso em: 20 jun. 2010.

MENDONÇA, M. B. M. **Auditoria de Sistema de Informação:** Uma análise da abordagem utilizada em uma empresa de auditoria e consultoria. 2008. 76 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Produção). Departamento de Engenharia de Produção, Universidade Federal de Pernambuco, Recife.

MENEZES, S. F.; **Proposta de um modelo de avaliação da segurança da informação nas organizações centrada no usuário.** 2008. 60 f. Dissertação (Mestrado em Engenharia de Produção). Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal de Pernambuco, Recife.

MIYAMURU, D. O. Tendências na Evolução dos Sistemas de Gerenciamento de Tráfego Aéreo no Brasil. In: SIMPÓSIO DE TRANSPORTE AÉREO – VII SITRAER, 2008, Rio de Janeiro. **Anais do VII SITRAER...** Rio de Janeiro: Sociedade Brasileira de Transporte Aéreo, 2008, p. XII-XVIII. Disponível em : <http://www.tgl.ufrj.br/viisitraer/anais.html> Acesso em: 10 abr. 2010

O'BRIEN, J. A. **Sistemas de Informação e as decisões Gerenciais na Era da Internet.** São Paulo: Saraiva, 2002.

POGIANELO, M. L.; MÜLLER, C. **Espaço aéreo brasileiro - análise da carga de trabalho dos controladores de tráfego aéreo por meio de simulação "*fast time*" - estudo de caso na terminal Recife.** In: SIMPÓSIO DE TRANSPORTE AÉREO – VII SITRAER, 2008, Rio de Janeiro. **Anais do VII SITRAER...** Rio de Janeiro: Sociedade Brasileira de Transporte Aéreo, 2008, p. 79-91. Disponível em : <http://www.tgl.ufrj.br/viisitraer/anais.html > Acesso em: 10 abr. 2010

SALVADORI, F. Mouse ao alto: o perigo do cibercrime. **Galileu.** Rio de Janeiro, ed. 221, dez. 2009. Disponível em: <http://revistagalileu.globo.com/Revista/Galileu/0,,EDR87249-7855,00.html> Acesso em: 01 mar. 2010

SIEWERDT, E. O Modelo de Controle do Espaço Aéreo Brasileiro e sua Integração com outros Sistemas. In: SIMPÓSIO DE TRAN SPORTE AÉREO – VII SITRAER, 2008, Rio de Janeiro. **Anais do VII SITRAER...** Rio de J aneiro: Sociedade Brasileira de Transporte Aéreo, 2008, p. LVIII-LXIII. Dispon ível em: <http://www.tgl.ufrj.br/viisitraer/ anais.html > Acesso em: 10 abr. 2010

SILVA, G. K. P. Adm inistração de Sistem as de Inform ação na Infraero – Desafio para a gestão d e TI. In: SIMPÓSIO DE TR ANSPORTE AÉREO – VIII S ITRAER / RED IBEROAMERICANA DE INVES TIGACIÓN EM TRANSPORTE AÉREO – II RIDITA, 2009, São Paulo. **Trabalhos apresentados ao VIII SITRAER / II RIDITA...** São Paulo: EPUSP, 2009, p. 47-62. Disponível em : <http://sitraer.pcs.usp.br/Evento/ VIII%20SITRAER%20-%20Anais.pdf> Acesso em: 10 abr. 2010

TCU. **Auditoria no Sistema de Tratamento e Visualização Radar X-4000.** Sumários Executivos - Tribunal de Contas da União; Secretaria d e Fiscalização de Tecnologia da Informação. Brasília, 2008. Disponível em : <http://portal2.tcu.gov.br/portal/page/ portal/TCU/comunidades/tecnologia_informacao/sumarios/sumario-x-4000_miolo.pdf> Acesso em: 15 mai. 2010

___. Levantam entos de infor mações para estru turação da SEFTI. Sum ários Exe cutivos - Tribunal de Contas d a União. Secretaria de Fiscalização de Tecno logia da Inf ormação. Brasília, 2009. Disponível em : <http://po rtal2.tcu.gov.br/portal/page/portal/TCU/ comunidades/tecnologia_informacao/sumarios/Sumario%20Executivo_Levantamento_ estrutura%C3%A7%C3%A3o_Sefti_inte.pdf> Acesso em 15 mai. 2010.

TURBAN, E.; RAINE R JR, R. K.; POTTE R, R. E. **Administração de Tecnologia da Informação:** Teoria & Prática. Rio de Janeiro: Elsevier, 2005.

UNITED S TATES DE PARTMENT OF TR ANSPORTATION – US DOT. Office of Inspector Genera l. **Audit of DOT's Information Security Program.** Washington, D.C., 8 out. 2008. Disponível em : <http://www.oig.do t.gov/item.jsp?id= 2369> Acesso em : 19 nov. 09

___. **Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems.** W ashington, D.C., 4 m ai. 2009. Di sponível em: <http://www.oig.dot.gov/ item.jsp?id=2465> Acesso em: 19 nov. 09

UNITED S TATES GE NERAL ACCO UNTING OFFIC E – US GAO. **Weak Computer Security Practices Jeopardize Flight Safety.** W ashington, D.C, 18 m ai.1998. Disponível em: <http://www.gao.gov/archive/1998/ai98155.pdf> Acesso em: 19 nov. 2009.

WALD, M. L. Backlog of Flight Delays After C omputer Problems. **New York Times**. New York, 19 nov. 2009. Disponível em : <http:// www.nytimes.com/2009/11/20/us/20air.html> Acesso em: 19 nov. 2009

XUEMEI, L.; YAN, L.; LIXING, D. Study on Information Security of Industry Management In: ASIA-P ACIFIC CONFERENCE ON INFORMATION PROCESSING, APCIP 2009, 2009, Shenzhen. **Conference Proceedings…** Shenzhen: Intelligent Information Technology Application Research Associati on, v. 1, p. 522-524. Disponível em : <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5197108&isnumber=5196971> Acesso em: 19 nov. 2009.