ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

Manual de CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA NA AVIAÇÃO CIVIL

MANUAL DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA NA AVIAÇÃO CIVIL

Setembro / **2021**

BASET – SUBGRUPO 4 – SEGURANÇA CIBERNÉTICA

Membros:

ORGANIZAÇÕES	*COLABORADORES*
Aena Brasil	Ana Carla Ramos de Lucena de Melo
Aeroportos Brasil Viracopos	Giovanni Allan Buranello
	Guilherme Dalto
Agência Nacional de Aviação Civil - ANAC	Leandro Costa Pereira Crispim de Sousa
	Luiz Gustavo Silva Cavallari
	Menotti Erasmo da Silva Machado
	Ricardo Nunes
	Rodrigo Pereira Damásio da Silva
Associação Nacional das Empresas Administradoras de Aeroportos - ANEAA	Douglas Rebouças de Almeida
	Mariana Silveira de Menezes
Azul Linhas Aéreas	Jefferson Souza Barbosa
BH Airport	Wesley Dias Santos
Departamento de Controle do Espaço Aéreo - DECEA	CON NS Bernard Souza da Silva
	TC Gerson Monteiro Siqueira
	CL Vanderlei A. Ribeiro
Gol Linhas Aéreas	Sabrina Verônica dos Santos
Latam Airlines Brasil	Christian Coutinho
	Emilio Antonio Cuevas Yañez
	Klaus Brum
Modern Logistics	Eduardo Seindenberger
Salvador Bahia Airport	Gerlan Alves
	Rafael Azevedo
Socicam Aeroporto de Cuiabá	Edjairson da Silva Pereira
	Leonardo Diasda Costa Torres

PROJETO GRÁFICO E DIAGRAMAÇÃO

Assessoria de Comunicação Social (ASCOM)

DÚVIDAS, SUGESTÕES E CRÍTICAS PODEM SER ENVIADAS PARA O E-MAIL

avsec@anac.gov.br

SUMÁRIO

SUMÁRIO

1. DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Este manual tem a finalidade de promover a conscientização sobre cibersegurança ("*cyber security*") para as organizações e indivíduos interessados nos serviços prestados na aviação civil. Desta forma objetiva-se permitir às organizações e indivíduos protegerem-se no uso do ciberespaço da aviação civil. A apresentação de diversos termos e conceitos utilizados no contexto de cibersegurança ajudarão a permitir a conscientização pretendida. Ele possui também o intuito de auxiliar os responsáveis AVSEC da aviação civil a promover e divulgar em suas organizações e junto a seus colaboradores, a importância em zelar pela segurança de seus ativos de Tecnologia da Informação e da Comunicação (TIC). De igual forma, tem o intuito de apresentar aspectos de redes de computadores e dos sistemas através de seus componentes básicos, o que permitirá propor e utilizar as melhores práticas para tratar com cada um deles do ponto de vista de cibersegurança. Ainda, as informações aqui contidas poderão servir de base para a realização de avaliação de risco em cibersegurança para operadores da aviação de forma geral, conforme já previsto no Regulamento Brasileiro de Aviação Civil nº 107 [RBAC 107, 2018] para operadores de aeródromo e no RBAC nº 108 para operadores aéreos [RBAC 108, 2020].

1.2 FUNDAMENTAÇÃO

- Decreto nº 7.168, de 5 de maio de 2010, que dispõe sobre o Programa Nacional de Segurança da Aviação Civil contra Atos de Interferência Ilícita (PNAVSEC).
- Resolução nº 167, de 17 de agosto de 2010 da ANAC, que estabelece diretrizes para o gerenciamento de risco à segurança da aviação civil contra atos de interferência ilícita pela ANAC.
- Regulamento Brasileiro de Aviação Civil nº 107 – RBAC nº 107 – denominado Segurança da Aviação Civil contra Atos de Interferência Ilícita – Operador de Aeródromo.
- Instrução Suplementar nº 107-001 – IS nº 107 – denominada Segurança da Aviação Civil contra Atos de Interferência Ilícita – Operador de Aeródromo, 2019.
- Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética – E-Ciber.
- Lei nº 12.965/2014, de 23 de abril de 2014 - que estabelece o novo Marco Civil da Internet Brasileira (MCI).
- Norma Complementar nº 02/IN01/DSIC/GSI/PR 2008, que define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta, de 13 de outubro de 2008.
- Norma Complementar nº 04/IN01/DSIC/GSI/PR 2013, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta, de 15 de fevereiro de 2013.
- Lei Geral de Proteção de Dados - LPDG, de 14 de agosto de 2018.

1.3 DEFINIÇÕES

Cibernética é a ciência que estuda o controle e o movimento das máquinas e animais. Nos longínquos anos 50, a palavra "*ciber*" foi usada como um sufixo para se referir a termos relacionados à cibernética e, posteriormente, "*ciber*" foi padronizado como "*computadorizado*". Nos anos 90 surgiu o termo *ciberespaço* indicando um espaço virtual que se acredita existir atrás das atividades eletrônicas dos dispositivos computacionais. Hoje em dia, o sufixo "*ciber*" é mais utilizado para introduzir termos relacionados a matérias de segurança da informação.

Ameaça Cibernética ou *ciberameaça* é uma ação perpetrada contra sistemas de Tecnologia da Informação e da Comunicação (TIC) com o objetivo de acesso ilegal ou intrusão utilizando o ciberespaço.

Ataque cibernético ou *ciberataque* é um ataque realizados a sistema de TIC utilizando o ciberespaço como meio.

Autenticação é o processo de verificar se alguém é quem ele afirma ser quando tenta acessar um computador ou um serviço computacional.

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados com a finalidade de invasão.

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

Botnet é uma rede de dispositivos infectada e controlada remotamente por um invasor (*hacker*), utilizada para executar, por exemplo, ataques de negação de serviço distribuída e disseminar e-mails com *spam*.

Bring Your Own Device (BYOD) quando a política de segurança de um órgão permite que alguém conecte a sua rede ou sua estrutura algum dispositivo pessoal como, por exemplo, dispositivos tais como memória *flash* do tipo *Universal Serial Bus* (USB), *notebook*, celulares, *tablets* e outros itens para a execução do trabalho no órgão ou empresa.

Confidencialidade é segurança que garante que uma informação não é divulgada para uma entidade não autorizada.

Contramedida ou *controle* é ação, dispositivo, procedimento ou técnica para reduzir vulnerabilidade e, assim o resultado do ataque, minimizando, prevenindo ou eliminando o dano que ele pode causar.

Crimes digitais próprios ou *puros* são condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático [Crespo, 2015].

Crimes digitais impróprios ou *mistos* são condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc [Crespo, 2015].

Defesa cibernética ou *ciberdefesa* é a defesa realizada contra ciberataque.

Disponibilidade é a garantia que permite que a informação esteja sempre disponível no momento da necessidade de acesso.

Engenharia Social é a ação através da qual uma pessoa persuade outra a executar outras ações, para ter acesso não autorizado a computadores ou informações confidenciais.

Firewall pode ser *hardware* ou *software* que é projetado para impedir o acesso não autorizado a computadores ou redes, a partir de um outro computador ou rede.

Hacker é alguém que viola a segurança de computadores por razões maliciosas, auto promoção ou ganhos pessoais.

Hoax é uma informação falsa, frequentemente transmitida por meios digitais, na tentativa de enganar um grupo de pessoas, fazendo-as acreditar que uma informação falsa é verdadeira, incitando os receptores a realizar transações ou tomar iniciativas, que frequentemente causam danos.

Incidente cibernético ou *ciberincidente* é a ocorrência no espaço cibernético que constitui uma ameaça a cibersegurança.

Infraestrutura Crítica é um sistema ou rede de sistemas que fornecem funções vitais que se interrompidas causam instabilidade socioeconômica, financeira, política, de defesa militar, ou de segurança [Tanbansky, 2011].

Sistema de Detecção de Intruso (Intrusion Detection System - IDS) é um dispositivo ou *software* que monitora uma rede ou sistema contra acessos não autorizados que possam violar a política de segurança do órgão ou sistema.

Integridade é a garantia que a informação e/ou o sistema não são modificados indevidamente e ou acidentalmente durante todo ciclo de vida da informação.

Internet das Coisas (Internet of Things – IoT) é a fusão de dispositivos e sensores através de uma rede de informação para habilitar capacidades autônomas. São encontrados, inclusive, em

sistemas de controle tais como: PLC (Controlador Lógico Programável), SCADA (Sistema de Controle e Aquisição de Dados), DCS (Sistema de Controle Distribuído) [CNPI, 2020].

Jammer são transmissores ilegais de frequência de rádio que causam interferência por saturação e embaraço em comunicações autorizadas.

Malvertising (malicious advertsing) é um golpe que consiste em criar anúncios maliciosos e, por meio de serviços de publicidade, apresentá-lo em páginas *web*.

Malware é um *software* malicioso desenvolvido para infiltrar, danificar, controlar ou desabilitar computadores.

Network firewall é um dispositivo que controla o tráfego de entrada ou saída de uma rede.

Personal firewall é um *software* executando sob um PC (Computador Pessoal – *Personal Computer*) que controla o tráfego da rede deste computador.

Phishing é o método usado por criminosos para obter informações de usuários de Internet, geralmente através do envio de e-mail, por organizações aparentemente legítimas, com o endereço de página eletrônica (URL) falso.

Ransomware é um *malware* que restringe o acesso ao sistema infectado com uma espécie de bloqueio e/ou criptografia, exigindo o pagamento do resgate para que para que o acesso possa ser restabelecido. É também conhecido como sequestro digital de dados.

Risco cibernético ou *ciber-risco* é o risco de um *ciberataque*.

Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Sandbox é uma ferramenta que possibilita a execução de programas suspeitos de forma isolada em ambiente virtual dentro da própria máquina do usuário, permitindo ao usuário analisar seu comportamento de forma segura, sem afetar sua máquina.

Screen scraper vem a ser um vírus ou dispositivo físico que registra informações enviadas para um dispositivo visual para capturar informação privada.

Sistemas de Críticos representam os sistemas essenciais à prestação de serviços à sociedade.

Sistemas Críticos de Tecnologia da Informação e das Comunicações são sistemas críticos que englobam a infraestrutura física de Tecnologia da Informação e das Comunicações (TIC), inclusive os componentes *hardware* e *software*, profissionais e os procedimentos essenciais para a prestação dos serviços à sociedade.

Segurança cibernética ou *cibersegurança* é o estado de proteção contra ciberataques ou qualquer atividade criminosa feita utilizando o ciberespaço como meio. De fato, é um conjunto de ferramentas, políticas, teorias de segurança contra atos de interferência ilícita, capacidades e procedimentos de segurança, práticas de segurança da informação, perícia, gerenciamento de risco e práticas para proteger as organizações do cibercrime [Von Solms e Van Niekerk, 2013].

Spam é uma mensagem eletrônica (e-mail) recebida, mas não solicitada, que possui conteúdo publicitário.

Spear Phishing é um *phishing* mais sofisticado, personalizado para um usuário ou departamento específico de uma organização.

Spoofing é a interferência por dissimulação de autenticação no canal. Um dispositivo se faz passar por outro. O objetivo é roubar dados, disseminar *malwares* ou contornar controles de acesso. Suas formas mais comuns são de IP, e-mail e DNS.

Spyware é o *malware* que monitora, coleta e passa informação sobre as atividades dos usuários de um computador para um local externo sem a autorização ou o conhecimento do proprietário. Alguns são instalados quando o usuário final aceita o contrato de licença para usar *softwares* gratuitos.

Teste de Intrusão (Penetration Test ou Pen Test) é uma ação controlada para avaliar uma ou mais vulnerabilidades através de um ataque simulado sobre um sistema de informação.

Trojan ou *Cavalo de Tróia* é um *malware* que pode entrar em um computador disfarçado como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de forma que usuários mal-intencionados possam invadir um PC.

Vírus é o *malware* que é carregado em um computador e executado sem permissão do usuário ou o conhecimento dos seus efeitos.

Website é o sítio eletrônico formado por um conjunto de páginas digitais da rede mundial de computadores.

Worm é o *malware* que se replica sozinho e pode ser espalhar para infectar outros computadores.

1.4 INFORMAÇÕES COMPLEMENTARES

- Apêndice A: exemplifica um conjunto de alguns ativos críticos que podem estar presentes em organizações da aviação civil;
- Apêndice B: apresenta os 10 (dez) passos para cibersegurança recomendados pelo Centro de Cibersegurança Nacional (NCSC) do governo do Reino Unido;

- Apêndice C: apresenta dispositivos e procedimentos nos quais podem ser realizados os controles de cibersegurança;
- Apêndice D: apresenta 20 (vinte) possíveis controles para sistemas de TIC;
- Apêndice E: apresenta uma Avaliação de Risco considerando o contexto de cibersegurança;
- Apêndice F: apresenta um conjunto de dicas para um usuário acessar seus recursos de TIC com segurança;
- Apêndice G: apresenta uma sequência de 8 (oito) passos para realização de uma avaliação de risco.

2. RESPONSABILIDADE PELA EXECUÇÃO

A tarefa de realizar a conscientização em cibersegurança é atribuição do setor de segurança de todas as organizações públicas e privadas envolvidas com a Aviação Civil. Assim, devem ser especificados:

- Um setor responsável pela segurança cibernética;
- As responsabilidades de todos os profissionais com relação à segurança cibernética através da assinatura de termo de compromisso e/ou responsabilidade – política de uso;
- A responsabilidade dos gestores e coordenadores em supervisionar suas equipes e divulgar e disseminar medidas preventivas, desenvolvendo assim uma cultura de segurança cibernética.

3. PERIODICIDADE

A conscientização em cibersegurança deve ser realizada continuamente, em razão do rápido avanço da ameaça cibernética e das constantes inovações nas formas de ciberataques. Além de reafirmar os cuidados a serem aplicados, a conscientização contínua permite a divulgação das consequências negativas que a falta de proteção pode acarretar.

4. CONTEXTO

4.1 INTRODUÇÃO

As organizações modernas estão totalmente voltadas para tecnologias emergentes, como a Internet das Coisas (IoT), a nuvem de armazenamento (*cloud computing*) e sistemas integrados para um gerenciamento eficiente e ininterrupto de desafios logísticos. Toda essa tecnologia interconectada também leva a uma enorme quantidade de novas vulnerabilidades e explorações em potencial que

tornam o ataque cibernético um risco real, especialmente na aviação civil. Este documento irá destacar alguns aspectos dos maiores riscos e desafios relacionados ao ataque cibernético para organizações da aviação civil, sobretudo aeroportos.

Nos dias atuais se faz cada vez mais uso de Tecnologia da Informação e da Comunicação (TIC) para a realização das tarefas diárias. O surgimento de novas tecnologia modernizou e melhorou a eficiência e o conforto das atividades dos seus usuários. No universo da aviação civil não é diferente e, tais mudanças, a afetaram diretamente, tanto na indústria, na comunidade aeroportuária quanto na experiência percebida pelos seus usuários. O uso de sistemas de conexão em rede, acesso a serviços de voo pela *web*, entretenimento a bordo, armazenamento e compartilhamento de dados em nuvem, conectividade através de dispositivos móveis, e serviços de sistemas de navegação aérea são alguns exemplos do uso destas novas tecnologias na aviação civil. Já existem lugares onde um passageiro pode adquirir seu bilhete de passagem e ir da sua origem ao seu destino de forma 100% digital, sem necessidade de interagir com pessoas.

Assim, dada as facilidades e os benefícios obtidos, a aviação civil está cada vez mais dependente da disponibilidade de sistemas de TIC, bem como da integridade e confidencialidade dos dados. Se informações confidenciais caírem em mãos de entidades não autorizadas, esta violação de segurança poderá afetar a aviação civil de forma significativa, interferindo nas operações aéreas e podendo levar, inclusive, a perdas de vidas. Sistemas de segurança de TIC aplicam-se a pessoas, procedimentos, dados, *software* e *hardware* que são usados para reunir e analisar informações analógicas e digitais usadas no gerenciamento das atividades da aviação civil. É importante destacar que *informação* é um dos mais importantes ativos das organizações prestadoras de serviço para a aviação civil e que necessita ser protegida.

Ao mesmo tempo, atrelado ao crescimento das facilidades proporcionadas por estas tecnologias da era cibernética, surgem também novas ameaças e riscos ao ambiente do transporte aéreo. Tal fato exigiu que temas como risco cibernético (*ciber-risco*), ameaça cibernética (*ciberameaça*), incidente cibernético (*ciberincidente*), ataque cibernético (*ciberataque*) e segurança cibernética (*cibersegurança*) estejam presentes na agenda dos Estados da comunidade internacional de aviação civil.

Em outubro de 2019, durante a 40a Assembleia da OACI, foi publicada a Estratégia de Cibersegurança para a Aviação [ICAO, 2019], afirmando que, na sua visão, o setor da aviação civil é resiliente a ciberataques e que permanece seguro e confiável globalmente, enquanto continua a inovar e crescer. Esta estratégia se alinha com outras iniciativas da OACI relacionadas a cibersegurança e coordenada com o gerenciamento da segurança operacional ("*safety*") e segurança contra atos de interferência ilícita ("*security*"). Ela será alcançada através de um conjunto de medidas, ações e princípios contidos em uma estrutura construída sobre sete pilares: cooperação internacional, governança, legislação e regulações efetivas, política de cibersegurança, compartilhamento de informações, gerenciamento de incidentes e planejamento de emergência, além de capacitação, treinamento e cultura de cibersegurança. Observava-se já na Resolução A39-19 da Assembleia da OACI, realizada em maio de 2016, a convocação da comunidade da aviação civil a implementar ações para entender e debelar ameaças cibernéticas contra os sistemas e os dados da aviação civil, estimulando os países membros

a trabalharem de forma colaborativa para desenvolver um protocolo visando enfrentar os desafios da cibersegurança [Emanuelli, 2019]. Um dos resultados obtidos com aquela resolução foi a criação do Grupo de Trabalho do Secretariado sobre Segurança Cibernética (SSCG), cuja função é estabelecer ações a serem adotadas pelos Estados e partes interessadas do sistema aéreo para contrapor as ameaças cibernéticas, além de compartilhar informações relacionadas a ameaças, incidentes e ações de mitigação de riscos [Emanuelli, 2019].

O Governo brasileiro publicou a *Estratégia Nacional de Segurança Cibernética*, em 5 de fevereiro de 2020 [E-ciber, 2020], que orienta a sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

A política de segurança cibernética define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra. É considerada como um importante mecanismo de segurança, tanto para as instituições como para os usuários, pois com ela é possível deixar claro o comportamento esperado de cada um. Desta forma, casos de mau comportamento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas [Cartilha, 2020].

A segurança cibernética tratará da proteção às instalações críticas, que podem ser conceituadas como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. No Brasil, as organizações a serem protegidas, no escopo daquela Estratégia, são as pertencentes ao setor de Telecomunicações, ao setor de Transportes, ao setor de Energia e ao setor de Água. Observa-se aqui que, em uma organização como um aeroporto, todos estes setores estão relacionados na sua constituição e suas operações, fazendo parte assim da sua infraestrutura crítica que requer segurança cibernética. Além disso, em geral, todos estes setores fazem uso da TIC instalada no aeroporto.

A Instrução Suplementar IS107-001D de 2019 da ANAC [IS 107, 2016], entre outros temas, versa sobre cibersegurança para o caso de avaliação de risco de ataque cibernético (vide itens F.1.2.1.1(f), F.1.2.1.2(c) e F.1.2.3.1). Sendo estes itens obrigatórios apenas aos aeroportos de classe AP3 ou que realizem operações de voos internacionais.

Sabe-se que a ameaça representada pelos ciberincidentes sobre a aviação civil está evoluindo rápida e continuamente, e encontra-se focada principalmente na interrupção da continuidade dos negócios e no roubo de informações. Mas estes atos podem evoluir e atingir os sistemas críticos da aviação civil em todo o mundo. Ademais, nem todas as questões de cibersegurança são atos de interferência ilícita contra a segurança da aviação civil, logo, deve-se considerar apenas aqueles que possam atingir os sistemas TICs essenciais à prestação de serviços. Isto indica a necessidade de um alinhamento de interpretação e trabalho colaborativo entre os órgãos reguladores e os regulados, visando o desenvolvimento de uma estrutura eficaz e coordenada pelas partes interessadas, a fim de enfrentar os desafios da segurança cibernética.

Entre os citados desafios, mostra-se necessário uma melhor conscientização sobre as ciberameaças, melhor conhecimento dos métodos de ataques utilizados e dos diversos tipos de vulnerabilidades e melhor entendimento sobre a aplicação de técnicas de *análise de riscos* para fazer frente às ciberameaças e sobre a importância e forma de funcionamento dos profissionais e dos equipamentos de resposta às emergências informáticas.

O aumento da probabilidade de violação da segurança das informações e dados utilizados se deve principalmente às vulnerabilidades encontradas nas novas tecnologias existentes. Tais violações, em geral, estão relacionadas à tecnologia da informação (TI) como, por exemplo, ataques com utilização de vírus de computador ou outro *software* malicioso, falhas nos sistemas ou corrupção de dados, ou podem ser ainda motivadas socialmente como, por exemplo, através do roubo de ativos ou outros incidentes causados por algum membro da equipe.

São alguns dos motivos para uma organização implementar um programa de segurança cibernética [ACRP, 2015]:

- Evitar a interrupção dos serviços;
- Evitar a perda de vidas e danos a propriedade;
- Evitar vazamento de informação;
- Preservar a reputação da organização;
- Conformar os requisitos da legislação sobre o assunto;
- Proteger a saúde e a segurança dos empregados; e
- Obter um perfil de menor risco.

Em [ACRP, 2015] é proposto um método para implementar segurança cibernética em aeroportos. Em [Emanuelli, 2019], entre outros temas, trata-se da política de cibersegurança na OACI e suas práticas recomendadas.

Este presente Manual apresenta um compilado de informações, históricos e bibliografia existentes sobre cibersegurança com o objetivo de orientar e conscientizar os operadores de aeródromo e aéreos, e seus prestadores de serviço quanto ao tema, em especial sobre sua complexidade e possíveis impactos nas operações, servindo como um meio de fomentar a proteção cibernética, que envolve ações desde a implementação de uma cultura preventiva nas instituições, até mesmo o investimento em recursos avançados de proteção.

Espera-se que deste manual, os profissionais da aviação civil possam ter uma iniciação ao tema, que possibilite consultas mais aprofundadas, cursos especializados, ou tão somente a criação de uma cultura pessoal que promova a percepção de quão complexo é o tema e quais ações pessoais e institucionais devem ser conduzidas para lidar com as ameaças cibernéticas.

4.2 ATORES, ALVOS E MOTIVAÇÕES DE AMEAÇAS EM POTENCIAL

As infraestruturas, os sistemas e as plataformas críticas são os principais alvos das ciberameaças na aviação civil. Dentre estes destacam-se os aeródromos ("*safety*" e "*security*"), as instalações físicas do controle de tráfego aéreo, os sistemas de gestão de passageiros e cargas de empresas aéreas e de controle de tráfego aéreo, aeronaves, sistemas de TIC, sistemas de instalações e manutenção, além de órgãos de regulação.

Um ator de uma ciberameaça contra a aviação civil pode ser qualquer um que tenha uma motivação específica. Podem ser pessoas, organizações e mesmo nações/Estados, por exemplo:

- Pessoas:
  - Terroristas;
  - Ativistas;
  - Criminosos;
  - Curiosos;
  - Vândalos;
  - Funcionários internos da organização (Empregados em Geral, Superusuários de TI, etc).
- Organizações:
  - Organizações criminosas;
  - Organizações terroristas;
  - Empresas concorrentes;
  - Empresas terceirizadas (equipe de segurança física, equipe de limpeza, equipe de TI etc);
  - Organizações ativistas.
- Estados/Nações:
  - Nações/Estados hostis;
  - Grupos financiados por Estados.

Objetivando a realização de um ciberataque à aviação civil, tais atores necessitam de alguma motivação. Cita-se como possíveis motivações: ganho financeiro, fraude, *ransonware*, espionagem industrial, destruição, diminuição de reputação, interrupção de serviços, ativismo, ações de geopolítica, obtenção de elogios, ações antagônicas aos interesses do Estado/Nação, etc. Assim, ataque é quando a vulnerabilidade do sistema é explorada com o objetivo de causar danos.

Uma pessoa mesmo sem motivação explícita também pode vir a ser um ator em um ato de ciberameaça, quando por desconhecimento ou falta de conscientização, realiza ou deixa de realizar uma ação, comprometendo a política de cibersegurança da organização. Exemplos deste tipo de ciberameaça ocorrem quando um profissional se ausenta do seu posto de serviço, que pode ser um ponto de identificação de passageiros e deixa o computador logado no sistema que fornece informações para o SIV, ou mesmo quando conecta um dispositivo USB pessoal ao computador da organização onde trabalha.

Os *atores de ataques cibernéticos* podem ser categorizados com relação a sua interação com o aeroporto:

- Ameaças internas: alguém das equipes do aeroporto com intenções maliciosas;
- Passageiros ou anônimos no aeroporto: são atores que estão presentes fisicamente no aeroporto com intenções maliciosas;
- Atores remotos: não estão presentes fisicamente no aeroporto e incluem, atores automáticos como *malwares*. Estão limitados a vetores de ataques disponíveis remotamente;
- Outros tipos: falhas, acidental ou ambiental, em *software* ou em equipamentos que podem causar incidentes de segurança.

Exemplos de potenciais alvos de ataques cibernéticos em aeroportos:

- Ativos de TIC que podem ser acessados pelos atores de ataques;
- Ativos de TIC que interagem com redes de comunicação *wireless*;
- Ativos de TIC que interagem com redes de comunicação cabeadas;
- Passageiros ou outros funcionários utilizados pelos atores de ataques; e
- Ataques dinâmicos entre ativos: quando um determinado ativo é violado e serve de base para o lançamento do ataque.

4.3 EXEMPLOS DE ALGUNS INCIDENTES CIBERNÉTICOS OCORRIDOS NA AVIAÇÃO CIVIL

2010 – o acidente da Spanair que se produziu em 2008, investigações revelaram que o sistema informático central utilizado para monitorar problemas técnicos no avião foi infectado com *malware*;

Julho de 2013 – o aeroporto de Istanblul Ataturk e o aeroporto internacional de Sabiha Gokçen foram vítimas de um ataque de *malware*. E os *ciberdelinquentes* tentaram roubar dados do sistema de controle de passaporte dos aeroportos. Muitos voos foram atrasados;

Agosto de 2013 - um motorista de caminhão equipado com um rastreador de gps ilegal interferiu nos sinais usados pelo sistema de navegação no solo no aeroporto de Newark;

Setembro de 2013 – Japan Airways informa que até 750.000 clientes do seu programa de milhas tiveram informações pessoais comprometidas devido a um ciberataque;

Outubro de 2013 – a companhia aérea malaia Malindo Air teve a conta do Twitter hackeada, onde o *hacker* postou o anúncio falso que a companhia estaria oferecendo 100.000 assentos grátis;

Março de 2014 – a Autoridade de Aviação Civil da Malásia foi "hackeada" um dia depois do informe do voo MH370 através de um e-mail com um documento com extensão "PDF" anexado;

Novembro de 2014 – cerca de 10 *websites* do governo da Jamaica, incluindo o da autoridade de aviação civil jamaicana, foram alvos de um ataque de negação de serviço (DoS);

Dezembro de 2014 - uma grande falha de computador no principal centro de controle de tráfego aéreo em Londres causou massivas interrupções nos voos chegando e partindo do "*hub*" global;

Janeiro de 2015 – o *website* da Malaysia Civil Aviation foi "hackeado" por um grupo se declarando do cibercalifado Lizard Squad;

Março de 2015 – a empresa British Airways congelou seu programa de passageiro frequente devido a um programa de computador automatizado procurar por vulnerabilidades em seus sistemas;

Junho de 2015 – *hackers* violaram os computadores da companhia aérea polonesa LOT, usados para emitir planos de voo. Como resultado do ataque, o *Hub* de Varsóvia não pode criar planos de voo, deixando 1400 passageiros em terra no aeroporto Chopin em Varsóvia. O ciberataque foi do tipo negação de serviço (DoS);

Novembro de 2015 – o uso de uma versão obsoleta de sistema operacional causou uma interrupção no Aeroporto de Orly Paris. A falha afetou um sistema conhecido por Décor, que executa sobre o Windows 3.1, e é usado para os controladores aéreos comunicarem informações meteorológicas aos pilotos;

Janeiro de 2016 – o Aeroporto Internacional de Kiev Boryspil teve seu sistema de TI, incluindo o controle de tráfego aéreo, atacado por um *malware*. O servidor de onde se originou o ataque se encontrava na Rússia;

Março de 2016 – "*hacker*" do Vietnam, Le Duc Hoan Hai, utilizando a credencial de um terceirizado conectado ao Aeroporto de Perth, acessou o sistema de computadores e roubou informação de segurança do aeroporto, em relação a medidas de segurança física e de projeto do aeroporto;

Abril de 2016 - após o pouso, o piloto de um voo da British Airways vindo de Genebra informou uma colisão com um drone enquanto se aproximava do aeroporto London Heathrow em 17 de abril. O incidente destacou os problemas enfrentados em relação aos drones. Embora a ameaça de colisão com aves tenha sido bem pesquisada, ainda há poucos dados sobre quanto dano um drone poderia causar a um avião;

Julho de 2016 – um grupo de *hacker* conhecido como "China 1937CN Team" comprometeu os sistemas de anúncio por voz e sistemas de informação de voo, dos principais aeroportos do Vietnam. Estavam motivados por disputas territoriais no Mar da China. Como resultado deste

ataque autoridades vietnamitas realizaram uma verificação abrangente dos dispositivos chineses e tecnologia para garantir a segurança da informação nos seus aeroportos;

Julho de 2016 - uma falha de terceiros no aeroporto de Roma Fiumicino, na Itália, originou a interrupção do sistema de check-in automático de passageiros, o que causou atrasos de duas horas na operação de inspeção de passageiros. A falha estava relacionada ao provedor de Internet que o aeroporto usa para acessar e processar dados de passageiros, usado para o check-in automático de passageiros;

Agosto de 2016 – milhares de passageiros aéreos ao redor do mundo ficaram presos depois que um corte de energia obrigou a companhia aérea americana Delta a suspender os voos. Ocorreu uma falha de energia durante a noite em Atlanta, perto da sede da Delta, causando falha nos sistemas de computador. O sistema de check-in do aeroporto, sistemas de informação, telas de aviso de passageiros, o *site web* da companhia aérea e aplicativos para *smartphones* foram afetados pela falha do sistema;

Abril de 2017 – uma empresa contratada pela Delta Airlines para serviço de "*chat*" *online* estava envolvida em um ciberincidente que levou à exposição informação de pagamento de seus clientes e da Delta também;

Março de 2018 – a companhia aérea Cathay Pacific, sediada em Hong Kong sofreu a maior violação de dados da aviação quando *hackers* acessaram 860.000 números de passaportes, 245.000 números de cartões de identidade de Hong Kong, 403 números de cartões de créditos expirados e 27 números de cartões de créditos válidos sem o código CVV. A companhia demorou 7 meses para informar da violação e teve uma queda considerável no seu valor de mercado;

Junho de 2018 – "*hackers*" interferem no sistema de informação de voo do aeroporto de Tabriz no Irã, em protestos contra medidas adotadas pelo governo;

Setembro de 2018 – o aeroporto de Bristol sofreu um ciberataque (*ransomware*) e ficou dois dias sem serviço de informação de voo. Os sistemas afetados foram reestabelecidos manualmente;

Janeiro de 2020 - uma página suspeita de Facebook, chamada RyanairUK, informando ser a página oficial da Ryanair, enganava as pessoas dando a falsa esperança de uma viagem gratuita e, ainda, apresentava um endereço *web* considerado suspeito;

Janeiro de 2020 – no aeroporto de Portland, um viajante plugou seu Playstation 4 e começou a jogar em um monitor que mostrava um mapa do aeroporto;

Janeiro de 2020 – pesquisadores de segurança acessaram a base de dados da empresa aérea indiana SpiceJet usando uma combinação fácil de caracteres de senha e encontraram informações pessoais não criptografadas de 1,2 milhão de passageiros.

Novembro de 2020 – a Embraer informou que sofreu ataque cibernético aos seus sistemas de tecnologia de informação, que resultou na divulgação de dados supostamente atribuídos à empresa, indisponibilizando o acesso a apenas um único ambiente de arquivos da Companhia.

Março de 2021 – Ataque *hacker* sofrido pela multinacional SITA (empresa que presta serviços de tecnologia da informação ao setor aéreo), expôs dados de passageiros no Brasil. O ataque foi direcionado a parte dos membros de programas de fidelidade.

Para mais informações, em [EATM-CERT, 2020] é publicado um relatório trimestral visando fornecer informações sobre as ameaças e vulnerabilidades cibernéticas ocorridas naquele período, com foco no setor de aviação.

4.4 DESENVOLVIMENTO

A OACI, através do DOC 8973 [Doc 8973, 2017] (ver Capítulo 18) apresenta uma estrutura de trabalho voltada para ciberameaça visando o gerenciamento do risco em cibersegurança. Seu intuito é auxiliar os Estados e as organizações a alinharem suas atividades de cibersegurança com seus requisitos de negócios, níveis de tolerância a riscos e recursos. A estrutura que foi proposta pela OACI é apresentada nesta seção com algumas adaptações, e baseia-se nas seguintes ações: *identificar* os sistemas de informação críticos e os dados da organização; *Proteger* os sistemas de TIC críticos e seus dados contra ciberataques e interferências; *Detectar* imediatamente um ciberataque pois é crítico para realizar operações seguras e para manter a disponibilidade dos sistemas críticos; *Responder* ao ciberataque através do emprego de um plano de resposta de cibersegurança visando controlar o incidente e reestabelecer os componentes críticos afetados; *estabelecer um plano de comunicação de crise* para uma efetiva e adequada comunicação entre as partes interessadas em resposta ao ciberincidente; e *realizar* uma minuciosa análise pós evento para assegurar que não exista futura recorrência.

Assim, para salvaguardar o sistema de tecnologia da informação e comunicação é também necessário abordar a segurança do ambiente em que estes sistemas funcionam, tais como sistemas de balizamento luminosos das pistas e sistemas de credenciamento automático, entre outros. Assim, a segurança da informação está relacionada com segurança física, fornecedores, serviços de infraestrutura e empresas contratadas que interagem com prestadores de serviço e autoridades regulatória e legais. As ações citadas são descritas a seguir.

4.4.1 IDENTIFICAÇÃO DE SISTEMAS DE INFORMAÇÃO CRÍTICOS

Um sistema de informação na aviação é considerado crítico quando contém ou usa dados e/ou ativos sensíveis; ou sua operação é indispensável para operação segura e disponibilidade das atividades da aviação. A identificação dos sistemas críticos deve ser conduzida através da classificação de todos os dados e/ou ativos de acordo com uma política ou classificação de dados predefinida, e

o desenvolvimento de uma análise de impacto nos negócios sobre a criticidade de cada um dos sistemas individuais.

A criticidade do sistema de informação pode ser identificada considerando-se padrões e estruturas de trabalho de TI muito bem conhecidos, tais como: *Control Objectives for Information and Related Technologies* (COBIT®) [Stroud, R.E., 2012],[COBIT, 2019], *Project Management Body of Knowledge* (PMBOK®) [PMI, 2013], *Capability Maturity Model Integration* (CMMI®) [Chrissis et all, 2011],[CMMI, 2020], *IT Infrastructure Library* (ITIL®) [Axelos (2019)], ISO 27001 [ISO 27001, 2013)] e *Open Group Architecture Framework* (TOGAF™) [Togaf, 2020].

Através de [GSIPR, 2008], o Gabinete de Segurança Institucional da Presidência da República do Brasil (GSIPR), criou os Grupos Técnicos de Segurança de Infraestrutura Críticas (GTSIC), para tratar da proteção de áreas prioritária para o Brasil, um deles é o do setor de transporte aéreo [Emanuelli, 2019]. Já, através de [GSIPR, 2010], o GSIPR instituiu o Subgrupo Técnico de Segurança de Infraestrutura Críticas de Transportes Aéreos (SGTSIC-TA), para tratar das infraestruturas críticas do setor de transportes aéreo. Tal subgrupo irá identificar e avaliar as vulnerabilidades das infraestruturas consideradas críticas para o setor, além de avaliar riscos e articular medidas para implementar um sistema de informação sobre tais infraestruturas para suportar decisões.

A seguir apresenta-se a visão global de ativos e grupos de ativos da ENISA (Agência da União Europeia para Segurança Cibernética - *European Union Agency for Cybersecurity*) [ENISA, 2016] a serem protegidos em aeroportos, organizados por grupos. A ideia é fornecer às partes interessadas uma visão sobre ativos e que eles possam adequar a sua realidade, em tamanho e características:

- Administrativo do Aeroporto:
  Sistema de gerenciamento da empresa, sistema de gerenciamento de inventário de ativos, sistema de gerenciamento de recursos humanos, sistema de gerenciamento de compras, sistema de gerenciamento de políticas, sistema de gerenciamento financeiro;

- Empresas aéreas e operações do lado ar:
  Gerenciamento de tráfego de pátio, métodos e auxílios a navegação aérea, sistema de rastreamento de voo, sistema de controle de partida local (pesagem e balanceamento), sistema de informação meteorológica, sistema de controle de partida, sistema de descongelamento, sistema de controle de iluminação do aeródromo e da pista de pouso e decolagem, sistema de processamento de cargas, sistema de reabastecimento da aeronave, carregador de dados de aeronaves portátil, sistema de gerenciamento de infraestrutura e recursos do aeroporto, sistema de serviço de portão de embarque, banco de dados do aeroporto, sistemas de controle de acesso;

- Operações do lado terra:
  Centro de controle do sistema de operações do lado terra do aeroporto, sistema de identificação de veículos automático, gerenciamento de combustível, sistema de detecção de

iluminação, pedágio de estacionamento eletrônico automático, sistema de gerenciamento de estacionamento, sistema de transporte público e privado, sistema de indicação de caminho (rodovia de acesso ao aeroporto e estacionamento);

- Serviços auxiliares ao consumidor:
  Caixa automático, pagamentos móveis, máquinas de ponto de vendas, serviços de gestão comercial;

- Sistemas TIC:
  Redes Locais, redes privadas virtuais (VPN), Sistemas de comunicação, dados armazenados, equipamentos de TI, redes móveis e seus aplicativos, serviço de *wi-fi* para passageiros, centro de operação de segurança, monitoramentos de registros de TI, notificação de eventos, gerenciamento e sistema de informação de voo, Sistema de Posicionamento Global (GPS), Serviços aplicações e dados baseados em nuvem, gerenciamento de segurança da rede, rede banda larga, rede WAN (*wide area network*), rede de comunicação comum, sistema de comunicação passageiro empresa aérea, sistema de comunicação do ar para o satélite, Sistema de Informação Geográfica (*Geographic Information System* - GIS);

- Gerenciamento de equipe de funcionários:
  Gerenciamento de registros de funcionários, sistema de gerenciamento de recrutamento, aplicações e sistemas móveis habilitados, sistema de autenticação de funcionários;

- Gerenciamento de passageiros:
  Sistema de logística dentro do aeroporto, dispositivos tipos quiosques, sistema de informação visual eletrônico, check-in e embarque de passageiros, dispositivos computacionais, registro do nome dos passageiros, sistema de reserva central, serviços de informação de localização;

- Instalações e manutenção:
  Manutenção de veículos do aeroporto, sistema de controle de instalações, sistema de gerenciamento de manutenção computadorizados, gerenciamento de energia, elevadores, escadas rolantes, esteiras rolantes, pontes de embarque, sistema SCADA (*Supervisory Control and Data Acquisition* – Controle Supervisionado e Aquisição de dados), sistema de gerenciamento ambiental (ruído, vida selvagem, condições ambientais, drenagem).

As proteções dos sistemas de TIC da aviação e de seus dados devem ser incluídas em um processo de avaliação de riscos estabelecido ao nível de operadores da indústria da aviação civil. Isto pode ser atingido revendo as ameaças comuns, vetores de ataques, probabilidade de uma ocorrência de ciberataque, vulnerabilidades conhecidas e a severidade do impacto para cada sistema de aviação crítico. A partir desta análise se deve estabelecer medidas mitigadoras cuja eficácia será averiguada através do monitoramento da conformidade das atividades.

Os operadores da indústria da aviação incluindo aeroportos, operadores aéreos, agentes de movimentação em solo e manutenção, provedores de serviços de revisão, devem estabelecer um ambiente e cultura onde gerenciamento e governança de cibersegurança seja levada aos *níveis executivos organizacionais*. Ademais, cada um destes entes organizacionais, citados e interessados que a aviação civil atinja seus objetivos, deverá identificar seus dados e sistemas de informação críticos, incluindo *hardware* e *software* usados nas suas operações. Cada estrutura de governança de cibersegurança das organizações da aviação civil deve determinar sua própria política de segurança cibernética alinhada com a política e regulamentações nacionais.

Seguindo a referência do Capítulo 18 do Doc 8973 [Doc 8973, 2017], item 18.2.1.2 cita-se alguns componentes dos interessados na aviação civil que podem ser considerados críticos do ponto de vista de TIC (dados e sistemas de informação e comunicação):

a) Aviação na perspectiva "*safety*": sistema de gerenciamento de tráfego aéreo; sistema de controle de partida; comunicação, navegação e outros sistema de segurança críticos de uma aeronave; e sistemas de comando, controle e expedição de uma aeronave.

b) Aviação na perspectiva "security": banco de dados de agente de carga acreditado e expedidor reconhecido; controle de acesso e sistema de alarme; sistema de vigilância de circuito fechado de televisão (CFTV); sistema de reconciliação de bagagem e passageiro; e sistema de inspeção e/ou sistema de detecção automática de explosivos.

c) Aviação na perspectiva da Facilitação: Sistemas de reservas de passagens e de check-in de passageiros; Sistema de informação de voo; Sistema de monitoramento e manipulação de bagagem; e Sistema de aduana e travessia de fronteiras.

Com relação ao Controle de Tráfego Aéreo, o DECEA possui norma interna que define quais são os sistemas de informação de missão crítica. De acordo com a ICA 7-31, são exemplos desse tipo de informação:

a) Informação sobre controle de tráfego aéreo;

b) Informação sobre gerenciamento de fluxo aéreo;

c) Mensagem aeronáutica;

d) Informação sobre gerenciamento de planos de voo;

e) Informação de meteorologia e condições de aeródromo;

f) Informação de defesa do espaço aéreo; e

g) Informação sobre balizas de emergência.

No anexo B de [ISO 27005, 2008] apresenta-se um exemplo para a identificação e valoração de ativos de TIC, e avaliação de impacto sobre a organização. No apêndice B de [ACPR, 2015], encontra-se uma extensiva lista de ativos de TIC encontrados em aeroportos, categorizada por tipos.

No Apêndice A deste texto, apresenta-se uma lista mais extensa de componentes dos sistemas da aviação civil que podem ser críticos do ponto de vista de TIC, caso seja utilizado. No capítulo 5, que apresenta cibervulnerabilidades, cita-se também, alguns destes sistemas críticos, vulneráveis do ponto de vista de TIC.

4.4.2 PROTEÇÃO AOS SISTEMAS DE TIC

a) Os sistemas

No intuito de *proteger* os sistemas de TIC críticos e seus dados contra ciberataques e quaisquer outras interferências, a organização deve fornecer provisões apropriadas para implementar sua política e programas de proteção. Programas de cibersegurança devem indicar quais funções e dados dos sistemas de TIC são críticos para a segurança da aviação civil, a fim de *protegê-los* contra acesso não autorizado, modificações, mau uso, falta de disponibilidade e/ou integralidade, além de impedir adulteração dos sistemas e de seus dados.

A *proteção* lógica e física de tais sistemas e dados deve começar na fase de projeto, para assim, assegurar que eles encontrem os objetivos de confidencialidade, integridade e disponibilidade (CIA), e sejam tão robustos quanto possível aos ciberataques. Segundo a OACI, uma das formas para obter esta proteção pode ser alcançada através da utilização de um método de controle multicamadas com: controles administrativos, controles de qualidade, controles lógicos ou técnicos e controles físicos [Doc 8973, 2017].

A *resposta ao risco* deve incluir o desenvolvimento de um compreensivo método para reduzir ou eliminar a vulnerabilidade identificada, tanto quanto a utilização de técnicas para evitar, mitigar, transferir e aceitar o risco. Para cada vulnerabilidade identificada, deve-se desenvolver uma resposta para gerenciamento ao risco. Da mesma forma, é essencial realizar uma revisão contínua dos esforços de mitigar o risco, com o propósito de manter o programa de gerenciamento do risco em cibersegurança. Neste manual, apresenta-se uma conhecida técnica de avalição de riscos, considerando a cibersegurança de ativos de TIC (ver Capítulo 6 e Apêndice E).

b) Os recursos humanos

Os operadores da aviação civil devem assegurar que os componentes do sistema de TIC críticos estejam sob a responsabilidade de uma equipe de profissionais devidamente selecionados e treinados. Para tanto, devem possuir um plano de treinamento para todo o pessoal que está usando, manipulando, instalando e desempenhando manutenção sobre sistemas de TIC críticos, incluindo, inclusive, os tripulantes e o pessoal de manutenção de aeronaves.

É desejável que o plano de treinamento aborde tópicos como: conscientização sobre vulnerabilidades em cibersegurança; como os sistemas podem ser atacados incluindo noções de engenharia

social; medidas de precaução que podem ser adotadas para impedir ou minimizar o ataque e suas consequências; quais possíveis recursos são alterados ou tem sua operação afetada; e procedimentos de contingência no caso de suspeita de um ciberataque.

c) As redes de computadores

Para a *proteção das redes de computadores* que fazem parte do sistema crítico de TIC e seus dados é recomendável a separação física e/ou lógica em zonas baseadas sobre sua função, uso e níveis de segurança. A conectividade a outros sistemas operacionais deve ser limitada ao mínimo possível. Onde as redes não possam ser separadas, todas as conexões e acessos devem ser continuamente monitorados por ferramentas de diagnósticos de redes.

Ainda, todas as redes devem ser projetadas e mantidas com considerações de cibersegurança em mente. A princípio, todas as conexões de rede devem ser consideradas inseguras a menos que um acordo específico de interconexão tenha sido estabelecido entre as entidades operacionais envolvidas na interconexão. Tais conexões devem ser documentadas, revisadas e atualizadas quando necessário com proteção contra intrusão no ponto final, o que pode ser conseguido com sistemas de detecção de intrusão (IDS).

A fim de fornecer mais robustez à segurança das redes contra ciberataques o operador deve estabelecer um programa de monitoramento que utilize escaneamento de vulnerabilidades, teste de penetração e escaneamento para a descoberta de serviços não autorizados.

d) Os fornecedores

É recomendável que os fornecedores de suprimentos para os sistemas de TIC informem em detalhes como a informação e a operação do sistema é segura, incluindo como o suporte e a manutenção é realizado, seja localmente ou remotamente. Quando a manutenção é realizada por empresas terceirizadas, é importante que o número de indivíduos que têm acesso ao *software* e ao *hardware* seja limitado e todo o processo de acesso devidamente documentado. É uma boa prática que a organização garanta que o *software* e seus fornecedores demonstrem que medidas de segurança são adequadas para proteger os sistemas críticos e seus dados, que detectam intrusos e ataques e que são capazes de *recuperá-los*. Uma medida interessante de prevenção é garantir que os fornecedores de *software* e *hardware* sejam legítimos e com boa reputação, além de garantir suporte seguro durante todo ciclo de vida do sistema.

e) O controle de acesso

No tocante ao *controle* de acesso aos sistemas críticos e a seus dados, os direitos administrativos dos usuários devem usar o conceito do privilégio mínimo e o acesso remoto só deve ser permitido em circunstâncias especificas e com dados criptografados, sendo o acesso removido tão cedo quanto possível. O pessoal responsável pelo suporte e manutenção deve ser autorizado, ter número limitado e só realizar o trabalho em horários acordados. Uma prática reconhecida é promover a realização da consulta de antecedentes criminais dos profissionais com acesso, tanto físico, quanto lógico aos ativos de TIC. Recomenda-se que os operadores do setor aéreo se certifiquem que os

fornecedores de *hardware* e *software* confirmem, através de contratos, que não existem acessos escondidos em seus sistemas que possam possibilitar um acesso não autorizado. É importante que o operador realize periodicamente testes de invasão, inspeções e auditorias em toda a infraestrutura do sistema crítico de TIC, para se certificar que todo o sistema de controle de acesso está funcionando adequadamente e que é capaz de resistir a situações emergenciais, tais como ataques cibernéticos.

f) O monitoramento contínuo

A fim de dar suporte às tomadas de decisões de risco organizacional, é recomendável que as entidades estabeleçam um *Sistema de Monitoramento Contínuo da Segurança da Informação* (ISCM) com o propósito de manter consciência de segurança da informação, vulnerabilidades e ameaças. O monitoramento contínuo é uma parte crítica do processo de gerenciamento de risco da organização. Tal sistema deve incluir:

- Métricas que forneçam indicadores significativos dos estados de segurança em todos os níveis organizacionais;
- Entendimento claro da tolerância ao risco organizacional, dos papéis e responsabilidades no monitoramento e na resposta à incidentes;
- Conformidade com missão organizacional e com os requisitos das leis regulamentares;
- Inventário detalhado de todo *hardware*, *software*, *firmware* e utilidades organizacionais incluindo modelos, versões e nível de inventário;
- Conhecimento e controle de mudanças nos sistemas e no ambiente operacional, incluindo monitoramento de configuração;
- Ciência da última ameaça e da comunicação regular para gerenciamento sobre a mudança do nível de ameaça e do relatório de avalição de riscos;
- Assinaturas de serviços que anunciam atualizações, "*patches*" e vulnerabilidades de produtos;
- Estabelecimento de um programa de gerenciamento regular de "*patches*";
- Revisão regular de controle de segurança;
- Revisão e auditoria de fraquezas identificadas para assegurar que a fraqueza não exceda níveis de tolerância preestabelecidos.

De fato, tal Sistema, o ISCM, permitirá que os controles das ameaças sejam continuamente monitorados, avaliados e abordados, o que indicará que a organização deu um grande passo no sentido de reduzir seu potencial de risco à cibersegurança.

4.4.3 AÇÃO DE DETECÇÃO DE CIBERATAQUES

Com o propósito de *detecção de ataques*, o conceito de ISCM contém um centro de operações de segurança ou de redes que apresenta inspeções constantes, avaliações e notificações de tráfego de rede e anomalias, usando detecção de intrusão e ferramentas de prevenção. Além disso, é igualmente importante o uso de ferramentas automatizadas, tais como escâner de vulnerabilidade e de rede, e de um programa de gerenciamento de registros de anomalias em redes e em pontos de

dispositivos finais. Sendo assim, o ISCM é composto também por um sistema de gerenciamento de eventos e informações de segurança para detectar irregularidades e anomalias.

Com o propósito de estabelecer, implementar e manter o ISCM, a organização deve considerar os seguintes passos:

- Definir uma estratégia ISCM;
- Estabelecer um programa ISCM;
- Implementar um programa ISCM;
- Analisar os dados e relatar os resultados;
- Responder aos resultados; e
- Revisar e atualizar a estratégia e o programa ISCM.

A eficácia do *controle de segurança* é medida pela exatidão da implementação e de quão adequado os controles implementados atendem às necessidades organizacionais de acordo com a tolerância atual ao risco (ou seja, o controle deve ser implementado em conformidade com o plano de segurança para tratar ameaças, o qual deve ser adequado a elas).

Uma das vantagens de se ter um programa da ISCM é ajudar a garantir que os controles de segurança implantados continuem a ser eficazes e que as operações permaneçam dentro das tolerâncias de risco organizacionais declaradas, à luz das inevitáveis mudanças que ocorrem ao longo do tempo. Nos casos onde os controles de segurança são considerados inadequados, os programas da ISCM facilitam ações de resposta de segurança priorizadas com base no risco.

Os operadores devem ainda estabelecer um *programa de conscientização e mecanismo de notificação para os usuários finais e partes interessadas*, reportando atividades suspeitas, anomalias e outras informações sobre a ocorrência de ataques.

O ISCM é uma etapa essencial da *Estrutura de Gerenciamento de Riscos* (RMF) de uma organização, pois fornece aos seus funcionários o acesso a informações relacionadas à segurança sob demanda, permitindo decisões de gerenciamento de risco oportunas, incluindo decisões de autorização. Atualizações frequentes de planos de segurança, relatórios de avaliação de segurança, planos de ação e marcos, inventários de *hardware* e *software* e outras informações do sistema também devem ser suportados por ele.

É recomendado que todas as organizações operando um ambiente de tecnologia estabeleçam um regime de ISCM, o qual contenha ferramentas de detecção de um ataque ou incidente, tais como: centro de operações de segurança ou de rede; rotina de uso de ferramentas automatizadas; um programa compreensivo de gerenciamento de registros; e o emprego de um sistema de gerenciamento de eventos e segurança da informação.

4.4.4 RESPOSTAS A CIBERATAQUES

Os operadores devem estabelecer um *plano de resposta de cibersegurança* que esboce um método organizacional para tratar um ciberataque. Tal plano deve incluir as ações realizadas pelas entidades envolvidas no processo de mitigar e neutralizar o ciberataque. O plano de resposta deve incluir, ainda, um plano de continuidade das operações, compreensivo e detalhado, a ser usado nos eventos em que um ou mais sistemas identificados como críticos se tornarem indisponíveis ou não confiáveis.

Características desejáveis para o Plano de Resposta de Cibersegurança:

- Metodologia de classificação para determinar a severidade de um incidente, para que respostas adequadas possam ser tomadas;
- Solução imediata para garantir operações contínuas seguras de aeronaves em voo, espaço aéreo ou aeroportos afetados pelo incidente;
- Plano de continuidade dos serviços com instruções para reestabelecer o sistema dentro de tempos de recuperação objetivos. Ou plano para manter as operações através de outros meios;
- Plano para assegurar que as vulnerabilidades identificadas não possam ser exploradas para colocar em perigo a segurança dos passageiros, tripulação e pessoal de terra;
- Plano para recuperação de desastre, para reestabelecer completamente as operações; e
- Plano para notificação de emergência para todos os interessados, com o objetivo de garantir o pessoal necessário para reestabelecer tão rapidamente quanto possível e fornecer informações essenciais para todos os parceiros.

A etapa de *prontidão de respostas* equivale não apenas à vigilância, por exemplo, sob a forma de monitoramento contínuo, mas também a disponibilidade de recursos. Uma equipe bem preparada e multifuncional deve estar apta para lidar com todos os aspectos de um incidente ou crise. Além disso, *simulação de crise e jogos de guerra* permitem que o gerenciamento entenda o que pode acontecer, quais passos tomar e se a organização está verdadeiramente preparada.

- As organizações devem estabelecer exercícios de cibersegurança para aumentar a prontidão dos sistemas e seus operadores construir planos de resposta a incidentes e capacidades e melhorar a comunicação e coordenação entre operadores de sistemas críticos e agências de governo relevantes.

No contexto de respostas a incidentes, visa-se conter ou gerenciar o incidente ocorrido. Sabe-se que uma resposta pobre pode até criar ou amplificar uma crise. Por outro lado, respostas vigorosas e coordenadas, limitam o tempo perdido, dinheiro gasto e perda de clientes, bem como danos à reputação e imagem e aos custos de recuperação. A gerência da organização deve estar preparada para comunicar, conforme necessário e em todas as mídias, incluindo as mídias sociais, de forma a garantir às partes interessadas que a resposta da organização reflete a situação real.

A resposta a incidentes deve conter:

- Análise do incidente para determinar a severidade do impacto;
- Priorização de ações a serem tomadas para reagir ao impacto com base na análise realizada;
- Mitigação de causas e efeitos do incidente, para estender a quarentena de códigos maliciosos, queda de sistemas, bloqueio de tráfego de rede, entre outros;
- Definição das medidas de mitigação quando essas afetarem as operações, *backup* ou procedimentos alternativos deveriam ser implementados para todos sistemas afetados;
- Definição de qual é o estado normal dos dados e sistemas como parte do inventário. O estado normal deve ser reestabelecido o mais rápido possível, após o incidente. Métricas podem ser usadas para definir a carga e o tráfego da rede.

Se possível, deve-se realizar a definição da causa raiz do incidente. É desejável o uso do Princípio de Gerenciamento de Configuração da Aplicação, com remoção de código malicioso ou retornar o sistema ao estado estável anterior ao incidente. Se a causa raiz não puder ser removida, é recomendado deixar o sistema inoperante, dada a possibilidade de infecção de outros sistemas.

Detalhes completos do incidente devem ser registrados e armazenados em ambiente seguro para futura análise de tendência e profundidade. É recomendável que os resultados das análises sejam disponibilizados às partes interessadas e pertinentes da indústria da aviação, como forma de conscientizar e orientar ao máximo em busca de evitar reincidências.

A depender da natureza do incidente, a comunicação com as autoridades apropriadas, autoridade da aviação civil, fabricantes de equipamentos e fornecedores de serviços, dentre outros, será importante habilitar a informação a ser compartilhada com outros usuários que possam ser afetados. É recomendado o uso de técnicas de *ciberforense* para entender o que ocorreu no incidente, qual o impacto, os danos e se possível identificar quem perpetrou o ataque, se este foi contido e o que pode ser feito para impedir uma recorrência do incidente e/ou do ataque.

Para relatar o incidente as organizações podem se utilizar do sistema de DSAC como uma forma de apresentação de relatórios de ciberataques. Para o compartilhamento de informações relatadas, a Agência distribui semestralmente aos regulados, um relatório de DSACs. Reconhece-se que a troca de informações sobre vulnerabilidades e ataques é um assunto com espaço para evolução, para que seja mais amplo e ágil. É importante que também seja desenvolvido um sistema de alerta para facilitar a comunicação entre operadores e outros interessados, preferencialmente baseado no princípio do anonimato. O item 5.5.4 deste manual faz uma breve abordagem sobre sistemas para esta finalidade.

Recomenda-se o uso de métricas para quantificar o impacto de um incidente e priorizar medidas de mitigação que reduzam a probabilidade da ocorrência de incidente similares no futuro.

4.4.5 PLANO DE COMUNICAÇÃO PARA SITUAÇÕES DE CRISE

O Estado e a indústria devem trabalhar em suas respectivas organizações para prepararem Planos de Crise para estabelecer as ações, inclusas as de comunicação, e os responsáveis durante o enfrentamento de uma situação de crise que envolva a ocorrência de ciberincidente.

Evitar uma crise cibernética geralmente se resume a gerir adequadamente um incidente cibernético antes, durante e após o seu desdobramento. Isso começa com uma visão ampla da gestão de crises cibernéticas. Em geral, os executivos veem incidentes cibernéticos como "*um problema de TIC*", quando a TIC é apenas um domínio envolvido.

Em uma gestão inovadora, as equipes reconhecem que o planejamento eficaz de crises envolve múltiplas funções e conjuntos de habilidades, bem como que tais funções e habilidades devem ser altamente coordenadas para um incidente possa ser adequadamente contido ou gerenciado.

A seguir, é detalhada a composição básica de um Plano de Comunicação de Crise Cibernética:

- Identificação de prováveis cenários de ciberincidentes e correspondentes planos de ações;
- Identificação do público alvo e partes interessadas para cada cenário de ciberincidente;
- Identificação de porta-voz primário e perito técnico que representará as organizações envolvidas e falará com a mídia;
- Identificação dos canais/plataformas de comunicação/divulgação; e
- Estabelecimento de uma equipe de gerenciamento de comunicação de crise e condições para sua ativação.

A IS 107-001 [IS 107, 2019] e a IS 108-001 [IS 108, 2019] apresentam, respectivamente, Plano de Contingência para Operadores de Aeródromo e Operadores Aéreos. Nos cenários de ameaça apresentados nesses regulamentos não há ainda a criação de fluxos de acionamento para casos de ameaças cibernéticas. No entanto, a estrutura de fluxos presentes nas IS pode servir de modelo para os operadores criarem os fluxos de acionamento e de ações nos casos de contingências envolvendo ameaças cibernéticas.

4.4.6 ANÁLISE PÓS-EVENTOS

A análise realizada após a conclusão da resposta ao incidente e o restabelecimento das operações normais da aviação é essencial para o estabelecimento de um ciclo de melhorias, no qual a experiência gerada por uma ocorrência passada é utilizada como subsídio para robustecer a proteção contra futuros ataques, eliminar ou mitigar determinadas vulnerabilidades, estabelecer novos mecanismos de proteção e reduzir o ciber-risco global.

A fim de identificar as possíveis causas raízes do(s) evento(s) é desejável que a análise seja realizada conjuntamente com fornecedores, construtores e autoridades apropriadas. As autoridades devem

compartilhar as análises com outros interessados da indústria para ajudar a criar um plano de resposta à futuros ataques, bem como fechar lacunas de vulnerabilidades. Após a análise do incidente de segurança, autoridades devem identificar referências cruzadas com as análises e/ou documentações pré-existentes.

Após esta etapa, todos os resultados encontrados e relatados à ANAC, via DSAC, serão divulgados para os operadores por meio de relatórios semestrais. Mesmo assim, a indústria da aviação civil pode também desenvolver seus próprios meios de compartilhamentos de informações acerca dos eventos de cibersegurança, propiciando ferramentas mais dinâmicas de troca de informações.

4.5 ASPECTOS DE SEGURANÇA CIBERNÉTICA RELACIONADOS A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A informação é um ativo que possui ampla relevância em qualquer tipo de organização. No caso de aeroportos e empresas aéreas essa constatação não poderia ser diferente: esse tipo de ativo possui uma dupla sensibilidade, pois a informação permite que o serviço seja prestado ao usuário final ao mesmo tempo em que gera uma série de vulnerabilidades que podem comprometer a segurança das organizações, ou seja, é um ativo extremamente importante tanto do ponto de vista operacional quanto do ponto de vista da segurança.

Está sendo dada cada vez mais atenção à informação no que tange à privacidade e à proteção de dados. Em especial, no Brasil, esse enfoque ganhou destaque quando da promulgação da Lei nº 13.709, de 14 de agosto de 2018 ("Lei Geral de Proteção de Dados" ou "LGPD"), a qual estabeleceu as regras e princípios aplicáveis às atividades de tratamento de dados pessoais.

Sendo assim, os ativos informacionais e dados pessoais sensíveis ganharam uma dimensão de importância não somente relativa à segurança operacional e à segurança contra atos de interferência ilícita, mas também no que toca à privacidade dos titulares de dados pessoais, na medida em que, por força normativa, sua violação incorre na responsabilização dos agentes econômicos que exercem atividades de tratamento de dados pessoais – categoria que inclui organizações interessadas na aviação civil. Por isso mesmo, quaisquer sistemas e ferramentas que visam a garantir a confidencialidade, integridade e disponibilidade da informação, isto é, a segurança da informação devem considerar e incorporar regras e princípios relativos à proteção de dados.

É complementar abordar os temas da cibersegurança e da proteção de dados, considerando suas diferenças, mas principalmente sua complementariedade simbiótica, destacando a importância de se pensar a cibersegurança a partir da privacidade de dados. Cibersegurança se enquadra como uma segmentação específica da segurança da informação, isto é, a objetivo principal da cibersegurança é a preservação da informação e da infraestrutura relacionada a ela no que concerne aos ativos cibernéticos e ao ciberespaço, comumente relacionados à tecnologia da informação. Assim, a cibersegurança está vinculada a ferramentas técnicas que permitam a proteção de dados

e informações dentro do ciberespaço, como gerenciamento de permissões, classificação de dados, gerenciamento de identidade e acesso (logs), estabelecimento de controles cibernéticos, *firewall*, câmeras de segurança, análise comportamental do usuário, entre outras.

Já a proteção de dados, por sua vez, não possui como objeto o dado em si, mas "seu objetivo está intrinsicamente vinculado à proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" [Maldonado, 2019]. Significa, que o alvo da tutela da privacidade de dados é o indivíduo em face de possíveis violações dos seus direitos e liberdades individuais com base no princípio de autodeterminação informativa, isto é, o controle pessoal sobre o fluxo de dados relativos ao próprio indivíduo titular de dados pessoais.

Vê-se, então que há uma diferença no foco entre a cibersegurança (enquanto componente da segurança da informação) e a proteção de dados. Esta protege a pessoa natural, o indivíduo titular de dados pessoais identificado ou identificável, enquanto a primeira visa assegurar a preservação do dado ou a informação. É importante notar que apesar da clara diferença de foco entre ambas, ainda assim há uma intersecção importante entre as matérias e é preciso que haja uma necessária compatibilização entre a atuação simultânea de cada.

A proteção de dados é de significativo interesse aos praticantes de cibersegurança, na medida em que inclui uma série de obrigações relacionadas à segurança de dados. A lei de proteção de dados, não é, contudo, um sistema generalizado endereçado a cada aspecto da cibersegurança. O foco permanece em princípios específicos adotados para apoiar direitos individuais em um contexto de tratamento de dados [Maldonado, 2019].

Em primeiro lugar, os recursos e ferramentas de cibersegurança utilizadas podem e devem ser aproveitados como medidas procedimentais que visam a proteger o titular de dados pessoais. Isto é, por um lado, o ferramental de cibersegurança garante a manutenção da confidencialidade, integridade e disponibilidade da informação e, pelo outro, disponibiliza recursos fundamentais a qualquer organização que lida com ativos informacionais cibernéticos para preservar o fluxo de tratamento dados pessoais de maneira adequada à legislação. Portanto, aderir e considerar conceitos e regras de proteção de dados aos sistemas que gerem a segurança da informação e a cibersegurança amplia o escopo de proteção do sistema ao otimizar os recursos para uma dupla função.

Ao se analisar melhores práticas e recomendações internacionais no tema, já se observa que a tendência mais recente e recomendada às organizações é a de que seus sistemas que regem a segurança da informação incorporem requisitos e diretrizes para a proteção de dados pessoais.

Com a crescente relevância e dimensão do tratamento de dados pessoais pelas organizações foi elaborada em conjunto pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC) – organizações internacionais de padronização de boas práticas – a ISO/IEC 27701, norma-padrão que atualiza as ISO/IEC 27001 e ISO/IEC 27002, as quais estabelecem, respectivamente, (i) requisitos para estabelecer, implementar, manter e aprimorar um Sistema

de Gestão de Segurança da Informação (SGSI) e (ii) diretrizes práticas para a implementação e gerenciamento de controles.

A ISO/IEC 27701 atualiza as referidas normas de modo que adiciona requisitos ao Sistema de Gerenciamento de Segurança da Informação - SGSI - para considerar a proteção da privacidade de dados pessoais. Em adição, atualiza e adiciona diretrizes práticas com relação às fornecidas pela ISO/IEC 27002, estendendo os controles para conter objetivos específicos para agentes de tratamento de dados pessoais. A ISO 27701 representa um avanço nas práticas de governança reconhecidas pelo mercado, sendo recomendada para as organizações que contemplem o tratamento de dados pessoais dentre suas atividades de relevância. A aplicação dos seus controles fornece a adequada preservação aos elementos da informação, enquanto traz consigo adequações aos controles para atendimento aos requisitos estipulados na LGPD e GDPR (*General Data Protection Regulation*).

Vale mencionar que algumas ameaças específicas da abordagem unicamente focada em segurança da informação podem não corresponder às fragilidades e questões a serem consideradas quando da violação dos direitos dos titulares. Além disso, a ausência dessas considerações impede que o desenho do sistema de cibersegurança possa ser adequado a respeitar os princípios da LGPD e atender aos direitos dos titulares.

Visando trazer um panorama sobre a importância de se considerar aspectos da proteção de dados para a cibersegurança em aviação civil, serão apresentadas algumas considerações de como privacidade de dados deve ser tida como extremamente importante aos agentes do setor.

Grandes organizações da aviação mundial se adequaram à legislação de proteção de dados. Diante da promulgação e vigência da legislação europeia relativa à proteção de dados (GDPR) tornou-se impossível que os agentes não incluíssem entre suas preocupações a privacidade e o adequado tratamento de dados pessoais.

Os operadores aeroportuários se adequaram às legislações relativas à proteção de dados pessoais disponibilizando avisos de privacidade e estabelecendo diversas políticas e processos ligados a atividades de tratamento de dados pessoais, como anonimização dos dados, informação dos direitos dos titulares, políticas de coleta, retenção e descarte de dados e adequação de serviços que utilizam dados pessoais (serviços de estacionamento, aplicativo do aeroporto, programas de pontos e prêmios, compras *online* e serviço de *Booking*).

A não conciliação de medidas adequadas à proteção de dados pessoais pode ensejar a sanções pecuniárias severas. Alguns casos de incidente de segurança da informação ligados à violação dos direitos de privacidade de dados demonstram a inevitável vinculação entre a proteção de dados e a cibersegurança. Destaca-se a importância que medidas adequadas de cibersegurança tem com relação à proteção de dados pessoais, ainda que não haja quaisquer violações à segurança operacional ou atos de interferência ilícita.

A inserção da proteção de dados na cibersegurança da aviação é amplamente reconhecida. Como vem sendo reforçado, a inserção de elementos da proteção de dados pessoais na cibersegurança é um elemento que deve ser considerado por qualquer agente econômico que lide com o tratamento de dados pessoais.

Ao cabo, visualize-se que atualmente, diante das evoluções normativas e organizacionais, tanto em âmbito nacional como internacional, existe uma inevitável intersecção simbiótica entre a proteção de dados e a segurança da informação, em especial a cibersegurança – apesar dos distintos focos. Essa interação também é considerada para a aviação civil.

Desse modo, endereçar o tema da cibersegurança a partir dos princípios e requisitos contidos na LGPD e demais normas relativas a boas práticas na privacidade de dados permite aproveitar sinergias ao passo em que se cumpre paralelamente os objetivos da segurança da informação e da proteção de dados pessoais com um mesmo recurso. Contudo, é preciso ressaltar que as sinergias decorrentes dessa interação podem ser suprimidas e até mesmo prejudicadas a partir do momento em que se distancie as ferramentas da cibersegurança das noções de proteção de dados.

Assim, é importante que os profissionais responsáveis AVSEC busquem conciliar as demandas de cibersegurança no enfoque AVSEC com as demandas de cibersegurança relacionadas a LGPD, que eventualmente são abordadas por áreas diferentes na estrutura organizacional das empresas. Sugere-se que haja interação com as áreas responsáveis pela proteção de dados, com a intenção de atacar vulnerabilidades que sejam compartilhadas.

5. INFORMAÇÕES IMPORTANTES PARA A REALIZAÇÃO DE AVALIAÇÕES DE RISCOS

No intuito de conscientizar as organizações da aviação civil, a proposta deste capítulo é abordar alguns tópicos relevantes sobre a realização de avaliação de riscos cibernéticos.

5.1 INFORMAÇÕES SOBRE A SITUAÇÃO PRESENTE DE UM ATAQUE EM POTENCIAL

As informações de situação apresentam o cenário atual em função de aspectos sociais, econômicos, políticos, legais, de logística, de lógica, acesso à serviços, dados e informações, classificação das informações, entre outros.

Ainda, para que a descrição do contexto da situação atual seja a mais fiel possível, deve-se responder a uma série de perguntas envolvendo os diversos aspectos elencados acima.

Como exemplificação, seguem abaixo questões que podem ser respondidas para alguns dos aspectos em discussão:

- Há voos que possam ser considerados alvos potenciais como, por exemplo, aqueles com ligação a localidades potencialmente sujeitas a atos de interferência ilícita?
- Há histórico de realização de eventos de grande visibilidade e repercussão na mídia nacional ou internacional na região de influência do aeródromo?
- Qual é o volume de tráfego semanal de voos regulares em operação no aeródromo?
- Existe problemas econômicos (qualquer estado de crise econômica capaz de resultar em severos cortes orçamentários, que possam impactar na manutenção das medidas de segurança da aviação civil)?
- O aeródromo tem um peso considerável na economia como infraestrutura crítica da país?
- Há presença de dignitários, celebridades ou pessoas que sejam potencialmente sujeitas a ataques individuais (custodiados de alta periculosidade, pessoas incluídas em programa de proteção à testemunha etc.)?
- Existência de crise interna (revolta, distúrbio ou comoção interna, tais como guerra civil iminente ou em andamento ou qualquer outra instabilidade política) na região de influência do aeródromo?
- Existe histórico de ciberataques, com potencial para conduzir ato de interferência ilícita contra a aviação civil no aeroporto?
- Há informações específicas acerca da possibilidade de ocorrer um ciberataque através desse cenário de ameaça?
- O Sistema de TIC desta organização está integrado à Internet?
- Sistema de TIC desta organização está integrado aos sistemas de TIC das aeronaves/linhas aéreas?
- Os dados desta organização estão armazenados na nuvem?
- Um ataque cibernético tem o potencial de causar estragos em grande escala nos principais centros de transporte aéreo em todo o país e levar a um grande número de atrasos, cancelamentos de voos e alertas de segurança mais rigorosos?
- O aeródromo tem um peso considerável na logística de transporte de cargas?
- A organização tem adotado uma metodologia de gerenciamento de risco para determinar os níveis de criticidade dos serviços e dos suportes de TIC?
- Têm sido identificados eventos de segurança que poderiam interromper os serviços de suporte dos processos de negócios críticos?
- Tem sido quantificada a sua probabilidade de ocorrência de ataque e seu potencial impacto ou consequência?
- Existe um inventário sobre ameaças à AVSEC e a vulnerabilidades conhecidas que possam ser usadas para suportar uma avaliação de risco?

5.2 CIBERAMEAÇAS

Aeroportos ao redor do mundo estão caminhando em direção a uma arquitetura centralizada objetivando a necessidade de compartilhamento de informações e fornecimento de serviços de modo eficiente. Isto significa que ativos físicos, tais como leitores de bilhetes de embarque (*scanners*) e monitores (painéis informativos), estarão conectados aos sistemas do aeroporto e *hackers* podem ganhar acesso aos sistemas internos através da conexão habilitada nestes ativos.

A indústria da aviação vem enfrentando o seguinte dilema: por um lado, objetiva proteger sistemas críticos com segurança e em várias camadas; por outro, é demandada a abrir plataformas para permitir um maior compartilhamento de informações e a colaboração entre seus parceiros e colaboradores, além de proporcionar uma experiência de conforto sem interrupções aos passageiros.

De acordo com o Diretor de Estratégia e Gerenciamento de Segurança da Agência Europeia de Segurança da Aviação (EASA), ocorrem cerca de 1.000 ciberataques por mês a aeroportos em todo o mundo [Euractiv, 2016]. Em adição, como exemplo da extensão das ameaças, a Cathay Pacific Airways, empresa aérea de Hong Kong, sofreu a maior quantidade de ataques cibernéticos no ano de 2018, um deles resultou no vazamento de 9.4 milhões de registros de dados [Cathay, 2018].

Certamente a aviação civil, como já descrito, é uma infraestrutura crítica de Estado, que é vulnerável a ameaças e que, para atingir a sua finalidade, necessita do uso de componentes críticos da tecnologia da informação e das comunicações, os quais são igualmente vulneráveis a ciberameaça de *hackers* e atores maliciosos [Schober et all, 2012], pois tais sistemas trabalham por natureza de forma interconectada.

Sabe-se que os sistemas de TIC foram originalmente projetados para fornecer disponibilidade, mas não segurança. Do mesmo modo, foram construídos de forma isolada com relação aos sistemas de Tecnologia Operacional (TO) (ex.: carroceis de bagagem, controle de iluminação, etc...), logo estes necessitam ser protegidos contra ataques cibernéticos.

Nesse contexto, a superfície de ataques cibernéticos cresceu com a integração da Tecnologia da Informação e das Comunicações (TIC), com a Tecnologia Operacional (TO), pois os invasores agora são capazes de explorar lacunas de segurança em redes de TIC e, depois moverem-se lateralmente para sistemas de TO, que são bem menos protegidos.

É recomendado que os regulados e seus parceiros façam a *identificação de seus sistemas críticos* de TIC e o levantamentos das *vulnerabilidades* destes, juntamente com os impactos em seus negócios, com propósito de implementação de uma *avaliação de riscos* focada na temática da cibersegurança de suas operações.

Em resumo, uma *ameaça* é qualquer circunstância ou evento com potencial para impactar negativamente as operações e ativos organizacionais, outras organizações, indivíduos ou a nação através de um sistema de informação via acesso não autorizado, destruição, interrupção,

ou modificação da informação, e/ou da negação de serviço [NIST, 2012]. As fontes de ameaças incluem ataques físicos ou cibernéticos, erros humanos de omissão ou comprometimento, falhas estruturais nos recursos da organização e desastres naturais e/ou causados pelo homem, acidentes e falhas fora de controle da organização.

Para *identificar* as ameaças é importante encontrar e registrar os perigos possíveis que possam estar presentes ou junto aos ativos de TIC. É importante contar, na equipe de identificação, com a presença de pessoas familiares e não familiares com o(s) ativo(s) em questão. Em ambos os casos, a pessoa ou a equipe que realizará a avaliação de riscos deve ter competência e um bom conhecimento sobre a ameaça que está sendo avaliada. Ainda, para que todas as possíveis ameaças sejam identificadas deve-se levar em conta atividades tais como: manutenção, reparo e limpeza; acidentes, incidentes, condições onde os procedimentos de controles estão indisponíveis, determinar se um componente de TIC pode ter a sua salvaguarda removida; revisar todas as fases do ciclo de vida do ativo; e examinar os riscos de presença de pessoas externas.

Para saber se uma ameaça pode causar um dano, cada um dos ativos de TIC deve ter o seu nível de risco determinado. Para tanto, é necessário observar requisitos de legislações e/ou padrões aplicáveis, experiências passadas, informação e documentação sobre o produto/serviço, boas práticas e a reputação das organizações envolvidas. Enfim, com tais informações em mãos, será possível ranquear ou priorizar as ameaças por níveis de seriedade, permitindo uma adequada alocação de recursos de segurança.

Vários modelos de risco são criados em função dos detalhes e complexidade com que as ameaças são identificadas. Assim, uma fase de conhecimento do contexto é bastante importante para a análise a ser desenvolvida. Se as ameaças podem ser identificadas com grande especificidade, cenários de ameaças podem ser modelados, desenvolvidos e analisados de forma mais precisa.

Ciberataques podem ocorrer a qualquer tempo e alguns tipos podem ser facilmente detectados, tais como: injeção de *malware*, método da força bruta, *ransomware* e negação de serviço distribuídos (DDoS). Já outros podem não ser identificados e permanecerem hibernando dentro da rede ou sistemas por longos períodos tais como: *worms*, cavalos de Tróia e outras ameaças persistentes, que aguardam a hora de agir. A imediata detecção destas ameaças é crítica para operações seguras e disponibilidade dos sistemas críticos de TIC.

Ainda, sobre as ameaças cibernéticas, elas podem ser entendidas como uma provável subversão, acidental ou premeditada, de um sistema de segurança dos ativos críticos de TIC e/ou TO.

O sistema de aviação civil, portanto, precisa melhorar sua resiliência a ameaças cibernéticas, ou seja, o sistema deve ser capaz de suportar e recuperar-se de um estado de desempenho reduzido resultante da ocorrência de ameaças e incidentes ciber-relacionados, incluindo entre outros, tanto a perda ou corrupção de dados e interrupções no sistema, quanto a perda de conectividade ou interoperabilidade.

5.2.1 EXEMPLOS DE TIPOS DE FONTES DE CIBERAMEAÇAS

Apresenta-se a seguir as ciberameaças mais conhecidas que podem atingir os sistemas críticos dos componentes do sistema de transporte aéreo organizados por contextos:

a) AMBIENTAIS

Incêndio, inundação, neve, vazamento de água, temperaturas extremas, tempestades de areia, roedores, vibração, terremotos, furacões, tornados, raios, interferência eletromagnética, carga eletrostáticas, humidade extrema, temperatura extrema, dificuldade de acesso, incidente nuclear, explosão vulcânica, incidentes químicos, pandemia, meteorito e lixo espacial.

b) FÍSICOS (Ações Pessoais)

Roubo, vandalismo, sabotagem, extorsão, terrorismo, ameaça da bomba, agitação civil, guerra, instabilidade política, uso de ferramentas magnéticas, falta de energia, manutenção inadequada, acesso não autorizado às instalações, mal aterramento (ruído elétrico).

c) TÉCNICOS

Operação imprópria, modificação não autorizada do *hardware/software*, duplicação não autorizada do *software*, acesso lógico não autorizado, uso não autorizado de *software* e ferramentas administrativas, instalação não autorizada de *software*, fraude de identidade, uso de informações de fontes não confiáveis, uso não sancionado ou excedente de licença, uso de *software* malicioso (vírus, *worm, trojan, rootkit, exploit kit, botnet, spyware, ransomware, scareware, adware*), *malwares, phishing*, modificação/deleção acidental de *software*, divulgação acidental de dados críticos, modificação/deleção acidental de dados, divulgação acidental de dados, descarte de mídia de dados, roubo de mídia de dados, erro no código de programas, registro de mensagem para uso posterior, Inundação de mensagem (negação de serviços) – DoS ou DDoS, conexão à linha de comunicação sem autorização, exploração de vulnerabilidades de *softwares*, ataques de interceptação –, ataque social, adulteração com dispositivos do aeroporto e erros de configuração.

d) FALHAS NO SISTEMA

Falhas nos dispositivos ou nos sistemas, falhas ou interrupções nos *links* de comunicação, falhas em partes de dispositivos, falhas ou interrupção no fornecimento de energia elétrica, falhas de *hardware* e erros de *software*.

e) FALHAS DE PARCEIROS FORNECEDORES DE SERVIÇOS

Provedor de serviço de internet, provedor de serviço de nuvem, provedor de utilidades (energia, gás, água), provedor de manutenção remota, companhias de testes de segurança.

As probabilidades de ocorrências de ataques de uma determinada ciberameaça baseiam-se na intenção do grupo ou do indivíduo e na sua real capacidade de realizar o ato. E são obtidas através de respostas objetivas realizadas às perguntas sobre as informações que representam o vetor de ameaças. Elas podem ser classificadas, por exemplo, em *Alta, Média Alta, Média, Média Baixa e Baixa*, as quais, em geral, podem possuir um valor numérico característico associado.

Em [Capec, 2020] apresenta-se uma classificação e enumeração de padrões de ataques comuns que são utilizados para explorar vulnerabilidades de *software* e/ou *hardware*. A lista de padrões de ataques está organizada por tipos de mecanismos de ataques ou opcionalmente por domínios de ataque.

Já no anexo C de [ISO 27005, 2008] apresenta-se uma lista de ameaças cibernéticas típicas e suas possíveis origens: deliberada, acidental ou ambiental, ao passo que no apêndice A de [ACPR, 2015], encontra-se uma extensiva lista de ameaças cibernéticas que podem afetar dados e sistemas de aeroportos.

5.3 VULNERABILIDADES

Muitos ciberataques tiveram sucesso porque exploraram bem conhecidas vulnerabilidades que não tinham sido tratadas apropriadamente, dada a falta de ação das organizações que não acreditavam que poderiam ser afetadas.

Vulnerabilidade é a qualidade ou estado de um recurso e/ou de seu ambiente ser exposto à possibilidade de ser atacado ou prejudicado. Vulnerabilidade reflete fraqueza, fragilidade, insegurança, instabilidade ou indefensabilidade de um sistema de informação, procedimento de sistema de segurança, controles internos, ou implementação que pode ser explorada por uma ameaça. A vulnerabilidade permite que uma ameaça se realize, seja por fraqueza ou omissão. Identifica-se *cibervulnerabilidade* quando o recurso e/ou seu ambiente envolve componentes da TIC ou TO.

Em geral, para a exploração das vulnerabilidades dos sistemas, os *hackers*, quando motivados, frequentemente fazem uma pesquisa e realizam o mapeamento, o mais completo possível, da empresa alvo antes de iniciarem o ataque. Em seguida, fazem uma varredura no computador ou em algum dispositivo da rede buscando por fraquezas na segurança, e logo que as localizam as exploram lançando um ataque de infiltração.

A engenharia social é um outro método bastante conhecido para se explorar vulnerabilidades cibernéticas. Em geral, o criminoso explora a natureza humana da confiança para violar práticas de segurança normais, e obter acesso não autorizado a redes de computadores e dados confidenciais. O clássico e-mail de "*phishing*" e os golpes com vírus, por exemplo, são repletos de insinuações de conotação social. Os e-mails de "*phishing*" tentam convencer os usuários de que são, de fato, de fontes legítimas, na esperança de conseguir obter qualquer dado pessoal ou corporativo, por menor que seja [Kaspersky].

Avaliações de vulnerabilidades são questões técnicas tipicamente desempenhadas através de acesso à documentação, configurações e pessoas com o propósito de obter o máximo de entendimento de toda a fraqueza potencial de segurança da organização. Dentre as avaliações técnicas que são mais frequentemente realizadas têm-se: teste de intrusão, determinação de

cumprimento de requisitos de conformidades, revisão de tráfego de rede, revisão de configurações dos sistemas, identificação de protocolos, portas e arquitetura de redes e escaneamento de vulnerabilidades.

5.3.1 EXEMPLOS DE ALGUMAS CIBERVULNERABILIDADES

A seguir apresenta-se uma lista não exaustiva de possíveis pontos de cibervulnerabilidades presentes em componentes do sistema de transporte aéreo, organizados por contextos:

a) COMUNICAÇÃO:
Comunicação sem fio inadequadamente assegurada; Uso de canais de comunicação não dedicados para comando e controle; Dados de controle e comandos não autenticados; Interrupção de serviço de telefonia; Dispositivos Móveis; Roteadores; Aplicações Móveis; Portais de Consumidores; Linhas de comunicação móveis abertas; Linhas telefônicas fixas desprotegidas; Canais de radiofrequência.

b) SOFTWARE
Falha de projeto; testes insuficientes; falta de treinamento em auditoria; pontos de acesso *wireless*; pontos de acesso em redes; banco de dados SQL inseguros; *firewalls* mal configurados; redes interconectadas com fraca segurança; falta de criptografia segura de dados; permissão de injeção de comando do sistema operacional; permissão de injeção comandos SQL para acesso a base de dados; possibilidade de estouro de capacidade de memória ("*buffer overflow*"); cálculo incorreto do tamanho do *buffer*; falta de autenticação simples e/ou dupla para funções críticas; restrição imprópria ao número de tentativas de autenticação; falta de autorização; autorização incorreta; uso de credencial codificada em *hardware*; permissão incorreta de uso de recurso crítico; carga ("*upload*") irrestrita de arquivos de tipos perigosos; confiança sobre entradas não confiáveis na decisão de segurança; permissão para a carga de códigos sem checar a integridade; uso de algoritmos incompletos; redirecionamento de URL a *sites* não confiáveis; caminho transversal; presença de defeitos nos códigos utilizados; constatações de senhas fracas; uso de *software* que já está infectado por vírus; execução com privilégios desnecessários; uso de senhas sem criptografia; *string* com formato não controlado.

c) HARDWARE
Falhas de projetos; humidade; poeira; sujeira; armazenamento desprotegido; modificação não autorizada; configuração não autorizada; erro de *hardware*; conexões em *hardware* não protegidas, tais como entradas USB, portas seriais, paralelas, *ethernet*, ou mesmo conexões sem fio, como *wi-fi* e *bluetooth*.

d) REDES
Linhas de comunicação desprotegidas; arquitetura de rede insegura.

e) PESSOAL/EQUIPE
Processo de recrutamento inadequado; conscientização de segurança da informação inadequada.

f) LOCALIZAÇÃO FÍSICA
Área sujeita à inundação; fonte de energia insegura.

g) ORGANIZACIONAL
Falta de auditorias regulares; falta de planos de continuidade de negócios; falta de segurança; sistema de controle de passaporte digital; sistema de controle de partidas; sistema de gerenciamento de voo; transporte de materiais perigosos; sistema de reservas de passagem.

5.3.2 LISTA DE QUESTÕES SOBRE CIBERVULNERABILIDADES

Em sequência se apresenta uma lista, não exaustiva, de questões que podem ser utilizadas para auxiliar a organização na identificação das vulnerabilidades do seu sistema de TIC.

a) SERVIÇOS / INFORMAÇÕES / DADOS
- Tem sido definido o ciclo de vida para os serviços e seus sistemas TIC relacionados?
- Está disponível documentação suficiente para os serviços e sistemas TIC relacionados?
- Os serviços e seus sistemas TIC relacionados têm sido testados usando algum critério de segurança antes da aceitação ou do desenvolvimento?
- Os dados de entrada das aplicações têm sido validados para assegurar o processamento correto e apropriado?
- A aceitação dos resultados dos testes de segurança e o risco residual incluem a aceitação do proprietário dos serviços?
- Têm sido segregados os ambientes dos serviços de desenvolvimento, testes e produção/ operacional e dos sistemas TIC relacionados?
- São fornecidos treinamentos adequados para o uso correto e operacional dos serviços e seus sistemas de TIC relacionados?

b) ACESSO A SERVIÇOS / INFORMAÇÕES (CONTROLE DE ACESSO)
- Na concessão de acesso externo, os riscos têm sido identificados? Um controle apropriado tem sido implementado?
- Foi estabelecida, documentada e revisada, uma política de controle de acesso para os serviços e sistemas, baseada nos negócios e requisitos de segurança?
- São os eventos relacionados à segurança registrados, preservados?
- Tentativas de login sem sucesso são monitoradas e contramedidas são adotadas quando um número máximo é atingido?
- Uma sessão de acesso é terminada após um período específico de inatividade?
- Existe um procedimento de registro e de eliminação de registro de usuário formal para conceder e revogar o acesso a todos os serviços?
- A alocação e o uso de privilégio são restritos e controlados?

c) ACORDOS DE NÍVEIS DE SERVIÇOS - SLA

- Os SLA estabelecidos com terceiros envolvendo informações e infraestrutura para processamento de informações cobrem requisitos AVSEC relevantes?
- O uso aceitável de bens e serviços de informação está claramente estabelecido?
- Tem sido identificado os requisitos por confidencialidade ou não interrupção dos acordos, refletindo as necessidades da organização por proteção à informação?

d) CLASSIFICAÇÃO DA INFORMAÇÃO

- A organização mantém um inventário de ativos de informação, sua propriedade e sua rastreabilidade para os serviços que expõem essas informações a terceiros?
- Existe um sistema de classificação documentado e acordado para informações que são usadas para definir medidas de proteção?
- Existe um conjunto apropriado de procedimentos para rotular e manusear informações de acordo com o esquema de classificação?
- Existe um conjunto apropriado de procedimentos para o descarte de material físico em função da classificação da informação?

e) INFRAESTRUTURA – PROTEÇÃO DO SISTEMA TIC

- O sistema de suporte de TIC define o uso de quotas para usuários, processos e serviços?
- O sistema de suporte de TIC tem controles e medidas protetivas para diferentes tipos de ataques de DDoS (ataque distribuído de negação de serviço)?
- O sistema de suporte de TIC está protegido conta a execução de código não autorizado?
- Os eventos de segurança são detectados, registrados e armazenados seguramente?
- Sessões inativas são terminadas após uma quantidade de tempo?
- O sistema de TIC é composto por *softwares* com origem, autenticidade e integridade?
- O sistema de TIC está sujeito a uma avaliação de vulnerabilidade anual documentada que inclui testes de penetração?

F) AUTENTICAÇÃO, AUTORIZAÇÃO E NÃO-REPÚDIO

- Existe uma política de autenticação definindo credenciais de segurança válidas, com ciclo de vida, força, processo de emissão e renovação, com armazenagem e transmissão seguras?
- O sistema de suporte à TIC identifica unicamente os usuários, serviços e dispositivos?
- Existe algum controle para habilitar a autenticação?
- O controle de acesso é controlado com base na função do usuário?
- É imposto o uso de senhas fortes?
- O acesso à entidade que controla o número de tentativas de autenticação é restrito?
- É imposto controle de acesso de qualquer requisição com origem ou destino a uma rede externa?

G) GERENCIAMENTO OPERACIONAL

- Existe algum mecanismo de proteção colocado para impedir a adulteração ou acesso não autorizado de logs/ferramentas, entre outros?
- Existem controles de detecção, prevenção e recuperação para proteger contra a execução de códigos maliciosos em todos os sistemas?
- O processo de aceitação inclui a aceitação dos resultados dos testes de segurança e risco residual pelo proprietário do sistema?
- Os itens de segurança têm sido obtidos e implementados de maneira adequada?
- Os sistemas de desenvolvimento, teste e infraestrutura operacional são separados para reduzir os riscos de acesso não autorizado ou alterações no sistema operacional?

Em [CWE, 2020] é apresentada uma lista com vulnerabilidades de segurança comuns em *hardware* e *software* que fornece uma linguagem de comum entendimento em TIC, um instrumento de medida para ferramentas de segurança, além de possibilitar a identificação de fraquezas, mitigação e esforços de prevenção. No apêndice D de [ISO 27005, 2008] encontra-se uma lista extensiva de vulnerabilidade cibernéticas e suas possíveis ameaças organizadas por tipos como: *hardware*, *software*, redes, pessoal, sítio e organização

5.4 IMPACTOS, PREJUÍZOS, CONSEQUÊNCIAS OU DANOS EM POTENCIAL

O fornecimento de uma visão detalhada de como um ciberataque pode impactar nos negócios e nas relações com os parceiros dará aos membros do conselho gestor da organização um melhor entendimento de quais prejuízos diretos e indiretos podem ser sofridos.

O impacto da ocorrência de uma ameaça é a severidade do dano que pode ser esperado resultar das consequências de interrupção, modificação, destruição não autorizada de informação, perda de informação ou de disponibilidade de sistema de informação. Assim, um dos fatores importantes para se avaliar o risco é a severidade de cada potencial impacto nos ativos críticos de TIC da organização.

Impactos também podem ser: perda da eficácia atual ou futura da missão/negócios devido à perda da confidencialidade dos dados; perda de confiança em informações críticas devido à perda de dados ou de integridade do sistema; indisponibilidade ou degradação de informações ou dos sistemas de informação.

É importante identificar as consequências das ocorrências de sucesso de cada uma das ameaças. Este passo é realizado sem considerar a aplicação dos controles ambientais e avaliando os *danos* causados se a ameaça for exercida. É uma função da natureza e da escala das consequências em termos dos aspectos apresentados nas seções 5.2 e 5.3 para o sistema da aviação civil, sendo expressas quantitativa ou qualitativamente. E podem ser escaladas como: Alta, Média Alta, Média, Média Baixa e Baixa, as quais, em geral, possuem um valor numérico característico associado. Geralmente, os riscos, quando mais de um, são agrupados de acordo os tipos de impactos.

5.4.1 EXEMPLOS DE IMPACTOS

A seguir se exemplifica tipos de impactos de ciberameaças organizados por contextos:

a) Econômicos
Perdas financeiras; Roubo de informação corporativa e/ou financeira; Roubo de dinheiro; Redução dos lucros; Redução de clientes; Redução de crescimento; Redução de investimentos; Interrupção de operações *online*; Interrupção de vendas; Perda de negócios ou contratos; Perda de capital; Queda no preço dos estoques.

b) Dano à Reputação/Imagem
Perda de clientes; Perda de vendas; Redução de lucros; Redução na possibilidade de negócios; Redução de créditos; Perda de parceiros comerciais; Perda de equipe chave; Perda de certificação; Perda de fornecedores; Dificuldade de recrutar equipe desejada; Julgamento na mídia; Dano à percepção pública; Multas regulatórias; Custo de investigação; Pagamento de extorsão; Pagamento de compensação; Perda de trabalho; Engano.

c) Legais
Perda de segurança de dados pessoais.

d) Psicológico
Depressão; Vergonha; Embaraço; Desconforto; Frustação; Confusão; Aborrecimento/ansiedade; Culpa; Perda de autoconfiança; Baixa satisfação; Chateação; Mudanças negativas na percepção.

e) Social/Societal
Mudanças negativas na Percepção pública (tecnologia); Queda na moral interna da organização; Interrupção das atividades diárias; Impacto negativo na nação.

f) Físico/Digital
Perda de vidas; Danos à infraestrutura; Destruição; Roubo; Infecção; Comprometimento; Exposição/vazamento; Redução de desempenho; Ferimento corporal; Dor; Acusação; Abuso; Destrato; Roubo e identidade.

5.5 CONTROLES OU CONTRAMEDIDAS PARA CIBERAMEAÇAS

Baseando-se em seus tamanhos, complexidades e tipos de sistemas de TIC, as organizações prestadoras de serviços à aviação civil podem selecionar o seu controle de cibersegurança apropriado entre vários os padrões internacionais relacionados. Destaca-se os padrões ISO/IEC 27001 [ISO 27001, 2013], COBIT [COBIT, 2019] e a família ISO/IEC 13335-4 [ISO 13335, 2000] como exemplos que podem ser utilizados. O descrito a seguir visa conscientizar as organizações sobre as suas existências e auxiliar na seleção dos seus controles de segurança.

Dentro do contexto deste texto, controle pode ser qualquer processo, política, metodologia, técnica, prática, dispositivo, ações ou condições que mantém ou modifica o risco. Os controles de cibersegurança são aplicados para proteger os sistemas de TIC das organizações da aviação civil contra a degradação da confidencialidade, integridade e disponibilidade de seus recursos, sejam elas de causas intencionais ou acidentais. Estes controles podem ser organizados em níveis a depender do risco do TIC atribuído pela organização.

De acordo o Doc 9985 da OACI [Doc 9985, 2018], os controles de segurança de TIC podem ser organizados em 9 categorias, a saber: controles de políticas e direção organizacional; controles de gerenciamento, cultura e organização; controles de recursos humanos; controles de segurança ambiental e física; controles de sistemas de operação de TIC; controles de infraestrutura e mecanismos técnicos; controle de desenvolvimento e aquisição; controles de auditoria e monitoramento; e controles de conformidades. Estes controles estão relacionados com o modelo Confidencialidade, Integridade e Disponibilidade (CIA), apresentado no capítulo 5 do citado Doc e cuja tabela de relacionamento entre as categorias de controle citadas e o modelo CIA está apresentada na Tabela 1.

Ainda, segundo o Doc 9985, o Programa Nacional de Segurança da Aviação Civil contra Atos de Interferência Ilícita (NCASP), PNAVSEC no caso do Brasil, deveria destacar 3 (três) áreas de interesse para programas de segurança de TIC: *proteção de sistemas contra acesso não autorizado; prevenção de violação de sistemas; e detecção de ataques sobre sistemas*. A ANAC planeja a inclusão destas áreas de interesse no PNAVSEC.

5.5.1 EXEMPLOS DESTAS CATEGORIAS DE CONTROLE PARA PROTEGER OS TICS

Considera-se 3 (três) áreas de interesse:

a) Proteção de sistemas contra acesso e uso não autorizado:

- Segurança física do perímetro da infraestrutura;
- Defesa em profundidade na arquitetura segura da rede;
- Gerenciamento de identidade e ferramentas de controle de acesso.

b) Prevenção de violação de sistemas:

- Ferramenta de integridade de arquivo;
- Segregação do sistema de direitos e mínimo privilégios.

c) Detecção de ataques sobre sistemas:

- Sistema de prevenção de intrusão;
- Sistema de detecção de intrusão;
- Monitoramento de operações seguras para alertas e alarmes;
- Coleção de sistema de registro de informação.

5.5.2 MODELO CIA (*CONFIDENTIALITY, INTEGRITY, AVAILABILITY* – CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE)

A criticidade de um componente do sistema de TIC deve ser avaliada quando algum de seus elementos tem pelo menos um dos seguintes conceitos afetados: confidencialidade, integridade e disponibilidade (modelo CIA). A avaliação de ciber-risco no contexto do modelo CIA envolve a resposta a três questões relacionadas aos níveis do modelo (ver Figura 1), a saber:

1) Sobre qual(ais) componente(s) do modelo CIA estão impactando a falha?

2) Que tipos de perigos podem resultar desta falha?

3) Que impacto estes perigos têm sobre a segurança do aeroporto/empresas aéreas?

Assim, no contexto da aviação civil, segurança cibernética refere-se à aplicação de controles para proteger os sistemas TIC das suas organizações contra a degradação da confidencialidade, da integridade e da disponibilidade, frente às ameaças intencionais ou acidentais.

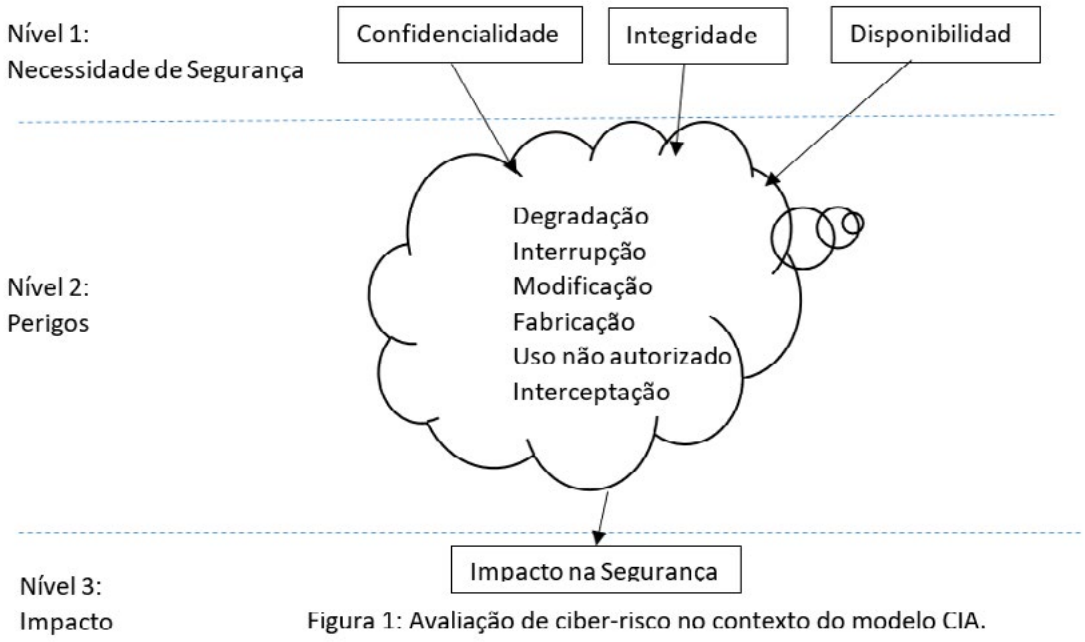


Figura 1: Avaliação de ciber-risco no contexto do modelo CIA.

A Tabela 1 relaciona os objetivos de segurança do modelo CIA com as 9 (nove) categorias de controles de segurança de TICs descritos na seção 6.4.

TABELA 1 – CATEGORIA DE CONTROLES E CIA

CATEGORIAS DE CONTROLE TIC	CONFIDENCIALIDADE	INTEGRIDADE	DISPONIBILIDADE
Política e Direção Organizacional	Política Organizacional dita a proteção da informação	Política garantindo que controles protegem integridade de dados	Política assegurando sistema propriamente dimensionado para garantir disponibilidade
Organização, Cultura e Gerenciamento	Procedimento de gerenciamento e Política de Proteção de Dados	Procedimentos e políticas para a manipulação de dados	Identificação de ativos e manutenção de recursos
Recursos Humanos	Treinamento de Empregados para a manipulação de Dados	Treinamento de empregados	Treinamento de empregados
Segurança Física e Ambiental	Perímetro de Segurança e proteções físicas	Segurança e controle de acesso a dados	Redundância e *backups* de equipamentos e *sites*
Operações de Sistemas TICs	Procedimentos para proteger mídias removíveis e Política de Interconexão	Controle de gerenciamento de mudanças	Acordo de nível de serviço para operações de sistema
Mecanismos Técnicos e Infraestrutura	Mecanismo de Criptografia	Ferramentas de Integridade de arquivos	Soluções de alta disponibilidade
Aquisição e Desenvolvimento	Requisitos de Operações para Proteção de Dados	Processo de gerenciamento de mudanças formais	Requisitos de operações para garantir disponibilidade
Monitoramento e Auditoria	Monitoramento e desempenho de auditoria da informação	Registros de Auditoria e Registro de mudança	Monitoramento da saúde e do uso os sistemas críticos
Conformidade	Controle de criptografia usado na conformidade com acordos e leis	Aderência à política relacionado com perdas, destruição ou falsificação de dados	Conformidade com planos de continuidade das operações

5.5.3 CUIDADOS GERAIS - BOAS PRÁTICAS

Com o intuito de auxiliar a comunidade aeroportuária, operadores de aeródromos, operadores aéreos e fornecedores a se protegerem de ameaças cibernéticas em evolução, a ENISA [ENISA, 2016] fez um compilado de boas práticas utilizadas atualmente. Essas práticas englobam fatores técnicos, baseados em ferramentas, políticas e normas, além de aspectos organizacionais, pessoas e processos. Em consulta a [ENISA, 2016] identificou-se em seus anexos um conjunto de boas práticas importantes de serem adotadas pela comunidade aeroportuária. O documento referenciado auxilia os decisores e pessoal de segurança a prevenir ataques cibernéticos e interrupções de serviço.

A seguir se resume as principais boas práticas:

- Use um sistema de detecção de intruso (IDS) o qual permitirá o monitoramento de dispositivos de *hardware* e *software* em redes cabeadas e sem fio. Os alertas de IDS devem ser analisados via ferramentas de investigação forense.

- Execute *softwares antimalwares* para detectar, remover ou colocar em quarentena *softwares* maliciosos. Eles podem ser utilizados em quiosques, equipamentos de TIC, sistemas de processamento de passageiros de uso comum, SCADA, serviços e dados sobre a nuvem.
- Mude as credenciais padrão dos dispositivos conectados à rede da empresa, tais como: roteadores, pontos de acesso, câmeras IP, câmeras de vigilância, quando não for necessário o acesso remoto, desabilite-o, e adote uma política de senhas fortes.
- Controle o uso do BYOD (*Bring Your Own Device*). É recomendável que o operador da entidade impeça que seus colaboradores conectem seus dispositivos pessoais nos sistemas do aeroporto. Onde isto não for viável, implante uma política de BYOD formal e completa, os empregados devem considerar seguir a política como parte de seu trabalho, aplique controles técnicos efetivos para proteger a organização e a infraestrutura de rede de dispositivos comprometidos. Para o caso do uso de mídias removíveis desabilite a auto execução ou a execução de arquivos portados.
- Monitore e audite em busca de invasores maliciosos: registros do sistema, monitoramento em tempo real, gerenciamento de integridade monitorando mudanças não autorizadas no sistema, e prevenção de perda de dados.
- Faça a atualização de *software* e *hardware*: o administrador do sistema do aeroporto deve planejar um procedimento de atualização do *software* para assegurar que o sistema é mantido atualizado, e assim mitigar a possibilidade de um ataque de segurança. O descarte de *hardware* obsoleto deve ser feito cuidadosamente para impedir o acesso a *software* e *hardware* especializados ou ainda com vida útil.
- Proteja a segurança dos sistemas: as entidades devem reduzir a superfície de vulnerabilidade do sistema: desabilitar instâncias de serviços, fechar portas, restringir o uso de dispositivos externos, regular *patches*. Nos dispositivos de redes só devem ter habilitados os serviços que serão de fato utilizados. Dispositivos externos (USB por exemplo) devem ser controlados e serem autorizado através de requisição explícita para evitar vazamento de dados e introdução não autorizada de *software*.
- Realize avaliação de segurança e teste de penetração.
- Sempre deve ser atribuído o menor privilégio ou autorização para usuários, processos, passageiros e empregados do aeroporto para desempenharem a sua função nos sistemas de TIC. Os dados do aeroporto devem ser classificados para assegurar que a informação é acessível apenas por quem tem direito ao acesso.
- Use criptografia de dados para proteção. Evite o uso de protocolos de comunicação inseguros e *wi-fi* não criptografados na rede. Use *Virtual Private Network* (VPN) para acesso remoto criptografado de colaboradores aos serviços do aeroporto.
- Proteja a borda da infraestrutura de rede do aeroporto com *firewall* para bloquear conexões remotas não confiáveis entre redes. O *firewall* deve ser configurado para permitir o acesso apenas para as portas e serviços requeridos. Adote a metodologia de defesa em profundidade para restringir o tráfego entre segmentos de rede e os *hosts*.
- Utilize um nível elevado de autenticação de usuário através de credenciais de nome e senha. O uso de autenticação biométrica pode favorecer a segurança no acesso aos sistemas e redes. Limitar o número de tentativas falhas no acesso pode mitigar o risco de ataques tipo força bruta ou de dicionários.

- Realize uma avaliação de risco para poder decidir entre configurar serviços e dispositivos que podem ser comprometidos de forma a permitirem o desligamento remoto por parte do operador do aeroporto frente a possibilidade de ataque remoto por *hackers*.
- Crie um plano de recuperação de incidentes/acidentes disponível para restaurar a operação de ativos críticos. Inclua aspectos técnicos e organizacionais no referido plano, estabeleça um critério para sequência dos sistemas que serão recuperados.
- Procure implementar padrões internacionais para gerenciamento do segurança da informação e para estrutura de segurança da informação.
- Estabeleça políticas de segurança da informação.
- Desenvolva processos de controle de qualidade e melhoria contínua.
- Estabeleça uma estrutura de trabalho de segurança de informação e de auditoria externa, com foco em certificações, de preferência seguido padrões internacionais, para avaliar a maturidade e demonstrar a conformidade.
- Nomeie um profissional responsável pela segurança da informação.
- Estabeleça um inventário de sistemas de informação.
- Desenvolva, monitore e reporte os resultados de medidas de desempenho de segurança da informação.
- Classifique sistemas de informação de acordo com a política de classificação de informação.
- Realize gerenciamento de riscos. Crie um registro e monitores.
- Desempenhe um contínuo monitoramento de segurança da informação.
- Solicite que fornecedores externos de sistemas de informação se alinhem com as políticas de segurança da informação da empresa ou se certifique de acordo com algum padrão internacional.
- Identifique todos os indivíduos que terão acesso ao sistema de informação da empresa.
- Gerencie o acesso físico e lógico dos usuários aos sistemas de informação da empresa.
- Certifique-se que antes de usuários terem acesso aos sistemas de informação da empresa aeroporto eles assinem um contrato de uso.
- Estabeleça requisitos de segurança, papéis e responsabilidades, para as equipes dos fornecedores.
- Forneça treinamento de conscientização para todo usuário do sistema de informação e treinamento especializado onde este for necessário.
- Documente e monitore as atividades de treinamento no uso dos sistemas de informação.
- Desenvolva um plano de contingência para o caso de acidentes envolvendo o sistema de informação, envolvendo a recuperação do ativo do sistema de informação e da sua operação.
- Treine os funcionários na contingência e recuperação do acidente.
- Teste e avalie os planos de contingência e recuperação.
- Forneça capacidades de respostas aos incidentes e teste os resultados.
- Treine os funcionários do aeroporto em seus papéis com relação ao sistema de informação.
- Rastreie e documente os incidentes do sistema de informação

Este tipo de classificação permite que a organização constitua em suas partes funcionais grupos menores de controles os quais deverão ser implementados para garantir o controle geral.

No anexo A de [ISO 27001, 2013], encontra-se uma lista de controles e objetivos de controles, alinhados com ISO/IEC 27002 [ISO 27002, 2013]. No apêndice C de [ACRP, 2015], encontra-se uma lista extensiva de contramedidas categorizadas e priorizadas que empresas podem considerar quando tratar vulnerabilidades e reduzir a probabilidade de um ataque cibernético bem-sucedido.

No apêndice C, deste manual, apresenta-se uma lista de outros 20 possíveis controles para sistema de TIC.

5.5.4 DIVULGAÇÃO RESPONSÁVEL DE VULNERABILIDADES

O Programa de Divulgação Responsável de Vulnerabilidades (*Vulnerability Disclosure Program*) consiste basicamente em um canal de comunicação entre um órgão/empresa com o mundo exterior, por meio do qual qualquer pessoa de fora da organização pode reportar vulnerabilidades presentes nos sistemas, processos ou plataformas tecnológicas da organização.

Atualmente existem duas normas ISO para auxiliar as organizações na criação de seus processos internos, sendo:

- *ISO 29.147 (Vulnerability Disclosure)*
- *ISO 30.111 (Vulnerability Handling Process).*

A ISO 29.147 tem por objetivo estruturar o processo de recebimento de vulnerabilidades, já a ISO 30.111 busca estabelecer os processos de gestão dessas vulnerabilidades.

É de suma importância que o processo de gestão das vulnerabilidades informadas tenha um nível de maturidade suficiente para poder atender aos requerimentos, do contrário será mais um problema a ser solucionado, gerando frustração tanto em quem informa como em quem recebe.

Para melhorar a segurança geral, cada organização precisa avaliar seus recursos e identificar e priorizar áreas que precisam de melhorias.

O *Vulnerability Coordination Maturity Model* (VCMM) fornece uma estrutura que avalia cinco áreas principais para ajudar as organizações a medir e desenvolver seus recursos de gerenciamento de vulnerabilidade. O Quadro 1 ilustra as cinco dimensões do modelo apresentado:

QUADRO 1 – DIMENSÕES DO MODELO

ÁREAS CHAVE	DESCRIÇÃO
Organizacional	Pessoas, processos, recursos para administrar as vulnerabilidades.
Engenharia	Capacidades para avaliar, remediar e propor melhorias.
Comunicações	Habilidades de comunicação (Interna/externa) a respeito das vulnerabilidades.
Analítica	Análise dos dados de vulnerabilidades e padrões para melhorar os processos.
Incentivos	Capacidade para encorajar os pesquisadores a reportar as vulnerabilidades diretamente para a sua organização

Recomendações:

- Execute a avaliação de maturidade para todas as 5 áreas do VCMM.
- Usando a avaliação, estabeleça metas e prioridades realistas para amadurecer a segurança de sua organização.
- Crie um roteiro para obter a conformidade com a ISO 30111 antes de tentar implementar a ISO 29147.
- Determine o orçamento necessário e contrate ou treine o pessoal interno.
- Meça as velocidades de resposta e a complexidade da vulnerabilidade para obter as métricas do processo.
- Trabalhe para melhorar a tríade de processos, pessoas e tecnologia.
- Divulgue os dados de forma transparente através de um relatório anual.
- Execute e aplique melhoria contínua por um período de pelo menos 2 (dois) anos antes de pensar em implementar um processo de caça de ameaças ("*Bug Bounty*").

Quando defeitos ou falhas de programação são detectados na fase do desenvolvimento da aplicação trazem menor custo comparado ao custo de remediar a vulnerabilidade em ambiente de produção. Por essa razão se faz necessário também investir na capacitação dos desenvolvedores de aplicações e em ferramentas e técnicas de desenvolvimento de *software seguro*. Outra recomendação pertinente é aplicar o conceito de "*security by design*", que significa que toda aplicação a ser desenvolvida parte da premissa de que precisa ser segura desde a sua concepção.

6. ASPECTOS DE AVALIAÇÃO E CONTROLE DE NÍVEL DE RISCOS

6.1 INTRODUÇÃO

O objetivo desta seção é gerar conscientização, aos interessados, sobre gerenciamento, avaliação e controle de níveis de risco. Geralmente um processo de gerenciamento de risco é um dos elementos que compõem a boa prática da governança corporativa. É um processo que quando adequadamente implementado, contribui para melhorar as tomadas de decisões e o desempenho da organização. De acordo com [ENISA, 2006], o processo de gerenciamento de risco de segurança da informação engloba o gerenciamento de risco e pode estar integrado ao gerenciamento de risco global da organização ou pode, também, ser realizado separadamente. Já o processo de avalição de risco pode ser considerado como parte integrante do processo de gerenciamento de riscos. Porém conforme observado também em [ENISA, 2006], em geral, as organizações que implementam o gerenciamento de risco, não implementam o processo de avaliação de riscos. Outras organizações implementam de modo mínimo os dois processos. E ainda, pequenas organizações não implementam nenhum dos dois processos.

Apesar de existirem vários padrões e boas práticas para a implementação de processos de gerenciamento de risco e de avaliação de risco, em geral, as organizações optam por customizarem seus próprios métodos, mas baseados naqueles padrões. Assim, podem adequá-los a sua estrutura, área de negócio ou setor.

Em geral, as organizações utilizam um único método para o gerenciamento do risco e múltiplos para a avaliação do risco, em função da multiplicidade da natureza do sistema avaliado. O processo de gerenciamento de risco de uma organização é fortemente influenciado por: sua missão e objetivos; seus produtos e serviços; seus processos de gestão e operação; práticas específicas empregadas e local físico, e condições ambientais e regulatórias. Além disso, é composto pelos processos: Definição de escopo, avaliação de risco, tratamento de risco, comunicação de risco, além de monitoramento e revisão do risco.

O processo de gerenciamento de risco assegurará que riscos serão sistematicamente analisados em termos de probabilidade de ocorrência da ameaça e da severidade de seus impactos, avaliados em termos de tolerabilidade e controlados em níveis aceitáveis pela implementação de medidas de mitigação.

No tocante ao processo de avaliação de risco observa-se que muitas vezes ele não é desempenhado mesmo quando o gerenciamento de risco está implementado [ENISA, 2006]. A ideia aqui é a conscientização sobre este fato e apresentar alguns aspectos que facilitem a implementação de um processo de avaliação de risco na organização. Como sabe-se, as organizações são diariamente expostas a um número crescente de ameaças e vulnerabilidades, as quais devem ser identificadas, analisadas, avaliadas e posteriormente tratadas. As fases que compõem o processo de avaliação de risco são: identificação de riscos, análise de riscos relevantes e, por fim, a avaliação dos riscos.

Para realizar uma avaliação de risco cibernético, uma organização da aviação civil pode iniciar por responder a algumas questões que permitirão saber contra o que se proteger, tais como: Quais são os ativos mais importantes de TIC que possuímos? Qual violação de dados teria o maior impacto nos negócios da organização? Quais são as ameaças cibernéticas à organização? Quais são as vulnerabilidades internas e externas à organização? Qual o impacto se as vulnerabilidades forem exploradas? Qual o nível de risco aceitável para a minha organização? Assim, é possível desenvolver controles e estratégias de segurança de TIC a fim de mitigar os riscos [Upguard, 2020].

Existem outras questões importantes que poderão auxiliar no entendimento do valor do ativo que se está tentando proteger e permitirão uma maior compreensão do processo de gerenciamento de risco no contexto das necessidades de proteção do negócio. Estas, quando respondidas, poderão tornar a avaliação de risco mais efetiva, são elas: Qual é o risco que se está reduzindo? Este é o risco de segurança de maior prioridade? O risco está sendo reduzido de forma mais efetiva em custo?
O processo de avaliação de risco deve ser conduzido por uma pessoa ou uma equipe competente com um bom conhecimento da situação estudada e contar com a colaboração de uma equipe de fonte de informações atrelados à operação, que sejam familiarizados com a operação do ativo em avaliação.

Ao se realizar uma avaliação de risco é muito importante saber o que se está analisando, quem tem o conhecimento necessário para avaliar o risco e se existem requisitos regulatórios a serem satisfeitos e/ou restrições orçamentárias impostas. Assim, para iniciar o processo de avaliação de risco, sugere-se que inicialmente se audite os ativos críticos que terão os seus ciber-riscos avaliados e se obtenha respostas às questões: De que ativos se tratam? Como e onde estão localizados? Os lugares onde estão localizados são seguros? Onde seus dados são armazenados? Como são protegidos e/ou documentados? Por quanto tempo são mantidos? Quem tem acesso a eles tanto internamente quanto externamente?

Após a auditoria realizada é possível mensurar quais ativos serão passíveis de avaliação. Agora pode-se definir os parâmetros para a realização da avaliação de risco. Para bem posicionar o processo de avaliação de risco que será realizado, inicialmente se pode responder às seguintes questões: Qual a proposta da avaliação de risco? Qual o escopo da avaliação de risco? Existem restrições a serem consideradas no processo de avaliação de risco? Quem na organização deverá ser consultado durante a realização do processo? Qual o modelo ou metodologia de risco que a organização usa para realizar a avaliação?

Assim, o processo de avaliação de risco auxilia na conscientização sobre ameaças e riscos aos ativos de TIC, determina se é requerido um programa de controle para uma ativo particular de TIC e se as medidas de controle já utilizadas são adequadas e suficientes, previne impactos de mal funcionamento de componente de TIC na fase de projeto e/ou planejamento, prioriza os perigos e medidas de controle, e ainda ajuda a obedecer aos requisitos legais, onde estes são aplicáveis.

A seção 6 de [ISO 31010, 2012] apresenta-se critérios para a seleção de técnicas para o processo de avaliação de riscos. Em seu apêndice A se realiza uma comparação entre diversas técnicas para o processo de avaliação de riscos, já o apêndice B descreve e exemplifica cada uma destas técnicas. Em [ENISA, 2006] encontra-se modelos de gerenciamento de risco, além de várias técnicas para avaliação de riscos. Nas seções seguintes deste trabalho, apresenta-se um resumo de conceitos utilizados por modelos de avaliação de risco baseados em padrões.

6.2 ASPECTOS DO MODELO ISO/IEC 31000

Risco pode ser definido como possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos da organização. Uma Fonte de Risco é um elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco. Já o Gerenciamento de Risco auxilia as organizações no estabelecimento de estratégia, no alcance de objetivos e na tomada de decisões fundamentadas, e considera os fatores internos e externos da organização, incluindo o comportamento humanos e fatores culturais.

De acordo com [ISO 31000, 2018] e [ISO 31010, 2012], o Gerenciamento de Risco envolve a aplicação de políticas, práticas e procedimentos para atividades de:

- Comunicação e Consulta – Auxilia na conscientização e compreensão dos riscos;
- Estabelecimento de:
  - Contexto – ambiente interno e/ou externo a atingir, relação com os objetivos organizacionais;
  - Escopo – em qual nível gerencial será aplicado; e
  - Critério – de avaliação e quantidades e tipos de riscos adotados.
- Processo de Avaliação de Riscos:
  - Identificação de Riscos – encontrar, reconhecer e descrever os riscos;
  - Análise de Riscos – compreender a natureza dos riscos e as suas características; e
  - Avaliação de Riscos – comparar os resultados da análise com os critérios de risco estabelecidos.
- Tratamento de Riscos – selecionar e implementar opções para abordar riscos;
- Registro e Relatos de Riscos – notificação e documentação por meio de mecanismos adequados; e
- Monitoramento e análise Crítica de Riscos – assegurar e melhorar a qualidade e eficácia do processo e gerenciamento de riscos.

Apesar da apresentação das atividades acima estar em forma de itens e sequencial, elas são iterativas. O Processo de Gerenciamento de Riscos pode estar integrado na estrutura, nas operações e nos processos da organização, podendo ter aplicação nos níveis estratégicos, operacional, de programas ou de projetos.

Existem várias razões para se realizar um processo de avaliação de riscos de TIC de uma organização, tais como: redução de custos a longo prazo, melhor conhecimento da organização, redução de perda de ativos e vazamento de informação/dados, redução de problemas regulatórios e fornecimento de uma base para avaliações de riscos futuras. A avaliação de riscos pode ser realizada por profissionais de TIC com conhecimento da infraestrutura digital de trabalho, por executivos que entendem como estão alocados os recursos de TIC e como eles funcionam, ou por empresas terceirizadas especializadas. Um dos objetivos de uma avaliação de riscos cibernéticos é auxiliar os decisores da organização e apoiar respostas adequadas aos riscos. A meta é tentar responder as seguintes perguntas: O que pode acontecer e sob que circunstâncias? Quais são as possíveis consequências? Quão provável são as possíveis consequências se concretizarem? O risco está efetivamente controlado ou futuras ações são necessárias?

Para realizar o planejamento do processo de avaliação de riscos é importante determinar:

- Escopo:
  - Tempo de vida do ativo de TIC;
  - Área onde estará localizado ou onde o processo ocorrerá;
  - Tipos de perigos existentes).
- Recursos necessários:
  - Treinamento para os realizadores;
  - Tipos de fontes de informação).

- Tipos de medidas de análise de risco que serão necessárias:
  - Exatidão da escala
  - Parâmetros necessários para fornecer uma avaliação relevante);
- Quem são as partes interessadas envolvidas:
  - Gerentes;
  - Supervisores;
  - Funcionários;
  - Fornecedores;
  - Representantes, etc.
- Leis, regulações e códigos relevantes ou padrões adotados na jurisdição ou políticas e procedimentos organizacionais.

A avaliação de risco, no contexto de cibersegurança da aviação civil, pode ser descrita como um processo ou método onde se identifica, analisa e avalia o risco associado com alguma ameaça que possa causar danos ou prejuízos à infraestrutura crítica de TIC da organização. Assim, busca-se identificar as ameaças à organização, as vulnerabilidades internas e externas à organização, os impactos aos seus negócios, que podem ocorrer dado o potencial da ameaça explorar as vulnerabilidades e a probabilidade de um dano ocorrer. Baseando-se na determinação do risco, em função do nível do dano e na probabilidade da ocorrência, procura-se determinar um modo apropriado de eliminar a ameaça ou controlar o seu risco a ela associado. Após feita a identificação, analisa-se e avalia-se quão provável e severo o risco poderá ser. Em seguida, decide-se quais medidas devem ser adotadas para efetivamente eliminar ou controlar os prejuízos da ocorrência. O processo de avaliação de risco de uma organização deve ser realizado regularmente para assegurar que esteja atualizado e que seja preciso e completo em todo o tempo.

Para a organização do processo de avaliação de risco é importante inicialmente entender como preparar a avaliação de risco, como conduzi-la, como comunicar os seus resultados para as pessoas responsáveis e/ou interessadas e como manter a avaliação de risco sobre o tempo. A organização pode empregar avaliação de risco sobre uma base dinâmica e permanente através do desenvolvimento do ciclo de vida e através de toda as partes da hierarquia do gerenciamento de risco. Sabe-se que a missão organizacional, os processos dos negócios, o sistema de informação, as ameaças, e o ambiente de operação podem mudar com o tempo, logo a avaliação de risco efetuada também tem uma validade limitada no tempo.

A próxima etapa é como responder de forma consistente ao risco em toda a organização, uma vez ele determinado, considerando-se sua estrutura organizacional. Deve-se desenvolver cursos de ação de possíveis respostas ao risco, avaliar estes cursos de respostas, determinar as ações apropriadas, consistentes com a tolerância ao risco e por fim implementar controles ao risco com base nas ações selecionadas.

Para monitorar os riscos no tempo, deve-se determinar a efetividade do andamento da resposta ao risco, identificar mudanças que impactam sobre os riscos nos sistemas de informações organizacionais e nos ambientes em que estes sistemas operam, verificar se as respostas

planejadas são implementadas, além de verificar se os requisitos de segurança da informação derivados e referentes a missões organizacionais, legislação, diretrizes, regulamentos, políticas, normas e diretrizes são cumpridos. Isto indica que a avalição de riscos deve ser feita toda vez que um novo processo ou ativo de TIC for introduzido, antes que mudanças sejam introduzidas nos processos ou ativos de TIC existentes ou quando uma nova ameaça for identificada.

Assim, se pode fazer a avaliação de risco seguindo a seguinte sequência de passos: identificar as ameaças; determinar a probabilidade de prejuízo e sua severidade; identificar ações necessárias para eliminar a ameaça ou controlar o risco usando a hierarquia dos métodos de controle de risco; avaliar se a ameaça foi eliminada ou o risco controlado de forma apropriada; monitorar para se certificar que o controle continua a ser efetivo; manter documentos e/ou registros do processo de avaliação de risco que possam vir a ser necessários no futuro [ISO 31000, 2018].

6.3 ASPECTOS DO MODELO NIST SP 800-30

Na visão de [NIST, 2011], para a realização da atividade de gerenciamento de risco se faz necessário o envolvimento de toda a organização. Esta atividade aborda o risco do nível estratégico ao nível tático, garantindo que as decisões baseadas no risco estejam integradas em todos os aspectos da organização.

De acordo com [NIST, 2011], um processo de gerenciamento de risco inclui as fases da estruturação do risco, avaliação do risco, resposta ao risco e o monitoramento do risco [NIST, 2012].

A fase de estruturação do risco visa estabelecer o contexto do risco, onde é descrito o ambiente em que decisões baseadas em riscos são efetuadas, além de propor a produção de uma estratégia para o gerenciamento do risco que define como a organização pretende avaliar, responder e monitorar o risco. A estratégia de gerenciamento do risco estabelece a base para gerenciar o risco e traça os limites para decisões baseadas em risco na organização.

A fase de avaliação do risco se propõe a identificar os componentes do risco, são eles: ameaças, vulnerabilidades, prejuízo ou impacto adverso, probabilidade de ocorrência do prejuízo. Por fim, a determinação do risco, em função do nível do dano e da sua probabilidade de ocorrência. Assim, aqui, o conceito para *risco* é uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento e é uma função do impacto adverso que pode surgir se a circunstância ou evento ocorrer; e da probabilidade de ocorrência [NIST, 2012].

A fase seguinte do processo de gerenciamento do risco se propõe a fornecer uma resposta ao risco encontrado na fase de avaliação de acordo com a estrutura do risco organizacional. De forma semelhante ao Modelo ISO/IEC 31000, deve-se desenvolver cursos de ações alternativos de resposta ao risco, avaliá-los, selecionar os cursos de ações adequados aos níveis toleráveis de riscos da organização, e implementar as respostas selecionadas.

Por fim, na fase de monitoração do risco, em essência, a organização deve determinar a efetividade da resposta ao risco, identificar o impacto das mudanças nos sistemas de informação organizacional e ambientes onde ele opera e verificar se os requisitos de segurança estão satisfeitos.

Os riscos de segurança da informação são aqueles riscos que surgem da perda da confidencialidade, integridade e disponibilidade da informação ou sistema de informação (modelo CIA) e reflete o potencial impacto sobre as operações da organização, ativos organizacionais, indivíduos, outras organizações e a nação.

[NIST, 2012], que foca em metodologia de avaliação de risco, a define como o processo de identificar, estimar e priorizar os riscos de segurança da informação. Para sua determinação se requer uma análise cuidadosa de ameaças e vulnerabilidades da informação.

Assim, na sua visão uma metodologia de avaliação de risco deve incluir:

- Um processo de avaliação de risco;
- Um modelo de risco: termos chave, fatores de risco avaliáveis e seus relacionamentos, ameaças, vulnerabilidades, impactos e probabilidade de ocorrência, etc;
- Um método de avaliação: quantitativo, qualitativo ou semi-qualitativo;
- Um método de análise: orientado a ameaça, impacto/ativo ou vulnerabilidade.

A escolha de quais modelos e métodos utilizar é uma questão cultural das organizações sobre avaliação de riscos [NIST, 2011]. As metodologias de avaliação de riscos devem ser definidas pelas organizações e são componentes da Estratégia de Gerenciamento de Risco desenvolvidas durante a fase de estruturação do risco. Ao explicitar o modelo de risco, a metodologia de avaliação e a abordagem de análise empregada, e requerer como parte do processo de avaliação, uma justificativa para os valores avaliados dos fatores de risco, as organizações podem aumentar a reprodutibilidade da sua avaliação de risco por outros profissionais, utilizando os mesmos dados, e a repetibilidade destas avaliações de risco em momentos futuros.

Uma especificidade do modelo de gerenciamento de risco proposto por [NIST, 2011] é a proposição de uma estrutura hierarquia, onde a avaliação dos riscos que afetam a organização é organizada em três níveis. Cada um dos níveis contempla um "terço" da estrutura hierárquica da organização. Os níveis são: nível da organização, nível da missão e processos de negócios e nível de sistema de informação. Visando precisão nas entradas de informações e na troca de informações entre os níveis, o processo de avaliação de riscos envolve comunicações contínuas e compartilhamento de informações entre as partes interessadas.

De acordo [NIS, 2012], o processo de avaliação de risco pode ser realizado em quatro passos:

1. Preparação da avaliação de risco:

Identificar a proposta da avaliação de risco;

Identificar o escopo;

Identificar premissas e restrições;

Identificar fontes de ameaças, vulnerabilidades e impacto; e

Definir o modelo de risco, o método de avaliação e o método de análise.

2. Condução da Avaliação:

Identificar fontes de ameaças;

Identificar eventos de ameaças das fontes;

Identificar vulnerabilidades e condições pré-existentes que possam ser exploradas pelas fontes de ameaças;

Determinar a probabilidade que a ameaça pode ser iniciada e a probabilidade de ter sucesso na sua ação;

Determinar a magnitude dos impactos resultantes da exploração das vulnerabilidades pela ação das ameaças; e

Determinar o risco de segurança da informação em função da probabilidade da ameaça explorar as vulnerabilidades e os impactos de tal exploração.

3. Comunicação dos resultados da avaliação:

Comunicar os resultados da avalição do risco aos tomadores de decisão para suportar as respostas ao risco; e

Compartilhar as informações desenvolvidas na execução da avaliação do risco, para suportar outras atividades de gerenciamento.

4. Manutenção da avaliação:

Monitorar os fatores de risco identificados na avaliação dos riscos; e

Atualizar os componentes da avaliação de risco de acordo as atividades de monitoração.

6.4 ASPECTOS DO MODELO APRESENTADO NO DOC 9985

Nesta seção discute-se o modelo de controle de segurança de TIC proposto e desenvolvido pela Eurocontrol, apresentado no Apêndice C do Doc 9985 da OACI [Doc 9985, 2018]. O modelo tem por objetivo auxiliar as organizações da aviação civil a implementarem requisitos regulatórios para cibersegurança e representam uma *compilação* dos padrões ISO/IEC 27001:2005, COBIT e da família ISO/IEC 13335-4. Esclarece-se aqui que o padrão ISO/IEC 27001 está atualmente, na atualização do ano de 2013 e o padrão ISO/IEC 13335-4 foi atualizada para o padrão 27005, com última atualização no ano de 2018, e integra agora a família do padrão ISO/IEC 27000.

Assim, levando-se em consideração a variabilidade de tamanhos de entidades prestadoras de serviços à aviação civil e de seus tipos de sistemas de TIC, por adequação, os controles de segurança foram agrupados em 6 (seis) níveis crescentes a depender do controle do nível de risco da ameaça. Cada um destes níveis de controle de risco variará em função da criticidade do serviço fornecida pela entidade, da vulnerabilidade do sistema de TIC e da natureza da ameaça para o sistema de gerenciamento de transporte aéreo. De acordo [ISO 27001, 2005], a organização terá até 9 categorias de controle, as mesmas foram apresentadas na seção 5.5 deste manual (ver Tabela 1), cada uma sendo avaliada em nível de avaliação de risco variando de 1 (um) a 6 (seis), os quais são apresentados como requisitos nas tabelas C2 a C10 disponíveis no apêndice C do DOC 9985 [Doc 9985, 2018]. A quantidade de requisitos a serem satisfeitos para cada um dos 6 níveis e cada uma das 9 categorias é apresentada na Tabela 3. Cada um dos 6 (seis) níveis deve ter um percentual de seus requisitos de controle satisfeitos para qualificar o seu percentual de conformação. Este percentual é definido em função das quantidades de respostas positivas às questões associadas a cada nível sobre a quantidade de questões totais daquele nível. Cada nível de controle é qualificado de acordo a Tabela 2:

TABELA 2 – PERCENTUAL DE CONFORMAÇÃO DO NÌVEL DE CONTROLE DA CIBERAMEAÇA

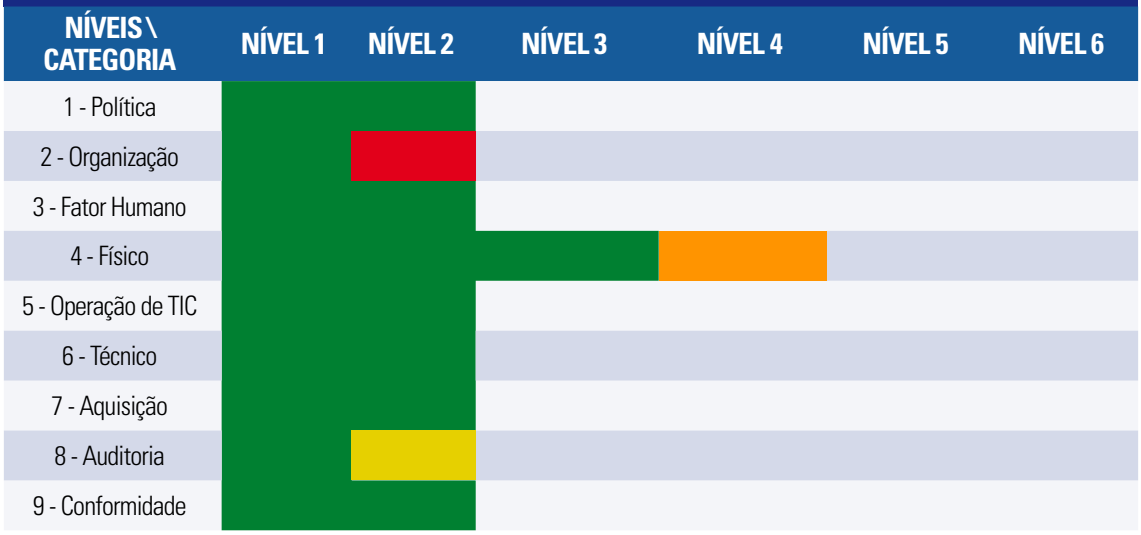
PERCENTUAIS DE CONFORMAÇÃO DO REQUISITO	QUALIFICAÇÃO
≥ 90%	Alta
≥ 60% e < 90%	Média Alta
≥30% e < 60%	Média Baixa
< 30%	Baixa

TABELA 3 - NÚMERO DE QUESTÕES PARA RELAÇÃO NÍVEL X CATEGORIA DE CONTROLE

NÍVEL\ CATEGORIA	1	2	3	4	5	6	7	8	9
Nível 1	1	10	6	5	12	15	5	5	4
Nível 2	2	4	3	1	8	4	4	2	2
Nível 3	1	9	3	3	14	11	6	3	3
Nível 4	0	3	3	2	7	5	3	2	0
Nível 5	0	1	2	1	5	2	1	1	0
Nível 6	0	0	1	1	2	1	1	0	0

Já a Tabela 4 ilustra uma situação de uma organização hipotética que apresenta o nível de controle 1 completamente satisfeito, mas para obter a qualificação alta no nível 2, deverá implementar mais mitigação nas categorias de Organização e Auditoria.

TABELA 4 - NÍVEIS DE CONTROLE DE UMA ORGANIZAÇÃO HIPOTÉTICA



É importante revisar e monitorar a avaliação para saber se ela foi completa e precisa, bem como para assegurar que mudanças que possam alterar a classificação de probabilidade da ameaça ou mesmo introduzir novas ameaças sejam endereçadas oportunamente. Uma boa prática para revisar a avaliação de risco é observar se os controles estão sendo efetivos.

Também é importante que a documentação do processo inclua a avaliação de risco e as ações de controles adotadas, observando tanto os requisitos legais quanto o do sistema de gerenciamento, caso existam. É importante também que os registros efetuados mostrem uma boa condução da revisão dos perigos, que os riscos dos perigos foram determinados, que foram implementadas medidas de controles adequadas para os riscos e que foram revistos e monitorados todos os riscos pertinentes.

Como já destacado anteriormente, as informações pertinentes ao processo de avaliação de riscos em cibersegurança devem ser atualizadas continuamente e utilizadas segundo a periodicidade adotada para aquele processo, ou tendo em vista alguma alteração nas instalações físicas, no *hardware*, no *software* ou algum procedimento de utilização desses.

6.5 MODELO DA TÉCNICA DE AVALIAÇÃO DE RISCO MATRIZ DE PROBABILIDADE/SEVERIDADE

Entre as diversas técnicas de avaliação de riscos existentes [ISO 3010, 2012], nesta seção apresenta-se a metodologia da matriz de avaliação de riscos para qualificar e quantificar o índice de risco. Através de seu uso se pode representar todos os aspectos envolvidos em um cenário de ataque cibernético. De acordo com o Doc 9859 da OACI – Manual de Gerenciamento de Segurança - a avaliação do risco é baseada na avaliação dos seguintes critérios: severidade do perigo, probabilidade (frequência) de sua ocorrência e tolerância de seus efeitos. Assim, risco é a probabilidade que o perigo em potencial (ameaça) cause prejuízo, caso seja realizado.

Esta metodologia de avaliação de risco é bem conhecida, e nela o risco pode ser visto como a probabilidade de perda de missão, imagem, reputação, financeira ou dos recursos gastos em resposta a um incidente no sistema de informação da organização e pode ser avaliado em qualificações ou níveis tais como, baixo, médio e alto. O risco está associado a incertezas e três fatores influenciam na sua definição: ameaça, vulnerabilidade e o valor da informação, e seus valores podem ser estimados respondendo a questões como: Qual é a ameaça? Quão vulnerável é o sistema? Qual é o impacto sobre os negócios da organização se um dano for causado ao ativo de TIC em questão? Respondida estas questões, o risco poderá ser encontrado através da relação:

Ciber-risco = ameaça x vulnerabilidade x valor da informação.

A matriz de probabilidade/consequência combina classificações qualitativas ou semi-qualitativas de consequências e probabilidades a fim de produzir um nível de risco ou a sua classificação [ISO 31010, 2012]. É uma técnica de seleção utilizada quando vários riscos são identificados. É também, comumente utilizada quando se deseja determinar se um dado nível de risco é aceitável ou não. A matriz de probabilidade/consequência apresentada na Figura 2 apresenta 5 (cinco) níveis de probabilidade de ocorrência de ameaça, A, B, C, D e E, sendo "A "a menor probabilidade e "E" sequencialmente a maior probabilidade, e 5 (cinco) níveis de severidade de impactos representados pelos números inteiros 1, 2, 3, 4 e 5 (matriz 5x5). Apresenta também 3 (três) níveis de riscos estimados representados pelas cores verde, amarelo e vermelho. Por exemplo, a matriz de probabilidade abaixo mostra a relação entre probabilidade e severidade da ocorrência (ver Figura 2).

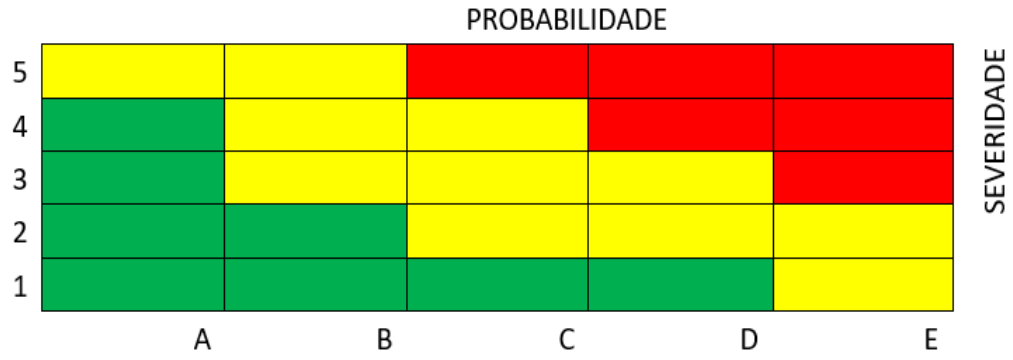


Figura 2 - Matriz de Probabilidade de Risco

O risco estimado pode ser classificado como: alto, em vermelho, que indicará a necessidade de implementação de controle imediatamente; médio, em amarelo, o que indica que um plano de controle deve ser desenvolvido e implementado tão logo quanto possível; e baixo, em verde, que indica que o monitoramento do processo deve ser mantido.

Em [Fair, 2010] apresenta-se uma metodologia de gerenciamento de risco de segurança da informação que foca sobre as suas definições de entradas, ações e saídas, realiza uma interessante avaliação do risco em quatro estágios: 1: identificar os componentes dos cenários; 2: estimar a frequência dos eventos de perda; 3: avaliar a magnitude da probabilidade de perda; e 4: derivar e articular riscos. Na técnica lá utilizada faz-se uso corrente de matriz de probabilidade (ver sua seção 4.3).

Em [ENISA, 2006] é apresentada uma visão geral de vária técnicas, ferramentas e boas práticas para gerenciamento e avaliação de risco. Em [Upguard, 2020] encontra-se um guia para a avaliação de risco a ser realizada em uma sequência de 8 (oito) passos após serem respondidas as questões citadas anteriormente nesta seção, as quais foram livremente traduzidas no Apêndice G.

No Apêndice E deste documento exemplifica-se a aplicação do método de avalição de risco utilizando a matriz de probabilidade/Severidade.

7. CONSIDERAÇÕES GERAIS SOBRE SISTEMAS ATM DE PRÓXIMA GERAÇÃO

A próxima geração de sistemas de ATM englobará o conceito de SWIM ("*System Wide Information Management*" – Sistema Global de Gerenciamento de Informação), visando a obtenção de uma arquitetura flexível e segura para a alocação e o gerenciamento de informação do sistema de aeroespaço. Uma vez implementado permitirá a todos os setores da aviação interessados acessarem os dados que eles requererem para realizar a sua função, claro no conhecimento de que é consistente com os dados utilizados por diferentes atores. A segurança do sistema de TIC terá uma maior importância ainda nestes sistemas. SWIM é uma iniciativa da indústria de ATM global e objetiva harmonizar a troca de informações aeronáuticas, meteorológicas, dados de voo, estado operacional do aeroporto para usuários e partes interessadas, porém não foi projetado com mecanismos que integrem requisitos de segurança cibernética. Ele faz parte do Plano de Navegação Aérea Global (GANP) da OACI, e é parte dos projetos: norte americano *Next Generation Air Transportation System (NextGen)*; e europeu *Single European Sky ATM Research* (SESAR) [Doc 9985, 2018][Harmonisation, 2018].

8. CONSIDERAÇÕES FINAIS

A proposta deste manual foi de realizar uma introdução sobre o tema de segurança cibernética no contexto da aviação civil, incluindo ameaças cibernéticas, vulnerabilidades, impactos, riscos e motivações dos atores das ameaças, considerações sobre gerenciamento e avaliação de riscos, além de alguns padrões geralmente utilizados no tratamento de segurança da informação, visando despertar a atenção das partes interessadas em implementar um programa de segurança cibernética na sua organização. Espera-se com isso conscientizar a comunidade da aviação civil sobre a importância do tema nas suas atividades cotidianas e despertar o interesse em implantar na sua organização uma cultura onde a cibersegurança tenha um lugar de destaque.

Existem três pontos que foram abordados no decorrer do texto e que são de fundamental importância para a conscientização em cibersegurança, principalmente para gestores de organizações da aviação civil, são eles: a identificação de seus ativos críticos de TIC; a escolha de um padrão para abordagem de segurança da informação para nortear o desenvolvimento da sua política de cibersegurança; e a importância do gerenciamento e avaliação de riscos como atividade relevante para implantação da política de segurança cibernética.

Os apêndices a seguir complementam o texto principal acrescentando informações importantes para o desenvolvimento da cultura da segurança cibernética na organização, eles abordam: uma lista de componentes críticos da aviação civil; um guia rápido para cibersegurança; listas de dispositivos e de procedimentos para controle em cibersegurança; uma lista de controles de cibersegurança críticos; um exemplo de um cenário de avaliação de riscos; dicas gerais e rápidas, em cibersegurança, para o usuário; e um procedimento passo-a-passo para realização de avaliação de riscos.

9. GLOSSÁRIO (SIGLAS EM INGLÊS EM TRADUÇÃO LIVRE)

ABNT – Associação Brasileira de Normas Técnicas

ACRP – Programa de Pesquisa Cooperativa de Aeroportos

ANAC – Agência Nacional da Aviação Civil

APF – Administração Pública Federal

ASCOM – Assessoria de Comunicação Social da ANAC

ATC – Controle de Tráfego Aéreo

ATM – Gerenciamento de Tráfego Aéreo

ATS – Serviços de Tráfego Aéreo

ATSP – Provedores de Serviços de Tráfego Aéreo

AVSEC – Segurança da Aviação Civil contra Atos de Interferência Ilícita

BS – Padrão Britânico

BYOD – Traga Seu Próprio Dispositivo

CIA – Confidencialidade, Integridade e Disponibilidade

CFTV – Circuito Fechado de TV

CMMI – Modelo de Capacidade e Maturidade Integrado

COBIT – Objetivos de Controle para Informação e Tecnologia Relacionada

COMAER – Comando da Aeronáutica

CVV – Código de Verificação de Cartão de Crédito

CWE – Enumeração de Fraquezas Comuns

DCS – Sistema de Controle Distribuído

DDoS – Negação de Serviço Distribuída

DNS – Servidor de Nomes de Domínios

DOC – Manual de Segurança para Salvaguardar a Aviação Civil

DoS – Negação de Serviço

DSAC – Documentos de Segurança da Aviação Civil

EASA – Agência Europeia de Segurança da Aviação

E-ciber – Estratégia Nacional de Segurança Cibernética

EASA – Agência Europeia para a Segurança da Aviação

ENISA – Agência da União Europeia para Cibersegurança

FDIS – Documento Final de Padrão Internacional

GANP – Plano de Navegação Aérea Global

GIS – Sistema de Informação Geográfica

GPS – Sistema de Posicionamento Global

GRSIC – Gestão de Riscos de Segurança da Informação e Comunicações

GSIPR – Gabinete de Segurança Institucional da Presidência da República

GTSIC – Grupos Técnicos de Segurança de Infraestrutura Críticas

HVAC – Aquecimento, ventilação e ar condicionado

ICA – Instrução do Comando da Aeronáutica.

ICAO – Organização da Aviação Civil Internacional

IDS – Sistema de Detecção de intruso

IEC – Comissão Eletromecânica Internacional

IoT – Internet das Coisas

IP – Protocolo Internet

IS – Instrução Suplementar

ISCM – Sistema de monitoramento Contínuo da Segurança da Informação

ISO – Organização de Padrões Internacional

ITIL – Biblioteca de Infraestrutura de Tecnologia da Informação

LPDG – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet Brasileira

NAS – Sistema de Aeroespaço Nacional

NAVAID – Auxílios de Navegação Aérea

NBR – Normas Brasileiras

NCASP – Programa de Segurança da Aviação Civil Nacional da OACI

NCSC – Centro de Cibersegurança Nacional

NEXTGEN – Sistema de transporte aéreo americano "*Next Generation*"

NIST – Instituto Nacional de Padrões e Tecnologia

OACI – Organização da Aviação Civil Internacional

PC – Computador Pessoal

PLC – Controlador Lógico Programável

PMBOK – Guia de Conhecimento em Gerenciamento de Projetos

PMI – Instituto de Gerenciamento de Projeto

PNAVSEC – Programa Nacional de Segurança da Aviação Civil contra Atos de interferência Ilícita

RBAC – Regulamento Brasileiro da Aviação Civil

RMF – Estrutura de Gerenciamento de Riscos

RPAS – Aeronave Remotamente Pilotada

SCADA – Sistema de Supervisão e Aquisição de Dados

SESAR – Programa Europeu para um melhor Gerenciamento de Tráfego Aéreo

SGTSIC-TA – Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos

SIV – Sistema de Informação de Voo

SLA – Acordo de Nível de Serviço

SP – Publicação Especial

SSCG – Grupo de Trabalho do Secretariado sobre Segurança Cibernética

SWIN – Sistema Global de Gerenciamento de Informação

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e comunicações

TO – Tecnologia Operacional

TOGAF – *Framework* de Arquitetura Corporativa de TI

USB – *Universal Serial Bus*

VCMM – *Vulnerability Coordination Maturity Model*

VPN – Rede Privada Virtual

WAN – Rede Global de Computadores

10. PADRÕES/*FRAMEWORKS* REFERENCIADOS

NIST SP 800-30

NIST SP 800-39

ISO/IEC 27001

ISO/IEC 27002

ISO/IEC 27701

ISO/IEC 29.147

ISO/IEC 13335-4

ISO/IEC 27005

ISO/IEC 30.111

ISO/IEC 31000

ISO/IEC 31010

CMMI®

COBIT®

ITIL®

PMBOK®

TOGAF™

11. REFERÊNCIAS BIBLIOGRÁFICAS

ACRP (2015). Airport Cooperative Research Program - ACRP 140: Guidebook on Best Practices for Airport Cyber security.

ACRP (2016). Airport Cooperative Research Program – ACRP Syntesis 71: Airport Safety Risk Management Panel Activities and Outcomes, A Sysnthesis of Airport Practice, Transportation Research Board, Washington D.C., www.trb.org.

Axelos (2019). ITIL Foundation: ITIL 4 Edition.

Anexo 17 (2011). International Report Civil Aviation Organization. Anexo 17 à Convenção Internacional de Aviação Civil (Convenção de Chicago) da OACI – Proteção da Aviação Civil Internacional contra Atos de Interferência Ilícita. 9th ed. Canadá.

BRASIL (2013). Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Classificação dos Sistemas de Informação do SISCEAB: 7-31. Rio de Janeiro, RJ, 2013.

CAA (2019). Aviation Cyber Security Guidelines - Civil Aviation Authority and Ministry of Transport & Communications – Qatar.

Capec (2020). na página web: http://capec.mitre.org, acessada em 15/03/2020.

Cartilha (2020). Cartilha de Segurança para Internet, na página web: http://cartilha.cert.br acessada em 13 abr. 2020.

Cathay (2018). Cathay Pacific data hack hits 9.4 million passengers, na página web: https://www.bbc.com/news/business-45974020, de 25/10/2018, acessada em 10 mar. 2020.

Chrissis, M. B., Konra, M. e S. Shrum (2011). CMMI® for Development: Guidelines for Process Integration and Product Improvement, Addison-Wesley Professional; Ed. 3.

COBIT (2019). COBIT® Framework: Introduction and Methodology, ISACA®, na página web: http://www.isaca.org/COBITuse.

CMMI (2020). CMMI, Capability Maturity Model Integration, V2.0, na página web: https://cmmiinstitute.com/cmmi, acessada em 15 abr. 2020.

CNPI (2020). CNPI – Center for the Protection National Infrastructure, Internet of Things and Industrial Control Systems, página web: https://www.cpni.gov.uk/internet-things-and-industrial-control-systems, acessada em 16/04/2020.

Crespo (2015). Marcelo. Crimes Digitais: do que estamos falando? 17/junho 2015, Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/, página acessada em: 15/04/2020.

CWE (2020). CWE: Common Weakness Enumeration, A Community-Developed List of Software & Hardware Weakness Types, na página web: http://cwe.mitre.org/, acessada em 20 abr. 2020.

Decreto (2010). BRASIL. (s.d.), Decreto nº 7.168, de 05 de maio de 2010. Dispõe sobre o Programa Nacional de Segurança da Aviação Civil Contra Atos de Interferência Ilícita (PNAVSEC). Brasília, DF, Brasil.

Doc 8973 (2017). International Civil Aviation Organization. Doc. 8973 – Aviation Security Manual. 10th ed. Canadá.

Doc 9859 (2013). International Civil Aviation Organization. Doc. 9859 – Safety Management Manual. Third ed. Canadá.

Doc 9985 (2018). International Civil Aviation Organization. Doc. 9985 – Air Traffic Management Security Manual. Canadá.

Duchamp, H., Bayram, I. and Korhani R. (2016). Cyber-Security, a new challenge for the aviation and automotive industries, Seminar in Information System: Applied Cybersecurity Strategy for Manager, 30 juin.

EATM-CERT (2020). EUROCONTROL EATM-CERT (European Air Traffic Management – Computer Emergence Response Team), 1st Quarter 2020 Cyber Threat Landscape & Activity Report for Senior Management.

E-ciber (2020). Decreto Nº 10.222, Estratégia Nacional de Segurança Cibernética, Fevereiro.

Emanuelli, G. B. (2019). Cibersegurança na Aviação Civil Brasileira, Trabalho de Conclusão de Curso na Escola Superior de Guerra – Campus Brasília – DF.

ENISA (2006). Risk Management: Implementation principles and Inventories for Risk Management/ Risk Assessment methods and tools, Technical Department of ENISA Section Risk Management, June.

ENISA (2016). Securing Smart Airports, Dezembro.

Euractiv (2016). Hackers bombard aviation sector with over 1,000 attacks per month, página web: https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/, de 11/07/2016, acessada em 10/04/2020.

Fakeeh, K.A. and Aziz, K. A. (2016). An Analysis of Airports Cyber-Security, Communications on Applied Electronics, Vol 4- Nº 7, March.

Fair (2010). Technical Guide FAIR™ – ISO/IEC 27005 Cookbook, The Open Group, Outubro.

Guide (2018). The Cyber Airport – A Practical Guide for Airport Executives – Overview Specific Risks Practical Information, Union des Aéroports Français & Francophones Associes.

Gopalakrishnan, K. et all, Cyber Security for Airports (2013). International Journal and Traffic and Transport Engineering, 3(4).

GSIPR (2008). Portaria nº 02, de 08 de fevereiro de 2008/GSIPR, do Gabinete de Segurança Institucional da Presidência da República. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. Diário Oficial da União, Brasília, DF, 11 fev. 2008.

GSIPR (2010). Portaria nº 28, de 27 de abril de 2010/GSIPR, do Gabinete de Segurança Institucional da Presidência da República. Institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos (SGTSIC - Transportes Aéreos) e dá outras providências. Diário Oficial da União, Brasília, DF, 28 ab. 2010.

Harmonisation (2018). NextGen-SESAR State of Harmonisation, Report prepared by the Coordination Commintee (CCOM) & Deployment Coordination Committee (DCOM) for the US-EU MoC Annex 1, EXECUTIVE Committee (EXCOM), September.

ICAO (2019). Working Paper A40, ICAO Cybersecurity Strategy. Assembly – 40th Session, 25 jun. 2019, Disponível em: https://www.icao.int/Meetings/A40/Documents /WP/wp_028_en.pdf.

ICAO (2016). Working Paper A39. Addressing Cybersecurity in Civil Aviation, Assembly – 39th Session, 30 mai. 2016, disponível em: https://www.icao.int/Meetings/a39/Documents /WP/wp_017_en.pdf

IS 107 (2019). Agência Nacional de Aviação Civil, Instrução Suplementar - IS Nº 107 - 001 - REVISÃO D - Segurança da Aviação Civil Contra Atos de Interferência Ilícita - Operador de Aeródromo.

IS 108 (2019). Agência Nacional de Aviação Civil, Instrução Suplementar - IS Nº 108 - 001 - REVISÃO C - Segurança da Aviação Civil Contra Atos de Interferência Ilícita - Operador de Aéreo.

ISACA (2014). Página web:https://www.isaca.org/resources/isaca-journal/past-issues/2014/critical-information-systems-processes, acessada em 10 abr. 2020.

ISO 13335 (2000). ISO/IEC TR 13335-4:2000 - Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards.

ISO 27001 (2005). ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements

ISO 27001 (2013). ABNT NBR ISO/IEC 27001 - Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos.

ISO 27002 (2013). ABNT NBR ISO/IEC 27002 – Políticas para segurança da informação.

ISO 27005 (2008). BS ISO/IEC 2005:2008, Information Technology – Security Techniques – Information Security Risk Management, British Standard. 5th Ed., June.

ISO 31000 (2018). ABNT NBR ISO/IEC 31000 – Comité Técnico de Gerenciamento de Riscos.

ISO 31010 (2012). ABNT NBR ISO/IEC 31010 – Gestão de Riscos – Técnicas para o Processo de Avaliação de Riscos, 1ª. Ed.

Karpersky (2020). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within, página web: https://www.kaspersky.com/blog/the-human-factor-in-it-security/, acessada em 20/03/2020.

Maldonado, Viviane Nóbrega; Blum, Viviane Nóbrega (2019). LGPD: Lei Geral de Proteção de Dados comentada. Edição do Kindle.

Manual (2017). Manual Conscientização dos Colaboradores sobre Cibersegurança, Arcon Serviços Gerenciais de Segurança, solicitado na página web: https://docs.nec.com.br/manual-conscientizacao-dos-colaboradores-sobre-ciberseguranca em 25 abr. 2020.

NCSC (2020). National Cyber Security Centrer - NCSC Common Cyber Attacks Infographic, na página web: https://www.ncsc.gov.uk/information/infographics-ncsc, acessada em 03/03/2020.

NIST (2011). NIST Special Publication 800-39 - Managing Information Security Risk - Organization, Mission, and Information System View.

NIST (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments.

PMI (2013). A Guide to the Project Management Body of Knowledge (PMBOK GUIDE). 5th. ed. [S.l.]: Project Management Institute, 2013.

PMP (2017). PMBoK Guide, PMP-PMBOK® Guide 6th Edition.

RBAC 107 (2018). Regulamento Brasileiro de Aviação Civil nº 107 – RBAC nº 107 – denominado Segurança da aviação civil contra atos de interferência ilícita – operador de aeródromo.

Resolução 167 (2010). Agência Nacional de Aviação Civil, Resolução Nº 167 - Estabelece diretrizes para o gerenciamento de risco à Segurança da Aviação Civil contra Atos de Interferência Ilícita (AVSEC) pela ANAC. BRASIL.

Schober, T., Koblen, I. and S. Szabo, (2012). Present and potential security threats posed to civil aviation, Incas Bulletin, Volume 4, Issue 2/, pp. 169 – 175.

Skybrary (2019). Risk Assessment - página web https://www.skybrary.aero/index.php/Risk_Assessment, acessada em 27/05/2019.

Silva, Mateus V. A. (2019). Panorama da Ameaça Cibernética à Aviação Civil, Revista Brasileira de Inteligência. Brasília: Abin, n. 14, dez.

Stroud, R.E. (2012). Introduction to COBIT 5 - página web:http://www.isaca.org/education/upcoming-events/documents/intro-cobit5.pdf.

Tabansky, L. (2011). Critical infrastructure protection against cyber threats. Military and Strategic Affairs ,3(2), 2.

Togaf (2020). An Introduction to the TOGAF® Standard, version 9.2 reference: W182, página web: http://publication.opengroup.org/w182, acessada em 21 abr. 2020.

Upguard (2020). How to Perform an IT Cyber Security Risk Assessment: Step-by-Step Guide, página web: https://www.upguard.com/blog/cyber-security-risk-assessment, atualizada em 05/03/2020, acessada em 10/04/2020.

Von Solms, R., e Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. doi:10.1016/j.cose.2013.04.004

APÊNDICE A

Componentes Críticos da Aviação Civil

APÊNDICE A: COMPONENTES CRÍTICOS DA AVIAÇÃO CIVIL

Como exemplo, abaixo segue uma lista não exaustiva de componentes de sistemas das organizações da aviação civil que fazem uso de recursos de TIC e/ou TO para a sua operação e que podem ser considerados críticos, do ponto de vista de cibersegurança da aviação civil.

- AEROPORTOS
  - *OPERADORES AEROPORTUÁRIOS*
    - *Sistemas Elétricos:*

      Eletricidade, ventilação, Sistema de iluminação geral, Sistema de balizamento luminoso de sistema de pistas, Sistema de fonte secundária de energia (geradores), Unidade de monitoramento de energia, Distribuição de energia elétrica, Sistema de alarme de incêndio, Sistema de atendimento ao público;

    - *Sistemas Mecânicos:*

      Elevadores, Escadas rolantes, Sistema de bomba d´água, Sistemas de condicionamento de ar, Resfriadores;

    - *Operação e Manutenção dos Sistemas:*

      Sistema de gerenciamento de manutenção computadorizado, Sistema de gerenciamento de crise, Sistema de informação de gerenciamento, Sistema de gerenciamento de recursos, Cliente Help desk;

    - *Comunicação:*

      Comunicação interna telefone fixo, Comunicação telefone móvel, Comunicação VOIP, Comunicação via rádio;

    - *Logística:*

      Guia de estacionamento, Gerenciamento de estacionamento de veículos, Reconhecimento de placas de veículos, Rastreamento de pessoas, Inspeção de veículo, Gerenciamento de trolley, Rastreamento de Frota;

  - *Segurança*

    Controle de Acesso automático (abertura de portas), Circuito Fechado de TV (CFTV), Equipamento de Raio X, EDS (Explosive Detector System), ETD (Explosive Trace Detector), Escâner corporal, Controle de Acesso (Pessoas, Bagagem de Mão,

Veículos), Sistema de Credenciamento(Pessoas, Veículos), Serviço de Aduana (Receita Federal), Serviço de Imigração - Polícia Federal (Passaporte eletrônico, Checagem de passageiro);

- *Aviação*

  Baggage Handling System (BHS), Sistema de docagem de aeronaves, Sistema de controle de portões (*Gates*), Sistema de Informação de Voo (SIV), Fonte de energia de 400 H;

- *Computação*

  Infraestrutura (computadores, cabeamento, conectores), Servidores (Serviço de *web*, Serviço e-mail, serviços de banco de dados), Rede de computadores (roteadores, pontes, *hubs*);

- *Informação/Dados:*

  Listagem de funcionários credenciados do aeroporto, listagem de equipamentos e veículos do aeroporto, escala de horários de vigilantes, escala de APACs dos aeroportos, horários das rondas de segurança do aeroporto, informações pessoais diversas, PSA do aeroporto.

- EMPRESAS AÉREAS
  - *OPERADORES AÉREOS*

    - *SERVIÇOS DE TRASPORTE AÉREO:*

      PESSOAS (check-in, conferência-embarque), BAGAGENS (etiquetagem, guarda, conciliação e reconciliação), CARGAS (recepção, expedição, conferência, etiquetagem);

    - *Computação:*

      Infraestrutura de TI (computadores, cabeamento, conectores), Servidores (Serviço de *web*, Serviço e-mail, serviços de banco de dados), Rede de computadores (roteadores, pontes, *hubs*).

    - *SERVIÇOS PARA PASSAGEIROS*

      Serviço *web* (reserva, check-in remoto, atendimento on-line e outros), Base de dados de clientes

- *OPERAÇÕES DE TERRA:*

  Telefone, Rádio Comunicação, Rede local

- *SERVIÇOS NA AERONAVE:*

  Serviço multimídia de bordo, Entretenimento à bordo

- *INFORMAÇÃO/DADOS:*

  Listas de passageiros dos voos, informações pessoais dos programas de fidelidade, PSOA da empresa aérea, lista de funcionários

- CONTROLE DO ESPAÇO AÉREO
  - *SERVIÇOS DE NAVEGAÇÃO AÉREA*
    - *Equipamentos de auxílio à navegação, radares (fixos ou móveis);*
    - *Controle de acesso automático (abertura de portas), Sistema de credenciamento, Circuito Fechado de TV (CFTV);*
    - *Infraestrutura de TI (computadores, cabeamento, conectores), Servidores (Serviço de banco de dados), Rede de comutadores (Roteadores, pontes, hubs);*
    - *Sistemas de comunicação (rádio, telefone, web, e-mail, etc);*
    - *Sistemas informatizados provedores de dados de voos*

- PROVEDORES DE SERVIÇOS AUXILIARES
  - *PROVISÕES DE BORDO*
  - *SERVIÇOS DE BORDO*
  - *PROTEÇÃO DE CARGA*
  - *VIGILÂNCIA*
  - *CONTROLE DE ACESSO*
  - *SISTEMA DE ORIENTAÇÃO E CONTROLE DE MOVIMENTAÇÃO EM SOLO – SOCMS (PROCEDIMENTOS)*

- *OPERAÇÕES*
- *MANUTENÇÃO*

- EXPLORADORES DE ÁREA AEROPORTUÁRIA
  - *HANGARES*
  - *TERMINAL DE CARGA AÉREA*
  - *AEROCLUBE*
  - *PARQUE DE ABASTECIMENTO DE AERONAVES*

APÊNDICE B

Guia Rápido - Modelo NCSC

APÊNDICE B: GUIA RÁPIDO - MODELO NCSC

Como um modelo de guia rápido, apresenta-se a seguir os 10 (dez) passos para cibersegurança recomendados pelo *National Cyber Security Center* (NCSC) do governo do Reino Unido [NCSC, 2020].

1. Segurança da Rede:

    - *Proteja a rede de ataque;*
    - *Isole o perímetro da rede;*
    - *Filtre o acesso de não autorizados;*
    - *Bloqueie conteúdo malicioso;*
    - *Monitore e teste os controles de segurança.*

2. Treine e conscientize os usuários

    - *Produza políticas de segurança para usuário – uso seguro e aceitável do sistema;*
    - *Inclua treinamento da equipe;*
    - *Manter conscientização dos ciber-riscos.*

3. Prevenção de *Malware*

    - *Produza políticas relevantes;*
    - *Estabeleça defesas anti-malware através da organização.*

4. Controle Mídias Removíveis

- *Produza política para controlar todo o acesso às mídias removíveis;*
- *Limite o tipo e uso de mídia;*
- *Escanei toda mídia antes de importar sobre o sistema da organização.*

5. Configuração de Segurança

- *Aplique patches seguros e assegure que a configuração segura de todos sistemas está mantida;*
- *Crie um sistema de inventário e defina uma linha base para todos dispositivos.*

6. Gerencie os Privilégios dos Usuários

- *Limite o número de contas com privilégios;*
- *Limite os privilégios dos usuários;*
- *Monitore a atividades dos usuários;*
- *Controle o acesso aos registros de auditorias e de atividades.*

7. Gerencie Incidentes

- *Estabeleça resposta aos incidentes;*
- *Estabeleça a capacidade de recuperação de desastres;*
- *Teste seu plano de gerenciamento de incidentes;*
- *Forneça treinamento especializado;*
- *Relate incidente criminosos às autoridades competentes.*

8. Monitoramento

- *Estabeleça estratégia de monitoramento e produza política de suporte;*
- *Monitore continuamente todos os sistemas e redes;*
- *Análise registros de atividade anormal.*

9. Trabalho Móvel e em Casa

- *Desenvolva uma política de trabalho móvel e treine a equipe para aderi-la;*
- *Aplique uma linha base de segurança para todo dispositivo;*
- *Proteja dados em trânsito e armazenado.*

10. Ajuste seu Regime de Gerenciamento de Risco

- *Avalie o risco para o sistema e informação da sua organização com o mesmo rigor que você faria para o risco regulatório, legal, financeiro e operacional;*
- *Embuta o regime de gerenciamento de risco através de todo a organização, suportada pelo conselho de administradores.*

APÊNDICE C

Dispositivos e Procedimentos

APÊNDICE C: DISPOSITIVOS E PROCEDIMENTOS

Apresenta-se alguns dispositivos e procedimentos possíveis para Controles em Cibersegurança:

1. Protocolos Seguros

    - *Criptografia/Decriptografia; Certificados Digitais e Assinaturas digitais*
    - *HTTPS, IPSEC (VPN)*
    - *Wi-Fi WPA2*

2. Controle de Acesso

    - *Mecanismo de autenticação e autorização*

3. Manutenção do Sistema

    - *Controle de Patch: combates às vulnerabilidades dos programas e na correção do controle do hardware.*

4. *Firewall* e Arquitetura de Redes
5. Sistema de Monitoração e Detecção de Intruso de Rede
6. Ferramentas antiDDoS
7. Garantia de Qualidade de *Software* e *Hardware*

    - *Inspeção de Código*
    - *Validação e Verificação*
    - *Teste de Segurança*

8. Controle Organizacional

- *Equipe confiável*
- *Controle de Acesso*
- *Controle de Dispositivos Portáteis*

9. Equipe treinada e conscientizada.

10. Leis penalizadoras.

APÊNDICE D

Controles de Cibersegurança Críticos

APÊNDICE D: CONTROLES DE CIBERSEGURANÇA CRÍTICOS

O Instituto SANS, junto com o Centro para Segurança para a Internet (CIS) e outras organizações, desenvolveu 20 Controles de Segurança Críticos (CSC) para efetiva ciberdefesa, são eles:

1. Inventário de *hardware* autorizado e não autorizado
2. Inventário de *software* autorizado e não autorizado
3. Configurações seguras para *Hardware* e *Software* para as quais as configurações são possíveis e estão disponíveis.
4. Configurações seguras de dispositivos de rede tais como *firewalls* e roteadores.
5. Defesa de fronteira de redes.
6. Manutenção e análise completa de registros auditoria de segurança
7. Aplicação para segurança de *software*
8. Controles do uso dos privilégios administrativos
9. Controle de Acesso inteligente
10. Teste e recuperação contínua de vulnerabilidades
11. Controle e monitoramento de contas inativas
12. Defesas *Anti-Malware*
13. Limite e Controle de Portas, Protocolos e Serviços
14. Controle de Dispositivos sem fio
15. Proteção contra vazamento de Dados (controle adicional crítico)
16. Engenharia de Rede segura
17. Exercícios "*Red Team*".
18. Capacidade de Resposta a Incidentes
19. Garantia de *Back-Up* de Dados
20. Avaliação de Perícia em segurança e treinamento preencher espaços

APÊNDICE E

Avaliação de Risco

APÊNDICE E: AVALIAÇÃO DE RISCO

Segue um exemplo de um Cenário de Avaliação de Riscos hipotético: Ataque do tipo DDoS na rede local do Servidor do sistema de gerenciamento do aeroporto;

Informação de Situação de um ataque em potencial:

	PERGUNTAS	5 PONTOS	DE 1 A 4 PONTOS	0 PONTOS	PONTOS	PESO
Q1	Há histórico de paralização das atividades da organização causado por invasão de sistema causado por ataque cibernético?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q2	Há histórico de invasões de algum sistema essencial de TIC para as atividades nesta organização?	Alto Potencial	Baixo Potencial	Ausência	3	1
Q3	Há relatos de perda ou vazamento de alguma informação ou banco de dados causada por ataque cibernético?	Alto Potencial	Baixo Potencial	Ausência	0	1
Q4	Há relatos de perda ou vazamento de alguma informação ou banco de dados causada por ataque cibernético em qualquer organização doméstica e/ou internacional de aviação civil?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q5	Qual é o volume de tráfego semanal de voos regulares em operação na organização?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q6	Há conhecimento de grupos "*hackers*" especializados em ataques aos sistemas da aviação civil?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q7	Os usuários possuem acesso irrestrito à qualquer página / área dos sistemas?	Alto Potencial	Baixo Potencial	Ausência	1	1

Q8	Há desacordos políticos/ comerciais entre o Brasil com outras nações que propiciariam algum ataque cibernético ao Estado/Governo e serviços essenciais como os prestados por ATSP?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q9	Há presença de Operadores Aéreos de países que são considerados alvos em potencial para ataques cibernético?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q10	Há informações específicas acerca da possibilidade de ocorrer um ataque através desse cenário de ameaça?	Há informações específicas de planejamento, intenção e capacidade de ataque.	Há alguma evidência de intenção e capacidade, mas nenhuma evidência de planejamento de ataque real.	Não há informações específicas ou sinais de possibilidade ou planejamento de ataque; ou há uma intenção teórica, mas sem capacidade aparente.	3	1
Q11	Um ataque cibernético tem o potencial de causar estragos em grande escala nos principais centros de transporte aéreo em todo o país e levar a um grande número de atrasos, cancelamentos de voos e alertas de segurança mais rigorosos?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q12	Os dados desta organização estão registrados na nuvem?	Alto Potencial		Ausência	0	1
Nível da situação de um ataque					30/13 = 2,3	

Gráfico de Calor da Probabilidade de Ataque:

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

Logo, a probabilidade de um ataque é Média-baixa

A severidade do impacto do ciberataque pode ser analisada através do gráfico de calor abaixo:

		TERMOS HUMANOS	TERMOS ECONÔMICOS	PARA O SISTEMA DE AVIAÇÃO
PROBABILIDADE	Alta (5)	Centenas de mortos	Bilhões de dólares	Interrupção severa dos serviços
	Média-alta (4)	Alguns, mas não todos os itens acima com alta severidade		
	Média (3)	Dezenas de mortos	Milhões de dólares	Interrupção moderada dos seviços
	Média-baixa (2)	Alguns, mas não todos os itens acima com média severidade		
	Baixa (1)	Feridos e eventualmente algum morto	Pouco impacto Econômico	Pouca interrupção dos serviços

Neste cenário, entende-se que a severidade é Média-baixa.

O Nível de ameaça pode ser obtido por meio do produto da Probabilidade de Ataque pelo Nível de Severidade dos seus impactos através da Matriz de Ameaça apresentada a seguir:

NÍVEL DE AMEAÇA		SEVERIDADE				
		BAIXA (1)	MÉDIA-BAIXA (2)	MÉDIA (3)	MÉDIA-ALTA (4)	ALTA (5)
PROBABILIDADE	Alta (5)	Média-baixa (5)	Média (10)	Média-alta (15)	Alta (20)	Alta (25)
	Média-alta (4)	Baixa (4)	Média-baixa (8)	Média (12)	Média-alta (16)	Alta (20)
	Média (3)	Baixa (3)	Média-baixa (6)	Média-baixa (9)	Média (12)	Média-alta (15)
	Média-baixa (2)	Baixa (2)	Baixa (4)	Média-baixa (6)	Média-baixa (8)	Média (10)
	Baixa (1)	Baixa (1)	Baixa (2)	Baixa (3)	Baixa (4)	Média-baixa (5)

Neste cenário obteve-se uma probabilidade de ataque Média-baixa e considerou-se a severidade dos impactos também Média-baixa, logo, o nível de ameaça é Baixa

Já o nível de vulnerabilidade cibernética da organização pode ser determinado considerando-se as medidas de segurança existentes frente às ciberameaças, para tanto pontua-se cada uma das questões apresentadas na tabela a seguir:

	PERGUNTAS	5 PONTOS	DE 1 A 4 PONTOS	0 PONTOS	PONTOS	PESO
Q1	Há regulamentação específica que estabeleça diretrizes para evitar e/ou mitigar esse cenário de ciberataque?	não	Sim, apenas para um cenário genérico de ciberataque	Sim, com variados cenários de ciberataque a diversos sistemas críticos.	5	1
Q2	Há procedimentos internos estabelecidos pelo aeroporto que fixem ações para evitar e/ou mitigar esse cenário de ciberataque?	não	Sim, porém sem procedimentos formalizados; ou formalizado apenas para um cenário genérico de ciberataque	Sim, com procedimentos formalizados para vários cenários de ciberataque e a diversos sistemas críticos	3	1
Q3	Há pessoal com capacidade adequada dedicado às ações de prevenção, identificação e mitigação de cenários de ciberataque?	não	Sim, com capacitação genérica em TI e/ou cenário genérico de ciberataque.	Sim, com capacitação específica para o sistema crítico em questão e esse cenário de ciberataque.	4	1

4	Há treinamento frequente para atualização dos conhecimentos do pessoal dedicado às ações de prevenção, identificação e mitigação de cenários de ciberataque?	não	Sim, porém com frequência inadequada ou sem disponibilidade para todos os envolvidos.	Sim, com frequência adequada e disponibilidade para todos os envolvidos.	4	1
5	O Sistema crítico em questão possui mecanismos de prevenção e detecção de ações de ciberataque (controle de acessos, *firewall*, criptografia e antivírus, etc)?	não	Sim, apenas para alguns dos seguintes: controle de acesso, *firewall*, criptografia, antivírus; ou sem atualização frequente.	Sim, com: controle de acesso, *firewall*, criptografia e antivírus todos atualizados frequentemente.	0	1
6	O sistema crítico em questão possui mecanismos de *backup* para o reestabelecimento de suas funções normais em caso de ações de ciberataque?	não	Sim, porém com frequência inadequada, ou sem armazenamento em local seguro ou sem restabelecimento célere quando necessário.	Sim, com *backup* com frequência adequada, armazenamento em local seguro e restabelecimento célere quando necessário	0	1
7	Há investimentos constantes na manutenção e atualização do *hardware* e *software* desse sistema crítico em questão, bem como das ferramentas de proteção do mesmo contra ação de ciberataque?	não	Sim, porém não no montante adequado; ou apenas das ferramentas de proteção do mesmo.	Sim, tanto do sistema crítico quanto das ferramentas de proteção do mesmo.	3	1
8	O Sistema crítico em questão pode ser acessado remotamente através da rede mundial de computadores?	Sim, com acesso livre através da internet	Sim, com controle de acesso e/ou autenticação eletrônica.	não	4	1
9	O Sistema crítico em questão pode ser acessado por pessoas que não façam parte do quadro de funcionários do operador do aeroporto?	Sim, com acesso livre ao público externo	Sim, restrito aos funcionários de empresas terceirizadas e/ou de empresas da comunidade aeroportuária.	não	4	1

10	Há registro do histórico de todos os acessos, rastreamento das ações realizadas nesse sistema crítico e possibilidade de identificação dos responsáveis?	não	Sim, porém com registro dos acessos; ou apenas com rastreamento das ações	Sim, com registro dos acessos, rastreamento das ações e identificação do responsável.	0	1
11	Há ações de conscientização junto aos operadores desse sistema crítico quanto a sua importância, criticidade e protocolos de segurança relacionados ao acesso e operação?	não	Sim, porém com frequência inadequada ou não oferecida para todos os envolvidos.	Sim, com frequência adequada e para todos os envolvidos.	5	1
12	Há ações de monitoramento e supervisão do sistema crítico em questão para assegurar o seu adequado funcionamento?	não	Sim, porém com o acúmulo de outras funções operacionais; ou o sistema possui apenas mecanismos automáticos de prevenção.	Sim, com funções dedicadas exclusivamente às ações de prevenção, identificação e mitigação de cenários de ciberataque	0	1
13	Uma falha no sistema crítico em questão afeta o adequado funcionamento de outros sistemas críticos?	sim		não	5	1
			Nível de Vulnerabilidade		37/13 = 2,8	

A tabela a seguir fornece a qualificação do nível de vulnerabilidade anteriormente encontrado através da média aritmética ponderada.

VULNERABILIDADE		
	Alta (5)	Não há procedimentos de segurança sendo realizados adequadamente para mitigar o risco.
	Média-alta (4)	Procedimentos de segurança realizados tem alcance limitado para mitigar o risco, ou áreas importantes não são abrangidas pelo efeito das medidas mitigadoras.
	Média (3)	Características das vulnerabilidades média-alta e média-baixa estão presentes.
	Média-baixa (2)	Procedimentos de segurança estão em vigor, mas podem ser parcialmente efetivos.
	Baixa (1)	Existem requisitos claros para mitigar o risco e os procedimentos de segurança estão sendo efetivamente realizados de forma adequada.

Logo, a vulnerabilidade encontrada é Média.

A fim de determinar o nível de risco da organização utiliza-se a matriz de nível de risco a seguir:

NÍVEL DE RISCO		PROBABILIDADE X SEVERIDADE				
		BAIXA (5)	MÉDIA-BAIXA (10)	MÉDIA (15)	MÉDIA-ALTA (20)	ALTA (25)
VULNERABILIDADE	Alta (5)	Média-baixa (25)	Média (50)	Média-alta (75)	Alta (100)	Alta (125)
	Média-alta (4)	Baixa (20)	Média-baixa (40)	Média (60)	Média-alta (80)	Alta (100)
	Média (3)	Baixa (15)	Média-baixa (30)	Média-baixa (45)	Média (60)	Média-alta (75)
	Média-baixa (2)	Baixa (10)	Baixa (20)	Média-baixa (30)	Média-baixa (40)	Média (50)
	Baixa (1)	Baixa (5)	Baixa (10	Baixa (15)	Baixa (20)	Média-baixa (25)

Como a vulnerabilidade é Média e como o nível da ameaça é Baixo, o nível de risco será Baixo.

Neste exemplo hipotético, o administrador do aeródromo considera aceitáveis os níveis de risco baixo e médio-baixo, o nível de risco para o cenário de ameaça "Ataque cibernético aos sistemas informatizados" está dentro dos níveis aceitáveis. Logo, não se tem a necessidade de adotar medidas mitigadoras ou medidas adicionais de segurança.

APÊNDICE F

Dicas Gerais e Rápidas para o Usuário de Sistemas TIC

APÊNDICE F: DICAS GERAIS E RÁPIDAS PARA O USUÁRIO DE SISTEMAS TIC

1 – Antes de clicar em um *link* passe o mouse ele e observe se a URL está correta;

2 – Observe se existem erros ortográficos ou gramaticais nos textos;

3 – Verifique se as imagens contidas na página são as que a empresa costuma utilizar;

4 – Ao receber uma mensagem que solicite uma ação imediata, certifique-se se você deveria receber esta mensagem;

5 – Observe se você conhece a pessoa que enviou a mensagem, se participou do evento ou se é seu banco;

6 – Verifique se mensagem que está solicitando sua ação é padrão. Cuidado com os anexos dos e-mails;

7 – Limpe a memória cache e o histórico do navegador com frequência;

8 – Conheça e siga as políticas de segurança cibernética da empresa;

9 - Não guarde cópias de login e senha em lugares fáceis de serem achados e acessados por terceiros;

10 – Utilize senhas fortes com pelo menos 8 caracteres, letras maiúsculas, minúsculas números e caracteres especiais e as modifique periodicamente;

11 - Especifique senhas diferentes para contas diferentes; não utilize as senhas de aplicativos de mídias sociais na organização onde trabalha;

12 – Sempre que possível adote autenticação com dois fatores, por exemplo: senha e código fornecido por SMS em um celular ou, preferencialmente, senha e código em um aplicativo autenticador;

13 – Não permita que terceiros conheçam a sua senha. Proteja-a durante digitação;

14 – Sempre feche ou bloqueie a sua seção quando se ausentar do uso do computador;

15 – Evite acessar sua conta em computadores de terceiros. Caso seja necessário utilize a navegação anônima em aplicativos buscadores, sempre que possível;

16 – Configure o computador para solicitar login e senha na tela inicial;

17 – Mantenha seus aplicativos atualizados e na mais recente versão;

18 - Sempre faça *backup* de dados importantes;

19 – Utilize criptografia em dados armazenados; e

20 - Utilize um *software antimalware* (antivírus).

APÊNDICE G

Passos para Realização de Avaliação de Risco

APÊNDICE G: PASSOS PARA REALIZAÇÃO DE AVALIAÇÃO DE RISCO

Passo 1: Determine o valor da informação;

Passo 2: Identifique e priorize os ativos;

Passo 3: Identifique as ameaças;

Passo 4: Identifique as vulnerabilidades;

Passo 5: Análise os controles existentes;

Passo 6: Calcule a probabilidade e o impacto de vários cenários em uma base anual;

Passo7: Priorize os riscos baseado sobre o custo da prevenção versus o valor da informação; e

Passo 8: Documente os resultados no relatório de avaliação de riscos.

ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL