ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

PAULO CESAR **FIALHO** DE SOUZA JUNIOR, Ten Cel Av

A Segurança da Informação na FAB: uma visão sob a ótica da ONU

Rio de Janeiro
2022

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

PAULO CESAR **FIALHO** DE SOUZA JUNIOR, Ten Cel Av

A Segurança da Informação na FAB: uma visão sob a ótica da ONU

Trabalho de conclusão de curso apresentado, como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior.
Linha de Pesquisa: Poder Militar.
Orientador: Evandro Carlos Baranzelli.

Rio de Janeiro
2022

RESUMO

O referido trabalho teve como objetivo analisar em que medida o nível de conscientização de Segurança da Informação dos usuários dos sistemas de TI atendiam às exigências que a ONU estabelece aos seus colaboradores. Tendo como referência as recomendações de Segurança da Informação (SI) abordadas no Curso Treinamento de Conscientização sobre Segurança da Informação (LMS-1834), aplicado pelo United Nations Department of Safety and Security, além do entendimento de SINOPEN (2000), ao elucidar que a SI tem associação direta com a Conscientização de Segurança da Informação. A metodologia utilizada foi uma revisão literária, visando identificar as principais recomendações de SI dispostas no LMS-1834 e na NSCA 7-13, analisando a compatibilidade existente entre eles. Então, foi mostrado que a NSCA 7-13, se respeitada a exigência da leitura da Cartilha de Segurança da Internet, tem um grau de compatibilidade elevado em relação ao LMS-1834 da ONU (95,24%) e que a simples recomendação dessa leitura adicional é capaz de elevar o nível de conscientização acerca da SI, já que aumentou a quantidade de militares capazes de identificar url's fraudulentos de 16,7% para 75%, sendo um subsídio fundamental para a garantia da Superioridade de Informações, característica almejada na concepção estratégica Força Aérea 100. Com isso, atingiu-se o objetivo da pesquisa ao verificar o nível de conscientização dos oficiais alunos do CACEM-2022.

Palavras-chave: Segurança da Informação; Guerra Cibernética; *Phishing*; Engenharia Social.

ABSTRACT

This work aimed to analyze to what extent the level of Information Security awareness of users of IT systems met the requirements that the UN establishes for its employees. Having as reference the Information Security (IS) recommendations addressed in the Information Security Awareness Training Course (LMS-1834), applied by the United Nations Department of Safety and Security, besides the understanding of SINOPEN (2000), when elucidating that IS has a direct association with Information Security Awareness. The methodology used was a literature review, aiming to identify the main IS recommendations set forth in LMS-1834 and NSCA 7-13, analyzing the compatibility between them. Then, it was shown that NSCA 7-13, if the requirement of reading the Internet Security Primer is respected, has a high degree of compatibility in relation to the UN's LMS-1834 (95.24%) and that the simple recommendation of this additional reading is capable of raising the IS awareness level, since it increased the amount of military personnel capable of identifying fraudulent url's from 16.7% to 75%, being a fundamental subsidy to guarantee the Information Superiority, a characteristic aimed at in the strategic conception of the Air Force 100. With this, the objective of the research was achieved by verifying the level of awareness of the student officers of CACEM-2022.
Keywords: *Information Security; Cyber Warfare; Phishing; Social Engineering.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACABQ	Advisory Committee on Administrative and Budgetary Questions
BCA	Boletim do Comando da Aeronáutica
CACEM	Curso Avançado de Comando e Estado-Maior
CIAER	Centro de Inteligência da Aeronáutica
CLM	*Centre for Learning and Multilingualism*
COMAER	Comando da Aeronáutica
COMGAP	Comando Geral de Apoio
CSI	Conscientização de Segurança da Informação
DCA	Diretriz do Comando da Aeronáutica
FAB	Força Aérea Brasileira
FCA	Folheto do Comando da Aeronáutica
ICA	Instrução do Comando da Aeronáutica
LMS	*Learning Management System*
MCA	Manual do Comando da Aeronáutica
NSCA	Norma do Sistema do Comando da Aeronáutica
OICT	*Office of Information and Comunications Technology*
ONU	Organização das Nações Unidas
PCSI	Programa de Conscientização sobre Segurança da Informação
SI	Segurança da Informação
TI	Tecnologia da Informação
UNDSS	*United Nations Department of Safety and Security*
UNOG	*United Nations Office at Geneva*
URL	*Uniform Resource Locator*

SUMÁRIO

1 INTRODUÇÃO

Em outubro de 2018, o Comando da Aeronáutica (COMAER) publicou uma atualização da DCA 11-45, documento que versa sobre a concepção estratégica, conhecida como Força Aérea 100, que tem a finalidade de estabelecer a visão de futuro da Força Aérea Brasileira (FAB) ao atingir 100 anos de sua criação no ano de 2041.

Com isso, a FAB passou a ser conduzida sobre a perspectiva de buscar ter grande capacidade dissuasória, além de ser moderna operacionalmente e de atuar, de maneira integrada, na defesa dos interesses nacionais.

Para nortear essa visão foram definidas algumas capacidades militares desejadas e, entre elas, está a Superioridade de Informações, que é ter competência para coletar, armazenar, processar, disseminar, produzir e proteger dados operacionais, além de negar a possibilidade de o adversário fazer o mesmo, dando liberdade de ação e segurança para as operações militares. (Brasil, 2018)

No entanto, para obter a Superioridade de Informações e alcançar a visão de futuro, estabelecida na Força Aérea 100, é essencial fortalecer a mentalidade de Segurança da Informação (SI) na cultura organizacional da FAB, já que houve o aumento no número de ataques cibernéticos durante a pandemia do COVID-19, elevando o grau de exposição e consequente vulnerabilidade das organizações militares. Além disso, entende-se que, quanto mais forte for a mentalidade de segurança da informação, maior será a defesa das organizações militares em relação aos ataques cibernéticos.

Então, em 2020, enquanto, em virtude da pandemia, o cenário internacional estava voltado para as questões sanitárias, adotando medidas de isolamento social, os criminosos intensificavam suas investidas em ataques cibernéticos, explorando as vulnerabilidades das pessoas que trabalhavam por meio de acesso remoto ou buscavam distrações em redes sociais.

Outrossim, militares mais conscientes da importância do papel deles na defesa das informações, passam a ser um auxílio valioso na proteção de dados essenciais ao alcance dos objetivos estratégicos institucionais.

Nesse contexto, por meio da Resolução A/RES/68/247, de 14 de janeiro de 2014, a Assembleia Geral da Organização das Nações Unidas (ONU) endossou a implementação de recomendações relacionadas ao fortalecimento da SI. Com isso, o Escritório de Tecnologia da Informação e Comunicações da ONU recebeu a incumbência de implementar um regime de gestão de risco de informação, estabelecer políticas de apoio e elaborar um plano de ação para verificar as fragilidades mais urgentes e mitigar os riscos.

Portanto, face ao exposto, diante dos desafios impostos pela pandemia do COVID-19 na obtenção da SI, cabe analisar, mais precisamente, a seguinte questão: em que medida o nível de conscientização de SI dos usuários dos sistemas de Tecnologia da Informação (TI) da FAB atende aos critérios fundamentais estipulados pela ONU?

Dessa forma, o presente trabalho partiu da hipótese de que os usuários dos sistemas de TI da FAB não atendem aos critérios fundamentais que a ONU exige para os seus usuários.

Já, o objetivo geral dessa pesquisa teve por finalidade analisar em que medida o nível de conscientização de SI atende às exigências que a ONU estabelece para os seus usuários.

Para direcionar o trabalho ao alcance do objetivo geral, foram estabelecidos os seguintes objetivos específicos (OE):

OE1) Discorrer acerca do treinamento da ONU LMS-1834, com foco nas recomendações de segurança da informação;

OE2) Descrever sobre a NSCA 7-13 com foco nas recomendações de segurança da informação;

OE3) Comparar a compatibilidade entre as recomendações de segurança da informação constantes na NSCA 7-13 e no LMS-1834

OE4) Analisar em que medida o nível de conscientização dos usuários da FAB atende às exigências fundamentais constante nas recomendações de segurança da informação estabelecidas pela ONU.

A relevância dessa pesquisa reside no entendimento de que a Superioridade de Informações é uma das capacidades militares essenciais para o alcance da visão de futuro estabelecida na Concepção Estratégica Força Aérea 100, já que ela garante segurança e liberdade de ação para a exploração do Poder Militar.

Afinal, um ataque bem-sucedido nos computadores de alguma Base Aérea seria capaz fornecer ao inimigo dados essenciais para exploração do domínio cibernético, expondo as nossas vulnerabilidades, além de aumentar a consciência situacional do inimigo acerca dos nossos Meios de Força Aérea, podendo refletir na obtenção de efeitos ofensivos e defensivos mais eficientes frente ao nosso Poder Militar.

Dessa forma, a presente pesquisa visou levantar subsídios para verificar se o nível de conscientização de SI dos militares da FAB estava abaixo daquilo que a ONU tem como referência, conforme a hipótese desse trabalho, com o objetivo de apontar uma possível vulnerabilidade em nossas bases militares para que, posteriormente, sejam adotadas medidas em prol da elevação desse nível, fortalecendo as nossas defesas face a um cenário de ataques cibernéticos que possam explorar a não observância das boas práticas de SI.

2 REFERENCIAL TEÓRICO

Para a compreensão do conceito de SI será adotado a definição de Williams (2001), que constitui na defesa dos ativos informacionais, no que tange às perdas, danos ou divulgação indevida de dados para qualquer informação guardada, divulgada ou propagada dentro de uma organização ou na comunicação interinstitucional.

Tomando como referência o entendimento de MITNICK e SIMON (2003), compreende-se que conforme vão sendo implementadas inovações, por meio de especialistas, realizando progressos contínuos de melhorias tecnológicas no âmbito da segurança e criando obstáculos para se explorar as fragilidades técnicas, os atacantes vão passando a concentrar seus esforços, cada vez mais, na exploração das vulnerabilidades do elemento humano.

Dessa forma, a FAB desenvolveu a DCA 14-8 a qual visa desenvolver ações para o cumprimento de suas diretrizes estratégicas, conforme a política de segurança da informação, justamente, por compreender que ameaças na SI podem gerar riscos não aceitáveis, os quais precisam ser monitorados e analisados de maneira constante (BRASIL, 2018).

Estas legislações, produzidas pelo COMAER, buscam adequar a Força Aérea ao conjunto de normalizações que têm como objetivo aprimorar os métodos de segurança da informação, em virtude do aumento de ataques cibernéticos (ABNT, 2006; ABNT, 2005).

De acordo com SINOPEN (2000), a Segurança da Informação nas instituições possui associação direta ao que ele chama de “Conscientização de Segurança da Informação” (CSI), referindo-se à compreensão que os usuários dos sistemas de TI têm acerca da importância do papel da SI para uma instituição.

No entanto, a resistência dos colaboradores ao cumprimento das regras de SI constitui-se como o fator essencial ao surgimento de brechas na proteção de dados, tornando primordial o desenvolvimento desse estado de conscientização na cultura organizacional de qualquer instituição (PUHAKAINEN e SIPONEN, 2010).

Além disso, para Puhakainen e Siponen (2010), os colaboradores que não agem em consonância com as recomendações da política de Segurança da Informação passam a ser um risco elevado para suas instituições, sendo necessário dar ênfase nos procedimentos de segurança, com a finalidade de que os colaboradores passam a compreender a gravidade das consequências advindas de um descumprimento das orientações de SI, levando-os a adoção de um comportamento mais seguro. Portanto, com base nessas elucidações, compreende-se que as organizações militares estarão mais seguras quanto maior for o nível de CSI dos usuários de TI.

Ademais, para se ter um parâmetro do nível adequado no que tange à conscientização acerca da SI, será adotada a abordagem de cibersegurança, conforme as recomendações da ONU, explícitas no Curso Treinamento de Conscientização sobre Segurança da Informação, aplicado pelo *United Nations Department of Safety and Security* (UNDSS).

3 METODOLOGIA

Levando em consideração o texto de Gil (2002), esta pesquisa foi classificada como descritiva no que tange aos seus objetivos, estabelecendo uma relação entre o nível de conscientização em SI dos usuários da TI da FAB, tendo como critério o grau exigido pela ONU aos seus usuários.

Além disso, foi efetuada uma revisão literária, com a finalidade de fornecer fundamentos para a elucidação do conceito de SI e da sua importância como uma linha de defesa das organizações militares em relação aos ataques cibernéticos, bem como para delimitar os pontos fundamentais inerentes à SI.

Em seguida, foi realizada uma pesquisa bibliográfica, com a finalidade de identificar as principais recomendações de SI dispostas no Treinamento Básico de Segurança da Informação da ONU (LMS-1834) e na Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13), comparando a compatibilidade existente entre elas.

Na última fase do trabalho, buscou-se verificar o nível de conscientização de SI dos usuários de TI, por meio de um questionário com seis questões, disposto no Apêndice C, que teve como finalidade levantar dados acerca das principais recomendações levantadas após a fase de averiguação de compatibilidade entre a LMS-1834 e a NSCA 7-13, conforme distribuição apresentada no quadro abaixo:

Quadro 1- Distribuição das questões com foco nos dados coletados

QUESTÃO	DADO COLETADO
1	Conhecimento acerca da Cartilha de Segurança da Internet
2	Critério qualitativo da senha utilizada para fazer login no computador do trabalho
3	Números de caracteres da senha utilizada para fazer login no computador do trabalho
4	Conhecimento sobre os sinais de alerta constantes nos e-mails de phishing
5	Atitude perante uma janela pop-up comumente usada em prática de phishing
6	Identificação de URL's fraudulentos

Fonte: O autor

Já nessa parte da pesquisa, o universo adotado foram os oficiais alunos que estão realizando o Curso Avançado de Comando e Estado-Maior no presente ano de 2022 (CACEM-2022), sendo disposto da seguinte forma: 01 Coronel Intendente, 50 aviadores no posto de Tenente-Coronel, 28 intendentes no posto de Tenente-Coronel, 3 infantes no posto de Tenente-Coronel e 16 aviadores no posto de Major. Desse universo, 5 foram designados para testar o questionário, 4 para a avaliação por pares, obtendo uma delimitação de 90 oficiais superiores.

A pesquisa limitou-se aos oficiais alunos do CACEM-2022, portanto, não foi analisado o nível de conscientização de oficiais subalternos ou intermediários, nem de graduados ou praças.

Então, a primeira etapa do questionário teve a finalidade de levantar se os usuários dos sistemas de TI tinham conhecimento acerca das competências deles, de modo a cumprir o estabelecido nos procedimentos de segurança conforme a NSCA 7-13.

Na etapa posterior, buscou-se avaliar o nível de conscientização de SI dos oficiais alunos do CACEM-2022, tendo como referência os 7 temas principais, dispostos no Curso Básico de Conscientização sobre Segurança da Informação da ONU (LMS-1834), considerando as recomendações mais relevantes, obtidas da análise de compatibilidade entre o Curso LMS-1834 e a NSCA 7-13.

4 APRESENTAÇÃO DE DADOS E ANÁLISE DE RESULTADOS

No presente capítulo foram divulgados os dados desse trabalho por meio de uma pesquisa bibliográfica, numa primeira fase, e, em seguida, através de um questionário com a finalidade de verificar o nível de conscientização sobre SI dos oficiais alunos.

4.1 O Curso Básico de Segurança da Informação (LMS-1834)

No parágrafo 107 da resolução 66/246, a Assembléia Geral da ONU solicitou ao *Advisory Committee on Administrative and Budgetary Questions* (ACABQ) que, por intermédio do Conselho Fiscal, fizesse uma auditoria, avaliando o tratamento das informações e dos assuntos de TI. Dessa forma, o Conselho Fiscal realizou a auditória em outubro de 2012, apresentando ao Secretário-Geral o Relatório A/67/651 em 19 dezembro de 2012.

No parágrafo 95 desse relatório, o Conselho de Auditores declarou que os Estados Unidos não possuíam um ambiente de informação adequadamente seguro e que os controles de

segurança existentes estavam aquém do que o Conselho esperaria de uma organização mundial moderna.

Além disso, afirmou que o Secretariado tinha capacidade extremamente limitada para o monitoramento de segurança não estando em condições de detectar e responder a todas as tentativas ou violações bem-sucedidas.

Já num relatório posterior (A/67/651/Add.1), divulgado em 16 de janeiro de 2013, o Secretário-Geral declarou que a recomendação, relacionada ao fortalecimento da Segurança da Informação e dos seus sistemas, estava sendo tratada com urgência mediante o desenvolvimento de um plano de ação, incluindo medidas de curto prazo para abordar as deficiências mais urgentes e a definição de uma estratégia sustentável de médio e longo prazo para a segurança da informação.

Com isso, por solicitação do Secretariado da ONU, o *Office of Information and Comunications Technology* (OICT) foi encarregado de estabelecer um sistema de Gestão de Risco da Informação e desenvolver políticas de suporte à Segurança da Informação. Dessa forma, foi desenvolvido Plano de Ação para atender às deficiências mais urgentes e mitigar os riscos específicos.

Esse plano de ação consistiu em 10 iniciativas com foco nas 3 áreas seguintes:

a) Recursos aprimorados de detecção e resposta da incidentes: com o objetivo de se adaptar para um ambiente aonde o risco de ameaças aumentou significativamente, o Secretariado da ONU implementaria sistemas adicionais de detecção de invasão e passaria a monitora a suas redes sistematicamente;

b) Governança, Risco e Compliance: ao implementar uma diretiva de Segurança da Informação, a qual estabeleceria os princípios fundamentais de SI na ONU, atuando como base para a ratificação e implementação dos instrumentos de política e governança.

c) Controles Preventivos: Com o compromisso de fortalecer os controles técnicos de infraestrutura de TI, o Secretariado comprometeu-se em estabelecer controles mais rígidos dos dispositivos de computação usadas nas redes ONU, em prevenir o uso prejudicial da internet e e-mail, fortalecendo medidas técnicas de proteção, em segmentar a rede para isolar áreas onde os vírus possam se esconder para ataques potenciais e, por fim, em melhorar a conscientização sobre segurança da informação entre os seus colaboradores, por meio de um treinamento.

Na Resolução A/68/552, divulgada em 25 de outubro de 2013, a qual tratou acerca do progresso na implementação das recomendações relacionadas ao fortalecimento da Segurança da Informação, no que tange aos Controles Preventivos, foi esclarecido que além da aquisição de sistemas de filtragem adicionais para o acesso à internet, do uso de e-mail e da

reconfiguração dos servidores para elevação dos níveis de segurança face às potenciais vulnerabilidades e da revisão da infraestrutura de firewall da Sede por uma tecnologia mais avançada, também, foi desenvolvido um curso de treinamento para aumentar o nível de conscientização sobre acerca da segurança da informação entre todos os funcionários da ONU.

Finalmente, por meio da Resolução A/RES/68/247, de 17 de janeiro de 2014, a Assembleia Geral da ONU, endossou a implementação das recomendações relacionadas ao fortalecimento da Segurança da Informação, aprovando o Programa de Conscientização sobre Segurança da Informação (PCSI).

Desenvolvido para todos os funcionários da ONU e a todos os usuários dos sistemas de TI, o PCSI oferece um treinamento de conscientização sobre segurança da informação, a fim de que eles adquiram os conhecimentos fundamentais para a manutenção da Segurança Cibernética.

Esse programa é dividido em três módulos, sendo eles:

LMS-1834 – Curso Básico de Conscientização sobre Segurança da Informação;

LMS-1837 – Curso Avançado de Conscientização sobre Segurança da Informação;

LMS-182 – Curso Adicional de Conscientização sobre Segurança da Informação.

Coordenado pelo Centre for Learning and Multilingualism do United Nations Office at Geneva (UNOG), o programa é realizado on-line por meio da plataforma inspira da ONU. E, de acordo com o Boletim do Secretário-Geral nº ST/SGB/2004/15, para que os usuários recebam a autorização para utilizar os sistemas de TI é necessário realizar o treinamento básico LMS-1834, seguido de uma avaliação de 20 perguntas (LMS-1835), aonde eles precisam obter o grau 8,0. Portanto, só após a conclusão desse treinamento básico e da realização bem-sucedida desse teste é que os funcionários da ONU receberão seus credenciamentos.

Para a análise de dados, o presente trabalho levantou as informações somente do LMS-1834, em virtude de ele ser o único curso de caráter obrigatório para o credenciamento.

O LMS-1835 abrange sete temas principais, dispostos em módulos, sendo considerados a base para se ter um nível adequado de conscientização de segurança da informação. São eles:

a) introdução à segurança da informação: esse módulo aborda sobre a importância da Segurança da Informação que cresceu com a era digital, juntamente com o aumento dos riscos e vulnerabilidades. Além disso, esse módulo aborda as duas principais políticas de Segurança da Informação da ONU dispostas nas resoluções ST/SGB/2004/15 e ST/SGB/2007/6. Por fim, conclui elucidando sobre a responsabilidade dos funcionários da ONU em proteger as informações contra o acesso não autorizado, modificação, destruição e divulgação.

b) protegendo informações sensíveis: esse módulo trata da análise de como se faz a proteção de dados sensíveis, além de esclarecer sobre as principais ameaças que os dados classificados estão sujeitos.

c) engenharia social: essa parte do treinamento visa a compreensão sobre a engenharia social e as ameaças associadas a ela. Trata, também, de maneiras para se identificar os métodos e táticas mais comuns de engenharia social, reconhecendo os principais ataques e golpes utilizados e esclarecendo sobre as formas de mitigação dos riscos.

d) seleção e uso de senha: nessa fase do curso são apresentadas as principais característica de senhas fortes, elucidando sobre as formas de se criar senhas mais fortes, bem como a compreensão dos erros comuns na criação de senhas e a melhores práticas para a segurança das senhas.

e) mensagens eletrônicas e phishing: esse módulo faz uma análise acerca da crescente ameaça da prática de phishing, listando os riscos associados às mensagens eletrônicas. Além disso, explica sobre os sinais alertas inerentes aos URL's fraudulentos e anexos com códigos maliciosos, apresentando as melhores práticas, como o uso de mensagens protegidas e a exclusão segura de informações.

f) acessando informações na internet: essa etapa refere-se a importância de navegar com segurança na internet, indicando os perigos potenciais de navegadores, URL's e sites, além de alertar sobre as responsabilidades de cada um em relação à navegação segura.

g) respondendo à incidentes: esse módulo final descreve sobre o que seria um evento ou incidente de segurança da informação, oferecendo subsídios para a identificação de um evento de segurança da informação e os procedimentos para a primeira resposta que deve ser dada ao se suspeitar de um evento ou incidente dessa natureza, bem como os processos para se relatar tais ocorrências.

Então, visando atender ao primeiro objetivo específico desse trabalho, após a pesquisa bibliográfica, foi confeccionado o quadro 1, constante no apêndice A, descrevendo os assuntos que continham as principais recomendações de segurança da informação para os usuários dos sistemas de TI.

4.2 A Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13)

A NSCA 7-13 teve sua reedição aprovada por meio da Portaria do Comando-Geral de Apoio (COMGAP) nº 42/ADLG, de 02 de maio de 2022.

Com a finalidade de orientar as Organizações do COMAER no que tange aos princípios de segurança da informação, visando a garantia da confidencialidade, integridade, disponibilidade e autenticidade das informações armazenadas, processadas ou em trânsito, a fim de garantir a Defesa do Escopo Cibernético do Comando da Aeronáutica.

Dentre os objetivos propostos, podem-se elencar três que possuem relação direta com os usuários de TI, sendo eles:

a) Elencar os princípios básicos a fim de garantir os níveis adequados de segurança da informação de ativos físicos, dos ativos de software e dos ativos de informação de interesse do COMAER;

b) Conscientizar os usuários de TI do COMAER e os colaboradores terceirizados, sobre a importância de conhecer e aplicar as normas e os procedimentos de segurança da informação preconizados nas legislações inerentes ao assunto, tanto as publicadas na esfera do COMAER, quanto às publicadas em outras esferas governamentais;

c) Conscientizar o público interno do Comando da Aeronáutica sobre as vulnerabilidades e riscos aos quais estão submetidos os recursos computacionais da Organização ou pessoais, seja para defesa da infraestrutura crítica da informação, ou seja, para possível resposta a ações ofensivas perpetradas por elementos adversos.

No capítulo três, a NSCA 7-13 discorre acerca dos procedimentos de segurança, abordando sobre o funcionamento do controle de físico e lógico aos sistemas de TI, além de tratar sobre os serviços de rede da intraer e da internet, enfatizando que a entrada em operação de sistemas ou serviços que utlizam a intraer e internet é feita mediante autorização do Órgão Central do STI.

Nessa parte, também, é elucidado sobre os procedimentos relativos às inspeções nos sistemas de TI, bem como o monitoramento das atividades, as etapas para reportar os incidentes de Segurança da Informação e os meios legais para a contratação de colaboradores terceirizados, por meio de cláusulas que adotem controles de segurança para os sistemas de TI, com o uso de termo de confidencialidade.

Em respeito às competências, a NSCA 7-13 define que os usuários do STI devem adequar suas atividades de TI, de modo a cumprir o estabelecido nos procedimentos de segurança descritos.

Além disso, para os Elos de Serviço de STI, ela define que seja implantado o conteúdo da cartilha “Boas práticas em segurança da informação, 4ª edição, 2012” ou a versão mais atualizada, a qual está disponível no site do Tribunal de Contas da União (www.tcu.gov.br).

Já para os usuários do STI, fica a incumbência de tomar conhecimento acerca do conteúdo da cartilha de segurança, disponível no site www.cert.br, com a finalidade de adquirir o conhecimento mínimo necessário a respeito do tema segurança da informação.

Por fim, a política de segurança de uso dos recursos computacionais consta no Anexo A do documento, abordando as principais recomendações de segurança da informação inerentes aos usuários dos sistemas de TI.

Com isso, para cumprir o segundo objetivo específico dessa pesquisa, foi produzido o quadro 2, constante no apêndice b, a qual descreve os principais assuntos que a NSCA 7-13 aborda, sendo apresentados conforme os 7 temas principais apresentados no LMS-1834.

4.3 A compatibilidade entre o LMS-1834 e a NSCA 7-13

Ao analisar a compatibilidade entre o Curso Básico de Segurança da Informação (LMS-1834) e a Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13), identificou-se que a NSCA 7-13 aborda 14 dos 21 assuntos tratados no LMS-1834.

No entanto, conforme já mencionado no capítulo anterior, a NSCA 7-13 recomenda que todos os usuários dos Sistemas de TI tomem conhecimento sobre o conteúdo da cartilha de segurança para internet, e, dos outros 7 assuntos que não são abordados na própria NSCA 7-13, 6 deles estão dispostos na Cartilha de Segurança da Internet, conforme quadro a seguir:

Quadro 4 - Assuntos não abordados na NSCA 7-13 que constam na Cartilha de Segurança da Internet

TEMA	ASSUNTO
Engenharia Social	O que é engenharia social e quais são suas ameaças
	Como identificar os métodos e táticas mais comuns da engenharia social
	Formas de mitigação dos riscos
Mensagens eletrônicas e phishing	Riscos associados às mensagens eletrônicas
	Uso de mensagens protegidas e exclusão segura de informações
Acessando informações na internet	Os perigos potenciais de navegadores, url's e sites

Fonte: O autor

No que tange à temática da Engenharia Social, embora nenhum assunto tenha sido tratado na NSCA 7-13, como essa prática utilizada pra cometer atos ilícitos não se restringe ao âmbito da internet, esse tema é amplamente tratado no Folheto do Comando da Aeronáutica (FCA 200-2), que dispõe sobre Mentalidade de Segurança e no Folheto do Comando da Aeronáutica FCA 200-3, o qual versa sobre a Prevenção à Engenharia Social.

Em relação ao tema "Mensagens eletrônicas e phishing", embora a NSCA 7-13 não trata, especificamente, dos riscos associados às mensagens eletrônicas, nem do uso de mensagens protegidas e exclusão segura de informações, em seu Anexo D, ela apresenta uma política de antivírus e códigos maliciosos, abrangendo a prevenção, detecção e erradicação de vírus, contaminações e códigos maliciosos.

No entanto, embora o Anexo D da NSCA 7-13 estabeleça normas de utilização de programa de antivírus com configuração periódica para atualização automática em intervalos regulares, bem como a adoção do procedimento de desconectar fisicamente da rede os computadores infectados até a sua descontaminação, nem a NSCA 7-13, nem a Cartilha de Segurança para Internet tratam acerca da identificação de Url's fraudulentos, sendo tal conteúdo enfatizado apenas no LMS-1834.

Já no tópico "Acessando informações na internet", a NSCA aborda acerca da importância de navegar com segurança na internet e das responsabilidades dos usuários dos sistemas de TI em relação à navegação segura, faltando apenas tratar dos perigos potenciais de navegadores, url's e sites, o que é complementado pela Cartilha de Segurança para Internet.

Vale ressaltar que, no que tange ao tema "Protegendo informações sensíveis", a compreensão da importância da classificação de dados, obviamente, não é baseada no Boletim do Secretário-Geral da ONU nº ST/SGB/2007/6, e sim na Política de Manipulação de Informações Classificadas, disposta no Anexo C, a qual está em consonância com a homologação do Centro de Inteligência da Aeronáutica (CIAER), conforme preconizado a Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ICA 205-47/2015).

Entretanto, as recomendações de segurança para o armazenamento e tramitação segura de informações sensíveis atendem aos requisitos do Boletim nº ST/SGB/2007/6, tendo em vista a exigência de criptografia, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, para o trâmite de dados e informações classificadas quando enviadas por meio eletrônico.

Por fim, em relação à seleção e uso de senha, a despeito da NSCA 7-13 tratar desse assunto no Anexo A, o qual engloba a "Política de Uso de Recursos Computacionais", definindo critérios para criação e utilização de senhas, existe uma divergência sobre o número mínimo de

caracteres para criação de senhas. Enquanto o LMS-1834 exige um número mínimo de 12 caracteres, a NSCA 7-13 adota um número mínimo de 8 caracteres.

Além disso, ainda que a NSCA 7-13 proíbe o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas, além de palavras que façam parte de dicionários ou de listas publicamente conhecidas (nomes de músicas, nomes de filmes, times de futebol, personagens de filmes e dicionários de diferentes idiomas), no Anexo A é recomendado que se priorize a utilização de frases complexas no lugar de palavras ou o uso de maiúsculas e minúsculas, números, sinais de pontuação ou símbolos.

Dessa forma, diferentemente do LMS-1834, que exige a adoção de letras maiúsculas e minúsculas, números e sinais de pontuação ou símbolos, a NSCA 7-13 não enfatiza, categoricamente, a utilização desses caracteres para compor as senhas, sendo identificada essa distinção entre eles.

Com isso, foi atendido o terceiro objetivo específico da presente pesquisa, constatando, de acordo com o gráfico 1, um grau de compatibilidade de 66,67% entre o LMS-1834 e a NSCA 7-13 e um grau de 95,24% ao se incluir o conteúdo da Cartilha de Segurança da Internet, considerando que os usuários dos sistemas de TI cumprissem a recomendação de tomar conhecimento da referida cartilha.

Quadro 5 - Compatibilidade entre o LMS-1834 e a NSCA 7-13

DOCUMENTOS LIDOS	GRAU DE COMPATIBILIDADE
Somente a NSCA 7-13	66,67%
NSCA 7-13 mais a Leitura da Cartilha de Segurança da Internet	95,24%

Fonte: O autor

Então, com base nos dados levantados na pesquisa bibliográfica encerrou-se a primeira fase desse trabalho, ao identificar as principais recomendações de SI que constam no LMS-1834 e na NSCA 7-13, bem como o nível de compatibilidade existente entre eles.

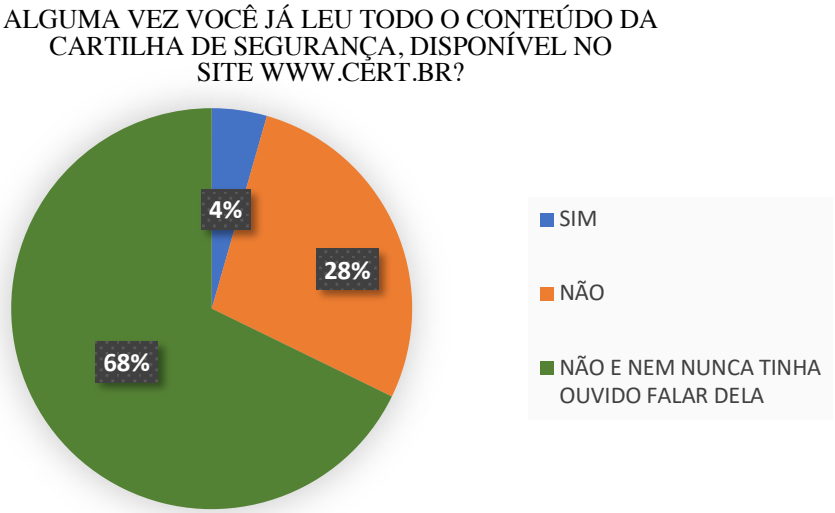
Em seguida, foi iniciada a segunda fase desse trabalho por meio de um questionário que teve como objetivo verificar o nível de conscientização de SI, adotando como universo os oficiais alunos que estavam realizando o Curso Avançado de Comando e Estado-Maior no ano de 2022 (CACEM-2022).

4.4 A conscientização em Segurança da Informação

Com os dados coletados no questionário iniciou-se a análise, averiguando o nível de conformidade dos usuários dos SI em relação ao item 5.5 da NSCA 7-13, o qual enfatiza como competência, inerente aos usuários dos sistemas de TI, a leitura da Cartilha de Segurança da Internet, disposta no site www.cert.br, com finalidade de eles obterem o conhecimento mínimo necessário sobre a SI.

Dessa forma, por meio da Questão 1 foi identificado que somente 4,4 % dos militares leram a cartilha mencionada e 67,8% sequer tinham o conhecimento da existência desse documento.

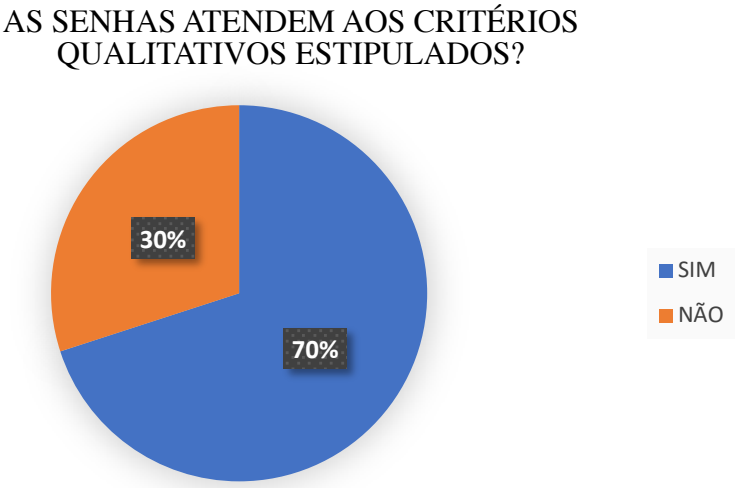
Figura 1 – Questão 1



Fonte: O autor

Na questão 2 foi verificado que 70% dos oficiais alunos atendem aos critérios qualitativos de confecção de senha, fazendo o uso de letras maiúsculas e minúsculas, números e sinais de pontuação ou símbolos, além de evitarem o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas, além de palavras que façam parte de dicionários ou de listas publicamente conhecidas, conforme figura 2 abaixo apresentada:

Figura 2 – Questão 2

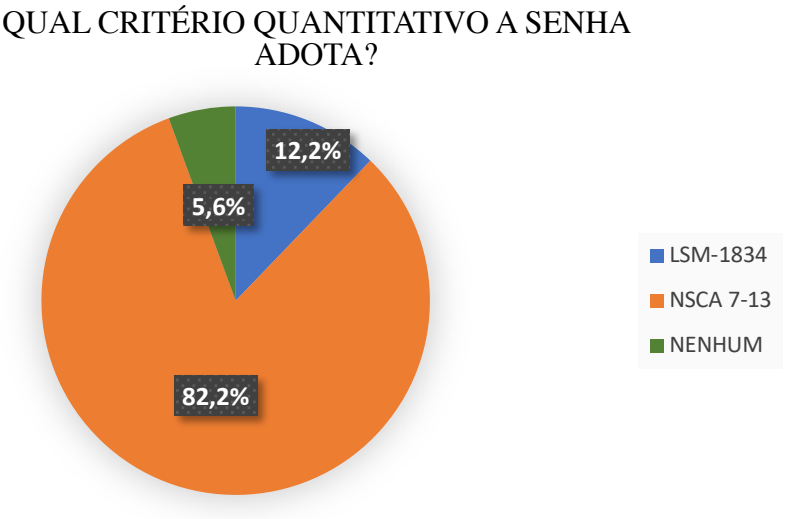


Fonte: O autor

Na questão 3, buscou-se coletar dados acerca da quantidade de caracteres utilizada para fazer o login no computador do trabalho. Vale ressaltar que, conforme já mencionado no item 4.3, a NSCA 7-13 exige o mínimo de 8 caracteres e o LMS-1834 defende que as senhas não devem ter menos do que 12 caracteres.

Dessa forma, constatou-se que 82,2% cumprem o critério estabelecido na NSCA 7-13 e 12,2% utilizam-se do critério mais restritivo estipulado no LMS-1834. Além disso, foi verificado que 5,6% dos oficiais alunos não atendem a nenhum dos dois critérios, tendo senhas de até 7 caracteres, possuindo senhas mais fracas no que diz respeito ao parâmetro quantitativo de criação de senha.

Figura 3 – Questão 3

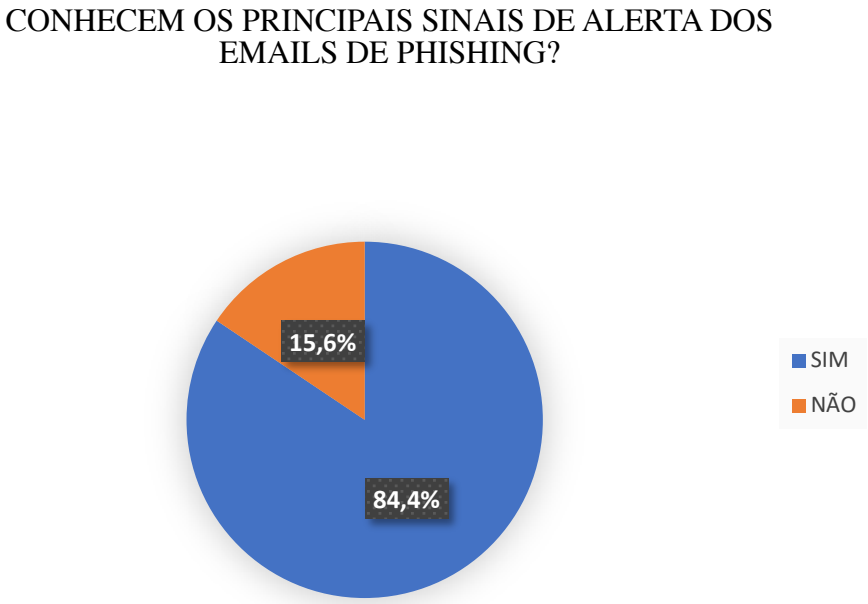


Fonte: O autor

Em seguida, na questão 4, por meio de uma pergunta objetiva, adotada, também, na avaliação do treinamento básico LMS-1834, buscou-se levantar dados sobre o conhecimento dos oficiais alunos em relação aos sinais de alerta que costumam constar nos e-mails de phinshing.

Dessa forma, foi constatado que 84,4% dos usuários dos sistemas de TI acertaram a questão 4, demonstrando que eles conhecem os principais sinais de alerta que ajudam a identificar os e-mails de phishing.

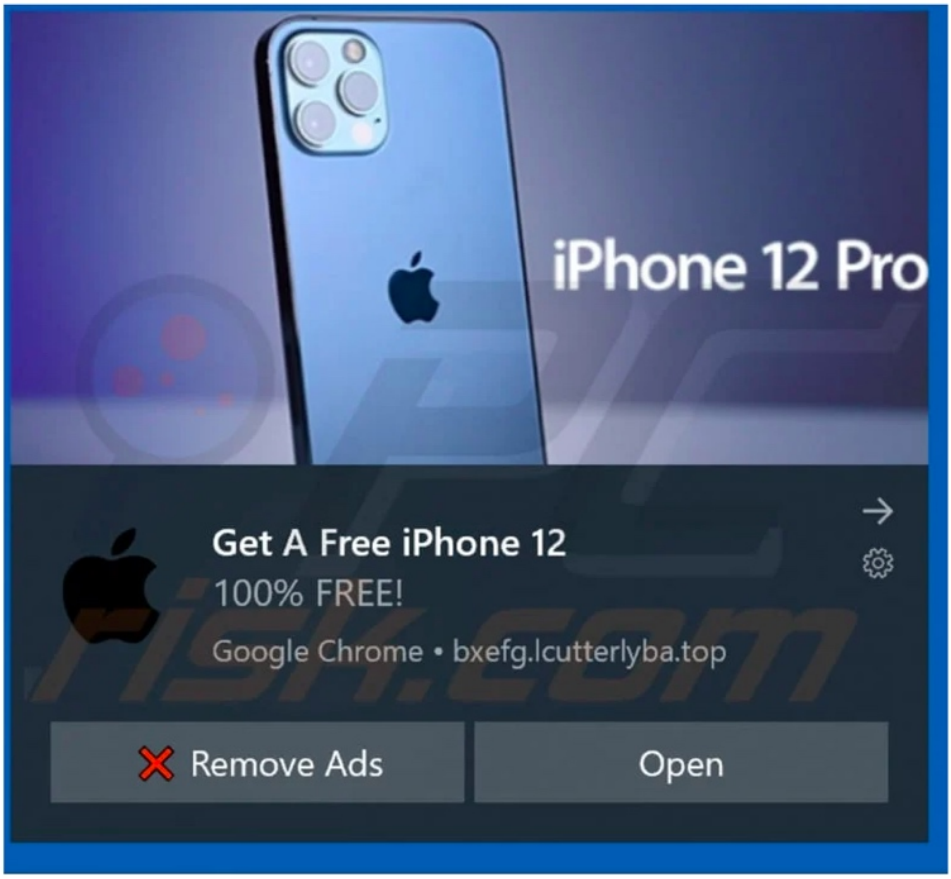
Figura 4 – Questão 4



Fonte: O autor

Ainda na temática de mensagens eletrônicas e phishing, por meio da questão 5, também, similar a adotada na avaliação do LMS-1834, visou coletar informação acerca da atitude que os oficiais alunos adotariam caso se deparassem com um janela pop-up comumente usada em prática de phishig, conforme figura abaixo:

Figura 5 – Janela pop-up comumente utilizada em prática de phishing.

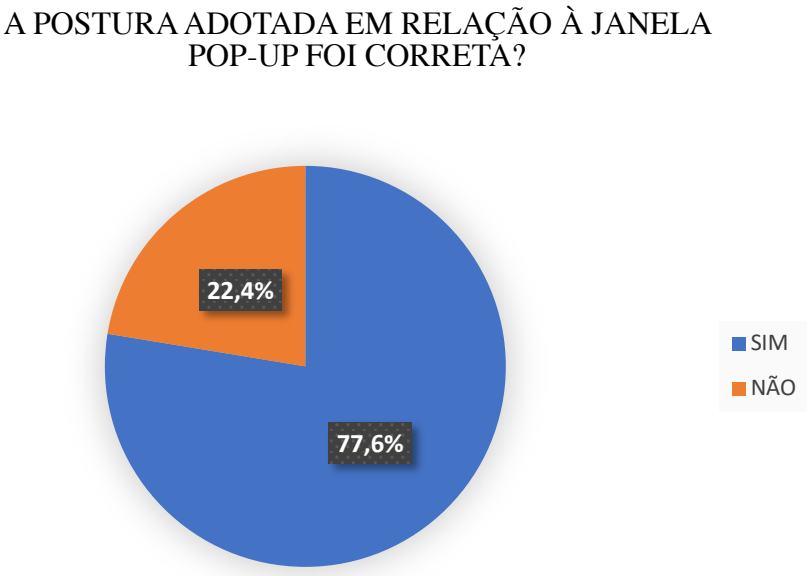


Fonte: https://www.pcrisk.com/removal-guides/19862-win-the-new-iphone-12-pop-up-scam

Então, nessa parte do questionário, verificou-se que 77,6% dos oficiais alunos foram capazes de tomarem a atitude correta face a um possível ataque de phishing, disfarçado por uma janela pop-up, oferecendo um celular de maneira gratuita.

Vale ressaltar que essa questão, deu três opções múltiplas escolhas, sendo elas: clicar na opção “open”, clicar na opção “remove ads” e fechar a janela com o atalho “alt+f4”, sendo está última opção a adequada, tendo em vista que até mesmo o botão “remove ads” pode ser um código malicioso. E, além das 3 opções fechadas, a questão 5 deixou uma opção de resposta livre para que fosse preenchida alguma outra atitude que o oficial aluno adotaria diante da referida situação apresentada, conforme apresentado na figura 6 logo abaixo:

Figura 6 – Questão 5



Fonte: O autor

Por fim, na pergunta 6 buscou-se identificar se os oficiais alunos tinham o conhecimento adequado para identificar url's, aparentemente fraudulentos.

Cabe ressaltar que o LMS-1834 enfatiza que como método para se prevenir ataques através do seu navegador, a primeira coisa que se deve procurar ao navegar é se o site utiliza o https, a fim de garantir que a conexão com os sites seja protegida para reduzir a ameaça de um invasor captar seu nome de usuário e senha, já que eles costumam manipular as url's para que pareçam sites confiáveis, expondo assim, os usuários ao seu conteúdo malicioso.

Portanto, na pergunta 6 foram apresentados 10 url's, aparentemente fraudulentos, sendo solicitado aos oficiais alunos que marcassem aqueles que eles julgassem se tratar de endereços não confiáveis, tendo esse resultado conforme exposto no quadro abaixo:

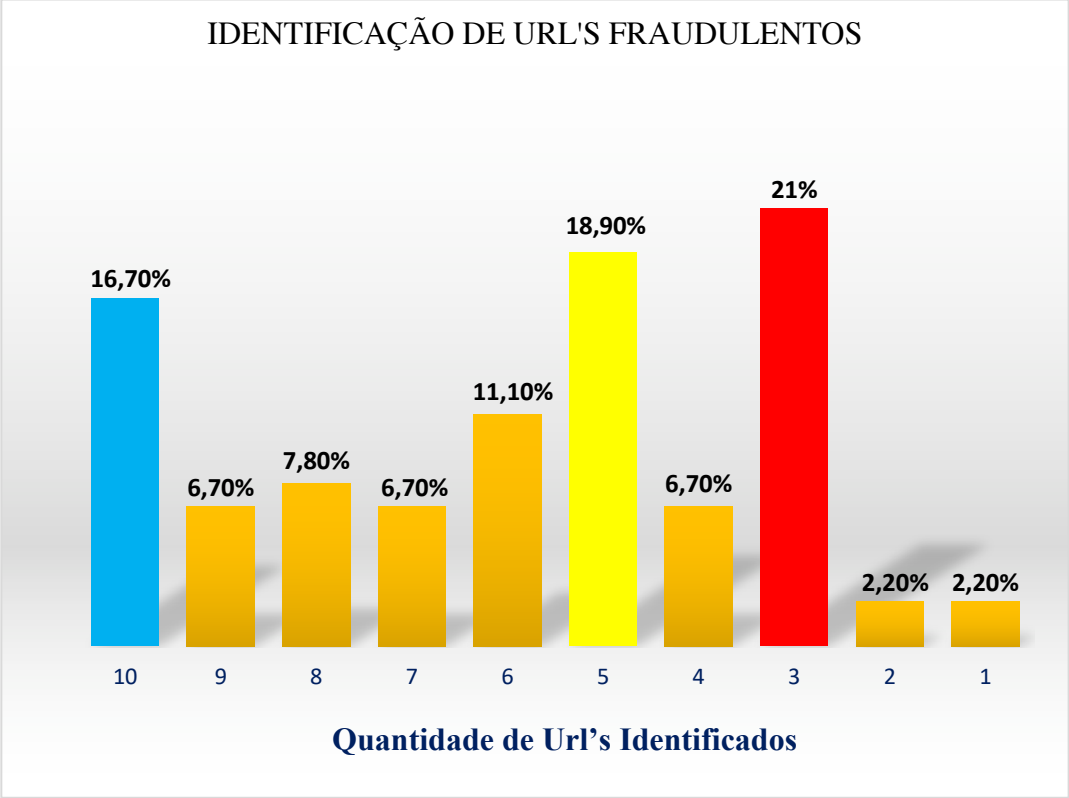
Quadro 6 – Questão 6

CARACTERÍSTICA DO URL	URL UTILIZADO	% DE ACERTOS
Reduzido e sem https	http://tinyurl.com/gh554632hfqz	84,4%
Só com números e sem https	http://205.62.12.90	75,6%
Site da aeronáutica sem a extensão mil.br e sem https	http://www.fab-ecemar.com	72,2%
	http://www.contracheque.fab-login.com	70%
Site de banco sem a extensão .br e sem https	http://www.bancodobrasil.com	62,2%
Site com erro de digitação e sem https	http://www.rnicrosoft.com	61,1%
Site do governo com a extensão .org e sem https	http://www.senado.org	47,8%
	http://www.funai.org	44,4%
Site sem https	http://www.cnnbrasil.com	38,9%
Site com hífen e sem https	http://www.turnitin-login.com	36,7%

Fonte: O autor

Ainda com base na questão 6, verificou-se que apenas 16,7% dos oficiais alunos foram capazes de identificar todos os 10 url's como aparentemente fraudulentos. Além disso, 18,9% deles reconheceram 5 url's e a maioria deles (21%) conseguiram detectar somente 3 url's, conforme disposto na figura abaixo:

Figura 7 – Questão 6



Fonte: O autor

Considerando os resultados apresentados até agora, inferiu-se que os maiores níveis de conscientização de SI dos oficiais alunos estão nos seguintes temas: seleção e uso de senhas, identificação de sinais de alerta em e-mails de phishing e postura a ser adotada perante um janela pop-up utilizada com prática de phishing.

Quadro 7 – Temas com os níveis mais elevados de conscientização de SI

TEMA	CONTEÚDO ANALISADO	GRAU
Seleção e uso de senha	Senha que atende aos critérios qualitativos da NSCA 7-13	70%
	Senha que atende aos critérios quantitativos da NSCA 7-13	82,2%
Mensagens eletrônicas e phishing	Identificação de sinais de alerta em e-mails de phishing	84,4%
	Postura adotada perante um janela pop-up utilizada em prática de phishing	77,6%

Fonte: O autor

No entanto, no que tange à identificação de url's fraudulentos, prática comumente utilizado por criminosos para transmitirem códigos maliciosos, os níveis de conscientização caem de maneira considerável.

Entretanto, se for considerar apenas as respostas dos oficiais alunos que leram a Cartilha de Segurança da Internet, o grau de conscientização em SI atinge patamares mais elevados, conforme mostra o quadro a seguir:

Quadro 8 - Identificação de url's fraudulentos

TEMA	CONTEÚDO ANALISADO	NÚMERO DE URL IDENTIFICADO	GRAU GERAL	GRAU SOMENTE DOS OFICIAIS QUE LERAM A CARTILHA
Mensagens eletrônicas e phishing	Identificação de url's fraudulentos	10 url's	16,7%	75%
		9 url's	6,7%	15%

Fonte: O autor

Por meio do quadro 5, verificou-se que 75% dos oficiais alunos, que tomaram conhecimento da Cartilha de Segurança da Internet, foram capazes de identificar todas as 10 url's com indícios de phishing e os outros 15% conseguiram identificar 9 das 10 url's apresentadas na questão 6.

No entanto, conforme já visto na figura 1, apenas 28% dos militares que responderam o questionário leram todo o conteúdo da Cartilha de Segurança da Internet e, além disso, 68% deles sequer tinham conhecimento da existência desse documento, cuja leitura é apresentada como competência inerente a todo usuário dos sistemas de TI, conforme NSCA 7-13.

5 CONCLUSÃO

A FAB apresentou em 2018 um programa de reestruturação, priorizando a redução do efetivo e a modernização da gestão de recursos humanos. O programa ficou conhecido pelo nome "Concepção Estratégica Força Aérea 100" e focou na melhoria das estruturas componentes do Poder Aeroespacial.

Conforme visto no presente trabalho, o COMAER definiu, na concepção estratégica Força Aérea 100, a obtenção da Superioridade de Informações como uma das características para o alcance da sua visão de futuro para o ano de 2041.

Entretanto, o aumento no número de crimes cibernéticos, ocorrido durante a pandemia do COVID-19, elevou o nível de exposição e de vulnerabilidade das organizações militares, surgindo a necessidade de uma mentalidade de Segurança da Informação forte o suficiente para que seja uma linha de defesa na proteção dos ativos informacionais.

O presente trabalho, na sua primeira fase, por meio de uma pesquisa bibliográfica, identificou as principais recomendações de Segurança da Informação tanto do Curso Básico de Conscientização sobre Segurança da Informação (LMS-1834), ministrado pela ONU, quanto da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13), identificando um grau de compatibilidade entre eles de 66,67%, sem levar em conta a leitura da Cartilha de Segurança da Informação, exigência da NSCA 7-13, e um grau de 95,24%, considerando a leitura dessa Cartilha.

Além disso, foram levantados os temas que continham as principais recomendações de SI, identificando as seguintes áreas como essenciais, com base nos módulos do LMS-1834, sendo eles: engenharia social; seleção e uso de senha; mensagens eletrônicas e phishing e acessando informações na internet.

Então, passou-se para a segunda fase do trabalho, utilizando-se de um questionário aplicado aos oficiais alunos do CACEM-2022, abrangendo esses módulos principais, com exceção do tema engenharia social, por se tratar de um assunto que não se resume apenas ao âmbito da internet, sendo abordado de maneira completa nos Folhetos do Comando da Aeronáutica FCA 200-2 e FCA 200-3.

Com isso, tendo como norte o objetivo geral de analisar em que medida o nível de conscientização de SI dos usuários dos sistemas de TI atendiam às exigências que a ONU estabelece a seus usuários, foram encontrados níveis adequados na maioria dos assuntos analisados:

a) 70% com senhas dentro dos critérios qualitativos da NSCA 7-13;

b) 82,2% com senhas dentro dos critérios quantitativos da NSCA 7-13;

c) 84,4% identificaram os sinais de alerta em e-mails de phishing; e

d) 77,6% adotaram a postura adequada diante de uma janela pop-up utilizada em prática de phishing.

No entanto, em relação à identificação de url’s com aparência de endereços não confiáveis, após apresentar 10 url’s aparentemente fraudulentos, apenas 16,7% foram capazes de reconhecer todos os 10 url’s apresentados como aparentemente fraudulentos e somente 6,7% conseguiram reconhecer 9 url’s, corroborando com a compreensão de Puhakainen e Sinopen (2010), ao esclarecer que os colaboradores que não cumprem as recomendações da política de segurança da informação passam a ser um risco elevado para suas instituições.

Além disso, confirmando o entendimento de SINOPEN (2000), ao elucidar que a SI tem associação direta com a Conscientização de Segurança da Informação, a medida em que os usuários dos sistemas de TI passam a ter uma compreensão maior acerca da importância do

papel da SI para a sua instituição, ao analisar a identificação de url's com aparência de endereços não confiáveis, somente dos oficiais alunos que cumpriram a exigência de leitura da Cartilha de Segurança da Internet, estipulada na NSCA 7-13, obteve-se que 75% deles foram capazes de identificar todos os 10 url's como aparentemente fraudulentos e os outros 15% reconheceram 9 url's dos 10 apresentados.

Dessa forma evidenciou-se a teoria de Puhakainen e Sinopen (2010), ao defenderem a ênfase nos procedimentos de segurança, com a finalidade de compreender a gravidade oriundas de um descumprimento das orientações de SI, já que a Cartilha de Segurança da Internet é um instrumento que tem como objetivo ressaltar a adoção de comportamentos mais seguros.

Portanto, a presente pesquisa mostrou que a NSCA 7-13, se respeitada a exigência da leitura da Cartilha de Segurança da Internet, tem um grau de compatibilidade elevado em relação ao LMS-1834 da ONU (95,24%) e que essa simples recomendação de leitura é capaz elevar a quantidade de militares capazes de identificarem url's fraudulentos de 16,7% para 75%, sendo um subsídio para a garantia da Superioridade de Informações, característica almejada na concepção estratégica Força Aérea 100.

A importância da pesquisa é evidenciada com base nos esclarecimentos de Puhakainen e Siponen (2010) ao enfatizarem que o não cumprimento de regras de SI contribui para o surgimento de brechas na proteção de dados, sendo fundamental o desenvolvimento de um estado de conscientização na cultura organizacional de qualquer empresa. Tal entendimento foi confirmado com o presente trabalho ao verificar que o grupo de oficiais que haviam lido o conteúdo da Cartilha de Segurança da Internet e, portanto, tinham um nível de conscientização mais elevado que os demais, apresentaram um resultado maior em relação à identificação dos url's com aparência de fraudulentos.

Além disso, como sugestão em pesquisas futuras fica a proposta de, por meio de especialistas, fazer o levantamento das competências essenciais no que tange à SI e compará-las com as desenvolvidas nas escolas de formação da FAB.

REFERÊNCIAS

ABNT, **NBR ISO/IEC 27001**- Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de Segurança da Informação – Requisitos. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

ABNT, **NBR ISO/IEC 27002** - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. **NSCA 7-13: Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica**. Rio de Janeiro, 2013.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. **PCA 7-15: Plano de Implantação da Segurança da Informação no Comando da Aeronáutica**. Rio de Janeiro, 2013.

BRASIL. Comando da Aeronáutica. Estado-Maior. **DCA 11-45: Concepção Estratégica, Força Aérea 100**. Brasília, 2018.

BRASIL. Comando da Aeronáutica. Estado-Maior. **DCA 14-8: Política de Segurança da Informação do Comando da Aeronáutica**. Brasília, 2018.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

MITNICK, Kevin D.; SIMON, William L. Mitnick – **A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Makron Books, 2003.

SIPONEN, M. T. **A conceptual foundation for organizational information security Information Management & Computer Security**, v. 8, n. 1, p. 31-41, UNDSS. Information Security Awareness Foudational. Disponível em: <https://training.dss.un.org/thematicarea/detail?id=19956>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution A/RES/66/246**, de 29 de fevereiro de 2012. Disponível em < https://undocs.org/A/RES/66/246>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution A/67/651**, de 19 de dezembro de 2012. Disponível em < https://undocs.org/A/67/651>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution A/67/651/Add.1**, 16 de janeiro de 2013. Disponível em < https://undocs.org/A/67/651/Add.1>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution A/68/552**, 25 de outubro de 2013. Disponível em <http://undocs.org/A/68/552>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution A/RES/68/247**, 27 de dezembro de 2013. Disponível em <https://undocs.org/A/RES/68/247>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution ST/SGB/2004/15**, 29 de novembro de 2004. Disponível em <https://undocs.org/ST/SGB/2004/15>. Acesso em: 26 fev. 2022.

UN GENERAL ASSEMBLY. **Resolution ST/SGB/2007/6**, 12 de fevereiro de 2007. Disponível em <https://undocs.org/ST/SGB/2007/6>. Acesso em: 26 fev. 2022.

WILLIAMS, P. A. **Information Security Governance. Information Security Technical Report**, Vol. 6, no. 3 pp. 60-70, 2001.

APÊNDICE A – Curso Básico de Segurança da Informação (LMS-1834)

Quadro 2- Curso Básico de Segurança da Informação (LMS-1834)

TEMA	ASSUNTO
Introdução à Segurança da Informação	Origem e importância da Segurança da Informação
	Definição de Segurança da Informação
	Responsabilidades dos usuários de TI conforme os boletins do Secretário Geral ST/SGB/2004/15 e ST/SGB/2007/6
Protegendo informações sensíveis	O que é proteção de informações sensíveis
	Principais ameaças aos dados classificados
	Compreender a importância da classificação de dados conforme o boletim nº st/sgb/2007/6
Engenharia social	O que é engenharia social e quais são suas ameaças
	Identificação dos métodos e táticas mais comuns da engenharia social
	Formas de mitigação dos riscos
Seleção e uso de senha	Principais características de senhas fortes
	Como criar senhas fortes
	Melhores práticas para a segurança das senhas
Mensagens eletrônicas e phishing	Riscos associados às mensagens eletrônicas
	Identificação de Url's fraudulentos e anexos com códigos maliciosos
	Uso de mensagens protegidas e exclusão segura de informações
Acessando informações na internet	A importância de navegar com segurança na internet
	Os perigos potenciais de navegadores, url's e sites
	Responsabilidades dos usuários de TI em relação à navegação segura
Respondendo a incidentes	Evento ou incidente de segurança da informação
	Procedimentos para a primeira resposta ao suspeitar de um evento ou incidente de segurança da informação
	Processos para relatar ocorrências de segurança da informação

Fonte: O autor

APÊNDICE B – A Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13)

Quadro 3 – Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13)

TEMA	ASSUNTO
Introdução à Segurança da Informação	Origem e importância da Segurança da Informação
	Definição de Segurança da Informação
	Responsabilidades dos usuários de TI
Protegendo informações sensíveis	O que é proteção de informações sensíveis
	Principais ameaças aos dados classificados
	Compreender a importância da classificação de dados
Engenharia social	O que é engenharia social e quais são suas ameaças *****
	Identificação dos métodos e táticas mais comuns da engenharia social *
	Formas de mitigação dos riscos *****
Seleção e uso de senha	Principais características de senhas fortes
	Como criar senhas fortes
	Melhores práticas para a segurança das senhas
Mensagens eletrônicas e phishing	Riscos associados às mensagens eletrônicas *****
	prevenção, detecção e erradicação de vírus, contaminações e códigos maliciosos
	Uso de mensagens protegidas e exclusão segura de informações *
Acessando informações na internet	A importância de navegar com segurança na internet
	Os perigos potenciais de navegadores, url's e sites *
	Responsabilidades dos usuários de TI em relação à navegação segura
Respondendo a incidentes	Evento ou incidente de segurança da informação
	Procedimentos para a primeira resposta ao suspeitar de um evento ou incidente de segurança da informação
	Processos para relatar ocorrências de segurança da informação
*** Conteúdo presente na Cartilha de Segurança para Internet**	

Fonte: O autor

APÊNDICE C – Questionário

A Segurança da Informação na FAB: uma visão sob a ótica da ONU

Prezado(a) colaborador(a),

Este questionário é um instrumento de coleta de dados para a realização de uma pesquisa científica, que servirá de subsídio para a elaboração de artigo, a ser apresentada à Escola de Comando e Estado-Maior da Aeronáutica, como requisito de conclusão do Curso de Comando e Estado-Maior.

O objetivo do questionário é analisar o nível de conscientização dos usuários dos sistemas de TI da FAB tendo como parâmetro a Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13) e as exigências que a ONU estabelece aos seus colaboradores, por meio do Curso Básico de Segurança da Informação (LMS-1834)

Todos os dados e opiniões emitidos serão analisados, mas apenas as conclusões serão expostas no corpo do trabalho.

Desde já agradeço a colaboração.
Paulo Cesar Fialho de Souza Junior, Ten Cel Av

QUESTÃO 1

Alguma vez você já leu todo o conteúdo da cartilha de segurança, disponível no site www.cert.br?

( ) Sim ( ) Não e nem nunca tinha ouvido falar dela ( ) Não

QUESTÃO 2

Marque abaixo todos os critérios atendidos pela senha que você utiliza para fazer o login no computador do seu trabalho (pode marcar quantas opções desejar):

( ) Possui números

( ) Contém nomes ou sobrenomes

( ) Contém palavras que fazem parte de dicionários ou de listas publicamente conhecidas, tais como: nomes de músicas, nomes de filmes, times de futebol, personagens de filmes e dicionários de diferentes idiomas

( ) Contém alguns dos seguintes itens: números de documentos, placa de carros, números de telefones ou datas
Possui letras maiúsculas e minúsculas

( ) Possui sinais de pontuação ou símbolos

QUESTÃO 3

Marque abaixo o valor que corresponde o número de caracteres que possui a senha que você utiliza para fazer o login no computador do seu trabalho:

( ) Possui até 07 caracteres

( ) Possui de 08 a 11 caracteres

( ) Possui de 12 a 13 caracteres

( ) Possui 14 ou mais caracteres

QUESTÃO 4

( ) QUAL DAS OPÇÕES ABAIXO É UM SINAL DE ALERTA DE E-MAIL DE PHISHING?

( ) ERRO GRAMATICAL NO CORPO DO E-MAIL

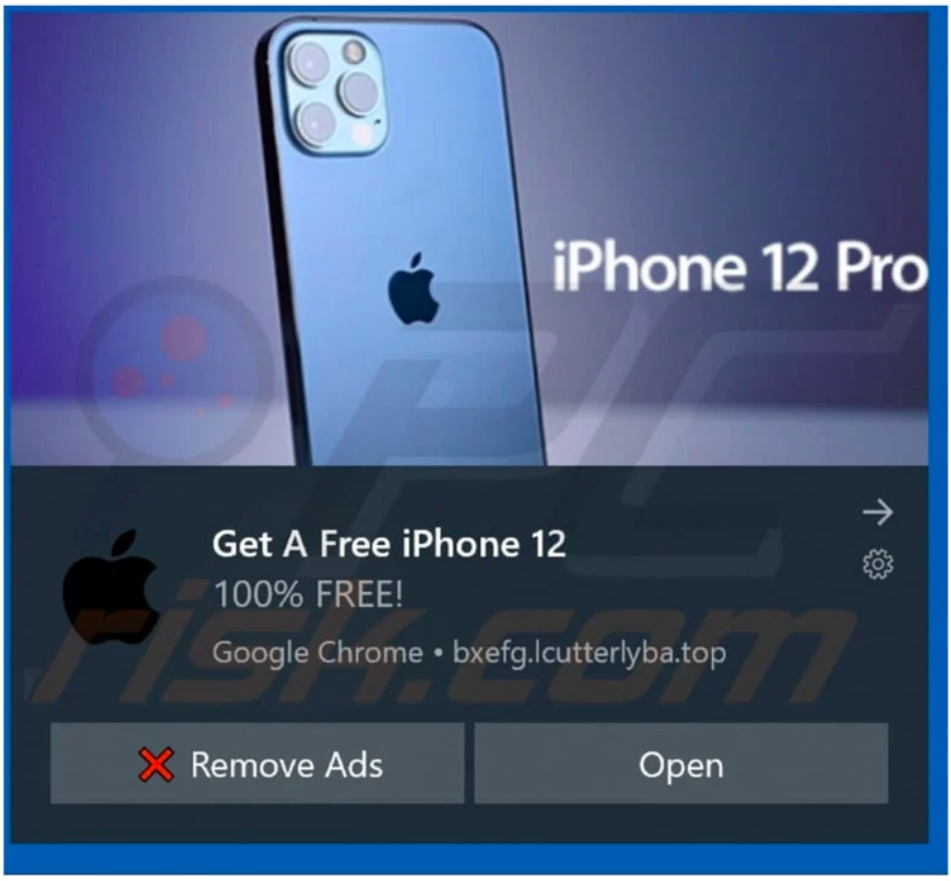
( ) LINK PARA UM E-MAIL DESCONHECIDO OU ENDEREÇO NÃO CONFIRMADO

( ) ANEXO ESTRANHO

( ) TODAS AS ANTERIORES

QUESTÃO 5

Se ao navegar na internet você se deparar com a seguinte janela pop-up, qual atitude você costuma adotar? (responda com base no comportamento que adota habitualmente).



( ) Clicaria na opção "open"

( ) Clicaria na opção "remove ads"

( ) Fecharia a janela com o atalho "alt+f4"

( ) Adotaria outra postura

QUESTÃO 6

Marque as url's abaixo que você acredita que, aparentemente, referem-se a endereços não confiáveis (pode marcar quantas opções desejar):

( ) http://www.senado.org

( ) http://tinyurl.com/gh554632hfqz

( ) http://205.62.12.90

( ) http://www.contracheque.fab-login.com

( ) http://www.turnitin-login.com

( ) http://www.rnicrosoft.com

( ) http://www.fab-ecemar.com

( ) http://www.bancodobrasil.com

( ) http://www.cnnbrasil.com

( ) http://www.funai.org