ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2023

FILIPE DE **PAULO** OLIVEIRA, Cap Av

A educação em Segurança Cibernética na EEAR à luz do Gerenciamento de Risco

Rio de Janeiro

2023

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2023

FILIPE DE **PAULO** OLIVEIRA, Cap Av

A educação em Segurança Cibernética na EEAR à luz do Gerenciamento de Risco

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Guerra Cibernética
Orientador: Wellington Azevedo dos Santos, Maj Inf

Rio de Janeiro
2023

FILIPE DE **PAULO** OLIVEIRA, Cap Av

A educação em Segurança Cibernética na EEAR à luz do Gerenciamento de Risco

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Wellington Azevedo dos Santos, Maj Inf
EAOAR

_____

Robertha Lima Souza da Silva, Cap Av
EAOAR

Rio de Janeiro

2023

RESUMO

O novo cenário estratégico do Setor Cibernético indicou que o Brasil precisa atentar-se ao ensino de Segurança Cibernética dos seus graduados especialistas, uma vez que pesquisas relataram o alto grau de analfabetismo digital dos brasileiros. Por esse motivo, este ensaio defende a tese que a implantação de um programa de alfabetização digital na EEAR reduzirá o risco cibernético e produzirá um ganho operacional para a FAB. Primeiramente, argumenta-se que a educação digital reduz a probabilidade de incidentes, pois uma tropa bem adestrada evitará expor-se às vulnerabilidades, dificultará a exploração e o ataque cibernético e reduzirá as ações de engenharia social. Em segundo lugar, o impacto nos meios de Comando e Controle (C^2) serão minimizados caso o ataque se concretize, uma vez que os reportes aumentarão, assim, a detecção acontecerá mais cedo e as respostas ocorrerão mais rapidamente. Assim sendo, a conscientização do aluno da EEAR permitirá reduzir a probabilidade de um ataque, além de motivá-lo a adotar uma postura proativa, ambas visando aumentar a operacionalidade da FAB através da maior proteção dos meios de C^2. Os benefícios da Educação em Segurança Cibernética citados neste ensaio não se limitam apenas à EEAR, mas podem ser aproveitados para todas as unidades que atuam com o ingresso de novos militares, temporários ou de carreira, e com a educação continuada do efetivo. Assim, contribuirá para uma Força Aérea com maior capacidade de Segurança e Defesa do ciberespaço e maior operacionalidade, por meio da maior segurança dos sistemas de C^2.

Palavras-chave: Consciência Cibernética. Ataque Cibernético. Comando e Controle. Risco Cibernético. Operacionalidade.

1 **INTRODUÇÃO**

Em 2008, a Estratégia Nacional de Defesa (END) definiu, pela primeira vez no Brasil, o Setor Cibernético como estratégico para o Estado, visto que a informação se tornou um ativo de elevado valor, pois afeta diretamente a soberania nacional. Diante do cenário apresentado, diversos documentos no país foram atualizados, outros redigidos e assinados, tais como a Doutrina Militar de Defesa Cibernética e a Estratégia Nacional de Defesa Cibernética (E-Ciber), a qual apresentou resultados de pesquisas que indicaram índices alarmantes de analfabetismo digital da população brasileira.

Na Força Aérea, especificamente na Escola de Especialistas de Aeronáutica (EEAR), a situação não é diferente. Apesar de já existirem duas disciplinas que abordam o tema Guerra Cibernética, quais sejam, Publicações do Ministério da Defesa (PMD) e Inteligência Cibernética (INTEL III), o conteúdo é pequeno para desenvolver nos alunos uma consciência cibernética adequada. Nota-se que são apenas cinco tempos de aula em dois anos de formação (BRASIL, 2020).

Além disso, os Alunos da EEAR têm um grande potencial de gerar impactos positivos ou negativos na Segurança Cibernética da FAB após formados e distribuídos por todo o território nacional nas diversas Organizações Militares (OM). Isso ocorre, pois, de acordo com Rezende (2011), a EEAR forma cerca de 800 graduados especialistas por ano e, até o ano de 2009, formou quase 63 mil sargentos.

Nesse diapasão, este ensaio defende a tese que a implantação de um programa de alfabetização digital na EEAR reduzirá o risco cibernético e produzirá um ganho operacional para a FAB.

Primeiramente, argumenta-se que a educação digital reduz a probabilidade de incidentes, pois uma tropa bem adestrada evitará se expor às vulnerabilidades, dificultará a exploração e o ataque cibernético e reduzirá as ações de engenharia social.

Em segundo lugar, o impacto nos meios de Comando e Controle (C^2) serão minimizados caso o ataque se concretize, uma vez que os reportes aumentarão, assim, a detecção acontecerá mais cedo e as respostas ocorrerão mais rapidamente.

2 **DESENVOLVIMENTO**

Tendo em vista o elevado índice de analfabetismo digital da população brasileira, citado anteriormente, somado ao elevado contingente de especialistas na FAB, é necessária a Educação em Segurança Cibernética dos alunos na Escola de Formação.

Além disso, tem-se que o Risco Cibernético é a “probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado” (BRASIL, 2014, p. 19). Portanto, o Risco possui duas parcelas fundamentais, quais sejam, a probabilidade e o dano. Quando se reduz uma ou ambas as parcelas, o risco, por sua vez, também reduzirá. Reduzindo o risco, ocorrerá um ganho de operacionalidade, pois os meios de C² estarão mais seguros.

Nesse sentido, a educação em segurança cibernética, visa a redução da probabilidade de ataque e a diminuição do impacto (dano), de ataques sofridos.

2.1 **Diminuição da probabilidade como forma de aumentar a operacionalidade**

Inicialmente, é preciso considerar, que a redução da probabilidade de ocorrência de um incidente cibernético através da conscientização em segurança cibernética dos alunos da EEAR resultará em um aumento da operacionalidade.

Em primeiro lugar, uma tropa bem adestrada evitará se expor às vulnerabilidades. Pois, para Oliveira (2019) a realização de programas de conscientização para capacitar os usuários, sejam civis ou militares do COMAER é uma ação a ser desenvolvida no âmbito da FAB. Defende, também, que esses programas deveriam ser desenvolvidos em cursos de formação, pós-formação e carreira. Tendo em vista que a EEAR é uma escola de formação, o Programa de Educação Cibernética pode ser aplicado. Portanto, a educação dos alunos em segurança cibernética irá reduzir a vulnerabilidade, por isso, reduzirá o risco.

Essa redução da vulnerabilidade pode ser exemplificada por meio do ensino de Defesa Cibernética na AFA. Segundo Guin (2022), a disciplina contribuiu para reduzir as vulnerabilidades e diminuir a probabilidade de um ataque cibernético, apesar de carecer de melhorias. Da mesma maneira, na EEAR, a implementação de um Programa em defesa cibernética reduzirá as vulnerabilidades. Pois, quando observamos o Plano de Unidades Didáticas (PUD) do CFS e do EAGS, existe apenas a carga horária de cinco tempos para as disciplinas que abordam o tema (PMD e INTEL III). Assim, percebe-se que há necessidade da implementação de um Programa de Conscientização sólido e eficaz.

Em segundo lugar, a educação digital dificultará os principais tipos de ações cibernéticas, que são a exploração e o ataque. O CERT (2012, p. 18) define que “um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.”

À vista disso, Allison e Stepney (2023) vão afirmar que uma compreensão mais profunda de segurança cibernética ensinaria aos usuários que as políticas não podem ser violadas, bem como as interfaces não podem ser ignoradas. Isso dificultaria a exploração e o ataque.

Ou seja, ensinando aos alunos da EEAR acerca da importância de seguir as políticas de segurança por meio de um Programa de Conscientização, haverá uma significativa redução nos incidentes da FAB. Isso ocorrerá devido ao elevado número de sargentos formados na EEAR com um alto nível de consciência cibernética. Assim, os futuros graduados contribuirão com a segurança das OM que forem designados.

Por esse motivo, De Jesus (2020, p. 30) afirma “é imprescindível que a mentalidade de todos os integrantes da instituição se volte ao mesmo objetivo: diminuir as brechas de segurança ao menor nível possível”. Portanto, o programa de educação cibernética para os alunos da EEAR contribuirá para desenvolver a mentalidade de segurança da FAB, diminuindo as brechas. Logo, com menos ataques, os sistemas de C² permanecem mais seguros, o que aumenta a Operacionalidade da FAB.

Por fim, a conscientização reduz golpes de Engenharia Social. Segundo Ulven e Wangen (2021, p. 30), “‘Engenharia social e ataques direcionados’ são ataques projetados para explorar pontos fracos na conscientização e conhecimento de segurança. No entanto, esses ataques são comuns à maioria dos setores e indústrias”. Em sua pesquisa, relataram que cerca de 28% dos ataques, dentro da categoria mais genérica “todo o resto” (a qual representa 20% de todos os ataques), foram causados por *phishing*. De acordo com o CERT (2012, p. 9), *phishing* é “o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.”

A FAB, por sua vez, não está isenta desses golpes ou fraudes. Por exemplo, Guin (2022) realizou um teste de *phishing* na AFA e detectou que 17,3% dos cadetes abriram o e-mail, repassaram para outros cadetes e 92,4% responderam o formulário falso. Prosseguindo em seus estudos, também alertou que, a conscientização de

segurança dos discentes reduz a probabilidade de cair em golpes de engenharia social na FAB. Provavelmente, não seria diferente na EEAR, onde os alunos possuem faixa etária e origem similares e passam por processos seletivos semelhantes, além de possuírem pouco tempo de instrução dedicado à Segurança Cibernética.

Desse modo, conclui-se que um programa de alfabetização digital na EEAR reduzirá as vulnerabilidades, dificultará a exploração e o ataque cibernético e minimizará as ações de engenharia social. Assim, reduzirá o fator da probabilidade de serem alvos de um ciberataque após se formarem, contribuindo para aumentar a operacionalidade da FAB por meio da maior segurança dos sistemas de C².

2.2 **Diminuição do Impacto como forma de aumentar a operacionalidade**

O impacto é o segundo componente da equação do risco. E como tal, quanto menor for o impacto, menor será o risco. Nesse sentido, a consciência cibernética é um fator contribuinte para a redução desse impacto, à medida que proporciona maiores reportes, detecções e correções mais rápidas. Tais medidas reduzirão a propagação do ataque cibernético, quando ele for bem-sucedido. Machado (2023) relata como as falhas ou ataques cibernéticos podem causar danos diversos, desde administrativos, financeiros ou até estratégicos.

Inicialmente, observa-se que o aumento de reportes irá contribuir para reduzir o impacto. Isso ocorre devido ao “importante papel dos programas de segurança cibernética para motivar os usuários a adotar comportamentos proativos” (ZWILLING *et al*, 2022, p. 91, tradução nossa). Isso significa que uma postura proativa, desenvolvida nos alunos, será caracterizada pela percepção de possíveis ataques e o devido reporte. Por esse motivo, a NSCA 7-13: Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica determina que:

> qualquer mau funcionamento de um sistema deverá ser imediatamente reportado à Equipe de TI da OM, pois a demora neste ato poderá levar a sérios danos aos sistemas, e até mesmo à indisponibilidade dos Recursos Computacionais envolvidos (BRASIL, 2022, p. 36).

Portanto, um programa de educação digital na EEAR alcançará grande parcela da FAB, em razão do número elevado de militares formados todos os anos. Os futuros sargentos precisam ter uma consciência cibernética elevada, a fim de contribuírem ativamente com o aumento de reportes de incidentes de segurança, ao mesmo tempo que reduz o impacto de um possível ataque nos meios de C².

Ao elevar o número de reportes, será possível acelerar a detecção e a correção de falhas ou ataques. Nesse sentido, a FAB adota o modelo de tratamento de incidentes cibernéticos através do Centro de Tratamento de Incidente de Segurança de Redes (CTIR.FAB). Esse centro “é o responsável pelo tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança” (BRASIL, 2022, p. 21). Ou seja, a elevada consciência cibernética dos futuros sargentos especialistas fornecerá mais reportes de incidentes de segurança para o CTIR.FAB, que os recebe através dos elos de TI.

Além disso, o tratamento de incidentes pode ser dividido “em duas atividades, a saber: a identificação de ameaças ou vulnerabilidades e a sua respectiva correção” (MAGALHÃES, 2012 *apud* DIAS, 2020, p. 8). Assim sendo, quanto mais cedo um incidente for reportado e identificado, o CTIR.FAB poderá agir no tratamento mais rapidamente. Nesse sentido, Souza Neto (2016) alerta sobre a importância da detecção de um ataque cibernético e as consequências catastróficas que ele pode ocasionar. No caso da EEAR, os Sargentos especialistas em Sistemas de Informações (SIN) serão os responsáveis por detectar esses ataques. Portanto, a conscientização é fundamental para acelerar o processo de detecção e diminuir o impacto.

Por fim, a correção é o último fator de tratamento de incidentes que deve ser acelerado. Conforme Oliveira e Silva (2011, p. 11) incidentes “podem afetar negativamente o negócio da empresa, causando danos, prejuízos ou repercussões, no mínimo indesejáveis”, por conseguinte, devem ser corrigidos com a maior brevidade possível.

No âmbito da FAB, os sistemas de C² são formados por sistemas de TI e as consequências podem ser devastadoras, caso um atacante obtenha sucesso (COIMBRA, 2009). Por isso, os graduados especialistas precisam adotar comportamentos de segurança cibernética advindos da conscientização, a fim de acelerar a implementação de correções essenciais após um incidente. Isso se faz necessário, pois os especialistas são grandes operadores dos diversos sistemas de C², os quais a FAB utiliza tanto para suporte à decisão, quanto para o cumprimento de missões operacionais.

Diante do exposto, a educação em Segurança Cibernética na EEAR aumentará o número de reportes, acelerará as detecções e correções, o que trará menos impacto em caso de incidentes e aumentará a operacionalidade.

3 **CONCLUSÃO**

Diante da nova realidade Estratégica do Setor Cibernético, pesquisas indicaram índices alarmantes de analfabetismo digital no Brasil. Por isso, a formação em Segurança Cibernética dos graduados especialistas merece atenção, uma vez que representam uma parcela bastante significativa do efetivo da FAB.

Assim sendo, este ensaio defendeu a tese que a implantação de um programa de alfabetização digital na EEAR reduzirá o risco cibernético e produzirá um ganho operacional para a FAB.

Para tanto, argumentou-se que a probabilidade de ocorrer um ataque é o primeiro fator a ser avaliado no gerenciamento de risco cibernético. Como tal, é mister que a FAB consiga reduzi-lo. Nesse contexto, três ações precisam ser consideradas como forma de mitigar o risco. São elas: reduzir vulnerabilidades, dificultar a exploração e ataque e reduzir os golpes de Engenharia Social. Dessa maneira, a conscientização cibernética é peça fundamental para reduzir a probabilidade de um ataque.

Argumentou-se, também, que o segundo fator relativo ao gerenciamento do risco é o impacto, o qual necessita ser reduzido. Assim sendo, existem três processos que contribuem para a redução dos impactos causados pelo incidente e que estão diretamente ligados um ao outro: reporte do incidente, detecção da falha e correção. Isso significa que, ao conscientizar o graduado formado na EEAR, ele adotará uma postura proativa e aumentará o número de reportes, contribuindo para aumentar a velocidade de detecção e, consequentemente, a correção.

Uma vez que o Programa desenvolvido na EEAR seja implantado, a FAB alcançará níveis elevados de pronta-resposta e segurança no ambiente cibernético. Além disso, devido à grande dispersão dos graduados recém-formados, o conhecimento adquirido será multiplicado por diversas unidades no país.

Ademais, os benefícios da Educação em Segurança Cibernética citados neste ensaio não se limitam apenas à EEAR, mas podem ser aproveitados para todas as unidades que atuam com o ingresso de novos militares, temporários ou de carreira, e com a educação continuada do efetivo. Assim, contribuirá para uma Força Aérea com maior capacidade de Segurança e Defesa do ciberespaço e maior operacionalidade, por meio da maior segurança dos sistemas de C².

REFERÊNCIAS

ALLISON, J; STEPNEY, O. **Cyber Security in English Secondary Education Curricula**: A Preliminary Study. 2023.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria COMGAP nº 42/ADLG, DE 2 de maio de 2022. Aprova a reedição da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n° 081, f. 5930, 03 maio 2022.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Escola de Especialistas de Aeronáutica. Portaria EEAR N° 33/SDGE, 20 de fevereiro de 2020. Aprova a reedição do “Plano de Unidades Didáticas do Campo Militar do Curso de Formação de Sargentos, para as turmas com ingresso a partir do ano de 2021. **Boletim Interno da EEAR**, Guaratinguetá.

BRASIL. Ministério da Defesa. **MD31-M-07. Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

CERT.BR. Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para Internet, versão 4.0**. São Paulo, 2012. Disponível em: https://cartilha.cert.br/livro/. Acesso em 21 jun. 2023.

COIMBRA, D. S. **A influência das atividades da guerra cibernética em um sistema de comando e controle**. 2009. 58 f. Trabalho de Conclusão de Curso (Curso de Comando e Estado-Maior)-Escola de Comando e Estado-Maior da Aeronáutica, Universidade da Força Aérea, Rio de Janeiro, 2009., Rio de Janeiro. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=9498. Acesso em: 12 jul. 2023.

DE JESUS, L. F. **Análise dos benefícios da aplicação de testes de intrusão regulares nas redes de computadores locais da FAB**. 2020. 45 p. Pirassununga, SP. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=78054. Acesso em: 21 jun. 2023.

DIAS, T. G. **A identificação de Stakeholders e sua influência no tratamento de vulnerabilidades cibernéticas**. 2020. 11 p. Rio de Janeiro. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=76808. Acesso em: 12 jul. 2023.

GUIN, L. F. P. **A profundidade do ensino de cibernética na Academia da Força Aérea.** 2022. 23 p. Pirassununga, SP. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=89585. Acesso em: 21 jun. 2023.

MACHADO, Eduardo Martins. **Computação em nuvem**: Uma solução para a alta confiabilidade dos Sistemas de Tecnologia da Informação e Comunicação da FAB, mesmo em um contexto de Guerra. 2023. 1 recurso online (13 f.) Trabalho de

conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação de MBA em Liderança, 1/2023, Rio de Janeiro. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=90008. Acesso em: 12 jul. 2023.

OLIVEIRA, P. S. **A Segurança da Informação e Engenharia Social na FAB à Luz dos casos RSA, Sony Pictures e Ubiquiti**. 2019, 121 f. Dissertação (Mestrado em Ciências Aeroespaciais). Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea. Rio de Janeiro: Universidade da Força Aérea, 2019

OLIVEIRA E SILVA, A. DE. Engenharia social: o fator humano na segurança da informação. **Coleção Meira Mattos:** revista das ciências militares, n. 23, 8 nov. 2011.

SOUZA NETO, O. **A consciência situacional nas ações de defesa cibernética**. 2016. 26 f. Trabalho de Conclusão de Curso (Curso de Comando e Estado-Maior) - Escola de Comando e Estado-Maior da Aeronáutica, Universidade da Força Aérea, Rio de Janeiro, 2016., Rio de Janeiro. Disponível em: https://redebia.direns.aer.mil.br/index.php?codigo_sophia=10791. Acesso em: 12 jul. 2023.

REZENDE, J. M. S. **Escolha sua profissão.** Aerovisão, Brasília, p. 3-21, jan. 2011

ULVEN, J. B.; WANGEN, G. **A systematic review of cybersecurity risks in higher education.** Future Internet, v. 13, n. 2, p. 39, 2021.

ZWILLING, M. *et al*. **Cyber security awareness, knowledge and behavior**: A comparative study. Journal of Computer Information Systems, v. 62, n. 1, p. 82-97, 2022.