ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE POLÍTICA E ESTRATÉGIA AEROESPACIAIS

FERNANDO RODRIGUES **DE SÁ**, Cel Av

Cultura de segurança cibernética: uma estratégia para mitigação de vulnerabilidades

Rio de Janeiro
2025

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE POLÍTICA E ESTRATÉGIA AEROESPACIAIS

FERNANDO RODRIGUES **DE SÁ**, Cel Av

Cultura de segurança cibernética: uma estratégia para mitigação de vulnerabilidades

Trabalho de conclusão de curso apresentado à Escola de Comando e Estado-Maior da Aeronáutica como requisito parcial para aprovação no Curso de Política e Estratégia Aeroespaciais.

Orientador: Cel Int Leonardo Freitas de Souza Lima.

Rio de Janeiro
2025

1 INTRODUÇÃO

O objetivo primordial dos ataques militares é, em geral, neutralizar centros de gravidade, que são pontos dos quais derivam a força, a capacidade de luta e a vontade de lutar do inimigo (CLAUSEWITZ, 2002). A neutralização ou destruição desses centros pode levar ao colapso do oponente de forma mais eficiente que ataques a alvos aleatórios ou menos significativos.

Durante a segunda guerra mundial, o poder aéreo emergiu como um componente essencial para o sucesso das operações. Ataques massivos a alvos inimigos, realizados por grandes quantidades de bombardeiros, demonstravam um elevado poder de destruição.

Nas décadas seguintes, os vetores de combate evoluíram tecnologicamente. Essa evolução substituiu os ataques em massa pelo emprego de aeronaves modernas, furtivas a radares, capazes de navegar com precisão e realizar ataques cirúrgicos.

No cenário atual, uma força aérea contemporânea não se limita a possuir somente os vetores mais modernos. O sucesso do combate depende de modernos sistemas de Tecnologia da Informação (TI) para suporte à missão. A integração entre novos vetores e sistemas de TI os torna cada vez mais críticos, mudando o enfoque da guerra moderna.

A guerra contemporânea evoluiu com a incorporação do domínio cibernético, ou ciberespaço, que é o ambiente global interconectado da tecnologia da informação. Neste contexto, o objetivo de neutralizar centros de gravidade inimigos não está restrito a ataques com bombas ou mísseis. Degradar o sistema de comando e controle do oponente por meio de um ataque cibernético pode, potencialmente, ter um efeito maior que um combate cinético.

Uma característica desse domínio é que ele não se restringe a atores estatais, tampouco a tempos de guerra ou crise. Indivíduos, grupos e estados utilizam o ciberespaço com objetivos variados, seja para coletar informações, obter vantagens financeiras por meios ilícitos ou até mesmo degradar sistemas críticos de infraestrutura.

Como exemplo, um dos vetores de ataque cibernético mais comuns é o *phishing*, que consiste no envio de e-mails, mensagens de texto ou outros tipos de comunicações eletrônicas fraudulentas, a fim de cometer diversos tipos de crimes, incluindo o acesso não autorizado a sistemas. Este tipo de ataque explora a confiança e falta de atenção das pessoas, baseando-se na manipulação psicológica, o que o torna uma das ameaças mais eficazes.

Usuários sem uma mentalidade de segurança cibernética são mais propensos a este e outros tipos de ataque, por não reconhecerem adequadamente os sinais de alerta. Desta forma, este ensaio defende a tese de que a construção de uma cultura de segurança cibernética é uma

estratégia efetiva para a mitigação de vulnerabilidades, frente às ameaças contemporâneas do domínio cibernético.

Para sustentação da tese, serão apresentados dois argumentos. O primeiro baseia-se no desenvolvimento da mentalidade de segurança, como forma de combater ameaças cibernéticas por meio da mitigação de vulnerabilidades causadas por usuários de sistemas de TI.

O segundo argumento é que o fator humano permanece como o elo mais vulnerável da cadeia de proteção, apesar dos avanços tecnológicos em cibersegurança. Conforme evidenciado no exemplo do ataque de *phishing*, as defesas tecnológicas, por mais robustas que sejam, podem ser contornadas pela exploração da psicologia humana e pela falta de discernimento dos usuários. Assim, a efetividade das estratégias de segurança cibernética está intrinsecamente ligada à mitigação dos riscos comportamentais, uma vez que a falha humana pode comprometer gravemente a integridade dos sistemas.

Desta forma, faz-se mister que a Força Aérea Brasileira adote estratégias adequadas para a mitigação de vulnerabilidades cibernéticas, em tempos de paz e de conflitos, de forma a garantir o cumprimento de sua missão institucional, combatendo de maneira efetiva as ameaças cibernéticas modernas.

2 DESENVOLVIMENTO

2.1 CONSTRUÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Cultura organizacional é o conjunto de pressupostos compartilhados que um grupo desenvolve ao longo do tempo para lidar com seus desafios. Transferindo esse conceito para o ambiente da segurança cibernética, é necessário estabelecer valores e rotinas que promovam a responsabilidade com os ativos digitais (SCHEIN, 2010).

A construção da cultura de segurança cibernética é pilar fundamental na mitigação de vulnerabilidades no ambiente digital. Esta cultura, para ser efetiva, necessita estar enraizada na mentalidade dos usuários dos sistemas de Tecnologia da Informação (TI), principalmente em instituições críticas como a Força Aérea Brasileira.

Desta forma, conforme apresentado no capítulo anterior, o primeiro argumento para fundamentação da tese proposta no presente ensaio, é o desenvolvimento da mentalidade de segurança, apresentado a seguir.

2.2 DESENVOLVIMENTO DA MENTALIDADE DE SEGURANÇA

Construir uma cultura de segurança exige mais do que simples normatizações ou legislações. De acordo com o *National Institute of Standards and Technology* (NIST), uma das principais referências mundiais em políticas de cibersegurança, a cultura de segurança deve ser incorporada à organização por meio da liderança exemplar, comunicação clara e políticas acessíveis e compreensíveis (NIST, 2023). Quando há desalinhamento entre os valores institucionais e o comportamento dos usuários, as estratégias de segurança tornam-se frágeis, mesmo que tecnicamente bem projetadas. Portanto, o desenvolvimento de uma mentalidade de segurança cibernética sólida transcende a técnica, pois exige transformação comportamental e institucional.

A educação e o treinamento contínuo são ferramentas indispensáveis. Fatores humanos como credenciais comprometidas e erros de configuração continuam entre as principais causas de violações de dados (IBM SECURITY, 2024). A adoção de boas práticas de segurança e programas de conscientização contribui para a redução do tempo de resposta e do impacto financeiro dos incidentes.

O desenvolvimento da mentalidade de segurança, portanto, não se dá por imposição normativa, mas pela internalização de valores que reforcem comportamentos seguros. Essa mentalidade é o alicerce da cultura de segurança cibernética, e sua consolidação é essencial para o êxito de qualquer estratégia de mitigação de vulnerabilidades. Porém,

independentemente da estratégia adotada, o fator humano permanece como o elo mais vulnerável da cadeia de proteção, conforme será aprofundado na próxima seção.

2.3 O FATOR HUMANO COMO ELO MAIS VULNERÁVEL

Apesar do avanço de sofisticadas soluções tecnológicas de cibersegurança, o fator humano ainda representa o elo mais vulnerável das cadeias de proteção. A engenharia social continua sendo uma das ferramentas mais exploradas por agentes mal-intencionados. O caso da invasão à conta oficial do Comando Central das Forças Armadas dos Estados Unidos, em 2015, ilustra essa realidade: o ataque foi viabilizado após um funcionário ser enganado por um e-mail de *phishing*. Situação semelhante ocorreu no Brasil, em 2020, quando o Superior Tribunal de Justiça (STJ) teve seus sistemas comprometidos pela propagação de e-mails contendo um *ransomware*, tipo de atividade maliciosa que impede o acesso a arquivos ou sistemas, geralmente criptografando-os, e exige um resgate para restaurar o acesso. Cerca de 74% das violações de dados envolvem algum tipo de elemento humano, seja por erro acidental, uso indevido de privilégios, credenciais comprometidas ou ataques de engenharia social (VERIZON ENTERPRISE, 2023). Esses episódios demonstram que, mesmo em instituições altamente protegidas, as vulnerabilidades cognitivas dos usuários ainda são portas de entrada relevantes para ataques cibernéticos.

Frente a esse cenário, torna-se urgente a adoção de medidas voltadas à mitigação dos riscos comportamentais. Estudos independentes indicam que organizações que implementam programas de conscientização interativos podem reduzir em até 60% os incidentes de segurança relacionados ao comportamento humano (PROOFPOINT, 2024). Dessa forma, é possível não apenas desenvolver habilidades técnicas, mas também promover mudanças de atitude. Mitigar riscos comportamentais é, portanto, uma medida essencial para fortalecer a resiliência institucional diante das ameaças cibernéticas contemporâneas.

2.4 UMA ESTRATÉGIA PARA MITIGAÇÃO DE VULNERABILIDADES

A construção de uma cultura de segurança cibernética sólida é um processo estratégico e contínuo que envolve mudanças no comportamento organizacional, na comunicação interna e na formação de valores institucionais. Ao reconhecer que as falhas humanas representam um dos principais vetores de risco, torna-se imprescindível adotar uma estratégia que promova o engajamento de todos os membros da organização na proteção do ambiente digital.

Para construção da cultura de segurança como estratégia para mitigação de vulnerabilidades, serão apresentadas a seguir cinco ações, que devem ser adotadas amplamente e reforçadas continuamente em todas as Organizações Militares da Força Aérea.

A primeira ação é a inserção da segurança cibernética no cotidiano da organização. Isso implica tratá-la não como um tema técnico isolado, mas como parte integrante das práticas diárias de trabalho. Pequenos hábitos, como a criação de senhas fortes, o bloqueio de telas, a verificação de remetentes de e-mails e o cuidado com o uso de dispositivos pessoais, devem ser incentivados e valorizados por meio de campanhas de comunicação interna. A repetição desses comportamentos no dia a dia ajuda a fomentar o senso de responsabilidade individual pela segurança coletiva.

A segunda ação é o exemplo da liderança, fator essencial para a consolidação de uma cultura organizacional robusta. Líderes que praticam e defendem os princípios de segurança inspiram suas equipes a fazerem o mesmo. Quando oficiais superiores participam ativamente de treinamentos, alertam para riscos e incorporam boas práticas digitais, transmitem uma mensagem clara de prioridade institucional. A cultura se fortalece quando a segurança é percebida como um valor da alta gestão, e não apenas uma obrigação técnica.

Como terceira ação, destaca-se a educação contínua e contextualizada. Ao invés de treinamentos genéricos, é recomendável desenvolver programas específicos para os diferentes perfis e funções da organização. Militares da área de TI e da área administrativa, por exemplo, possuem realidades distintas e, portanto, necessitam de formações ajustadas às suas rotinas. A aplicação de simulações realistas, como ataques de *phishing* controlados, estimula o aprendizado pela experiência e aumenta a capacidade de resposta a incidentes reais.

Outra ação fundamental é o uso de mecanismos de reforço positivo, como reconhecimento e recompensas por boas práticas. A gamificação é um exemplo prático: ao atribuir pontos ou destaques simbólicos aos usuários que adotam comportamentos seguros, cria-se um ambiente motivador e colaborativo. Essa abordagem transforma a segurança cibernética em um valor compartilhado, não imposto.

Além disso, é preciso instituir espaços para escuta e feedback, nos quais os usuários possam relatar dúvidas, incidentes ou comportamentos suspeitos sem receio de punição. Essa confiança é a base de uma cultura madura, onde todos se sentem corresponsáveis pela segurança digital.

Por fim, a atualização e coerência de normas e legislações também exerce papel importante. Políticas de segurança devem ser claras, acessíveis e compatíveis com as

demandas da organização. A dissonância entre normativos e realidade fragiliza a adesão e compromete a cultura.

Em síntese, mitigar vulnerabilidades por meio da cultura de segurança cibernética é uma tarefa institucional de longo prazo, que depende da mudança de mentalidade, da repetição de boas práticas e da promoção do comprometimento coletivo com a missão de proteger os ativos digitais.

3 CONCLUSÃO

A crescente dependência de sistemas de TI na estrutura organizacional e operacional da FAB evidencia a urgência de adoção de estratégias efetivas para mitigar vulnerabilidades cibernéticas. No atual cenário geopolítico, o ciberespaço tornou-se um domínio estratégico de disputa, no qual as ameaças não se limitam a ofensivas tecnológicas, mas exploram, sobretudo, as fragilidades humanas.

O primeiro argumento deste ensaio mostrou que o desenvolvimento da mentalidade de segurança entre os usuários de sistemas de TI representa uma das formas mais efetivas de proteção contra ataques cibernéticos. A capacitação contínua, alinhada a valores institucionais de responsabilidade digital, tem o poder de transformar o comportamento organizacional, tornando os membros da instituição agentes ativos da segurança cibernética.

Em complemento, o segundo argumento evidenciou que o fator humano, embora muitas vezes negligenciado, permanece como o elo mais vulnerável. A exploração da engenharia social pelos adversários mostra que, sem o engajamento e a vigilância dos usuários, até os sistemas mais avançados podem ser comprometidos. Por isso, a mitigação de riscos comportamentais exige uma abordagem multidisciplinar, com treinamentos personalizados, feedback contínuo e iniciativas inovadoras.

Mitigar vulnerabilidades cibernéticas vai além de adotar soluções técnicas: exige uma transformação cultural que envolva toda a organização. A segurança cibernética deve ser compreendida como uma responsabilidade coletiva e estratégica, indispensável para o cumprimento da missão institucional da Força Aérea Brasileira em tempos de paz, crise ou conflito. Desta forma, reforça-se a tese deste ensaio, que defende a construção de uma cultura de segurança cibernética como estratégia efetiva para a mitigação de vulnerabilidades, frente às ameaças contemporâneas. Construir uma cultura de segurança cibernética é mais do que uma necessidade técnica, trata-se de uma prioridade estratégica para a manutenção da prontidão operacional e da soberania nacional.

Por fim, como principal contribuição deste trabalho e consolidando a tese apresentada, foram apresentadas cinco ações para a construção de uma cultura de segurança cibernética como estratégia para mitigação de vulnerabilidades, alicerces fundamentais para que o comportamento seguro se integre à rotina organizacional. Mais do que soluções tecnológicas, é a cultura, enraizada nas atitudes e no dia a dia dos usuários, que sustenta a resiliência diante das ameaças do domínio cibernético.

REFERÊNCIAS

CLAUSEWITZ, C. VON. **Da guerra**. Tradução: Maria José. 2. ed. rev. ed. [s.l.] Martins Fontes, 2002.

IBM SECURITY. **Custo das violações de dados 2024**. Armonk, NY: IBM Security, 2024. Disponível em: <https://www.ibm.com/reports/data-breach>. Acesso em: 28 jul. 2025.

NIST. National Institute of Standards and Technology. **Framework for improving critical infrastructure cybersecurity**. [s.l.] NIST, 2023. Disponível em: <https://www.nist.gov/cyberframework>. Acesso em: 20 jul. 2025.

PROOFPOINT, Inc. **State of the phish report 2024 – today's cyber threats and phishing protection**. Sunnyvale, CA: Proofpoint, 2024. Disponível em: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>. Acesso em: 25 jul. 2025.

SCHEIN, Edgar H. **Cultura organizacional e liderança**. 5. ed. São Paulo: Atlas, 2010.

VERIZON ENTERPRISE. 2023 **Data breach investigations report**. New York: Verizon Enterprise, 2023. Disponível em: <https://www.verizon.com/dbir>. Acesso em: 20 jul. 2025..