ESCOLA SUPERIOR DE GUERRA

LEANDRO TADEU GARCIA JACOBINI

DO CÓDIGO À SOBERANIA AÉREA:

metodologias seguras no desenvolvimento de software para a Força Aérea Brasileira

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: CL R/1 João Azevedo

Rio de Janeiro

2024

CSSDC 2024 ESG

Este trabalho, nos termos de legislação que resguarda os direitos autorais, é considerado propriedade da ESCOLA SUPERIOR DE GUERRA (ESG). É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa.
Os conceitos expressos neste trabalho são de responsabilidade do autor e não expressam qualquer orientação institucional da ESG.

Documento assinado digitalmente
LEANDRO TADEU GARCIA JACOBINI
Data: 22/10/2024 13:33:22-0300
Verifique em https://validar.iti.gov.br

LEANDRO TADEU GARCIA JACOBINI

RESUMO

Este ensaio acadêmico aborda as metodologias seguras de desenvolvimento de software no contexto da Força Aérea Brasileira (FAB), enfatizando sua importância para a segurança nacional, padronização das equipes e celeridade nas entregas de forma segura. O estudo apresenta uma visão geral das metodologias SDLC (Software Development Life Cycle) mais recentes, analisando criticamente sua aplicabilidade no âmbito da FAB e seus Centros de Computação da Aeronáutica (CCA). São discutidos os desafios específicos de segurança enfrentados pela instituição no desenvolvimento de software, propondo adaptações e melhorias nas metodologias SDLC para atender às necessidades particulares da FAB. O trabalho conclui com recomendações para a implementação de metodologias seguras de desenvolvimento, visando fortalecer a postura de segurança cibernética da Força Aérea Brasileira.

Palavras-chave: metodologias seguras; desenvolvimento de software; Força Aérea Brasileira; segurança cibernética; SDLC.

ABSTRACT

This academic essay addresses secure software development methodologies in the context of the Brazilian Air Force (FAB), emphasizing their importance for national security, team standardization, and secure, swift deliveries. The study presents an overview of the most recent SDLC (Software Development Life Cycle) methodologies, critically analyzing their applicability within the FAB and its Air Force Computing Centers (CCA). The specific security challenges faced by the institution in software development are discussed, proposing adaptations and improvements to SDLC methodologies to meet the particular needs of the FAB. The work concludes with recommendations for implementing secure development methodologies, aiming to strengthen the Brazilian Air Force's cybersecurity posture.

Keywords: secure methodologies; software development; Brazilian Air Force; cybersecurity; SDLC.

1 INTRODUÇÃO

Nas últimas décadas foi possível verificar a compressão das ondas de inovação teorizadas pelo filósofo austríaco Joseph Schumpeter (1883-1950), principalmente no que tange ao ramo da informática. Nessa ciência, a crescente velocidade de evolução e automação das tarefas tornam, da mesma forma, as ameaças cada vez mais sofisticadas. Com isso, é observado um aumento na preocupação em desenvolvimento seguro de softwares por diversas organizações e instituições em todo o mundo, com o fito de protegerem seus clientes e usuários.

Na Força Aérea Brasileira (FAB) não é diferente. A FAB é uma das três Forças Armadas da República Federativa do Brasil e figura como uma das principais instituições responsáveis pela segurança nacional. Como tal, enfrenta o desafio de desenvolver e manter sistemas de software que, além de atender às suas necessidades operacionais, garantam a segurança, disponibilidade, integridade, confidencialidade e autenticidade de seus dados.

No entanto, apesar dos crescentes cortes orçamentários e contingenciamentos sofridos, a FAB permanece aplicada em manter seu portifólio atualizado com as novas tecnologias, bem como focada na contratação de talentos com o fito de desenvolver e aplicar metodologias seguras para o desenvolvimento de seus softwares.

Para isso, o emprego de metodologias seguras para o Ciclo de Vida de Desenvolvimento de Software (SDLC – do inglês *Software Development Life Cycle*), conjuntamente com práticas de segurança cibernética, tornará possível a atuação proativa dos desenvolvedores da FAB, promovendo a inserção de medidas de proteção e antecipando possíveis ameaças durante todo o processo de desenvolvimento. É dessa forma que as metodologias seguras, como o SAFe, *Agile Security* e o DevSecOps, incorporam técnicas de segurança em cada fase do desenvolvimento, diferentemente do que é observado nas abordagens tradicionais, onde a segurança é verificada somente ao final do ciclo de desenvolvimento.

Esse incremento na segurança durante o ciclo de desenvolvimento não só se justifica, como torna-se uma obrigação em função do papel desempenhado pela FAB em manter a soberania do espaço aéreo nacional e integração do território nacional com vistas à defesa da pátria. Dentro da missão síntese afeta à FAB, encontra-se, também, a proteção e controle do espaço aéreo brasileiro, compreendendo a gestão

de sistemas complexos e vitais para o monitoramento, controle e coordenação das atividades aéreas. Tais sistemas são compostos por softwares de comando e controle, comunicação e rede, e são críticos para a Força. Ademais, é importante salientar que, como todo sistema de TI, são suscetíveis a ataques cibernéticos, podendo comprometer a operação e a segurança de dados estratégicos.

Para fortalecer a defesa cibernética, estimular a capacidade operacional e proporcionar inovações com o fito de viabilizar a eficiência e eficácia dos sistemas corporativos, encontra-se a Diretoria de Tecnologia da Informação da Aeronáutica (DTI), órgão do Comando da Aeronáutica que, por meio dos Centros de Computação da Aeronáutica (CCA) e do Centro de Defesa Cibernética da Aeronáutica (CDCAer), é responsável, dentre outras atividades, pela padronização de aquisição de equipamentos, elaboração e execução de práticas e políticas de TI na FAB, bem como trabalha para garantir o desenvolvimento seguro dos sistemas utilizados tanto administrativamente quanto operacionalmente. Assim, a preocupação com tais tarefas mostra-se em conformidade com o mundo acadêmico, principalmente no que tange ao desenvolvimento seguro de softwares, onde Dias (2021) ratifica a necessidade do desenvolvimento seguro, da conscientização e da capacitação da equipe para superar as adversidades do desenvolvimento seguro, com o fito de colaborar na construção de um ambiente digital confiável e mais protegido.

Ainda no que tange ao desenvolvimento de softwares, um fator importante a ser considerado é a agilidade nas entregas em virtude da volatilidade tecnológica atual. Por este motivo metodologias tradicionais de desenvolvimento, como o *Waterfall*, nas quais as fases são necessariamente sequenciais e rígidas, têm sido substituídas por metodologias ágeis ou híbridas, dependendo do projeto. No entanto, a substituição total para metodologias ágeis poderia gerar vulnerabilidades graves para os sistemas de defesa em virtude da priorização do tempo de entrega em detrimento de controles de segurança. Por esse motivo, é determinante que as novas práticas sejam implementadas de forma adaptada na cultura organizacional relativa ao desenvolvimento de sistemas da FAB. Tal fato é evidenciado por Kim et al. (2021) quando descrevem que a chave para o sucesso na adoção de metodologias ágeis seguras está na integração contínua da segurança desde a concepção do software, integrando as equipes e promovendo a cultura do DevSecOps.

Nesta senda, faz-se relevante analisar as metodologias mais recentes de desenvolvimento de software e mais empregadas no mercado atualmente, com o foco voltado para a adoção e implementação de práticas de segurança durante cada fase do Ciclo de Vida de Desenvolvimento de Software (SDLC).

2 DESENVOLVIMENTO

2.1 Visão Geral das Metodologias SDLC

O Ciclo de Vida de Desenvolvimento de Software é um processo que descreve as fases que constam da criação e desenvolvimento de sistemas e softwares. O referido método possui diversas etapas previstas, como o planejamento, a definição de requisitos, o design, o desenvolvimento, os testes, a implantação e a manutenção. Assim, cada etapa é revestida com extrema importância visando assegurar o desenvolvimento do software de maneira segura, eficiente e segundo os objetivos organizacionais. Aos poucos, a referida metodologia SDLC foi evoluindo com o fito de garantir também a segurança cibernética, sem deixar de lado a eficiência no desenvolvimento. Essa necessidade é preponderante em setores críticos, assim como no militar. Segundo Pressman e Maxim (2021), essa evolução é marcada pela transição de modelos lineares e rígidos para abordagens mais ágeis e iterativas, que incorporam práticas de segurança em todas as fases do desenvolvimento.

Na Força Aérea Brasileira, onde alguns sistemas são desenvolvidos para tramitar informações sensíveis e/ou armazená-las, o que pode trazer risco à segurança nacional em caso de vazamento ou acesso indevido, as metodologias SDLC tradicionais vêm se mostrando limitadas para conter os riscos emergentes. Essa necessidade de incorporar a segurança em todas as etapas do ciclo de desenvolvimento fez surgir as metodologias modernas, que priorizam a proteção contra ameaças cibernéticas, além de garantir as entregas de forma célere e eficiente. Assim, Dias (2021) argumenta que a integração de práticas de segurança desde as fases iniciais do desenvolvimento não apenas reduz as vulnerabilidades, mas também diminui o custo total de remediação dos sistemas de software.

Para efeitos deste estudo, dentre as metodologias modernas e mais relevantes para a FAB, serão abordadas a DevSecOps, *Agile Security*, SAFe e o *Waterfall*, que, apesar desta última figurar como uma abordagem mais tradicional, ainda possui aplicabilidade em projetos militares específicos.

2.1.1 DevSecOps

Essa metodologia surgiu como uma evolução da DevOp, que concilia desenvolvimento (Dev) com operações (Op) em um fluxo contínuo de produção, priorizando a automação e a integração entre equipes. A novidade primordial do DevSecOps foi a incorporação de práticas de segurança (Sec) desde o início do ciclo de desenvolvimento. Com isso, a segurança passou a ser reconhecida como um componente fundamental em todas as etapas do processo, e não somente como um complemento ou como uma preocupação secundária a ser tratada ao término do desenvolvimento do software. De acordo com Dias (2021), a automação de testes de segurança no DevSecOps permite que falhas sejam identificadas e corrigidas de maneira proativa, minimizando o período de inatividade e os prejuízos provocados por ataques.

Segundo Kim et al. (2021), o DevSecOps promove uma cultura de segurança integrada, onde cada membro da equipe de desenvolvimento é responsável pela segurança, contribuindo para o incremento da proteção institucional. Dessa forma, a adoção dessa prática será extremamente importante para a FAB, pois qualquer falha na segurança pode comprometer missões críticas e a própria defesa nacional. Ademais, a automação de testes unitários e de integração, testes de segurança, o emprego de ferramentas de análise de código estático e dinâmico e a integração contínua (CI) figuram como os pilares do DevSecOps, propiciando a detecção e correção de problemas de segurança precocemente, negando a exploração das vulnerabilidades por adversários.

Uma outra vantagem da aplicação do DevSecOps reside na metodologia proporcionar a correta adaptação às crescentes complexidades dos sistemas modernos. Com a implantação do DevSecOps seria possível incrementar significativamente a identificação e a mitigação de vulnerabilidades, além de promover uma maior velocidade no ciclo de desenvolvimento em ambientes como o da FAB, onde os sistemas são compostos por várias camadas de infraestrutura e comunicação. Ademais, por intermédio da automação e da análise contínua, o DevSecOps favoreceria a adaptação a novas ameaças cibernéticas e promoveria uma resposta mais ágil a incidentes. Conforme observa Kim et al. (2021), “em vez de inspecionarmos a segurança em nosso produto ao final do processo, vamos criar e integrar controles de segurança no trabalho diário de Desenvolvimento e Operações”.

2.1.2 Agile Security

Esta metodologia surgiu como forma de adaptar as metodologias ágeis tradicionais, como o *Scrum* e o *Kanban*, com a integração práticas de segurança no desenvolvimento de softwares. Ela se diferencia de metodologias tradicionais, como o Waterfall, por não seguir uma abordagem sequencial rígida, incorporando ciclos curtos de desenvolvimento (*sprints*), possibilitando que o software seja desenvolvido de forma incremental. No que tange à segurança, esta metodologia a considera em cada Sprint, assegurando que as vulnerabilidades sejam tratadas de forma contínua. Segundo Pressman e Maxim (2021), a ênfase na criação de casos de teste iniciais em cada sprint reduz a probabilidade de falhas críticas, evitando a necessidade de correções caras e demoradas após o desenvolvimento.

Dessa forma, a flexibilidade de se adaptar às mudanças figura como uma das principais particularidades do Agile Security, o que é extremamente importante para ambientes como o da FAB, onde novos requisitos de segurança podem surgir intempestivamente. Além disso, esta metodologia promove a colaboração entre as equipes de desenvolvimento, segurança e operações, fomentando uma abordagem holística para a criação de softwares seguros. Segundo Kim et al. (2021), a segurança deve ser parte integrante de cada iteração no desenvolvimento ágil, de modo que as vulnerabilidades sejam detectadas e corrigidas durante o processo, e não depois que o software é entregue.

Outrossim, no contexto militar, esta metodologia favorece a entrega célere de novos sistemas ou funcionalidades, sem comprometer a segurança. Tendo em vista que o ambiente militar deve prover respostas rápidas às ameaças, o *Agile Security* disponibiliza a flexibilidade necessária com o fito de adequar as necessidades de desenvolvimento conforme as demandas operacionais, ao mesmo tempo em que mantém a segurança como fator central. Corroborando essa afirmação, Butler (2024) afirma que esta abordagem mantém a flexibilidade do desenvolvimento ágil enquanto incorpora práticas de segurança em cada iteração. Com isso, o *Agil Security* figura como uma metodologia pujante para o desenvolvimento de sistemas sensíveis ao integrar práticas de segurança, como a revisão de código seguro, a implementação de políticas de autenticação robustas e a análise de vulnerabilidades.

2.1.3 SAFe (Scaled Agile Framework)

O SAFe figura como uma metodologia ágil escalável, sendo desenvolvida para atender as necessidades de grandes organizações, nas quais diversas equipes trabalham em conjunto para o desenvolvimento de sistemas complexos. Esta metodologia também poderia ser aplicada na FAB, onde os diversos Centros de Computação da Aeronáutica e o Centro de Defesa Cibernética da Aeronáutica podem estar simultaneamente envolvidos no desenvolvimento de projetos, oferecendo uma estrutura robusta para coordenar as atividades de várias equipes, mantendo a concatenação e a segurança em todas as fases do SDLC. Segundo Bell et al. (2017), o SAFe é eficaz para grandes projetos, onde a gestão de risco é ampliada para além do nível da equipe, pois incorporam um planejamento e design iniciais bem definidos, relatórios e pontos de verificação de integração entre equipes, além de funções extras para a arquitetura e gestão de programas, a fim de gerir riscos e dependências entre os times.

A capacidade de integração da segurança no nível de portfólio figura como uma das principais vantagens do SAFe, assegurando que as decisões estratégicas acerca da segurança e do desenvolvimento sejam tomadas de forma centralizada e empregadas de maneira uniforme por todas as equipes envolvidas. Outrossim, Bell et al. (2017) acrescenta que, além das tecnologias automatizadas de testes de segurança, que podem ser facilmente integradas aos fluxos de trabalho dos desenvolvedores, a equipe de segurança deve procurar maneiras de facilitar o trabalho da equipe de desenvolvimento, permitindo que a equipe desenvolva e implante o software com mais rapidez, garantindo ao mesmo tempo maior segurança. Ademais, o SAFe proporciona a criação de “equipes ágeis”, as quais trabalham em estreita colaboração com especialistas em segurança com o fito de assegurar que os requisitos de segurança sejam plenamente atendidos em cada estágio do ciclo de desenvolvimento.

Com isso, o emprego desta metodologia na FAB se justificaria em função da complexidade dos sistemas que são desenvolvidos e pela necessidade de integrar a segurança em todos os níveis do SDLC. Assim, o SAFe permitiria que a segurança fosse tratada de forma holística, com uma abordagem coordenada e consistente em toda a organização, diferentemente das metodologias ágeis aplicadas a pequenas equipes ou projetos isolados. Dessa forma, este referido modelo facilitaria a

colaboração entre os CCA e o CDCAER, assegurando que todos os projetos e sistemas desenvolvidos estejam alinhados com os objetivos estratégicos do Comando da Aeronáutica (COMAER), bem como com os padrões de segurança exigidos.

O foco em capacitação contínua das equipes e treinamento constante são outros atributos importantes do SAFe. No ambiente militar, onde surgem regularmente novas ameaças cibernéticas, é importante que os programadores e especialistas em segurança mantenham-se atualizados sobre as melhores práticas. Ao fomentar uma cultura de aprendizado constante, o SAFe garante que as equipes estejam sempre prontas para aplicar as soluções mais seguras e eficazes.

2.1.4 Waterfall

Apesar do crescente destaque das metodologias ágeis e adaptáveis nos últimos anos, o *Waterfall* (Cascata) ainda mantém a pertinência para projetos com requisitos estáveis e bem definidos, especialmente em setores como o militar, onde a previsibilidade e o controle rígido são fundamentais. A metodologia *Waterfall* adota uma abordagem linear e sequencial, na qual cada etapa do desenvolvimento – “análise e definição dos requisitos, projeto do sistema e do software, implementação e teste de unidade, integração e teste de sistema, operação e manutenção”. (SOMMERVILLE, 2018) – precisa ser finalizada antes de dar início à próxima. Ademais, a segurança no modelo Waterfall costuma ser vista como um estágio separado, frequentemente durante a fase de testes, o que pode levar a vulnerabilidades de segurança que são descobertas somente após o processo de desenvolvimento.

Embora seja visto como um procedimento mais convencional, o Waterfall pode ser eficiente em alguns projetos da FAB, onde os requisitos são bem definidos desde o começo e há pouca flexibilidade para alterações durante o desenvolvimento. Este modelo proporciona maior controle sobre cada etapa, possibilitando uma documentação completa e assegurando que cada fase seja meticulosamente verificada antes de seguir adiante. Segundo Sommerville (2018), a natureza sequencial do Waterfall é adequada para grandes sistemas de software que requerem uma validação detalhada em cada fase, especialmente em sistemas críticos, onde qualquer falha pode resultar em consequências severas.

Apesar do modelo Waterfall proporcionar clareza no processo de desenvolvimento, ele apresenta suas restrições em relação à rápida adaptação a alterações e à incorporação de práticas de segurança durante o ciclo de vida. Para a FAB, que opera em um ambiente dinâmico e sempre em transformação, o modelo Waterfall pode não ser o mais apropriado, especialmente quando a segurança é uma questão crucial desde o começo do processo de desenvolvimento. Como afirmam Pressman e Maxim (2021), modelos tradicionais como o Waterfall falham ao integrar considerações de segurança nas fases iniciais do desenvolvimento, deixando muitas vulnerabilidades graves passarem despercebidas até as fases mais avançadas.

Após essa sucinta apresentação das metodologias selecionadas, a intenção é apontar a aplicação dos referidos modelos de forma segura e eficaz, balanceando as necessidades de segurança com a agilidade e eficiência necessárias para a FAB no desenvolvimento de softwares.

2.2 Aplicabilidade no Contexto da FAB e dos CCA

A Força Aérea Brasileira (FAB) exerce um papel fundamental na segurança do país, assegurando o controle e a soberania do espaço aéreo do Brasil. Neste cenário, a criação de sistemas de software seguros é uma meta estratégica crucial, especialmente levando em conta o aumento da digitalização das suas atividades. A incorporação de métodos seguros de desenvolvimento de software, tais como DevSecOps, Agile Security, SAFe e Waterfall, nos projetos da FAB proporciona soluções que harmonizam segurança, rapidez e uniformidade, essenciais para satisfazer as necessidades operacionais e de defesa cibernética.

Os Centros de Computação da Aeronáutica (CCA) têm a tarefa de criar e administrar sistemas essenciais que apoiam as atividades da FAB. Estes sistemas abrangem desde plataformas de comando e controle até sistemas de comunicação, sistemas de segurança cibernética e redes internas que possibilitam a transferência de informações confidenciais entre as diversas Bases e Unidades da Força Aérea. Cada um desses sistemas, devido ao seu caráter, necessita de robustez e segurança durante seu processo de desenvolvimento, para assegurar a integridade das operações militares. Em seguida, abordaremos a utilização de diversas metodologias SDLC no âmbito da FAB e dos CCA, destacando os obstáculos e vantagens particulares de cada uma.

2.2.1 DevSecOps no contexto da FAB

A abordagem DevSecOps, que combina práticas de desenvolvimento, operações e segurança em um fluxo ininterrupto, possui uma relevância considerável no contexto da FAB. No ambiente militar, onde a segurança digital é uma questão crucial, o DevSecOps se ressalta pelo seu potencial de automatizar processos e incorporar a segurança desde os estágios iniciais do ciclo de vida do desenvolvimento de software. Isso é fundamental em ambientes como os dos Centros de Computação da Aeronáutica, onde brechas de segurança podem prejudicar missões críticas e dados sensíveis. Conforme afirma Dias (2021), a integração dos testes de segurança no processo de desenvolvimento é essencial para mitigar as vulnerabilidades em sistemas, promovem uma cultura de segurança contínua e garantem o desenvolvimento de forma segura, preservando os dados e os ativos da instituição contra os riscos cibernéticos.

Como instituição militar, a FAB se depara com um cenário de ameaças cibernéticas em constante transformação. Espionagem, ataques de negação de serviço (DDoS) e a exploração de vulnerabilidades em sistemas militares são algumas das ameaças que se apresentam. Neste contexto, a implementação do DevSecOps possibilita a mitigação dessas ameaças durante todo o processo de desenvolvimento, assegurando que cada nova linha de código seja automaticamente verificada quanto à existência de vulnerabilidades. Segundo Kim et al. (2021), a implementação de ferramentas que automatizam a análise de código, testes de segurança e rastreamento de vulnerabilidades podem agilizar o processo de desenvolvimento e mitigar a chance de falhas humanas, considerando que todos os sistemas críticos devem ser rigorosamente testados antes de serem colocados em operação.

A Força Aérea Brasileira também pode se favorecer da possibilidade do DevSecOps em diminuir o prazo de entrega de sistemas seguros. O DevSecOps, com sua característica de desenvolvimento ágil e constante, corresponde à demanda da FAB para reagir prontamente a novas ameaças e modificações nos requisitos de desenvolvimento. Por exemplo, sistemas de monitoramento e controle em tempo real podem ser desenvolvidos e melhorados continuamente, incorporando atualizações de segurança ao código sem precisar interromper significativamente as operações. Isso assegura a continuidade das operações e mitiga o perigo de exposição a vulnerabilidades, um elemento crucial para a segurança do país. Conforme discutido

por Bell et al. (2017), essa abordagem permite melhorar o feedback e reduzir o tempo de colocação no mercado além de permitir lançamentos mais frequentes e confiáveis.

2.2.2 Agile Security e a flexibilidade necessária para a FAB

A abordagem Agile Security, uma variação das metodologias ágeis voltadas para a segurança, também é altamente aplicável no cenário militar. Esta metodologia proporciona a adaptabilidade requerida para gerenciar projetos dinâmicos, nos quais os requisitos podem ser alterados rapidamente devido a novas ameaças cibernéticas ou a novas demandas operacionais. No contexto militar, que exige inovação e constante adaptação, o Agile Security possibilita que os times de desenvolvimento dos CCA forneçam novas funcionalidades de maneira incremental, enquanto incorporam revisões e verificações de segurança em cada sprint. A abordagem ágil possibilita a incorporação dinâmica dessas alterações, enquanto o Agile Security assegura que a segurança seja um fator crucial em cada fase do ciclo de desenvolvimento (Butler, 2024).

Um caso concreto de uso do Agile Security na FAB seria a criação de sistemas de defesa cibernética e monitoramento de ameaças, nos quais a rapidez na implementação de novas funcionalidades precisa ser balanceada com a proteção do sistema. Em cada ciclo de desenvolvimento (sprint), é possível implementar e validar novos componentes de software, verificando sua robustez e resiliência. Segundo Bell et al. (2017), a abordagem iterativa e incremental do Agile Security garante que as funcionalidades sejam desenvolvidas rapidamente, sem comprometer a segurança do sistema como um todo.

Ademais, o Agile Security fomenta uma cultura de cooperação entre as equipes de desenvolvimento e segurança, um elemento essencial para o contexto dos CCA. Com equipes atuando em conjunto, é possível identificar e solucionar os riscos de segurança antes que prejudiquem as operações militares. Isso diminui a demanda por correções de segurança emergenciais, que frequentemente são dispendiosas e prolongadas, além de assegurar que a FAB esteja constantemente à frente no que diz respeito à defesa cibernética. De acordo com Sommerville (2018), as metodologias ágeis adaptadas para a segurança, como o Agile Security, permitem que a segurança seja integrada ao desenvolvimento sem sacrificar a velocidade ou a flexibilidade.

2.2.3 SAFe e a coordenação de equipes nos CCA

O SAFe (Scaled Agile Framework) proporciona uma estratégia expansível para a metodologia ágil, sendo perfeito para gerir várias equipes de desenvolvimento em contextos complexos, como os dos Centros de Computação da Aeronáutica. Na Força Aérea Brasileira, onde vários projetos de software são executados ao mesmo tempo, o SAFe permite que várias equipes de desenvolvimento trabalhem de forma coordenada em diferentes componentes de um projeto, garantindo que os princípios de segurança e agilidade sejam mantidos em todas as fases (Opposit Int, 2024).

Um dos principais benefícios do SAFe é a sua possibilidade de gerenciar a complexidade de projetos de grande escala, particularmente em um contexto militar como o da FAB. Por exemplo, sistemas de comando e controle são criados por diversas equipes que atuam em diversos módulos. O SAFe possibilita a integração coordenada desses módulos, assegurando que todos cumpram as mesmas normas de segurança e que o sistema final seja sólido e seguro. Como discutido por Bell (2017), o SAFe é projetado para garantir que grandes projetos sejam conduzidos considerando sobremaneira o gerenciamento de risco, criando dependência entre as equipes, sem comprometer a segurança e a qualidade do software.

Ademais, o SAFe fomenta uma governança centralizada de segurança, crucial em contextos como os CCA, onde a salvaguarda de dados sensíveis é essencial. A aplicação de revisões de segurança em nível de portfólio possibilita que os administradores da FAB mantenham um controle estrito sobre todos os projetos em andamento, assegurando que nenhum elemento de segurança seja desprezado. Assim, o SAFe possibilita à FAB manter elevados níveis de segurança, mesmo em projetos complexos e de longa duração, como a criação de sistemas de defesa.

2.2.4 Waterfall: a aplicação em projetos de requisitos fixos

Apesar da crescente popularidade das metodologias ágeis, o Waterfall ainda possui utilidade no cenário da FAB, particularmente em projetos de longo prazo com requisitos bem definidos. Em projetos com poucas mudanças e exigência de validação rigorosa, o Waterfall proporciona uma estratégia estruturada que possibilita um controle minucioso de cada etapa do processo de desenvolvimento.

O Waterfall pode ser aplicado em projetos de infraestruturas vitais, tais como sistemas de comunicação segura, onde os requisitos são bem definidos desde o

começo e há pouca margem para modificações durante o processo de desenvolvimento. Essa abordagem assegura que cada etapa, desde a definição dos requisitos até a realização de testes e implementação, seja finalizada de maneira sequencial e validada antes de prosseguir para a seguinte. Esta estratégia é especialmente eficaz ao lidar com sistemas onde a integridade e a confiabilidade são fundamentais, e onde erros podem levar a falhas de grande magnitude.

Segundo Sommerville (2018), o Waterfall é uma escolha apropriada para os sistemas críticos em segurança, onde os requisitos são estáveis e há a necessidade de uma extensa análise e documentação antes de iniciar a sua implementação. Para a Força Aérea Brasileira, essa metodologia pode ser empregada na criação de sistemas de longa duração, com ênfase em segurança, conformidade e estabilidade. No âmbito militar, sistemas como os utilizados para o controle de tráfego aéreo, gerenciamento de informações logísticas ou defesa aérea requerem processos rigorosos de validação e verificação antes de sua efetiva implementação. A previsibilidade do Waterfall assegura a completa validação de cada etapa antes de prosseguir para a próxima, reduzindo a probabilidade de erros ou falhas que possam afetar a segurança de operações críticas.

No entanto, a demanda crescente por rapidez e resposta imediata a ameaças cibernéticas emergentes obriga a FAB a adotar métodos mais adaptáveis, como o DevSecOps e o Agile Security, que possibilitam uma integração constante de segurança e uma maior capacidade de adaptação. Para a FAB, a fusão de métodos tradicionais e ágeis proporciona o melhor de cada abordagem, possibilitando um desenvolvimento robusto e seguro, sem prejudicar a habilidade de reagir a modificações ou emergências.

2.3 Desafios Específicos de Segurança Enfrentados pela FAB

A Força Aérea Brasileira (FAB) atua em um cenário onde a proteção da informação é vital, e os problemas com segurança cibernética que a instituição enfrenta são tanto extensos quanto complexos. Com o progresso das tecnologias da informação e a evolução dos ataques cibernéticos, os sistemas da FAB, responsáveis por tudo, desde operações aéreas até comunicações estratégicas, se transformam em alvos valiosos para os adversários. As ameaças abrangem desde espionagem e sabotagem até ataques diretos a infraestruturas vitais, demandando da FAB uma atitude firme e proativa em relação à segurança no desenvolvimento de software.

Um dos maiores obstáculos que a FAB enfrenta é a defesa contra a espionagem. Instituições militares, como a FAB, tratam informações classificadas, como informações sobre operações, capacidades militares e comunicações estratégicas. Essas informações são frequentemente objeto de tentativas de espionagem por parte de outros países ou organizações cibercriminosas, com o objetivo de obter dados que possam afetar a soberania do país. A espionagem cibernética pode ser realizada por meio de diversos métodos de ataque, como a exploração de falhas em softwares internos ou a implementação de *backdoors* durante a fase de desenvolvimento do software.

Um segundo desafio significativo é a sabotagem, que consiste na introdução proposital de vulnerabilidades ou falhas em sistemas vitais, que podem ser utilizadas para provocar falhas graves em operações militares. Durante o desenvolvimento de software podem ocorrer sabotagens, principalmente se os processos de segurança não forem rigorosamente implementados em todas as fases do ciclo de vida do desenvolvimento. De acordo com Pressman e Maxim (2021), a falta de controles adequados durante o desenvolvimento pode permitir que vulnerabilidades sejam inseridas nos sistemas sem serem detectadas, abrindo caminho para futuras explorações maliciosas. Para reduzir esse perigo, é crucial que a FAB implemente metodologias como o DevSecOps, que incorporam a segurança desde o começo e automatizam a análise constante de vulnerabilidades.

Um outro obstáculo importante que a FAB enfrenta é a defesa contra ataques cibernéticos diretos. Esses ataques podem se manifestar como negação de serviço (DDoS), malware, ransomware ou ataques de dia zero, que se beneficiam de vulnerabilidades não identificadas ou ainda não corrigidas nos sistemas da FAB. A complexidade das operações militares requer que os sistemas estejam sempre acessíveis e em pleno funcionamento. Um ataque cibernético bem-sucedido pode levar à perda de controle sobre os sistemas de defesa, erros em operações de comando e controle e até mesmo à incapacidade de reação em cenários de emergência. Neste cenário, assegurar a continuidade da operação dos sistemas é tão crucial quanto resguardar a integridade e a confidencialidade das informações. Pressman e Maxim (2021) destacam a importância de uma avaliação contínua de riscos e práticas de segurança cibernética integradas durante todo o processo de desenvolvimento.

A FAB, além dos ataques cibernéticos tradicionais, também confronta o desafio de integrar os sistemas antigos de maneira segura. Vários dos sistemas atualmente em funcionamento na FAB foram criados há anos e empregam tecnologias que podem não estar mais em conformidade com as melhores práticas de segurança contemporâneas. A combinação de novos sistemas com essas plataformas antigas pode gerar vulnerabilidades extras, especialmente se não houver uma análise de risco apropriada ou o emprego de um processo de atualização constante. Segundo Sommerville (2018), “os sistemas de software precisam se adaptar e evoluir para que continuem sendo úteis e que a modificação e a evolução de um software devem ser consideradas partes integrantes da engenharia de software “.

A Força Aérea Brasileira também se depara com o desafio de proteger as suas infraestruturas críticas, tais como sistemas de controle de tráfego aéreo, sistemas de comunicação militar e plataformas de defesa cibernética. Essas infraestruturas são essenciais para o funcionamento da FAB e, por isso, são comumente alvos de ataques cibernéticos. A salvaguarda dessas estruturas exige não só a aplicação de medidas de segurança convencionais, como firewalls e sistemas de detecção de invasões, mas também a aplicação de tecnologias de ponta, como inteligência artificial e aprendizado de máquina, com o fito de detectar e atenuar riscos em tempo real.

Ademais, a falta de especialistas competentes em segurança cibernética também constitui um grande obstáculo para a FAB. O desenvolvimento seguro de softwares exige equipes altamente qualificadas, aptas a detectar e corrigir falhas em todas as etapas do ciclo de vida do software. Contudo, a demanda crescente por especialistas em segurança cibernética, tanto no âmbito público quanto no privado, tem provocado um déficit considerável de profissionais qualificados.

Outrossim, a utilização cada vez maior de tecnologias emergentes, como a computação em nuvem e a Internet das Coisas (IoT) no contexto militar, apresenta novos desafios de segurança para a FAB. A implementação dessas tecnologias pode ampliar a área de ataque, estabelecendo novas entradas para criminosos cibernéticos. A aplicação de medidas de segurança apropriadas para salvaguardar essas tecnologias demanda uma modificação das técnicas de desenvolvimento de software e a implementação de novos mecanismos de segurança. Ao incorporar a segurança diretamente no processo de desenvolvimento, o DevSecOps proporciona uma resposta para minimizar esses novos perigos, assegurando que todas as

tecnologias emergentes sejam aplicadas de maneira segura. Dias (2021) reforça a necessidade de uma abordagem abrangente de capacitação, onde diz que o treinamento deve cobrir não apenas as ferramentas, mas também a cultura de segurança, de modo que todos os envolvidos no projeto entendam sua responsabilidade na proteção de dados e sistemas.

Destarte, os obstáculos de segurança que a FAB enfrenta no desenvolvimento de software figuram como complexos e multifacetados. A espionagem, a sabotagem, os ciberataques direcionados, a integração com os sistemas legados, a proteção de infraestruturas críticas, a escassez de profissionais qualificados e o crescente uso de tecnologias emergentes são apenas alguns dos elementos que requerem monitoramento constante. Assim, mostra-se necessário que a FAB integre metodologias seguras de desenvolvimento de software com ações de segurança proativas com o fito de preservar a integridade de seus sistemas em um contexto de ameaças cibernéticas cada vez mais avançadas.

2.4 Adaptações e Melhorias nas Metodologias SDLC para a FAB

A Força Aérea Brasileira (FAB) atua em um cenário de alta criticidade, no qual a segurança cibernética representa um sustentáculo importante para a salvaguarda das operações e da soberania do país. No desenvolvimento de software, é necessário adaptar as metodologias convencionais do SDLC para lidar com os desafios específicos que a FAB enfrenta, como a salvaguarda de informações sensíveis, a defesa contra ataques cibernéticos e a integração com sistemas de defesa de países aliados. Portanto, é essencial desenvolver um framework que incorpore práticas de segurança específicas desde os estágios iniciais do desenvolvimento até a manutenção ininterrupta, assegurando a robustez e a confiabilidade dos sistemas.

2.4.1 Segurança desde a concepção

A adoção de medidas de segurança desde a concepção do software é crucial para garantir a integridade dos sistemas da FAB, isto é, assegurar que as ameaças e vulnerabilidades sejam detectadas e sanadas nas etapas iniciais do ciclo de desenvolvimento. Normalmente, a segurança em projetos de desenvolvimento de software era abordada apenas nas etapas finais ou após a conclusão total do sistema, o que levava a uma significativa majoração de custos e riscos. Contudo, essa estratégia se revela ineficiente em contextos militares, onde qualquer brecha de

segurança pode prejudicar operações críticas. De acordo com Pressman e Maxim (2021), a segurança deve ser considerada desde o início do ciclo de vida, integrando testes e revisões em todas as fases do desenvolvimento.

Ao integrar a segurança desde o estágio de concepção, a FAB pode assegurar que os requisitos de segurança sejam incorporados ao planejamento e design do sistema, garantindo que todas as funcionalidades sejam criadas seguindo critérios rigorosos de defesa contra ameaças externas e internas. É primordial que as equipes de desenvolvimento mantenham uma interação contínua com especialistas em segurança, que são capazes de conduzir análises de risco e sugerir medidas preventivas para cada fase do projeto. Segundo Pressman e Maxim (2021), a introdução precoce de práticas de segurança no ciclo de vida de desenvolvimento reduz drasticamente a probabilidade de falhas críticas e permite uma melhor alocação de recursos para a mitigação de riscos.

Na Força Aérea Brasileira, essa abordagem pode ser empregada em sistemas complexos, tais como plataformas de controle de tráfego aéreo, sistemas de comando e controle ou soluções de comunicação militar, assegurando que, desde o começo, todos os elementos de software estejam em conformidade com os mais rigorosos padrões de segurança.

2.4.2 Automação de testes de segurança

Outra prática essencial é a automatização de testes de segurança para assegurar a robustez dos sistemas criados pela FAB. Em virtude do aumento da complexidade dos ataques cibernéticos e da demanda por respostas ágeis, é impraticável executar verificações de segurança manualmente a cada nova versão de um programa. A aplicação de testes de vulnerabilidades constantes e automatizados ao longo de todo o processo de desenvolvimento possibilita a validação de cada nova linha de código antes de sua incorporação ao sistema final, assegurando a aderência aos padrões de segurança militar.

Na esfera militar, em que os sistemas devem operar com elevada precisão e confiabilidade, a identificação antecipada de vulnerabilidades é fundamental para prevenir que falhas sejam exploradas em ambientes reais de operação. Ferramentas como a Análise Estática de Código (SAST), a Análise Dinâmica de Aplicativos (DAST) e os *Scanners* de Vulnerabilidades podem ser incorporadas ao processo de

desenvolvimento para examinar a performance do software em busca de vulnerabilidades. Essas ferramentas realizam testes de penetração e validações de segurança de forma automática durante o processo de integração contínua, possibilitando que o time de desenvolvimento da FAB repare os erros antes da implementação do software em ambientes operacionais. De acordo com Dias (2021), a integração de testes de segurança permite que as equipes de desenvolvimento identifiquem e corrijam as vulnerabilidades tão logo elas sejam identificadas, garantindo a implementação da correção de forma mais eficiente e menos onerosa antes do software ser colocado em produção.

Ademais, a automatização dos testes de segurança assegura que toda atualização ou alteração no software seja imediatamente verificada para aferir a sua aderência às normas de segurança. No contexto militar, onde as ameaças cibernéticas se desenvolvem continuamente, é essencial que as atualizações de sistemas sejam realizadas de maneira rápida e segura, preservando a estabilidade e a integridade das operações.

2.4.3 Gestão de incidentes cibernéticos

A gestão de incidentes cibernéticos é outro elemento fundamental para as operações da FAB. Devido à importância crítica dos sistemas militares, é imprescindível adotar uma estratégia proativa na resposta a incidentes, com planos de contingência claramente estabelecidos e que unam as equipes de desenvolvimento e operações, seguindo os princípios do DevSecOps. Esta estratégia fomenta uma cooperação constante entre programadores e operadores, possibilitando a rápida detecção e neutralização de ameaças.

A gestão de incidentes cibernéticos na Força Aérea Brasileira deve transcender a simples identificação de ataques. É preciso criar processos que possibilitem a identificação ágil de vulnerabilidades de segurança, a avaliação de seu efeito nas operações e a execução de ações corretivas imediatas. Isso exige uma estrutura de supervisão constante, apta a identificar comportamentos atípicos nos sistemas em tempo real e emitir alertas para que as equipes encarregadas possam agir de forma célere.

Além disso, é primordial que os sistemas da FAB possuam resiliência cibernética, o que implica que, em caso de incidente, possam continuar operando com

segurança em níveis mínimos até que as falhas sejam resolvidas. Para tal, a Força Aérea Brasileira pode implementar estratégias como a segmentação de redes, isolamento de serviços e redundância de sistemas críticos, assegurando que as atividades militares não sejam interrompidas em situações de crise.

2.4.4 Treinamento constante

Finalmente, uma das medidas mais fundamentais para assegurar a proteção dos sistemas da FAB é a capacitação contínua das equipes de desenvolvimento e operações, pois o cenário cibernético é mutável e as ameaças se modificam constantemente. Isso requer que as equipes se mantenham constantemente informadas sobre as melhores práticas de segurança, além das mais recentes técnicas de ataque e defesa.

O adestramento constante pode envolver a execução de simulações de ataques cibernéticos e exercícios práticos com o fito de que as equipes adquiram habilidades para enfrentar variados cenários de perigo. As simulações de ataques de negação de serviço (DDoS), phishing e ransomware podem capacitar os especialistas para reconhecer e neutralizar ameaças reais de maneira mais eficiente. Ademais, capacitações nas técnicas mais modernas de desenvolvimento seguro, tais como codificação defensiva, práticas de revisão de código seguro e políticas de gestão de vulnerabilidades, são fundamentais para preservar a integridade dos sistemas criados pela FAB.

Destarte, no âmbito militar, onde a segurança é essencial para a realização das operações, investir no treinamento dos profissionais não é apenas uma prática adequada, mas uma exigência estratégica.

3 CONSIDERAÇÕES FINAIS

Este ensaio evidenciou a relevância de métodos seguros para o desenvolvimento de software no âmbito da Força Aérea Brasileira (FAB), enfatizando a necessidade de adaptar as práticas mundiais de segurança cibernética ao contexto militar. Conforme as operações da FAB dependem cada vez mais de sistemas tecnológicos sofisticados, a criação de softwares seguros não é somente um fator de eficiência operacional, mas também um elemento estratégico fundamental para a segurança do país. A defesa de sistemas críticos, tais como os empregados no gerenciamento do tráfego aéreo,

comando e controle de operações militares e comunicações seguras, está diretamente ligada à implementação de metodologias que incorporem a segurança em todas as etapas do ciclo de vida do desenvolvimento de software.

O DevSecOps se apresenta como uma metodologia promissora para a FAB, sobretudo pela sua metodologia que combina desenvolvimento, segurança e operações de maneira ininterrupta e automatizada. Esta abordagem possibilita a inclusão de segurança desde o começo do processo de desenvolvimento, reduzindo riscos e vulnerabilidades antes mesmo da implementação do software. No âmbito militar, onde a segurança de dados classificados e a integridade de sistemas de missão críticas são fundamentais, a automação de procedimentos de segurança se torna primordial para assegurar a atualização constante do software e a defesa contra as ameaças mais recentes.

A implementação do DevSecOps na FAB proporciona diversos benefícios, principalmente quando associada a práticas inflexíveis de metodologias convencionais, como o Waterfall. Essa combinação resulta em um framework híbrido que harmoniza a rapidez e automação com a exigência de rigor e aderência aos padrões de segurança previamente definidos. Enquanto o DevSecOps possibilita respostas ágeis a novas ameaças e a incorporação de segurança em ciclos de desenvolvimento reduzidos, o Waterfall assegura uma validação mais rígida para sistemas de maior complexidade e requisitos estáveis, garantindo que cada etapa seja cuidadosamente verificada antes de avançar para a próxima. A combinação dessas metodologias é especialmente benéfica em projetos militares, onde a adaptabilidade para gerir novos riscos deve estar em harmonia com o rigor requerido em sistemas de alta criticidade.

Ademais, a aplicação desse framework híbrido na FAB precisa estar em sintonia com a capacitação constante das equipes de desenvolvimento e operações. O cenário cibernético é dinâmico e está em constante transformação, apresentando novas ameaças com frequência. Portanto, as equipes devem estar aptas a lidar com essas modificações e implementar as melhores práticas de segurança na criação de sistemas. Programas de treinamento, que reproduzem situações reais de ataques cibernéticos, são essenciais para que os profissionais da FAB possam reconhecer e minimizar os riscos de maneira eficaz e proativa. A proteção de sistemas militares não

se limita apenas às tecnologias empregadas, mas também à instrução e à experiência dos especialistas encarregados de seu desenvolvimento e manutenção.

Outro aspecto importante discutido no ensaio foi a automação de procedimentos de segurança, essencial para a FAB, principalmente ao lidar com grandes quantidades de código e sistemas de alta complexidade. A automação possibilita a análise automática de cada nova linha de código em busca de vulnerabilidades, diminuindo o tempo necessário para a identificação de erros e potencializando a eficácia dos times de segurança. No contexto militar, onde a agilidade e a exatidão são fundamentais, a automação de testes de segurança se apresenta como um recurso eficaz para assegurar que os sistemas desenvolvidos estejam sempre em sintonia com os mais rigorosos padrões de segurança.

Além os benefícios oriundos do DevSecOps e das metodologias ágeis, a gestão de incidentes cibernéticos na FAB também se beneficia com a adoção desse modelo híbrido. Ao integrar continuamente as equipes de desenvolvimento e operações, a FAB pode reagir de forma mais ágil e eficiente a incidentes de segurança, reduzindo o efeito de eventuais ataques. A aplicação de planos de contingência bem delineados e a implementação de monitoramento contínuo possibilitam que a FAB conserve seus sistemas operacionais, mesmo diante de incidentes severos, assegurando a manutenção das operações críticas em períodos de crise.

Destarte, este ensaio enfatizou a necessidade de pesquisas futuras que analisem mais profundamente a implementação de métodos seguros de desenvolvimento de software no cenário militar do Brasil. Apesar de práticas contemporâneas, como o DevSecOps e métodos ágeis, terem demonstrado um grande potencial para aprimorar a segurança e a eficácia no desenvolvimento de sistemas militares, ainda há muito a ser pesquisado sobre como essas metodologias podem ser especificamente ajustadas para atender às especificidades das Forças Armadas do Brasil. A integração com sistemas de defesa estrangeiros, a incorporação de tecnologias emergentes, como a inteligência artificial e a Internet das Coisas (IoT), e a defesa de infraestruturas críticas são apenas alguns dos tópicos que requerem uma avaliação mais detalhada.

O progresso das ameaças cibernéticas mundiais, aliado ao aumento da dependência da FAB em tecnologias digitais, torna imprescindível o aprimoramento constante das práticas de desenvolvimento seguro de software. O estudo e a criação

de novas metodologias, juntamente com um entendimento aprofundado das demandas militares do Brasil, são fundamentais para assegurar que a FAB esteja apta a lidar com os desafios futuros. Assim, sugere-se que pesquisas futuras incluam a avaliação de novas soluções tecnológicas, bem como o desenvolvimento de frameworks customizados que incorporem as melhores práticas mundiais às particularidades da defesa nacional.

Nesta senda, a adoção de métodos seguros de desenvolvimento, como o DevSecOps, aliada a treinamentos contínuos e à automatização de processos, é fundamental para que a FAB prossiga no desenvolvimento de sistemas eficientes, defendendo a soberania do país e assegurando o êxito das operações aéreas e cibernéticas. O rumo para um desenvolvimento seguro envolve a constante adaptação às ameaças emergentes, assegurando que as Forças Armadas estejam sempre na vanguarda da defesa cibernética.

REFERÊNCIAS

BELL, Laura et al. ***Agile Application Security:*** *Enabling Security in a Continuous Delivery Pipeline*. Estados Unidos da América: O'Reilly Media, 2017.

BUTLER, Nick. ***Security in Agile Software Development:*** *a simple guide*. Disponível em: https://www.boost.co.nz/blog/2022/02/security-in-agile-software-development. Acesso em 10 OUT 2024.

DIAS, Eduardo R. ***Coding for Security*****:** Guia completo para desenvolvimento seguro. São Paulo: Novatec, 2023.

KIM, Gene et al. **Manual de DevOps:** como obter agilidade, confiabilidade e segurança em organizações tecnológicas. Rio de Janeiro: Alta Books, 2021.

OLIVEIRA, Tiago Cavalcanti de. **Desenvolvimento Seguro:** O guia definitivo. Recife: Independently published, 2022.

OPPOSIT INT. ***Latest FAFe 6 Scaled Agile Framework in Depth*****.** EUA: Independently publised, 2024.

PRESSMAN, Roger S.; MAXIM, Bruce R. **Engenharia de Software:** Uma abordagem profissional. 9. ed. Porto Alegre: AMGH, 2021.

SOMMERVILLE, Ian. **Engenharia de Software**. 10. ed. São Paulo: Pearson Education Brasil, 2018.