Segurança da Informação para Ambiente Híbrido – uma Aplicação do DevSecOps

Sara B. O. Gennari Carturan[1], Denise H. Goya[2]
[1]Programa de Pós-Graduação em Ciência da Computação, [2]Centro de Matemática, Computação e Cognição
Universidade Federal do ABC (UFABC)
sarabogcarturan@gmail.com, denise.goya@ufabc.edu.br

Abstract: O DevSecOps (ou SecDevOps) apresenta uma abordagem para o processo de implementação de mudanças no ambiente de produção, além de incorporar práticas de segurança da informação a um ambiente de TI e de promover a colaboração entre as equipes de desenvolvimento e de operações considerando o ciclo de vida de uma demanda. Também pretende promover automação dos processos de TI para que o desenvolvimento das aplicações e/ou serviços seja rápido e seguro. Porém existe uma carência de detalhamento nas definições dos processos para orientar a implementação e uso do DevSecOps em um ambiente de TI, principalmente quando se intenciona mesclar computação em nuvem a infraestruturas convencionais preexistentes. O presente trabalho tem o objetivo de apresentar resultados obtidos na implementação de alguns processos de TI e de Governança seguindo padrões DevSecOps em uma instituição financeira brasileira de grande porte.

1. Introdução

A Computação em ambiente Cloud é muito mais abrangente do que adotar padrões, políticas, provedores remotos, serviços, etc. Existe um leque de oportunidades para o ambiente computacional, influenciando o Modelo Operacional da TI, sua Arquitetura de Referência, Infraestrutura, Governança, metodologia de desenvolvimento de soluções, relacionamento com as áreas de Negócio, entre outras áreas. Em muitos casos, o ambiente Cloud se integra com o ambiente tradicional de TI existente. Desta forma, o ambiente híbrido apresenta muitos desafios e ao mesmo tempo oportunidades de inovação com identificação de riscos e procedimentos de Segurança da Informação [1,2,3]. O conceito está baseado na automação dos processos e fluxo contínuo [4]. Os principais benefícios de um ambiente Cloud são escalabilidade no Negócio, adaptabilidade ao mercado, flexibilidade nos custos, extensão dos Processos de TI, personalização orientada ao cliente e integração de ambientes [5,6,7].

Para a construção deste Modelo de TI deve-se considerar as práticas DevOps, que é um método de desenvolvimento de software que enfatiza a colaboração entre os desenvolvedores de Software (Desenvolvimento) e os profissionais de Tecnologia e Infraestrutura de TI (Operações) de forma a diminuir o tempo de desenvolvimento sem, no entanto, impactar na qualidade e segurança da informação, o que chamamos de DevSecOps ou SecDevOps [8,14].

Este trabalho apresenta as principais dificuldades enfrentadas e conclusões obtidas durante o processo de implementação de mudanças em processos de TI, de governança e de Segurança da Informação para transformar um ambiente tradicional de TI em híbrido.

2. Conceitos DevSecOps

O DevSecOps busca alcançar vários benefícios, mas para isto é necessário integrar alguns sistemas legados aos ambientes Cloud, governança e garantir que todos os envolvidos tenham o conhecimento e comportamento adequado do DevSecOps [6], o que depende de se possuir uma tecnologia integrada aos sistemas, não importando se eles estão em diferentes plataformas [3]. Além disto, estes sistemas devem ser compatíveis com os sistemas de seus clientes, fornecedores, terceiros e parceiros. O DevSecOps é a base para a estruturação das necessidades do ambiente Nuvem e o método ágil para o desenvolvimento de aplicações para Cloud [5, 6, 7]. Assim, o DevSecOps está frequentemente associado aos conceitos de desenvolvimento ágil de software, de entrega contínua e segurança [9,10,11].

O DevOps é a contração dos termos Development and Operations, sendo um conjunto de práticas que visa diminuir o tempo de desenvolvimento de uma mudança de uma aplicação e o tempo de esta ser transferida para o ambiente de produção, mantendo a qualidade do software em termos de código e de mecanismos de entrega [3]. Para que as práticas DevOps possam ser implementadas deve-se preferir padrões abertos, flexíveis, confiáveis, com código fonte

extensível o qual permitirá que as soluções sejam compatíveis e com características de escalabilidade para poderem evoluir no futuro [10,15].

A proposta do DevSecOps é ter um fluxo sempre constante envolvendo todo o processo: planejamento, desenvolvimento e testes com processo de qualidade, implementação seguindo um pipeline de entrega e operação (monitoração e feedbacks de usuários). O objetivo deste fluxo é permitir a rápida reação por parte do Negócio a mudar seu planejamento e execução, caso necessário deixando-o mais aderente aos *feedbacks* [6,15].

O foco do DevSecOps é uma implantação rápida, melhoria contínua, foco na automação, colaboração e *feedbacks* [8, 10, 11, 12]. A equipe de segurança deve ser envolvida o mais rápido possível desde o início para garantir que a comunicação ocorra no momento certo e que a habilidade de entrega seja contínua [9, 13, 14]. No entanto, para esse envolvimento de especialistas em segurança, os processos documentados na literatura científica não são adequadamente completos, nem são claros sobre como os variados modelos existentes devem ser adaptados ao contexto de cada organização, modelo de negócio, área de atuação ou porte e complexidade dos sistemas [1, 13]. Ainda, do lado dos gestores, há grande dificuldade em avaliar *status* do projeto de forma atualizada, gestão de defeitos, monitoração de indicadores antes que as implantações ocorram para que ações preventivas possam ser tomadas para proteger o ambiente produtivo de uma organização. Também é imprescindível avaliar resultados e retornos durante e depois das implementações para que o processo de *feedback* ocorra e propicie a melhoria contínua [1, 4].

3. Metodologia

Foi elaborada a proposta de um novo Modelo Operacional de TI, respectivos processos e direcionadores de segurança, a serem detalhados na próxima Seção. Para tanto, foi definido um plano estratégico de implementação do modelo híbrido de TI envolvendo alguns pontos focais representantes das áreas envolvidas de TI. Posteriormente foi elaborado um planejamento detalhado das mudanças e neste ponto a equipe de envolvidos cresceu, inclusive com envolvimento das áreas de negócio. Finalmente iniciou-se a implementação com monitoramento profundo e rápidos ajustes, quando se fizeram necessário. Criou-se um comitê de decisões gerenciais para dar a agilidade necessária. A implementação dos processos de TI foi de forma paralela, gradual e considerando pré-requisitos, para garantir pequenas, porém constantes, implementações. A coleta de *feedbacks* foi importante para dar a velocidade possível de tal forma a não impactar os processos de TI atuais.

4. DevSecOps e o Modelo Operacional de TI Proposto

O Modelo Operacional de TI é o alicerce para a jornada de transformação, conforme proposto na Figura 1. Este modelo contempla desde a identificação da demanda de TI, desenvolvimento da solução até sua efetiva entrega no ambiente produtivo. Para suportá-lo, também são necessários os processos de TI e os aspectos de segurança, como: Usuário, Aplicação, Ambiente, Informação, Monitoração para abordar os quesitos de segurança do modelo DevSecOps. A partir deste ponto, devem ser definidos os direcionadores de Segurança, modelo de governança de TI Híbrida e arquitetura de referência necessários ao ambiente híbrido de TI. Deverá ser tomada atenção para não duplicar processos conforme seus ambientes de origem e consequentemente dificultar a manutenção do mesmo.

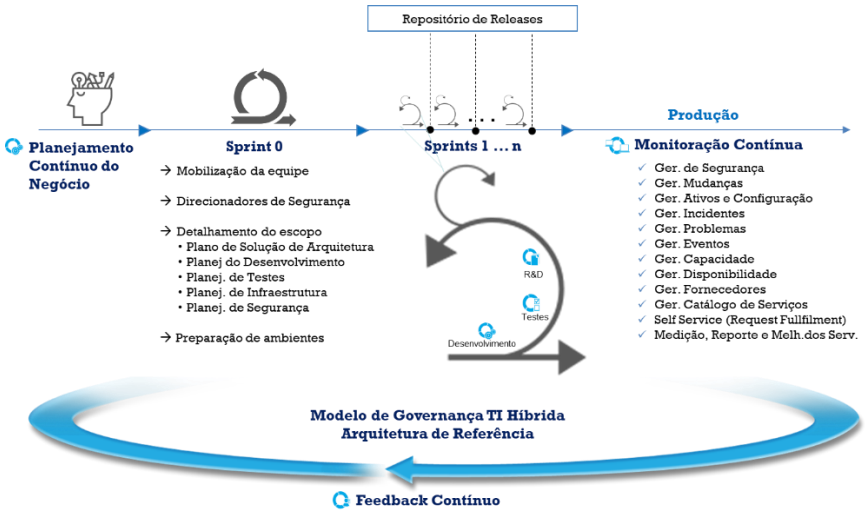

Fig. 1: Modelo Operacional de TI Proposto
Fonte: Elaborado pelo autor baseado nos conceitos DevSecOps, ITIL e metodologia de desenvolvimento ágil

5. Resultados preliminares

Durante a implementação da metodologia proposta e implantação do novo Modelo Operacional de TI (Figura 1), chegou-se a conclusões preliminares que são sintetizadas a seguir.

A transformação do modelo tradicional de TI para um modelo híbrido possui várias dimensões de atuação.

Visão Estratégica: para a transição ao modelo híbrido de TI deve ser definida uma estratégia que identifique todos os projetos necessários e os priorize segundo a respectiva geração de valor ao Negócio e pré-requisitos tecnológicos. Também deverão ser identificadas as aplicações apropriadas para o ambiente Cloud e/ou as de possível migração, juntamente com uma análise quanto ao custo de redesenho e arquitetura. Os direcionadores de Segurança e a gestão de riscos propiciarão integridade de dados e continuidade operacional. A existência de uma metodologia fim-a-fim, que aborde desde a estratégia à implementação e a gestão de projetos complexos de transformação apoiará os processos de Governança de TI. O modelo híbrido de TI requer algumas decisões iniciais, como: Desenvolver novas aplicações já preparadas para Cloud ou migrar aplicações existentes? Como e onde gerenciar os dados: localização, retenção, criptografia e arquivamento. Como aproveitar o "portfólio de infraestrutura"? Como estender as estruturas tradicionais de integração de TI para os ambientes de nuvem?

Segurança da Informação: rever e adaptar a segurança para a TI Híbrida, através de direcionadores, da mobilização das equipes de Segurança e da administração de segurança para o ambiente híbrido com gestão de acessos (usuários, privilégios, clientes), segurança de redes (monitoração de anomalias, correlação e alerta de eventos e proteção contra ameaças), proteção de dados (base de dados, workloads, conteúdo), segurança de aplicações (desenvolvimento de App seguro, avaliação de vulnerabilidades, gestão de atualizações) e carga de trabalho centrada (gestão de Segurança e DevSecOps). É fator crítico de sucesso que as equipes considerem a área de Segurança da Informação como um agente viabilizador do modelo híbrido de TI, seguindo os padrões requeridos.

Governança da TI Híbrida: deve atuar para garantir a gestão do modelo, mantendo e evoluindo as metodologias e os modelos de Arquitetura de Referência para Cloud com seus princípios e padrões, alinhando as ações requeridas pela Segurança da Informação no ambiente Cloud e questões de Auditoria e Jurídico, além de fomentar a melhoria contínua. Também deverá adquirir, aprofundar e/ou disseminar conhecimento nas tecnologias utilizadas pelo ambiente Cloud provendo quando necessário a investigação em tecnologias emergentes, melhores práticas, além do suporte em questões mais operacionais, coleta de indicadores, elaboração de relatórios, etc.

Processos de TI: a adequação dos processos de TI para o ambiente híbrido representa uma Jornada de Transformação. Eles devem ser alterados gradativamente para não impactar o ambiente atual e também para ganhar maturidade de implementação. Todos os processos devem ter suas políticas e princípios adequados ao modelo híbrido, bem como seus papéis e responsabilidades revisados e adequado conforme necessidades do modelo híbrido. As ferramentas atuais devem ser revisadas segundo as necessidades futuras do modelo híbrido e sempre que possível, devem ser reaproveitadas. Deve-se tomar cuidado em não proliferar desnecessariamente ferramentas, pois além dos custos, dificulta a manutenção e operação.

A metodologia de desenvolvimento e os artefatos devem ser revisados e adaptados para os conceitos de desenvolvimento ágil. Os tipos de testes devem ser revistos e identificados os elementos-chave para a realização de testes contínuos. Os ambientes de testes também devem ser adaptados às necessidades do modelo híbrido.

Para os processos de TI voltados a operação, os itens de configuração devem ser identificados para o ambiente híbrido, com atualização automática do CMDB (*Configuration Management Database*). O processo de gestão de mudanças deve ser adaptado ao modelo de Sprints e devem ser definidas as mudanças pré-aprovadas a fim de dar a agilidade necessária. Também devem ser definidos as categorias de incidentes que serão abertos automaticamente, com acompanhamento de indicadores. O processo de Gestão de Capacidade deve contemplar a medição automatizada da capacidade de Servidores e do tráfego de redes. O catálogo de serviços deverá ser atualizado com os serviços do ambiente híbrido, contemplando o procedimento para criação do serviço no Catálogo. As ferramentas de monitoração devem contemplar as solicitações de monitoração no ambiente híbrido.

Processos & Cultura: é imprescindível para o bom andamento do projeto a identificação das pessoas corretas e no momento adequado para a formação de grupos representativos e necessários às decisões e detalhamentos. Deverá ser garantido que as competências e recursos adequados possuam a expertise correta e as tecnologias necessárias disponibilizadas.

Estas ações fazem parte de um processo contínuo de transformação devendo ser alimentado com feedbacks e revisões contínuas do plano estratégico de implementação.

6. Conclusão

Foi apresentada uma proposta de Modelo Operacional de TI com base no DevSecOps, ITIL e desenvolvimento ágil, para adaptação dos processos preexistentes a um novo ambiente híbrido com computação em nuvem. Resultados e conclusões preliminares sobre a implantação do modelo foram sumarizados. Como trabalho futuro, pretende-se

detalhar e documentar o Modelo, bem como desenvolver métricas para avaliação de resultados ao longo e ao final de sua implantação, em corporações de variados porte, setores e modelos de negócio.

7. Referências

[1] H Myrbakken; R Colomo-Palacios. *DevSecOps: A Multivocal Literature Review. Proceedings of Software Process Improvement and Capability Determination*, in 17th International Conference, SPICE 2017. CCIS vol. 770, 2017.

[2] A Balalaie; A Heydarnoori; P Jamshidi. Microservices Architecture Enables DevOps: Migration to a Cloud-Native Architecture. IEEE Software (Volume: 33, Issue: 3, May-June 2016, p. 42-52)

[3] L. Riungu-Kalliosaari; L. E. Lwakatare; S. Makinen T. Männistö. DevOps Adoption Benefits and Challenges in Practice: A Case Study. Product-Focused Software Process Improvement: 17th International Conference, PROFES 2016, Trondheim, Norway, November 22-24, 2016, Proceedings (pp.590-597).

[4] M. K. Aljundi. Tools and Practices to Enhance DevOps Core Values. Dissertação de Mestrado. Lappeenranta University of Technology - School of Business and Management - Degree Program in Computer Science.

[5] L. E. Lwakatare, P. Kuvaja, and M. Oivo, "Dimensions of DevOps," in 16th International Conference on Agile Software Development (XP). Springer International Publishing, 2015, pp. 212–217.

[6] Reid, J. (2014). DevOps in Practice. Retrieved from O'Reilly

[7] L. E. Lwakatare, P. Kuvaja, M. Oivo. Relationship of DevOps to Agile, Lean and Continuous Deployment A Multivocal Literature Review Study. Proceeding of Product-Focused Software Process Improvement, 17th International Conference, PROFES 2016. Lecture Notes in Computer Science LNCS 10027, pp. 399-415. Springer International Publishing.

[8] J. Davis; R. Daniels. Effective DevOps - Building a Culture of Collaboration, Affinity, and Tooling at Scale. Publisher: O'Reilly Media, Inc. June 2016 [eBook]

[9] E. Belis (2015, November). DevOps Enterprise Summit 2015 (DOES15) Ed Bellis Kenna Cofounder & CTO - Security as Code A SecDevOps Use Case [Video file].

[10] S. K. Bang; S. Chung; Y. Choh, M.Dupuis. A Grounded Theory Analysis of Modern Web Applications - Knowledge, Skills, and Abilities for DevOps. Proceedings of the 2nd annual conference on Research in information technology (RIIT '13). ACM, New York, NY, USA, 61-62.

[11] F. M. A. Erich; C. Amrit; M. Daneva. 2017. A qualitative study of DevOps usage in practice. J. Softw. Evol. Process 29, 6 (June 2017), n/a-n/a. DOI: https://doi.org/10.1002/smr.1885

[12] A. P. Magalhães; A. Andrade; R. S. Maciel. 2016. A Model Driven Transformation Development Process for Model to Model Transformation. In Proceedings of the 30th Brazilian Symposium on Software Engineering (SBES '16), Eduardo Santanda de Almeida (Ed.). ACM, New York, NY, USA, 3-12.

[13] B. B. N. França; H. Jeronimo Jr; G. H. Travassos. 2016. Characterizing DevOps by Hearing Multiple Voices. In Proceedings of the 30th Brazilian Symposium on Software Engineering (SBES '16), Eduardo Santanda de Almeida (Ed.). ACM, New York, NY, USA, 53-62. DO

[14] V. Mohan; L. B. Othmane SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps. In 2016 11th International Conference on Availability, Reliability and Security (ARES).

[15] SHARMA, Sanjeev; COYNE, Bernie. DevOps For Dummies, 3a. Edição Limitada IBM., 2017 [eBook].