Validação do Software: Testes de Software e Aplicações de Segurança no Sistema

Procedimentos para garantir a segurança do software

Bloco 1

Luís Otávio Toledo Perin

Objetivos de aprendizagem

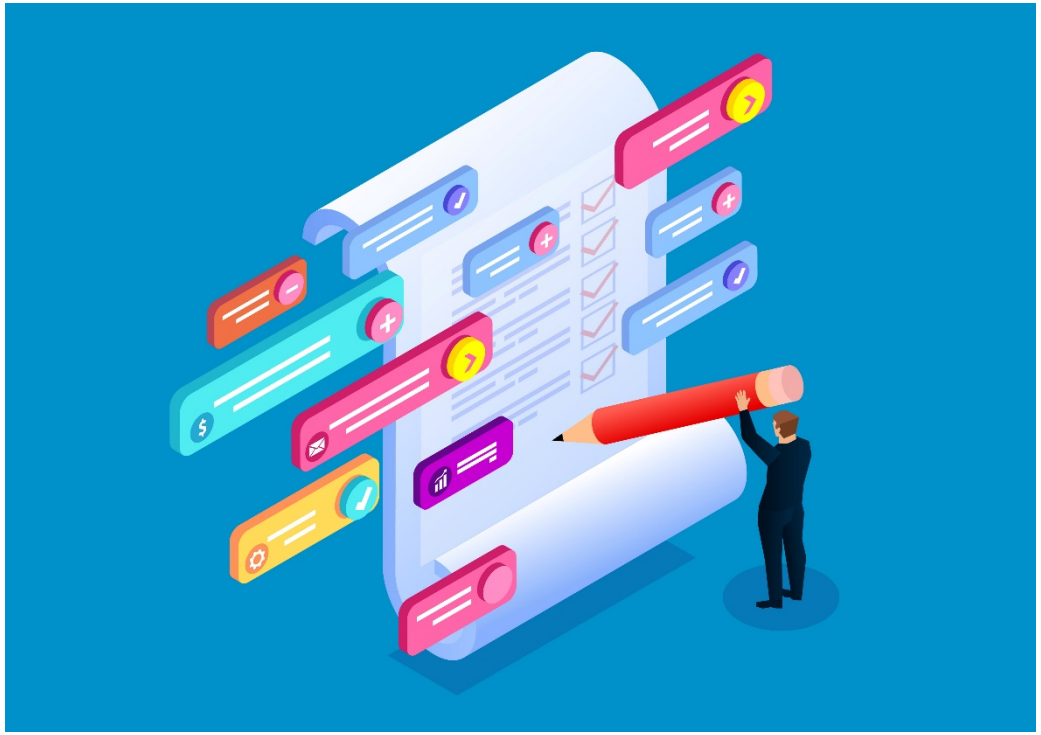
1. Definir o que é segurança de software.
2. Compreender o processo de segurança de software.
3. Apresentar normas de segurança de software.

COMPREENDA O QUE VOCÊ DEVE SABER E ATÉ ONDE DEVE ESTUDAR NESTE BLOCO.

Algumas perguntas para refletir...

- O que essa imagem representa? **Segurança? Teste? Qualidade?**
- Segurança no software é importante? O que vem a sua mente?
- Processo isolado ou alinhado a outro?

Figura 1 – Validação processos



Fonte: sesame/iStock.com.

Devemos pensar...

- No produto?
- Em sua utilização?
- Benéfico para o ambiente ou o negócio?

Qualidade e segurança...

Figura 3 – Reunião trabalho

Fonte: monkeybusinessimages/iStock.com.

- Caminhar lado a lado.
- Técnicas e métricas bem aplicadas.
- Gestão da qualidade e quesito segurança!
- Usabilidade final do produto.

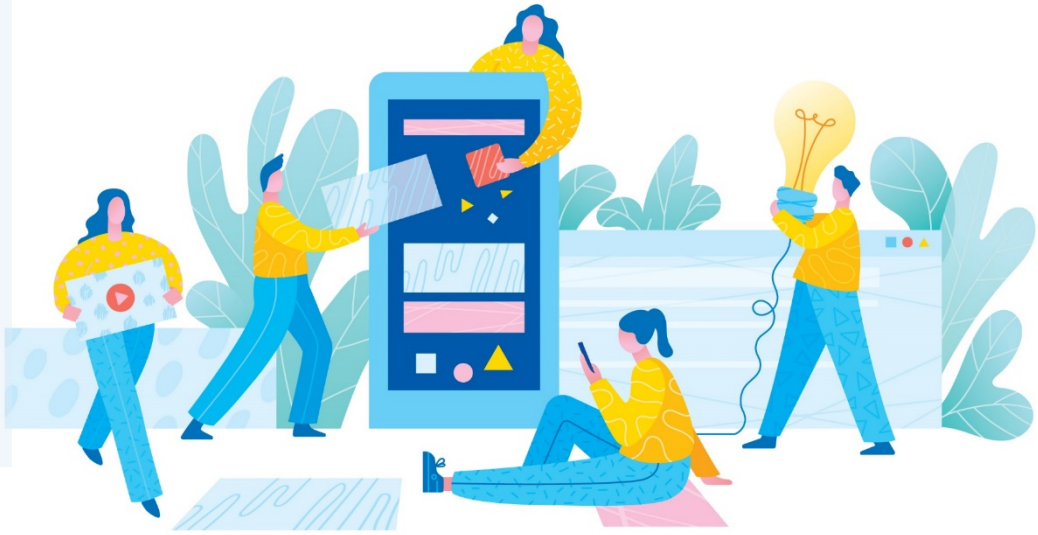
Para Gary McGraw (2005, p. 369):

“A segurança de software se relaciona inteira e completamente à qualidade. Devemos nos preocupar com a segurança, a confiabilidade, a disponibilidade e a dependência — nas fases inicial, de projeto, de arquitetura, de testes e de codificação, ao longo de todo o ciclo de vida [qualidade] de um software”.

Padrões, métricas e métodos...

- Caminhar lado a lado
- Técnicas e métricas bem aplicadas
- Gestão da qualidade e quesito segurança!
- Usabilidade final do produto.

Figura 3 – Software pensado



Fonte: miakievy/iStock.com.

A metodologia...

Figura 4 – Metodologia pensada

Fonte: Bigmouse108/iStock.com.

- Qual a melhor metodologia ou prática de segurança a ser escolhida?
- NBR ISO/IEC 27001.
- NBR ISO/IEC 27002.
- ISO/IEC 15408.

Para Ferreira e Araújo (2008):

“São várias as possibilidades e depende da necessidade da empresa em selecionar qual será a que melhor se adeque ao modelo de negócio trabalhado. Outro fator que deve ser levado em consideração na escolha, diz respeito a tecnologia empregada, já que este é um fator muito flutuante, haja vista que há atualizações constantes nesta área”.

Procedimentos para garantir a segurança do software

Bloco 2

Luís Otávio Toledo Perin

NBR ISO/IEC 27001 e NBR ISSO/IEC 27002

Figura 5 – Controle software

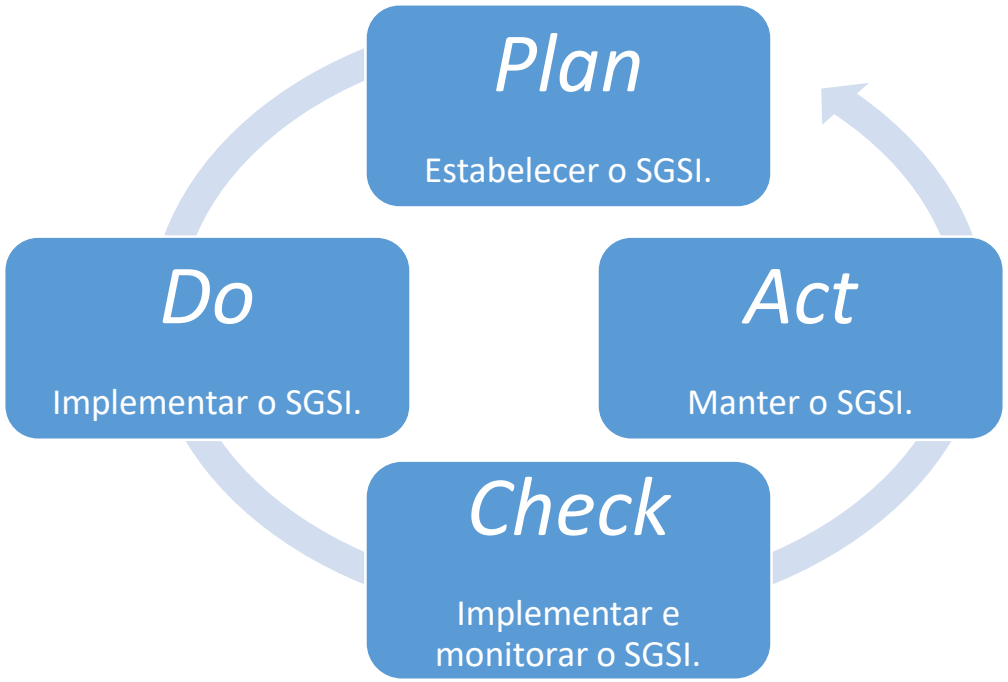
Fonte: ilyast/iStock.com.

- Em conjunto – completo padrão da segurança da informação.
- Normas e controles internacionais.
- Aperfeiçoamento do processo.

ISO/IEC 27001

- Ciclo PDCA (*Plan-Do-Check-Act*).
- Resultado: ISMS (*information security management system*) ou SGSI (sistema de gestão de segurança da informação).
- Planejamento preciso e confiável.

Figura 6 – SGSI



Fonte: do autor.

Procedimentos para garantir a segurança do software

Bloco 3

Luís Otávio Toledo Perin

ISO/IEC 15408

- Documento norteador – *common criteria.*
- Conjuntos de critérios fixos.
- Avaliação que determine o nível de segurança – sete níveis (EAL).

- EAL 1: funcionalmente testado.
- EAL 2: estruturalmente testado.
- EAL 3: metodicamente testado e verificado.
- EAL 4: metodicamente projetado, testado e verificado.
- EAL 5: semi-formalmente projetado e testado.
- EAL 6: semi-formalmente projetado, testado e verificado.
- EAL 7: formalmente projetado, testado e verificado.

Modelo SDL

- Foco na segurança.
- Microsoft.
- Modelo denominado SDL (*Security Development Lifecycle*).
- Atividades e produtos com foco no software seguro - durante a fase de desenvolvimento do software.

Modelo SDL

Quadro 1 – Processo de desenvolvimento SDL da Microsoft

Training	*Requirements*	*Design*	*Implementation*	*Verification*	*Release*	*Response*
Core Security Training	▪ *Establish Security Requirements.* ▪ *Create Quality Gates / Bug Bars.* ▪ *Security & Privacy Risk Assessment.*	▪ *Esblish Design Requirements.* ▪ *Analyze Attack Surface.* ▪ *Threat Modeling.*	▪ *Use Approved Tools.* ▪ *Deprecate Unsafe Functions.* ▪ *Static Analysis.*	▪ *Dynamic Analysis.* ▪ *Fuzz Testing.* ▪ *Attack Surface Review.*	▪ *Incident Response Plan.* ▪ *Final Security Review.* ▪ *Release Archive.*	▪ *Execute Incident Response Plan.*

Fonte: elaborado pelo autor.

Modelo SDL

- Treinamento de segurança.
- Requisitos.
- Design.
- Implementação (codificação segura).
- Verificação.
- Release (liberação de versões).
- Resposta.

Procedimentos para garantir a segurança do software

Bloco 4

Luís Otávio Toledo Perin

Reflita sobre a seguinte situação

Imagine que você já seja **formado na área de T.I. há algum tempo**, assim como **trabalha** na **mesma empresa a cerca de dez anos**, e também sabe das tecnologias utilizadas e tem domínio sobre o ciclo de desenvolvimento de software dela. Sabe-se, ainda, que **a empresa não** se **utiliza** de **práticas** bem definidas **sobre a análise, planejamento e criação dos produtos** que são ofertados aos clientes. Como a cidade que reside é de porte médio e você tem conhecidos em outras empresas do mesmo setor, **fica sabendo de ataques de crackers sobre sistemas de concorrentes**, mas que trabalham com a mesma tecnologia e situação de desenvolvimento que a empresa que trabalha. Diante desta situação, **qual seria a atitude que você tomaria**, sabendo que um ataque da mesma magnitude pode ocorrer a qualquer momento?

Norte para a resolução...

- Solicitar uma reunião e expor o que está havendo com as outras empresas.
- Propor análise da situação atual.
- Elencar principais falhas.
- Averiguar melhor e, se necessário, implementar nova metodologia.

Dica do Professor

Bloco 5

Luís Otávio Toledo Perin

Dica do professor

- Como visto acima, devemos nos preocupar com a segurança do software ofertado, uma vez que o usuário está confiando na aplicação e, deste modo, falhas devem ser evitadas ao máximo, já que a confiança pode ser abalada!

- Neste sentido, manter-se informado de técnicas e práticas, bem como participar de comunidades e fóruns na web que tratam do assunto é de vital importância.

- O site “micreiros.com.br” faz parte deste ambiente tecnológico e seguro, além de sempre possuir material atualizado sobre diversos temas. Como indicação, o artigo ***Boas Práticas para Desenvolvimento de Softwares seguros*** vem ao encontro com o nosso assunto, trazendo várias dicas para enriquecer seu conhecimento. Vale a pena conferir!

Referências

FERREIRA, Fernando N. F.; ARAÚJO, Márcio T. de. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. 2. ed. rev. Rio de Janeiro: Editora Ciência Moderna, 2008.

MCGRAW, G. **Bridging the gap between software development and information security**. IEEE Security and Privacy, 2005.

PRESSMAN, Roger S. **Engenharia de software:** uma abordagem profissional. 7. ed. Porto Alegre: AMGH, 2011.

Bons estudos!