Aula 6

Segurança em Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

Segurança dos Sistemas e do *Software* em Geral

Agenda

- Desenvolvimento e teste
- Operação e manutenção
- Gestão de configuração e mudanças
- Dispositivos móveis
- Internet das coisas

Contextualizando

- A dependência da segurança dos sistemas
- A segurança da informação:
  - no ciclo de vida do *software*
  - na computação móvel
  - na internet das coisas

Desenvolvimento e Teste

- Modelos
  - Cascata
  - Iterativo
  - RAD
  - UP
  - Espiral
  - Ágeis
- Teste de *software*

- O processo de desenvolvimento de *software* deve considerar os riscos à segurança da informação. Ele próprio, porém, pode representar novos riscos advindos:

- do ambiente
- de componentes
- das ferramentas
- da complexidade
- da maturidade
- etc.

- Portanto, é necessário planejar etapas de teste com base nos riscos identificados. O cuidado no desenvolvimento e o teste são fatores que influenciam diretamente:

- a qualidade do SW
- a tolerância às falhas
- a reação às ameaças
- a SegInfo

- Os modelos de desenvolvimento podem facilitar a abordagem da segurança da informação, na medida da ênfase de cada fase do processo

- Isso não significa que um modelo seja melhor do que outro, mas que pode ser mais adequado face às características do *software*, do projeto e até mesmo da maturidade do time de desenvolvimento

- Para o modelo cascata:
  - ☑ ênfase no planejamento
  - ☑ definição das entregas

- ☑ documentação formal e abrangente
- ☒ avaliação total e efetiva só é possível no final do processo
- ☒ dificuldade de incorporar o gerenciamento de riscos em projetos de maior porte

- Para o modelo iterativo:
  - ☑ identificação de problemas na especificação de requisitos
  - ☑ permite correções e mudanças durante quase todo o ciclo

- ☒ pode ser difícil particionar o *software* de modo funcional
- ☒ revisões, mudanças e várias integrações podem trazer novos erros e falhas

- Para o modelo RAD:
  - ☒ a excessiva simplificação pode deixar falhas latentes
  - ☒ a pressão por resultados é um fator crítico que pode resultar em falhas

- ☒ a necessidade de pessoal altamente especializado limita a visão crítica
- ☒ o custo de pessoal pode limitar a disponibilidade de profissionais de SegInfo

- Para o modelo do processo unificado (RUP):
  - ☑ a orientação a objetos auxilia o processo de modelagem, construção e validação
  - ☑ o uso de componentes de *software* reduz o risco e simplifica o teste

- ***softwares*** **mais complexos podem apresentar falhas na integração**
- **a gestão de configuração durante o ciclo torna-se um fator crítico**

- **Para o modelo espiral:**
  - **a evolução da maturidade é natural e acompanha o ciclo de desenvolvimento**
  - **as mudanças acontecem com base na confiabilidade das entregas**

- **há a necessidade de forte interação e de um bom relacionamento**
- **a análise de riscos e a gestão de mudança tornam-se fatores críticos**

- **Para os modelos ágeis:**
  - **a maturidade da equipe tende a reduzir as falhas (como no RAD e no UP)**
  - **automatização e ferramentas avançadas ajudam a evitar falhas**

- **a pressão por resultados pode relegar a segurança a um segundo plano**
- **a documentação simplificada ou reduzida dificulta a gestão de riscos**

- **O teste do *software*, no caso o de segurança, é a atividade que vai garantir a qualidade e a confiabilidade do *software*. Para isso, é indispensável considerar:**

- o planejamento precoce dos testes (no início do processo)
- a realização do teste de modo cíclico e recorrente
- os riscos e as ameaças à informação
- a automação do teste
- o uso de bases de conhecimento

Operação e Manutenção

- Avaliação da segurança pós-implantação
- Registro de ocorrências e estudo de causa raiz
- Atualização da base de conhecimento

- Registro das interações com usuários
- *Feedback* dos usuários e do SW
- Preservação do valor
- Lei de Lehman

- Após ser implantado, é importante o acompanhamento do *software*, no intuito de manter a segurança no nível adequado. Isso requer:

- o recebimento
- a classificação
- o refinamento
- o armazenamento
  - ✓ Das informações relativas à SegInfo

- O *software* não é estático, precisa acompanhar a evolução dos negócios e fazer frente às novas ameaças, sendo necessário atentar-se para:

- **mudanças de cenário e dos requisitos**
- **aumento da complexidade e degradação da qualidade**
- **estabilização das ocorrências**
- **percepção e resultados**
- ***feedback* constante**

Gestão de Configuração e de Mudanças

- **Processo da qualidade do *software***
- **Controle e confiabilidade**

- **Rastreabilidade das mudanças**
- **Interação do *software* com o ambiente**
- ***Frameworks* ITIL e COBIT**

- **O gerenciamento de configuração, ou, *Configuration Management*, é parte do processo da qualidade de *software*. É baseado em padrões e tem por objetivo manter o controle e a confiabilidade do *software* gerado, nas diversas etapas ou ciclos de seu desenvolvimento**

- **O gerenciamento de mudanças ou, *Change Management*, é um processo que tem por objetivo reduzir o risco e o impacto das alterações e evoluções do *software*, uma vez que estas intervenções sempre tendem a gerar problemas, falhas e interrupções**

***Software* para Dispositivos Móveis**

- **Procedimentos, mecanismos e controles que dão suporte às estratégias**
- **Diversidade de elementos e controles diferenciados por:**
  - **segurança física**
  - **segurança lógica**

- ✓ **Segurança física: prevenção detecção e combate às ameaças físicas, como:**
  - **incêndios**
  - **desabamentos**
  - **descargas elétricas**

- **alagamento**
- **acesso indevido de pessoas**
- **forma inadequada de tratamento e manuseio dos ativos e da informação**

- ✓ **Segurança lógica: prevenção, detecção e combate às ameaças "digitais", representadas principalmente por:**
  - ***malware***
  - **acessos remotos furtivos**
  - ***backup* desatualizado**

- **cópias não autorizadas**
- **negação de serviço**
- **pichação de *site***
- **violação de senhas**

- **Os mecanismos de defesa devem ser compatíveis com as estratégias de defesa e em linha com a PSI e com o negócio, pois, caso contrário, podem:**
  - **incorporar novos riscos**
  - **causar o efeito contrário ao desejado**

- **comprometer os resultados da organização**
- **causar repulsa nos indivíduos**
- **estimular a sabotagem ou as ações contra a segurança da informação e dos sistemas**

Internet das Coisas

- Práticas da boa gestão
- Transparência
- Reconhecimento pelo público externo
- Confiabilidade
- ITIL
- COBIT

- A governança é resultado de um esforço comprovado e contínuo para a melhoria dos processos, produtos e serviços, detecção, correção e antecipação dos problemas, do bom relacionamento e atendimento, da correta prestação de contas e da garantia da confiabilidade

- O ITIL (*Information Technology Infrastructure Library*) é um guia para orientar o gerenciamento eficiente da área de TI para que esta possa prestar os seus serviços de maneira otimizada e eficaz. (...)

(...) É um conjunto de melhores práticas de gestão de TI que surgiu no final dos anos 80

- O COBIT (*Control Objectives for Information and Related Technology*) é um guia que propõe o nível de excelência na gestão de TIC. (...)

(...) É voltado para a gestão de TIC e recomendado pelo ISACA/ISACF, cujo objetivo é apoiar os gestores na avaliação do risco e no controle dos investimentos de TIC da organização

- Juntamente com esses dois *frameworks*, as normas ISO ajudam a estabelecer as condições para a organização atuar em conformidade com as leis, as normas, as boas práticas e as recomendações de governança, isto é, para que esteja em situação de *compliance*

Síntese

- Tópicos vinculados à segurança dos sistemas e do *software* em geral
- A segurança no desenvolvimento, na operação e na manutenção

- Gestão de configuração e de mudança
- Segurança no *software* para dispositivos móveis
- Internet das coisas e a segurança

Referências de Apoio

- ABNT. Segurança da Informação – Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.
- COSTA, G. C. G. Negócios eletrônicos: uma abordagem estratégica e gerencial. Curitiba: Intersaberes, 2013.
- Gartner Group. Worldwide Smartphones Sales to end Users by OS. Disponível em: <http://techcrunch.com/2014/12/15/gartner-301m-smartphones-sold-in-q3-as-xiaomi-muscles-into-the-top-5-at-samsungs-expense/>. Acesso em: 21 de maio de 2015.
- GALVÃO, M. C. Fundamentos em Segurança da Informação. São Paulo: Pearson Education, 2015.

- GOERTZEL, K. M.; WINOGRAD, T.; HAMILTON, B. A. Safety and Security Considerations for Component-Based Engineering of Software-Intensive Systems. Disponível em: <https://buildsecurityin.us-cert.gov/sites/default/files/NOSSA-SafeSecureSWComposition-02012011.pdf>. Acesso em: 20 de maio de 2014.

- ITU. ITU Key 2005 – 2014 ICT data. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls>. Acesso em: 22 de maio de 2015.

- LAPOLLA, M.; MARTINELLI, F.; SGANDURRA, D. A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials, v. 15, n. 1, first quarter of 2013: 446–471.

- MUNASSAR, N; GOVARDHAN, A. A Comparison Between Five Models of Software Engineering. International Journal of Computer Science Issues, v. 7, Issue 5, September 2010: 94–101.

- OLIVEIRA, F. B. (Org). Fundação Getúlio Vargas. Tecnologia da Informação e da Comunicação: a busca de uma visão ampla e estruturada. São Paulo: Pearson Education, 2007.

- SOMMERVILLE, I. Engenharia de Software. 6. ed. São Paulo: Pearson-Addison Wesley, 2003.

- **TAURION, C. Sua empresa está preparada para o BYOD? IBM developerWorks. Disponível em: <https://www.ibm.com/developerworks/community/blogs/ctaurion>. Acesso em: 23 de maio de 2015.**