# Métodos Ágeis e Segurança: Uma análise do cenário das empresas da Grande Porto Alegre

**Rafael Dreher**
**OWASP Porto Alegre Chapter Co-Founder**
**Security Consultant @ Dell**
dreher@owasp.org

**OWASP**

Caxias do Sul, 20/06/2012



**The OWASP Foundation**

http://www.owasp.org

# Problema

- Trabalhos sobre segurança de software foram baseados em estudos das metodologias clássicas de desenvolvimento.
- Não existe um estudo direcionado para as metodologias ágeis de desenvolvimento de software.

# Solução

- Estudo de McGraw propõem controles baseados nos artefatos gerados em cada uma das fases do desenvolvimento.
- McGraw divide o desenvolvimento de software nas seguintes fases:
  - Requisitos e Casos de Uso;
  - Arquitetura e Design;
  - Planos de Teste;
  - Codificação;
  - Testes;
  - Feedback dos Usuários.

# Solução

- Artefatos são comuns entre algumas metodologias de desenvolvimento de software.
- Metodologias ágeis de desenvolvimento de software também geram artefatos como:
  - Requisitos;
  - Código Fonte;
  - Testes;
  - Etc.

# Solução

- Solução encontrada para avaliar o desenvolvimento com métodos ágeis foi mapear cada uma das fases e artefatos destas metodologias com o que foi propostos por McGraw.

# Pesquisa

- Foram propostas 21 perguntas para identificar se os controles propostos por McGraw se aplicavam no ciclo de desenvolvimento com métodos ágeis das empresas pesquisadas.
- Cada pergunta representava um controle específco, salvo perguntas que visavam identificar se determinado controle era aplicado por uma equipe interna ou externa.
- Questionário foi respondido presencialmente, através de uma entrevista.

# Resultados

| Requisitos de Segurança | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|
| Pergunta 1: A empresa dispõe de uma Política de Segurança da Informação? | 100% | 0% | | | | |
| Pergunta 2: A Política de Segurança da Informação aborda questões relacionadas ao desenvolvimento de software? | 80% | 20% | | | | |
| Pergunta 3: A Política de Segurança da Informação é utilizada como subsidio na geração de requisitos para a criação do *Backlog*? Ex: Existe uma diretiva para proteção de dados confidenciais aplicada no desenvolvimento de software, de forma a proteger estes dados contra acesso não autorizado. | 60% | 40% | | | | |
| Pergunta 4: Existe a definição de requisitos de segurança para o software? | 20% | 80% | | | | |
| Pergunta 5: A empresa utiliza metodologia de análise de riscos para identificação prévia dos riscos e ameaças que o processo de negócio está exposto, utilizando as saídas deste processo para a inclusão de requisitos no software? | 20% | 80% | | | | |
| Pergunta 6: São utilizados cenários de ataques (Casos de Abuso), a fim de identificar vulnerabilidades, para a criação de *User Stories* específicas para a inserção de requisitos segurança no software? | 0% | 100% | | | | |
| Pergunta 7: São previstas *User Stories* específicas para inserir requisitos de segurança no software? | 0% | 100% | | | | |

# Resultados

| | | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|---|
| **Arquitetura e Design** | | | | | | | |
| | Pergunta 8: A empresa faz uso de técnicas como Modelagem de Ameaças (*Threat Modeling*) para identificação de falhas que a arquitetura e componentes do software possam ser expostos? | 0% | 100% | | | | |
| | Pergunta 9: A empresa faz uso de uma metodologia de análise de riscos para identificação de riscos na arquitetura do software? | 0% | 100% | | | | |

# Resultados

| | | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|---|
| **Planos de Teste** | | | | | | | |
| | Pergunta 10: Os cenários de ataques (Casos de Abuso) são utilizados como entrada para a criação de Casos de Teste? | 0% | 100% | | | | |
| | Pergunta 11: São criados Casos de Teste a partir dos requisitos de segurança inseridos no Backlog? | 20% | 80% | | | | |

# Resultados

| Codificação | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|
| Pergunta 12: Existe um processo de revisão do código fonte específico para identificação de falhas de segurança? | 60% | 40% | | | | |
| Pergunta 13: É utilizada alguma ferramenta automatizada para a verificação de segurança do código fonte? | 60% | 40% | | | | |
| Pergunta 14: Quem executa a verificação de segurança no código fonte? | | | 40% | 0% | 60% | 0% |

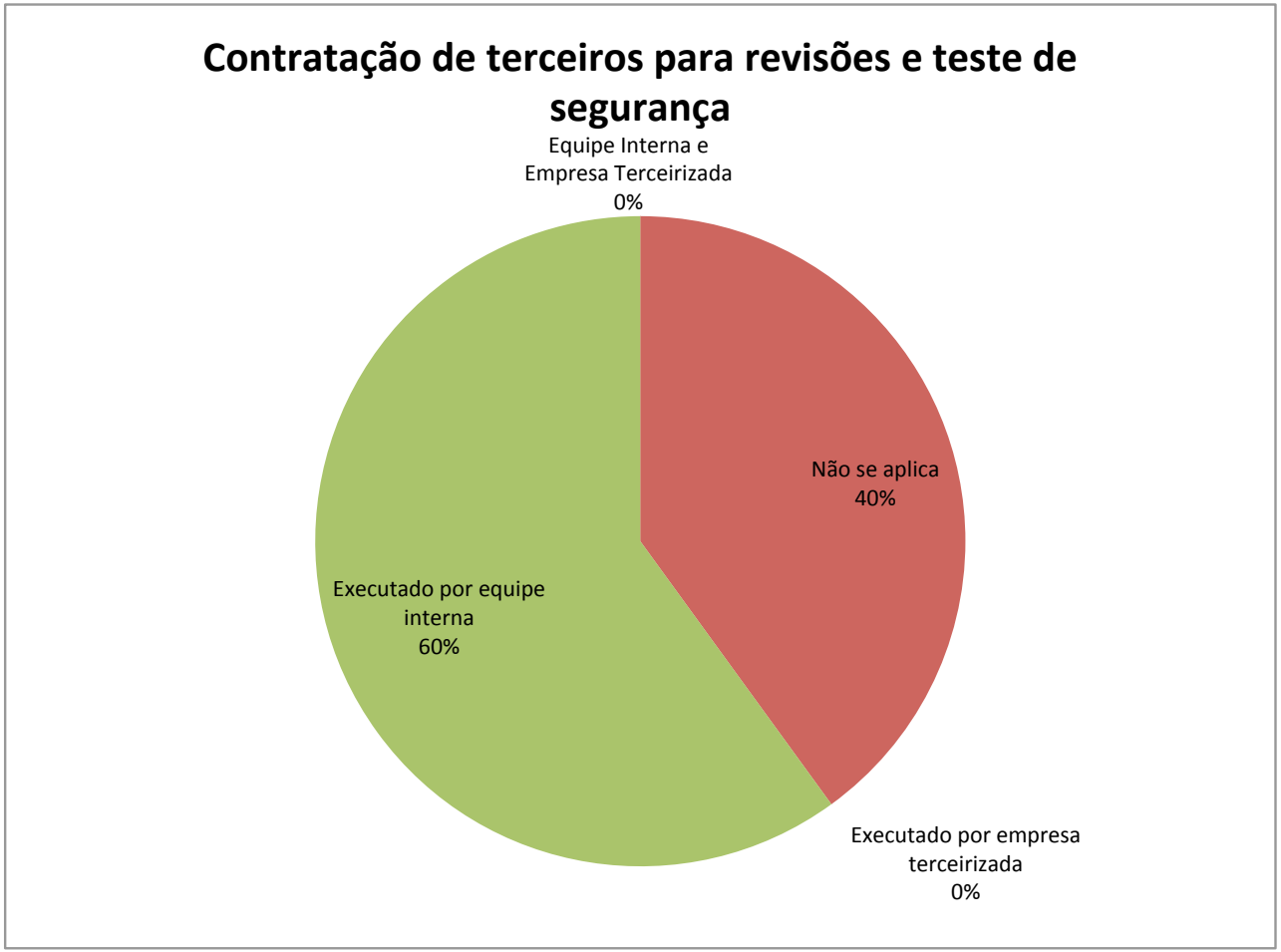
# Resultados

| Testes | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|
| Pergunta 15: São executados Testes de Penetração (Penetration Tests) no software durante o seu desenvolvimento? | 60% | 40% | | | | |
| Pergunta 16: São executados Testes de Penetração (Penetration Tests) no software uma vez que ele esteja executando em produção? | 60% | 40% | | | | |
| Pergunta 17: Quem executa os Testes de Penetração? | | | 40% | 0% | 60% | 0% |
| Pergunta 18: São utilizadas ferramentas automatizadas para os Testes de Penetração (Penetration Tests)? | 60% | 0% | 40% | | | |
| Pergunta 19: São utilizadas técnicas manuais para os Testes de Penetração (Penetration Tests)? | 60% | 0% | 40% | | | |

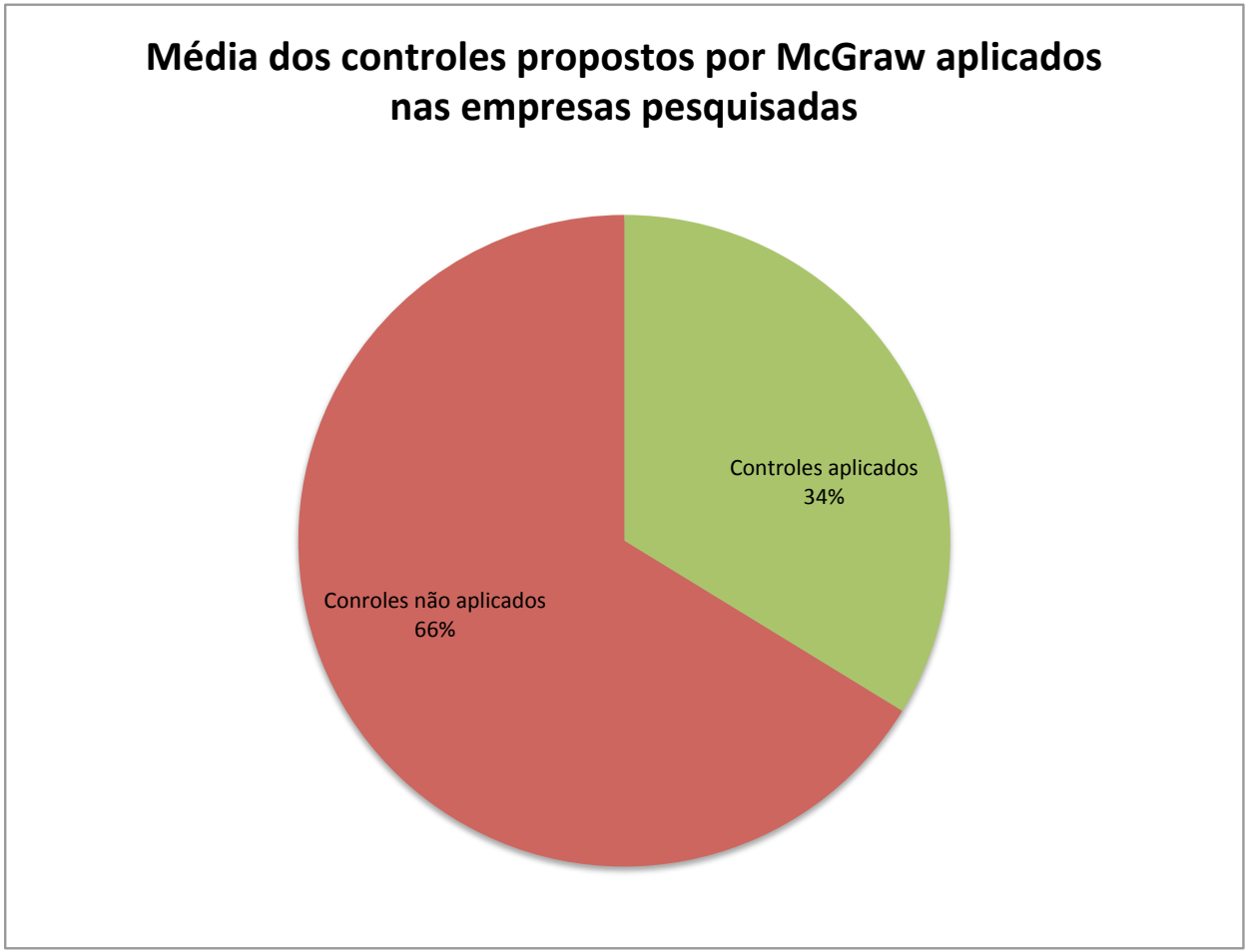
# Resultados

| Feedback dos Usuários | Sim | Não | Não se aplica | Empresa Terceirizada | Equipe Interna | Equipe Interna e Empresa Terceirizada |
|---|---|---|---|---|---|---|
| Pergunta 20: O cliente (usuário) interage de forma a prover informações sobre a criticidade e riscos que o processo de negócio está exposto, com o propósito de prover requisitos de segurança para o software? | 0% | 100% | | | | |
| Pergunta 21: O cliente (usuário) informa de alguma maneira falhas/ incidentes de segurança que o software possa apresentar? Estes incidentes/falhas são priorizados para correção pela equipe de desenvolvimento? | 60% | 40% | | | | |

# Resultados


Contratação de terceiros para revisões e teste de segurança
Equipe Interna e Empresa Terceirizada 0%
Não se aplica 40%
Executado por equipe interna 60%
Executado por empresa terceirizada 0%

# Resultados


Média dos controles propostos por McGraw aplicados nas empresas pesquisadas
Controles aplicados 34%
Conroles não aplicados 66%

# Conclusões

- Resultados obtidos na pesquisa mostram que existe um foco muito grande nos controles técnicos de segurança;
- Maior parte das empresas pesquisadas deriva requisitos de segurança partir da Política de Segurança da Informação ou de Normas;
- Não se observou preocupação com a definição de requisitos funcionais de segurança, obtidos das análises de riscos ou de Casos de Abuso;

# Conclusões

- Apesar de grande parte das empresas afirmarem que definem requisitos de segurança para o software, não se observa a transformação destes requisitos em User Stories;
- As empresas entendem requisitos como autenticação e autorização simplesmente como requisitos funcionais, e não próprios para endereçar questões de segurança;
- A pesquisa mostrou que nenhuma das empresas pesquisadas se preocupa com a segurança na arquitetura das aplicações;

# Conclusões

- Os testes tem foco puramente técnico, não validando requisitos funcionais, pelo fato de os mesmos não serem definidos;
- Grande parte das empresas pesquisas realizam Testes de Penetração nas aplicações, sem auxílio de terceiros;
- O mesmo cenário é encontrado no quesito Revisão de Código Fonte.

# Conclusões

- Aspectos mais complexos como a modelagem de Casos de Abuso, ou o uso de modelagem de ameaças, são atividades que necessitam de um amadurecimento maior das empresas para a sua adoção;
- O cenário delineado pela pesquisa não é desanimador, pelo contrário. Maior parte das empresas pesquisadas já implementa processos básicos, como a revisão de código fonte e testes de penetração.

# Trabalhos Futuros

- Ampliação da pesquisa em uma população maior, em âmbito estadual e até mesmo nacional;
- Alterações nos controles propostos por McGraw para maior aderência às metodologias ágeis de desenvolvimento de software;
- Definição de um framework de segurança, com controles específicos para as metodologias ágeis ,sem que os mesmos afetem o princípio básico da agilidade destes métodos;

# Trabalhos Futuros

- Um modelo de avaliação da maturidade de segurança para metodologias ágeis de desenvolvimento de software.

# Perguntas?