OWASP PARAÍBA

20 DE JANEIRO Day

# O Ciclo do Software Inseguro

Rodrigo Jorge

CEO

@rodrigojorge

rodrigo.qualitek@qualitek.com.br

Qualitek

SISTEMAS PROTEGIDOS.
NEGÓCIOS GARANTIDOS.

# Agenda

Qualitek

Ciclo do Software Inseguro

Problemas

- Contratação
- Desenvolvimento
- Formação

Existe solução?

# Ciclo do Software Inseguro

# Pesquisa Informal

Email

Conversa pessoal

Telefone

# Desenvolvedores

Qualitek

1. Você ao estudar programação/desenvolvimento, teve alguma disciplina/conteúdo/módulo sobre desenvolvimento de código seguro e testes de segurança em código?

2. A Software House que você trabalha, já contratou algum teste de segurança nas aplicações desenvolvidas por ela?

3. Você é incentivado no trabalho, a estudar sobre desenvolvimento seguro e/ou realizar testes de segurança no código desenvolvido?

4. Você acha que a aplicação entregue ao cliente final é segura?

# Desenvolvedores

Maioria (90%) nunca estudou Segurança da Informação

Nenhuma SW House contratou testes de Ssegurança da Informação

90% não é incentivado a estudar Segurança da Informação no trabalho

Todos acham que a aplicação entrega é insegura

# Formação

1. Nos cursos relacionados à Computação e/ou Sistemas, há alguma disciplina sobre Desenvolvimento Seguro de Software?
2. Se sim, qual?
3. Se não, há projeto? Para quando? Qual disciplina?

Qualitek

UNICAMP

curso 42 - Ciência da Computação - Currículo Pleno
Catálogo 2011

**Núcleo Comum ao Curso:**

| | |
|---|---|
| CE304 Direito | CE738 Economia para Engenharia |
| CE839 Introdução à Administração para Computação | F 128 Física Geral I |
| F 129 Física Experimental I | F 328 Física Geral III |
| F 329 Física Experimental III | MA111 Cálculo I |
| MA141 Geometria Analítica e Vetores | MA211 Cálculo II |
| MA311 Cálculo III | MA327 Álgebra Linear |
| MC009 Computação e Sociedade | MC038 Introdução à Redação Científica |
| MC102 Algoritmos e Programação de Computadores | MC202 Estruturas de Dados |
| MC302 Programação Orientada a Objetos | MC346 Paradigmas de Programação |
| MC358 Fundamentos Matemáticos da Computação | MC404 Organização Básica de Computadores e Linguagem de Montagem |
| MC426 Engenharia de Software | MC437 Projeto de Sistemas de Informação |
| MC458 Projeto e Análise de Algoritmos I | MC504 Sistemas Operacionais |
| MC536 Bancos de Dados: Teoria e Prática | MC558 Projeto e Análise de Algoritmos II |
| MC602 Circuitos Lógicos e Organização de Computadores | MC626 Análise e Projeto de Sistema de Informação |
| MC658 Projeto e Análise de Algoritmos III | MC714 Sistemas Distribuídos |
| MC722 Projeto de Sistemas Computacionais | MC750 Construção de Interfaces Homem-Computador |
| MC822 Teleprocessamento e Redes | MC833 Programação de Redes de Computadores |
| ME323 Introdução aos Modelos Probabilísticos | MS211 Cálculo Numérico |

# UNICAMP

**Disciplinas Eletivas**
30 créditos dentre:

----- Qualquer disciplina oferecida pela UNICAMP

08 créditos dentre:

| | |
|---|---|
| MC851 Projeto em Computação I | MC853 Projeto em Sistemas de Programação |
| MC855 Projeto em Sistemas de Computação | MC857 Projeto em Sistemas de Informação |
| MC859 Projeto em Teoria da Computação | MC861 Projeto em Computação II |
| MC911 Projeto em Compiladores | |

04 créditos dentre:

MC--- Qualquer disciplina com código MC---

04 créditos dentre:

| | |
|---|---|
| MC919 Tópicos Especiais em Processamento Gráfico | MC920 Introdução ao Processamento de Imagem Digital |
| MC930 Computação Gráfica | MC940 Processamento e Análise de Imagens |
| MC949 Visão Computacional | MC950 Recuperação de Imagens por Conteúdo |

04 créditos dentre:

| | |
|---|---|
| MC886 Aprendizado de Máquina | MC896 Processamento de Línguas Naturais |
| MC906 Introdução à Inteligência Artificial | MC959 Tópicos em Inteligência Artificial I |

06 créditos dentre:

| | |
|---|---|
| MC019 Estágio Supervisionado em Ciência da Computação | MC030 Projeto Final de Graduação |
| MC032 Estudo Dirigido | MC033 Estudo Dirigido II |
| MC040 Estágio de Iniciação Científica I | |

FATEC-SP

Qualitek

*Quadro de Equivalências entre disciplinas do curso de PD com o novo curso ADS*

| Curso: PROCESSAMENTO DE DADOS | | | Curso: ANÁLISE E DESENVOLVIMENTO DE SISTEMAS |
|---|---|---|---|
| Semestre (D/N) | Disciplina | Aulas | Disciplina |
| 1/1 | SIST COMP | 72 | Arquitetura e Organização de Computadores |
| 1/1 | MICRO | 72 | Microinformática Aplicada |
| 1/3 | TEOR SIST | 36 | Interface Humano Computador |
| 1/3 | ADM I | 72 | Administração |
| 1/1 | MAT I | 108 | Calculo I |
| 1/2 | INGL | 72 | Inglês Instrumental I e II |
| 1/1 | INT LOG | 36 | Matemática Discreta |
| 1/1 | LTP I | 72 | Algoritmos e Lógica de Programação |
| 2/2 | SIST OPER I | 72 | Sistemas Operacionais I |
| 2/4 | BD I | 72 | Banco de Dados |
| 2/4 | APS I | 72 | Engenharia de Software I |
| 2/4 | ADM II | 72 | Sistemas de Informações |
| 2/2 | MAT II | 72 | Cálculo II |
| 2/2 | Optativa | 72 | Eletiva |
| 3/3 | SIST OPER II | 72 | Ambiente Operacional |
| 3/3 | ESTR DADOS | 72 | Estruturas de Dados |
| 3/5 | ADM III | 72 | Gestão de Projetos e Segurança da Informação |

OWASP PARAÍBA 20 DE JANEIRO Day


## 8º Semestre

| Disciplina | CH | T | P |
|---|---|---|---|
| Empreendedorismo em SI | 2 | 2 | |
| Infraestrutura para Conversão Digital | 2 | 2 | |
| Segurança e Auditoria em SI | 2 | 2 | |
| SI para Educação | 2 | 2 | |
| Técnicas de Consultoria em SI | 2 | 2 | |
| Tendências em Tecnologia de SI | 2 | 2 | |
| Tópicos em Gerência de Projetos | 2 | 2 | |
| Disciplinas de Ênfase | 12 | 12 | |
| **TOTAL:** | **26** | **26** | |

# Software Houses

Qualitek

1. Você realiza testes de Segurança de Software nas aplicações entregues aos clientes?

2. Você tem alguma responsabilidade contratual para reparação ao cliente final, no caso de prejuízos gerados por incidentes de segurança ocorridos na aplicação fornecida?

3. Você já investiu em Segurança de Software na sua empresa? Se sim, como?

# Software Houses

Qualitek

Todos responderam que não realizam testes de SI

Todas responderam que não possuem responsabilidade contratual de realizar testes e/ou reparar danos

Nenhuma investiu em SI nas aplicações desenvolvidas até hoje

# Gestores de TI

1. Você possui alguma aplicação contratada de terceiros rodando em seu ambiente, incluindo website, webmail?

2. Você possui alguma aplicação web de terceiros, rodando em datacenter externo?

3. Na contratação, foi exigida da empresa comprovação de que são realizados testes de segurança regulares na(s) mesma(s)?

# Gestores de TI

4. Você já contratou algum teste de segurança nas suas aplicações?

5. Caso ocorra um incidente de invasão no site externo, manchando a imagem da empresa, você sabe a quem responsabilizar judicialmente?

6. No contrato com os fornecedores de ERP e Folha, há alguma clausula onde os fornecedores se responsabilizam por reparação material, caso incorram prejuízos causados por incidentes de segurança da informação explorados em falhas deixadas por eles em suas aplicações?

# Gestores de TI

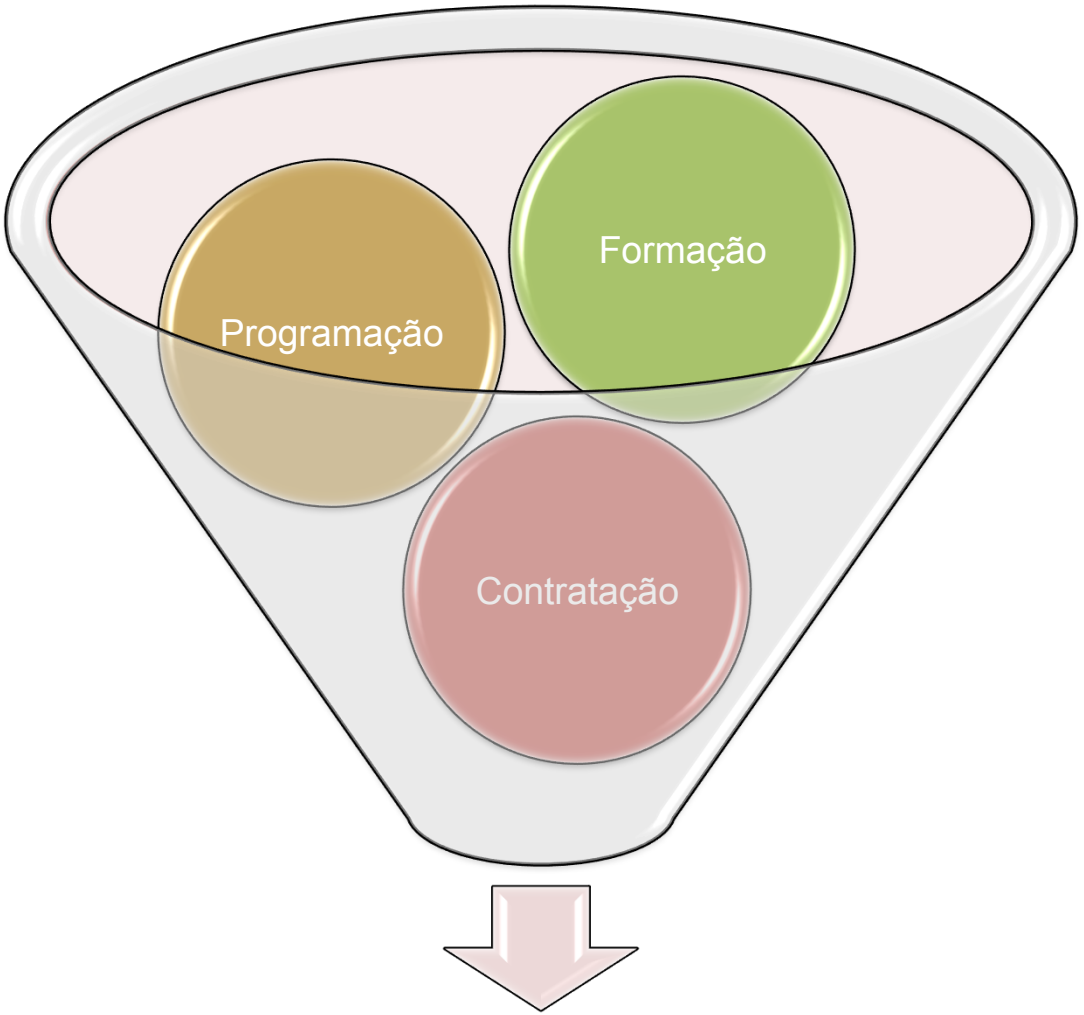
Maioria tem sistemas de terceiros dentro do ambiente

Maioria possuí aplicação rodando em DC externo

Nenhum exigiu comprovação de testes de SI

Não sabem quem responsabilizar em caso de incidente

Não atentaram para termos contratuais

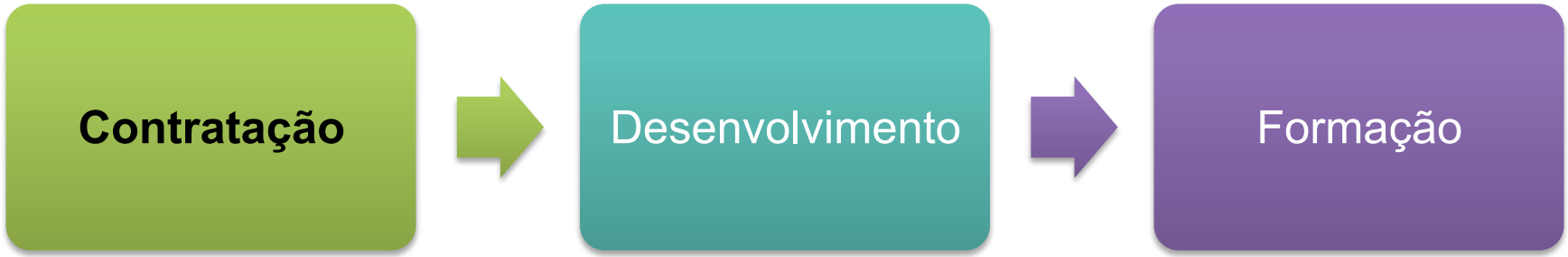



# Software Inseguro

Qualitek

# por onde começar???

OWASP PARAÍBA 20 DE JANEIRO Day


Contratação
Desenvolvimento
Formação

Qualitek

Desafio 1

Conscientização dos Consumidores de SW (Organizações e Pessoas)

- Contratação
  - Verificar padrão de desenvolvimento seguro
  - Conhecer procedimentos de testes internos
  - Quantidade e Resultado dos Testes externos
  - Selo de Software Auditado pode ser uma boa opção
  - Reparação prevista nas obrigações contratuais
- Manutenção
  - Auditar testes da Software House
  - Contratar terceiros para testar


Contratação
Programação
Formação

Desafio 2

Qualitek

**Mudança nas Software Houses**

- Desenvolvimento de Código Seguro
- Manutenção
- Preparação da equipe atual
- Recrutamento de Profissionais já preparados

Qualitek

Desafio 3

Qualitek

**Mudança nas Escolas de Formação**

- Desenvolvimento de Código Seguro em todas discplinas
- Formação de profissionais já capacitados em SI
- Garantia de Emprego para seus egressos

# E nós?

Qualitek

Engajamento de Todos

OWASP e similares

Associações de Empresas

Buscar melhores práticas e padrões

# Perguntas?

Qualitek

OWASP PARAÍBA 20 DE JANEIRO Day

Qualitek

# Tks!

@rodrigojorge

OWASP PARAÍBA 20 DE JANEIRO Day