**GRUPOS DE APRESENTAÇÕES ORAIS 2013.2  
De 22/11 à 29/11/2013**

**1.**  **Gestão de Segurança da Informação  
Livro: Sistema de Segurança da Informação, André Campos, Visual Books, Segunda Edição, 2007:** Controlando os Riscos, Análise de Riscos, Auditoria de Sistema e Política de Segurança.

Grupo 1:  
Cap4 e Cap5:  
A Segurança da Informação e as Estratégias de Negócio. Definindo o Escopo de um SGSI (aqui aparece a análise de risco).    
  
  
Grupo 2:  
Cap4 da Parte II e Cap6 da Parte I, Cap6, Cap7, Cap8 e Cap9 da Parte I:  
Estruturando a Segurança da Informação, Implementando, Monitorando, Revisando e Melhorando do Sistema de Segurança da Informação.    
  
  
Grupo 3:  
Cap5 e Cap8 da Parte II:  
Gestão de Ativos e Gestão das Operações de TI. (2 membros)  
  
Grupo 4:   
Cap 9 e Cap 10:  
Controle de Acesso, Aquisição, Desenvolvimento e Manutenção.  
  
**2.** **Organização da Segurança da Informação** (Normas ISO 27000)  
Grupo 5: **ISO/IEC 27000** é um conjunto de normas para sistema de gestão da [segurança da informação](http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o) publicado em outubro de 2005 pelo [International Organization for Standardization](http://pt.wikipedia.org/wiki/International_Organization_for_Standardization) e pelo [International Electrotechnical Commision](http://pt.wikipedia.org/w/index.php?title=International_Electrotechnical_Commision&action=edit&redlink=1). Seu nome completo é *ISO/IEC 27001:2005 - Tecnologia da informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação* : ISO 27001, ISO 27002, ISO 27003, ISO 27004 e ISO 27005  
<http://www.datasecurity.com.br/index.php/cursos/iso-27000>

**3. Segurança no Desenvolvimento de Software**Grupo 6:   
Cap10 Modelos de Especificação de Segurança  
Cap11 Especificação da Segurança Desejada  
Cap12 Segurança do Ambiente de Desenvolvimento  
  
Grupo 7:   
Cap13 Segurança no Ciclo de Vida de Desenvolvimento da Aplicação  
Cap14 Garantia da Segurança da Aplicação  
  
  
Grupo 8:    
**Anexo 3**do Livro **Segurança e Auditoria em Sistemas da Informação** (último anexo do livro) Ciclo de Vida de Desenvolvimento Seguro de Software  
  
Grupo 9:   
Parte IV, Cap23:  Política de Segurança. (Pode ser um estudo de caso).    
  
Grupo10:  
**Anexo 2** do Livro **Segurança e Auditoria em Sistemas da Informação** (segundo anexo do livro) Norma NBR ISO/IEC 17.799 de 2005: Código de prática de gestão da segurança da informação.   
  
Grupo11:  
**Anexo 1**do Livro **Segurança e Auditoria em Sistemas da Informação** (final do livro)  
Critério Comum para Avaliação de Segurança de Tecnologia da Informação (Noema IEC/IEC 15.408). Especificar a segurança de uma aplicação de forma não ambígua a partir de características do ambiente da aplicação.

# 4. Metodologias de Teste de Segurança Grupo 12:

* [Why Pen Testing? Why Penetration Testing is Important?](http://www.pen-tests.com/why-pen-testing-why-penetration-testing-is-important.html)
* [Penetration Testing Framework](http://www.pen-tests.com/penetration-testing-framework.html)

Grupo 13:

* [OWASP Testing Guide](http://www.pen-tests.com/owasp-testing-guide.html)

Grupo 14:

* [Open Source Security Testing Methodology (OSSTM)](http://www.pen-tests.com/open-source-security-testing-methodology-manual-osstmm.html)

Grupo15:

* [NIST Guideline in Network Security Testing](http://www.pen-tests.com/nist-guideline-in-network-security-testing.html)

Grupo 16:  
 **ISSAF** - Information Systems Security Assessment Framework

**5. Sistemas de Autenticação**

Grupo 17:  
Identidade Federada: cenários, arquitetura, implementações e aplicações em nuvem  
  
<http://www.gta.ufrj.br/grad/11_1/geren-id/index.php?file=kop5.php>  
  
<http://msdn.microsoft.com/pt-br/library/aa479079.aspx>

<http://www.slideshare.net/jarddel/gerncia-de-identidades-federadas-em-nuvens>

**6. Sistemas de Defesa**  
Grupo 18:  
**Sistemas de Detecção de Intrusão (IDS)**Baseado em Rede Neural

Grupo 19: **Sistemas de Detecção de Intrusão (IDS)**Baseado em um sistema imunológico artificial   
  
Grupo 20:  
**Sistemas de Detecção de Atacantes**Honeypots  
 **7. Ferramentas para Análise de Tráfego e Vulnerabilidades em Redes**

Grupo 21:  
**Análise de Tráfego ou Ataques Man-in-the-Middle**Wireshark

Grupo 22:  
**Análise de Tráfego ou Ataques Man-in-the-Middle**Ettercap

**8. Segurança em Documentos Eletrônicos**Grupo 23:

**9.** **Ferramentas de Aquisição de Informações, Scanner de Web e Bancos de Dados**Grupo 24:  
**Aquisição de Informações**   
Maltego

Grupo 25:  
**Scanner de Aplicações Web**Paros

Grupo 26:  
**Auditoria em Bancos de Dados**DB Audit Free Edition – ferramenta de auditoria e análise de segurança para bancos de dados *Oracle*, *Sybase*, *DB2*, *MySQL* e *Microsoft SQL Server*. [http://www.softtreetech.com](http://www.softtreetech.com/)

Grupo 27:  
**Auditoria em Bancos de Dados**SQL Map – ferramenta automática em linha de comando para testes de *sql-injection*. [http://sqlmap.sourceforge.net](http://sqlmap.sourceforge.net/)

**10. Outras Propostas**  
  
Grupo 28:  
???????? (Jean Pacher)