SBSEG'08 VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

Gestão de Riscos de Segurança

José Eduardo Malta de Sá Brandão
Joni da Silva Fraga
je.brandao@ipea.gov.br
fraga@das.ufsc.br

Ipea Instituto de Pesquisa Econômica Aplicada

DAS Departamento de Automação e Sistemas
Centro Tecnológico
Universidade Federal de Santa Catarina

Sumário

- Motivação
- Conceitos
- Principais Padrões
- Méticas
  - *Common Vulnerability Scoring System* (CVSS)
- Estudo de Caso

Motivação

Qual é o Risco ?

Mitigação do Risco

Por que Gerenciar Riscos ?

- A noção correta dos riscos permite que se definam caminhos e ferramentas para mitigá-los
- “Os riscos podem ser identificados e reduzidos, mas nunca totalmente eliminados” (Garfinkel et al. 2003)

Quando Gerenciar os Riscos ?

- É comum a aplicação de ferramentas de análise de risco em protótipos desenvolvidos em projetos de software científicos ou comerciais
  - Análise de Vulnerabilidades
- Problemas encontrados:
  - Vulnerabilidades inerentes à tecnologia adotada
    - Decisão: troca da tecnologia ou aceitação de um risco maior do que o desejado ?
  - Tratar os riscos apenas no ponto de protótipo pode ser extremamente dispendioso e, em alguns casos, os resultados podem inviabilizar o próprio projeto
- As vulnerabilidades encontradas poderiam ter sido facilmente identificadas na etapa de planejamento do projeto.

Conceitos Iniciais

Propriedades de Segurança

- **Integridade**:
  - garante que a informação não será alterada ou destruída sem a autorização adequada.
- **Confidencialidade**:
  - garante que a informação não será revelada sem a autorização adequada.
- **Disponibilidade**:
  - garante que a informação estará acessível aos usuários legítimos quando solicitada.

Violações de Segurança

- Quando há a quebra de uma ou mais propriedades de segurança
  - Violação de confidencialidade
    - Revelação não autorizada da informação
  - Violação de integridade
    - Modificação não autorizada da informação
  - Violação de disponibilidade
    - Negação de serviço

Vulnerabilidade

- "Defeito ou fraqueza no design ou na implementação de um sistema de informações (incluindo procedimentos de segurança e controles de segurança associados ao sistema), que pode ser intencionalmente ou acidentalmente explorada, afetando a confidencialidade, integridade ou disponibilidade" (Ross et al. 2005)

Risco

- "É o impacto negativo da exploração de uma vulnerabilidade, considerando a probabilidade do uso do mesmo e o impacto da violação" (Stoneburner et al. 2002)

Estimativa do Risco

- O risco pode ser expressado matematicamente como uma função da probabilidade de uma origem de ameaça (ou atacante) explorar uma vulnerabilidade potencial e do impacto resultante deste evento adverso no sistema e, conseqüentemente, na empresa ou organização.

Gestão de Riscos

- "A gestão de riscos baseia-se em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos" (ISO/IEC Guide 73:2002)
- Envolve um processo criterioso e recursivo de documentação, avaliação e decisão durante todas as fases do ciclo de vida do projeto

Estudo de caso

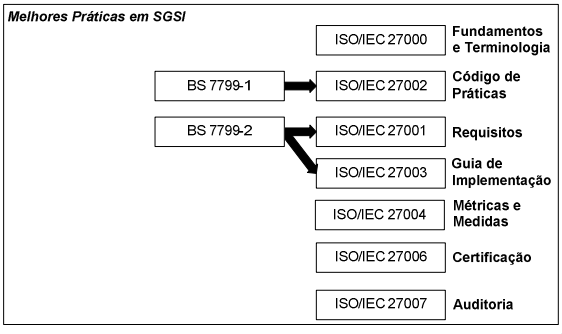
- Ilustração prática da aplicação da gestão de riscos em um projeto científico
- Gestão de Riscos no Projeto de Composições de IDSs
- Adotou inicialmente a norma AS/NZ4360 e posteriormente adaptada para o padrão ISO 27005
- Será apresentado em conjunto com a metodologia

Principais Padrões Relacionados à Gestão de Riscos

- Melhores Práticas
- *Common Criteria* (CC)
- *Normas de Gestão de Riscos*
  - NIST SP800-30
  - AS/NZS 4360, ISO 27005 e ISO 31000ca

Melhores Práticas em SGI

Família de Normas ISO 27000



Norma ISO 27000

- Está em desenvolvimento
- Irá definir os conceitos fundamentais e o vocabulário de segurança da informação adotado na família de documentos ISO 27000

Norma ISO 27001

- Baseada na BS 17799-2
- Foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)

Norma ISO 27002

- Baseada na BS/ISO 17799-1
- Introduz os conceitos de segurança da informação e faz uma discussão inicial a respeito das motivações para o estabelecimento da gestão de segurança.
- Na maior parte do documento são detalhadas as práticas de segurança, que são associadas aos os objetivos de controles, e os controles de segurança citados na norma ISO 27001

Norma ISO 27003

- Em desenvolvimento
- É baseada no anexo B da norma BS 7799-2
- Basicamente um **guia para a implantação** do SGSI

Norma ISO 27004

- Em desenvolvimento
- Definirá **métricas e medidas** para o acompanhamento do SGSI

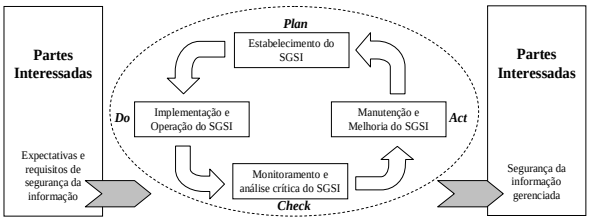
Norma ISO 27006

- Define critérios para as pessoas e empresas que farão a **certificação e auditoria** do SGSI
- Segue o padrão da norma 17021

Norma ISO 27007

- Em desenvolvimento
- Definirá critérios específicos para a **auditoria** dos processos do SGSI
- Baseada na norma ISO 19011

O Modelo PDCA



Plan

- O ciclo do PDCA começa com o estabelecimento da política, dos objetivos, dos processos e dos procedimentos do SGSI, que sejam relevantes para a gestão de riscos e a melhoria da segurança da informação e que produzam resultados de acordo com as políticas e objetivos globais de uma organização.

Do

- Envolve a implantação e a operação da política, dos controles, dos processos e dos procedimentos estabelecidos na primeira etapa

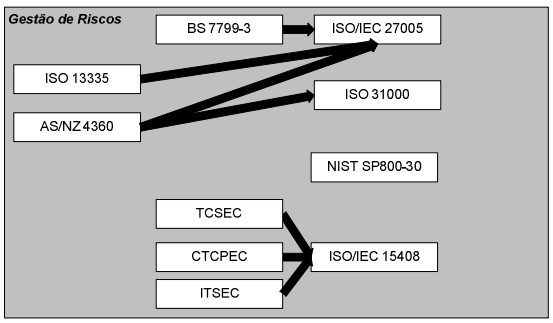
Check

- É feita a avaliação e, quando aplicável, a medição do desempenho de um processo frente à política, aos objetivos e à experiência prática do SGSI, apresentando os resultados para a análise crítica pela direção.

Act

- Cabe a execução das ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.
- Após esta etapa, o ciclo é reiniciado, tomando como base o aprendizado do ciclo anterior. O resultado esperado da adoção do PDCA é a segurança da informação devidamente gerenciada.

Normas de Gestão de Riscos



Common Criteria (CC)

- Conjunto de normas ISO/IEC 14
  - Derivado do "livro laranja" (TCSEC), do CTCPEC (Canadá) e do ITSEC (UE).
- Metodologia de testes e acompanhamento de projeto de produtos de segurança (*target of evaluation* - ***TOE***)
- Definição de perfís com requisitos de Segurança (*protection profiles* – ***PP***), independentes de implementação.
- Define conjunto de requisitos e especificações para ser usado como base para avaliação de um TOE específico (*security targets* - ***ST***)

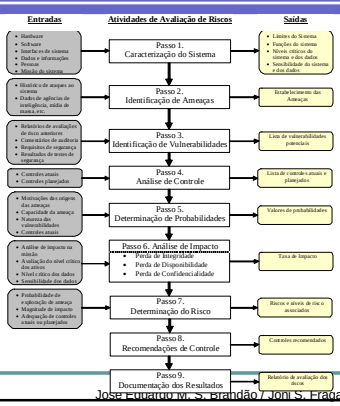
Cerifificação CC

- Produtos recebem uma certificação de nível de garantia (*Evaluation Assurance Level* - *EAL*):
  1. teve seu funcionamento testado
  2. teve sua estrutura testada e envolve a cooperação do fabricante
  3. foi metodicamente testado e checado
  4. foi metodicamente projetado, testado e checado
  5. seja projetado e testado de maneira semi formal
  6. Foi projetado, verificado e testado de maneira semi formal
  7. foi projetado, verificado e testado de maneira formal

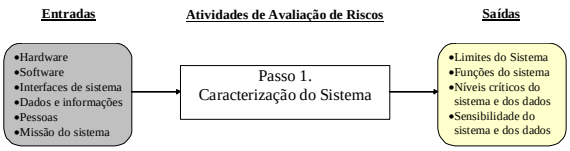
NIST SP800-30

- *Risk Management Guide for Information Technology Systems (2002)*
- Duas etapas:
  - avaliação de riscos (ou determinação dos riscos); e
  - atenuação de riscos

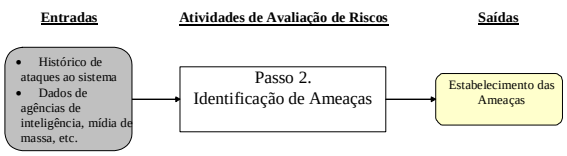
Processo de Avaliação



Caracterização do Sistema

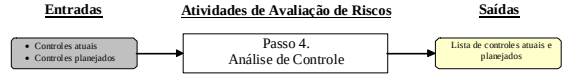


Identificação de Ameaças

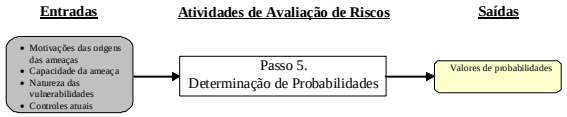


Identificação de Vulnerabilidades

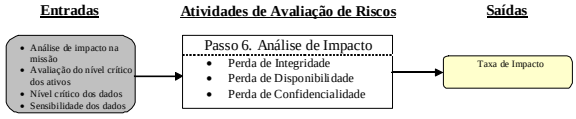
Análise de Controle



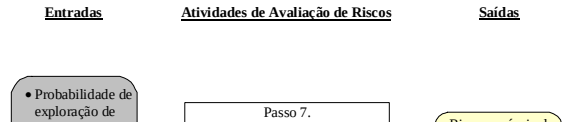
Determinação de Probabilidades



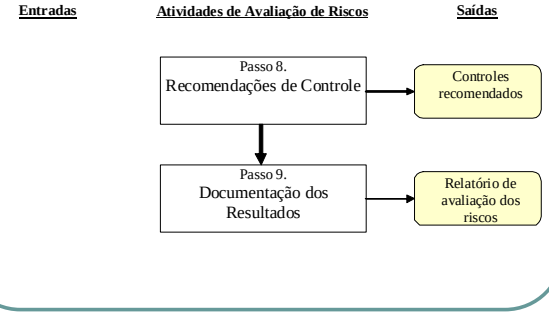
NIST SP800-30



Determinação do Risco



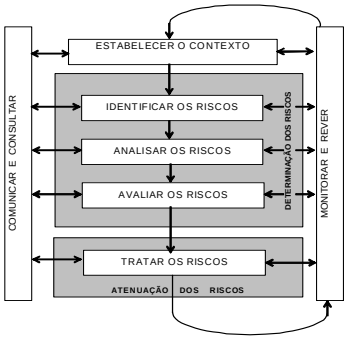
Recomendações de Controle Documentação dos Resultados



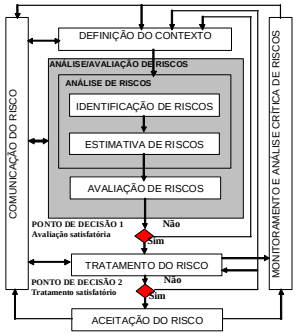
AS-NZS4360

- Desenvolvida pelos governos da Austrália e Nova Zelândia
- Serve de referência para as normas atuais
- Guia de Aplicação: *Risk Management Guidelines Companion to AS/NZS 4360:2004 - HB 436:2004*

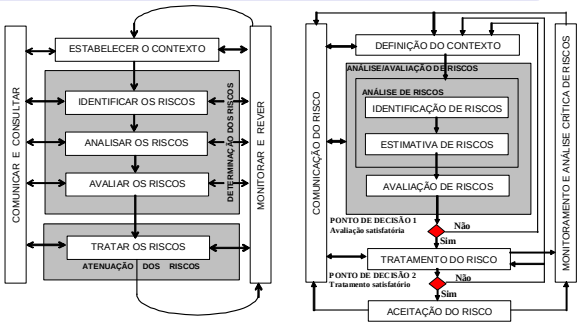
Processo AS/NZS 4360 e ISO-3100



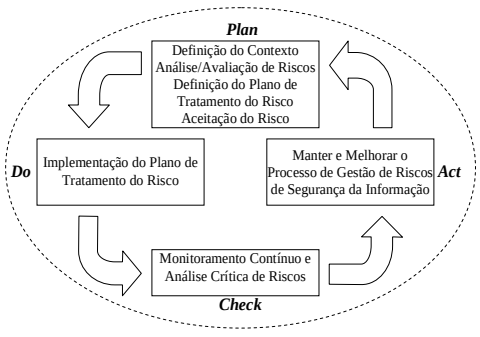
Processo ISO 27005



AS/NZS4360 x ISO 27005



Alinhamento da ISO 27005 com o PDCA



Comunicação do Risco

- Identificação das partes interessadas
- Papéis e responsabilidades delimitados
- Desenvolver um plano de comunicação que permita a cada uma destas partes conhecer o andamento do processo e fornecer subsídios para seu desenvolvimento

Comunicação do Risco Aplicada

1. **Membros do projeto de pesquisa** – pessoas diretamente relacionadas ao desenvolvimento do projeto;
2. **Membros do grupo de pesquisa** – pessoas que pertencem ao mesmo grupo de pesquisa, mas não estão diretamente relacionados à pesquisa em desenvolvimento;
3. **Comunidade científica** – pessoas interessadas nos resultados da pesquisa, como membros de comitês de programa e revisores de simpósios e periódicos, participantes de congressos científicos e leitores dos trabalhos publicados;
4. **Instituições e órgãos de pesquisa** – instituições e órgãos de pesquisa aos quais o projeto de pesquisa está vinculado;
5. **Instituições e órgãos de fomento** – responsáveis pelo custeio do projeto.

Plano de Comunicação e Consulta

Objetivos	Participantes	Perspectiva dos Participantes	Métodos Usados	Avaliação
Estabelecimento de diretrizes e revisão contínua do projeto	Membros do projeto de pesquisa	Processo contínuo de avaliação dos riscos	Reuniões periódicas e apresentação de relatórios técnicos.	Auto-avaliação
Identificação de possíveis falhas, troca de experiências e obtenção de críticas e sugestões	Membros do grupo de pesquisa	Conhecimento de novas tecnologias	Seminários e encontros.	Análise periódica das contribuições apresentadas.
Obtenção de críticas e sugestões, identificação de novas aplicações, troca de experiências e avaliação do projeto	Comunidade científica	Divulgação e conhecimento de novas tecnologias	Submissão de artigos científicos para prospecção, publicação de resultados e apresentação de artigos.	Compilação e análise das revisões, sugestões e críticas dos artigos.

Definição do Contexto

- Parâmetros básicos, por meio dos quais serão identificados os riscos que precisam ser geridos e qual será o escopo do restante do processo de gestão de riscos.
- Critérios que serão utilizados na identificação, avaliação, impacto e aceitação dos riscos.
  - Determinação das conseqüências de segurança e os métodos usados para a análise e avaliação dos riscos
- Tem como entrada todas as informações relevantes sobre a organização, que sejam relevantes para a definição do contexto da gestão de riscos de segurança.
- Descrição dos objetivos do projeto e dos ambientes nos quais eles estão contextualizados

Descrição do Projeto

- As composições de IDSs envolvem a combinação de diversos sistemas de monitoramento que coletam e analisam dados de forma distribuída e oferecem a flexibilidade da configuração dinâmica para atender a novas situações, mesmo que temporárias.

Definição dos Objetivos

O1: **Detecção de Intrusão Distribuída**

O2: **Uso de Elementos Heterogêneos**

O3: **Composição Dinâmica de IDSs**

O4: **Adoção de Padrões de Interoperabilidade**

O5: **Segurança dos Elementos e da Composição**

Definição dos Critérios Básicos

- Conseqüências
  - **Confidencialidade** - Informações críticas são reveladas a usuários não autorizados
  - **Integridade** - Informações críticas são alteradas ou eliminadas por usuários não autorizados
  - **Disponibilidade** - Elementos de software ou hardware têm sua performance reduzida ou seu funcionamento interrompido.
- Fatores de riscos associados às questões:
  - qual é a **ameaça** (exploração de vulnerabilidades);
  - **o que pode ocorrer** (conseqüências); e
  - **como pode ocorrer** (ataque).
- Cálculo dos riscos:
  - Adoção das métricas básicas do CVSS
- Aceitação dos Riscos
  - Riscos Baixos.
  - Os riscos Médios, cujos controles para sua redução sejam Altos, também poderão ser aceitos.

Identificação de Riscos

- Determinar os eventos que possam causar perdas potenciais
  - Como, onde e por que ?
- Identificar:
  - Ameaças
  - Controles existentes
  - Vulnerabilidades
  - Conseqüências
- Dificuldades:
  - Critérios subjetivos
- Referências:
  - Literatura Científica
  - Consulta à comunidade
    - Usuários, parceiros, interessados
    - Submissão de trabalhos e *Feedback* de revisões

Registro de riscos: IDSs Distribuídos

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Negação de Serviço	Afeta a disponibilidade do sistema	Desativação de Elementos por ataques diretos, explorando vulnerabilidades	Uso de mecanismos automáticos para detecção de falhas de funcionamento e Reativação automática dos elementos	Yegneswaran et al. 2004] Ptacek and Newsham 1998] Dacier 2002] Yu e Frincke, 2004]
			Replicação de elementos	
			Filtragem de tráfego	
			Seleção dinâmica de novos elementos	
		Elementos maliciosos enviam grande quantidade de dados falsos	Controle do fluxo e filtragem da quantidade de mensagens que excedam determinado limite	
Mascaramento	Afeta a integridade e privacidade do sistema	Um elemento malicioso pode se passar por um elemento verdadeiro	Autenticação mútua dos elementos	Yegneswaran et al. 2004]
Ofuscação	Afeta o desempenho do sistema	Elemento malicioso envia grande quantidade de dados falsos para ofuscar o processo de detecção	Controle do fluxo e filtragem da quantidade de mensagens que excedam determinado limite	Yegneswaran et al. 2004]
		Elemento malicioso envia pequena quantidade de dados falsos para ofuscar o processo de detecção	Mecanismos de correlação de dados eficientes	
		Tentativa de localização (*scanning*) furtiva ou coordenada dos elementos	Controle de acesso nos mecanismos de registro e pesquisa para localização dos elementos	
			Uso do maior número possível de elementos a fim de detectar tentativas de *scanning*	

Agrupamento dos Riscos

Risco	Ameaça	Conseqüências	Como pode ocorrer
RS1.1	Espionagem	Confidencialidade	Atacantes interceptam as mensagens de alerta trocadas entre os elementos de IDS
RS1.2	Espionagem	Confidencialidade	Elementos comprometidos são usados para coletar e enviar informações sigilosas
RS1.3	Negação de Serviço	Disponibilidade	Desativação de Elementos por ataques diretos, explorando vulnerabilidades
RS1.4	Negação de Serviço	Disponibilidade	Elementos maliciosos enviam grande quantidade de dados falsos
RS1.5	Mascaramento	Integridade e Confidencialidade	Um elemento malicioso pode se passar por um elemento verdadeiro
RS1.6	Ataque de Evasão	Disponibilidade	O sistema alvo aceita pacotes que o IDS rejeita. Atacante envia pacotes truncados ou com uma ordem trocada para iludir o sensor
RS1.7	Ataque de Inserção	Disponibilidade	O IDS aceita pacotes que são rejeitados pelo sistema alvo. Atacante envia pacotes diretamente ao sensor a fim de iludi-lo.
RS1.8	Ofuscação	Disponibilidade	Elemento malicioso envia grande quantidade de dados falsos para ofuscar o processo de detecção
RS1.9	Ofuscação	Disponibilidade	Elemento malicioso envia pequena quantidade dados falsos para ofuscar o processo de detecção
RS1.10	Ofuscação	Disponibilidade	Tentativa de localização (*scanning*) furtiva ou coordenada dos elementos
RS1.11	Filtragem de Alertas	Disponibilidade, Integridade e Confidencialidade	Atacantes interceptam mensagens com alertas sobre suas atividades, descartando-as, redirecionando-as ou alterando-as seletivamente
RS1.12	Comprometimento de Elementos de IDS	Disponibilidade, Integridade e Confidencialidade	Atacantes alteram o código ou a configuração do elemento
RS1.13	Interrupção ou desvio de conexão (*hijacking*)	Disponibilidade, Integridade e Confidencialidade	Atacantes interceptam ou desviam uma conexão entre elementos de IDS

Agrupamento dos Controles

Item	Controle	Referências	Custo
CS1	Autenticação	[Yegneswaran et al. 2004] [Demchenko et al 2005] [Yu et al., 2005] [Lindqvist and Jonsson 1998] [Han e Zheng, 2000]	BAIXO
CS2	Assinatura	[Demchenko et al 2005] [Yu et al., 2005] [Dacier 2002]	BAIXO
CS3	Controle de Acesso	[Demchenko et al 2005] [Yu et al., 2005] [Yegneswaran et al. 2004]	BAIXO
CS4	Controle de fluxo	[Lindqvist and Jonsson 1998] [Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Feiertag et al., 2000b] [Frincke, 2000]	BAIXO
CS5	Criptografia	[Mell et al 2000] [Dacier 2002] [Demchenko et al 2005] [Yu et al., 2005]	BAIXO
CS6	Detecção de falhas	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Demchenko et al 2005] [Yu et al., 2005] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	BAIXO
CS7	Filtragem de Tráfego	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Feiertag et al., 2000a, 2000b]	BAIXO
CS8	Reativação automática	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	BAIXO
CS9	Sensores baseados em aplicação	[Ptacek and Newsham 1998]	BAIXO
CS10	*Timestamps* e *cache*	[Demchenko et al 2005] [Yu et al., 2005]	BAIXO
CS11	Análise de Conteúdo	[Demchenko et al 2005] [Yu et al., 2005]	MÉDIO
CS12	Correlação de dados	[Yegneswaran et al. 2004] [Dacier 2002]	MÉDIO
CS13	Distribuição de sistemas	[Yegneswaran et al. 2004] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	MÉDIO
CS14	Diversidade	[Ptacek and Newsham 1998]	MÉDIO
CS15	Política de Segurança	[Lindqvist and Jonsson 1998] [Feiertag et al., 2000a, 2000b]	MÉDIO
CS16	Replicação	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Dacier 2002] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	MÉDIO
CS17	Seleção dinâmica	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002]	MÉDIO
CS18	Gerenciamento	[Lindqvist and Jonsson 1998] [Han e Zheng, 2000] [Charfi e Mezini, 2005] [Feiertag et al., 2000a, 2000b] [Demchenko et al 2005] [Yu et al., 2005] [Frincke, 2000]	MÉDIO
CS19	Uso de recursos exclusivos	[Mell et al 2000] [Dacier 2002]	ALTO

Estimativa de Riscos

- Dados que irão auxiliar na decisão sobre quais riscos serão tratados e as formas de tratamento com melhor eficiência de custos
- Todo risco tem um custo e este custo pode ser quantificado de forma mais ou menos precisa

Metodologias para a Estimativa de Riscos

- Qualitativa
  - Escala com atributos qualificadores que descrevem a magnitude das potenciais conseqüências e a probabilidade destas conseqüências ocorrerem
- Quantitativa
  - Escala de valores numéricos tanto para conseqüências, quanto para a probabilidade
- Combinação de ambas

Probabilidades

- A probabilidade de um evento ocorrer durante um período de tempo determinado é expressa por um número entre zero e um.
- Quanto maior for o período de tempo considerado, maior será a probabilidade.
- Calculadas por meio de análises de dados de ataques ou ameaças.
  - Experiências na própria empresa
  - Coletâneas adquiridas de organizações especializadas.

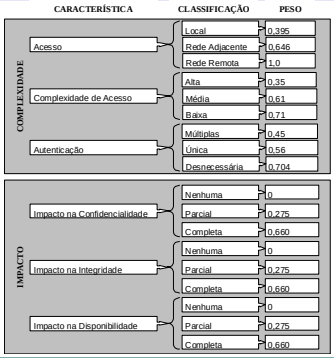
Common Vulnerability Scoring System – CVSS

- Adotado pelo NIST para a classificação de vulnerabilidades no *National Vulnerability Database* (NVD)
- Permite calcular os riscos que uma vulnerabilidade inflige no ambiente real
- Dispensa dados estatísticos precisos sobre ataques anteriores ou análises financeiras complexas.
- Aplicado ao inventário atualizado dos ativos, sistemas e serviços de TI.

Metodologia do CVSS

- Critérios qualitativos para a caracterização das vulnerabilidades
- Três áreas:
  - Métricas básicas
  - Métricas temporais
  - Métricas ambientais
- As características são valoradas e processadas para obter uma pontuação final ajustada, que irá representar as ameaças que uma vulnerabilidade apresenta em determinado instante de tempo para um ambiente específico
- Pontuação entre 0 (sem riscos) e 10 (maior risco)
- Classificação:
  - Baixo: 0 – 3
  - Médio: 4 – 7
  - Alto: acima de 7

Métricas Básicas



Complexidade

- Vetor de Acesso (AV)
- Autenticação (AU)
- Complexidade de Acesso (AC)

20 * AC * AU * AV

Impacto:

- Confidencialidade (CI)
- Integridade (II)
- Disponibilidade (AI)

10,41 * (1 - (1 - CI) * (1 - II) * (1 - AI))

Risco Básico

(0,6 * Impacto + 0,4 * Complexidade - 1,5) * f(Impacto)

- **f(Impacto)**, terá o valor 0 (zero) se o Impacto for igual a zero. Caso contrário, receberá o valor 1,176.

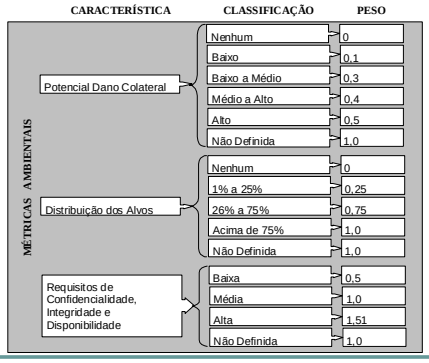
Métricas Temporais

Risco Temporal

- Explorabilidade (EX),
- Nível de Remediação (RL)
- Grau de Confiança (RC)

Risco Básico * EX * RL * RC

Métricas Ambientais



Variáveis das Métricas Ambientais

- **Potencial Dano Colateral (CD)**
  - Nenhum;
  - Baixo, se há danos físicos, perda de lucros ou de produtividade leves;
  - de Baixo a Médio, com danos físicos, perda de lucros ou de produtividade moderados;
  - de Médio a Alto, se houver danos físicos, perda de lucros ou de produtividade significativos;
  - Alto, quando há a possibilidade de danos físicos, perda de lucros ou de produtividade catastróficos.
- **Distribuição dos Alvos (TD)**
  - Baixo, entre 1% e 25%;
  - Média, entre 26% e 75%;
  - Alta, acima de 75%; e
  - Nenhum
- **Requisitos de Segurança**
  - Requisito de Confidencialidade (CR)
  - Requisito de Integridade (IR)
  - Requisito de Disponibilidade (AR)

Ajuste Temporal

- **Risco Temporal** recalculado, substituindo o **Risco Básico** pelo **Impacto Ajustado**
- Impacto Ajustado:

**min (10, 10,41 *
(1 - (1 - CI*CR) * (1 - II*IR) * (1 - AI*AR)))**

Risco Ambiental

**((Ajuste Temporal +
(10 - Ajuste Temporal) * CD) * TD)**

Exemplo: Vulnerabilidade *CVE-2008-1947* do Tomcat

- Vetor de Acesso (AV) = Remota = 1,0
- Complexidade de Acesso (AC) = Média = 0,61
- Autenticação (AU) = Desnecessária = 0,704
- Impacto na Confidencialidade (CI) = Nenhuma = 0
- Impacto na Integridade (II) = Parcial = 0,275
- Impacto na Disponibilidade (AI) = Nenhuma = 0
- Métricas Temporais = Não Definidas = 1
- Potencial Dano Colateral (CD) = Baixo = 0,1
- Distribuição dos Alvos (TD) = 5% = 0,25
- Requisito de Disponibilidade (AR) = Alta = 1,51
- Requisito de Integridade (IR) = Alta = 1,51
- Requisito de Confidencialidade (CR) = Alta = 1,51

Cálculo do Risco Básico

- **Impacto**
  10,41 * (1 - (1 - CI) * (1 - II) * (1 - AI)) =
  10,41 * (1 - (1 - 0) * (1 - 0,275) * (1 - 0)) = 2,9
- **Complexidade**
  20 * AC * AU * AV =
  20 * 1 * 0,61 * 0,704 = 8,6
- **Risco Básico**
  (0,6 * Impacto + 0,4 * Complexidade - 1,5) * f(Impacto) =
  (0,6 * 2,86 + 0,4 * 8,6 - 1,5) * 1,176 = 4,3
- Risco Básico **Médio**

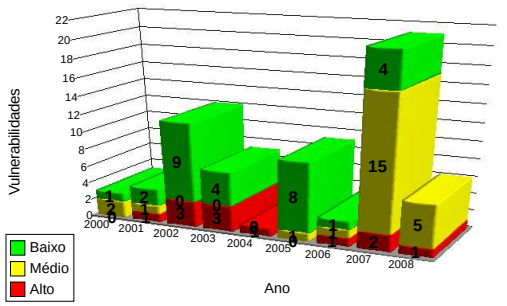
Cálculo do **Risco Temporal**

- **Impacto Ajustado**
  min(10, 10,41 * (1 - (1 - CI*CR) * (1 - II*IR) *
  (1 - AI*AR))) =
  min(10, 10,41 * (1 - (1 - 0 * 1,51) * (1 - 0,275 * 1,51) *
  (1 - 0 * 1,51))) = **4,3**
- **Risco Básico Ajustado**
  (0,6 * 4,3 + 0,4 * 8,6 - 1,5) * 1,176 = **5,3**
- **Risco Temporal**
  Risco Básico * EX * RL * RC =
  5,3 * 1 * 1 * 1 = **5,3**
- Risco Temporal **Médio**

Cálculo do Risco Ambiental

- **Risco Ambiental**
  ((Ajuste Temporal + (10 - Ajuste Temporal)
  * CD) * TD) =
  ((5,3 + (10 - 5,3) * 0,1) * 0,25) = 1,4
- Risco Ambiental **Baixo**

Distribuição das Vulnerabilidades do Tomcat



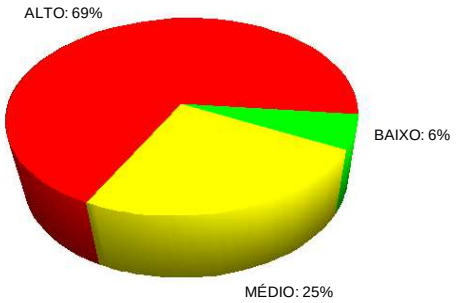
Níveis de Risco de Segurança

Item	Acesso	Complexidade de Acesso	Autenticação	Impacto na Confidencialidade	Impacto na Integridade	Impacto na Disponibilidade	Score	Nível de Risco
1.1	REMOTO	BAIXA	DESNECESSÁRIA	COMPLETA	NENHUMA	NENHUMA	7,8	ALTO
1.2	LOCAL	ALTA	ÚNICA	COMPLETA	NENHUMA	NENHUMA	3,8	BAIXO
1.3	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	PARCIAL	COMPLETA	8,5	ALTO
1.4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	COMPLETA	7,8	ALTO
1.5	LOCAL	ALTA	ÚNICA	COMPLETA	PARCIAL	NENHUMA	4,5	MÉDIO
1.6	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.7	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.8	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.9	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.10	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.11	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	PARCIAL	7,3	ALTO
1.12	LOCAL	ALTA	ÚNICA	COMPLETA	COMPLETA	COMPLETA	6,0	MÉDIO
1.13	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	7,6	ALTO

Avaliação de Riscos

- Tomar decisões
- Resultados da análise de risco
  - Identificação
  - Estimativa de Riscos
- Considerações
  - Propriedades
  - Importância para o negócio ou projeto
  - Custo-benefício
- Ao término da avaliação é verificado se seu resultado é satisfatório

Níveis de Risco Iniciais



Tratamento do Risco

- Identificação de opções de tratamento
- Avaliação das opções
- Preparação para a implementação dos tratamentos selecionados
- Lista de riscos ordenados por prioridade
- Opções de tratamento
  - Redução
  - Retenção
  - Evitação
  - Transferência
- Riscos residuais

Riscos Tratados

Risco	Controles	Acesso	Complexidade de Acesso	Autenticação	Impacto na Confidencialidade	Impacto na Integridade	Impacto na Disponibilidade	Escore	Nível de Risco
1.1	C19	LOCAL	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
1.1	C5	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
1.2	C4	LOCAL	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	1,0	BAIXO
1.3	C6 + C8	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C16	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C7	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C17	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.4	C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.5	C1	LOCAL	ALTA	ÚNICA	COMPLETA	PARCIAL	NENHUMA	4,5	MÉDIO
1.6	C9	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.6	C14	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.7	C9	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.7	C14	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.8	C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.9	C12	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.10	C3	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	PARCIAL	2,1	BAIXO
1.10	C13	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.11	C2 + C5	REMOTO	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	2,1	BAIXO
1.12	C16	LOCAL	ALTA	ÚNICA	PARCIAL	NENHUMA	PARCIAL	2,4	BAIXO
1.13	C5	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	PARCIAL	PARCIAL	4,0	MÉDIO

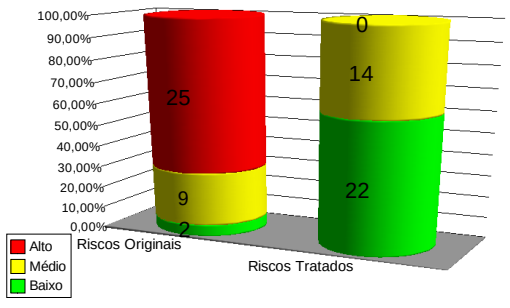
Avaliação e Seleção dos Tratamentos de Segurança

Risco	Controles	Escore Original	Escore Tratado	Nível de Risco Original	Nível de Risco Tratado	Custo	Aplicação
1.1	C19	7,8	0,0	ALTO	BAIXO	ALTO	Não
1.1	C5	7,8	0,0	ALTO	BAIXO	BAIXO	Sim
1.2	C4	3,8	1,0	BAIXO	BAIXO	BAIXO	Sim
1.3	C6 + C8	8,5	5,0	ALTO	MÉDIO	BAIXO	Sim
1.3	C16	8,5	5,0	ALTO	MÉDIO	MÉDIO	Não
1.3	C7	8,5	5,0	ALTO	MÉDIO	BAIXO	Sim
1.3	C17	8,5	5,0	ALTO	MÉDIO	MÉDIO	Não
1.4	C4	7,8	5,0	ALTO	MÉDIO	BAIXO	Sim
1.5	C1	4,5	4,5	MÉDIO	MÉDIO	BAIXO	Sim
1.6	C9	5	2,6	MÉDIO	BAIXO	BAIXO	Sim
1.6	C14	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.7	C9	5	2,6	MÉDIO	BAIXO	BAIXO	Sim
1.7	C14	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.8	C4	5	5,0	MÉDIO	MÉDIO	BAIXO	Sim
1.9	C12	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.10	C3	5	2,1	MÉDIO	BAIXO	BAIXO	Sim
1.10	C13	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.11	C2 + C5	7,3	2,1	ALTO	BAIXO	BAIXO	Sim
1.12	C16	6	2,4	MÉDIO	BAIXO	MÉDIO	Sim
1.13	C5	7,6	4,0	ALTO	MÉDIO	BAIXO	Sim

Aceitação do Risco

- Análise do risco residual
- Registro formal e responsabilização
- Resultados nem sempre satisfatórios
- Fatores como tempo e custos podem justificar a aceitação dos riscos

Comparativo dos Níveis de Risco de Segurança



Monitoramento e Análise Crítica dos Riscos

- Os riscos não são estáticos
- Monitoração para verificar a eficácia das estratégias de implementação e mecanismos de gerenciamento utilizados no tratamento dos riscos
- Processo contínuo e dinâmico
- Mudanças organizacionais ou externas
  - Alteram o contexto da análise
  - Revisão completa da gestão de riscos
- Revisões periódicas

Considerações sobre o Estudo de Caso

- Identificação de riscos nas composições de IDSs;
- Análise e avaliação dos riscos de segurança;
- Tratamentos para riscos operacionais discutidos na literatura científica;
- Identificação de riscos e tratamentos associados a IDSs distribuídos;
- Identificação de riscos e tratamentos associados ao uso de COTS; e
- Identificação de riscos e tratamentos associados à composição dinâmica de IDSs.
- A gestão de riscos também pode ser aplicada em outras etapas do projeto, como na avaliação dos produtos utilizados no desenvolvimento do protótipo.

Conclusões

- Com a utilização da metodologia de gestão de riscos, espera-se a identificação e o tratamento da maioria das vulnerabilidades conhecidas e pertinentes às soluções adotadas em um projeto de Tecnologia da Informações.
- Isso sem dúvida auxilia no entendimento dos problemas de segurança que seriam enfrentados, tendo como conseqüência a melhoria do projeto como um todo.
- Infelizmente, não é possível garantir que o projeto seja totalmente seguro. Contudo, podemos afirmar que, com a realização de boas práticas de gestão de risco, são tomadas todas as medidas preventivas necessárias à atenuação do impacto negativo que possíveis vulnerabilidades infringiriam ao projeto.

Contatos:

- José Eduardo Malta de Sá Brandão
  je.brandao@ipea.gov.br
- Joni da Silva Fraga
  fraga@das.ufsc.br