Projeto 2.02
Proposta do Modelo de Qualidade de Requisitos de Segurança para Aplicativos de Software na Web

Rio de Janeiro, 02 de setembro de 2011

Equipe da DSSI: **Regina M Thienne Colombo**
Amândio F Balcão Filho
Ana Cervigni Guera

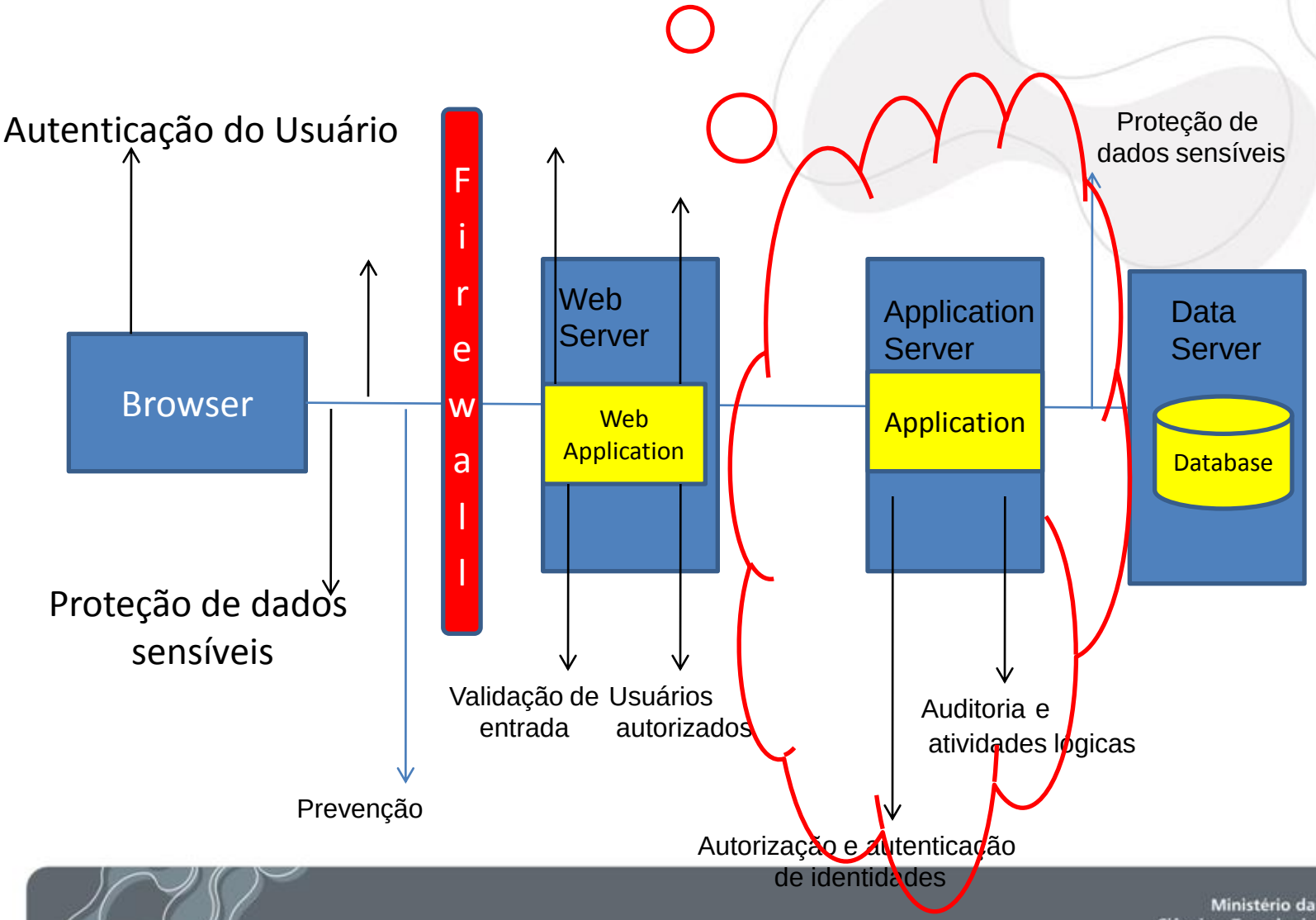
Conteúdo

- Objetivos
- Justificativa
- Proposta
- Resultados esperados
- Características
- Referências

Objetivos

- Especificar e avaliar requisitos de segurança para aplicativos Web;
- Propor um Modelo de Requisitos de Segurança, que dará a estrutura conceitual para medições de Segurança em aplicativos Web;
- O Modelo é direcionado a vulnerabilidades e ameaças, é centrado em requisitos;
- O Modelo utiliza a abordagem de decomposição de requisitos para obter os componentes mensuráveis (BMC);
- O Modelo utiliza métodos formais consagrados (AHP) para possibilitar a confiança nos componentes mensuráveis;
- A avaliação de requisitos de Segurança será utilizado na fase de operação e uso da aplicação.

Aplicação WEB - Arquitetura



Justificativa

- Aumento de riscos/ameaças/vulnerabilidades de segurança em aplicativos web
- Pesquisa do Instituto Ponemom de 2010
- Falta de uma abordagem sistemática de medição de segurança
- Trabalhos correlatos atuais
- Modelos e padrões de Segurança de Aplicação Web
- Experiência com avaliação de qualidade de produtos de SW

Considerações

Como revelado na pesquisa, as aplicações web estão em risco, pelas seguintes razões:

- 70 % não acreditam que suas organizações alocam recursos suficientes para proteger aplicativos Web crítico.
- 34 % das vulnerabilidades de urgência não são corrigidos.
- 38 % acreditam que levaria mais de 20 horas de tempo de desenvolvedor para corrigir uma vulnerabilidade.
- 55 % acreditam que os desenvolvedores estão ocupados demais para responder a questões de segurança

Mais importante, o risco para Aplicações Web devem ser reconhecidos por altos executivos como uma ameaça real para ativos de informação da organização. As organizações estão ignorando este risco a seu próprio prejuízo.

Técnicos
Experts em Segurança

Código Fonte

Dados

Servidor

Redes

Hackers

Curiosos

Ameaças e Ataques

Gestão de Negócios de TI

Usuários

Riscos

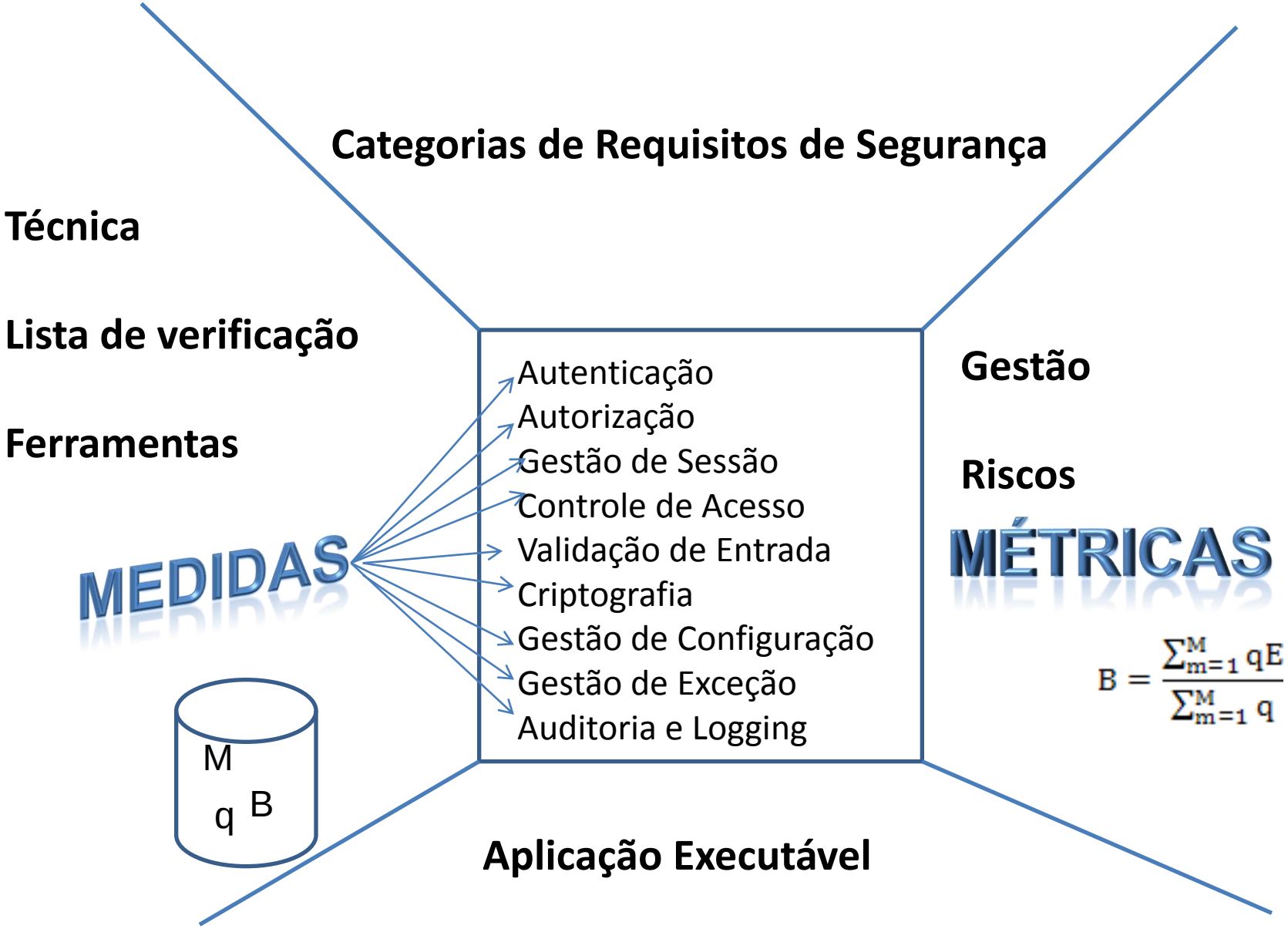
Proposta

Aplicações Web
Executáveis
Vulneráveis

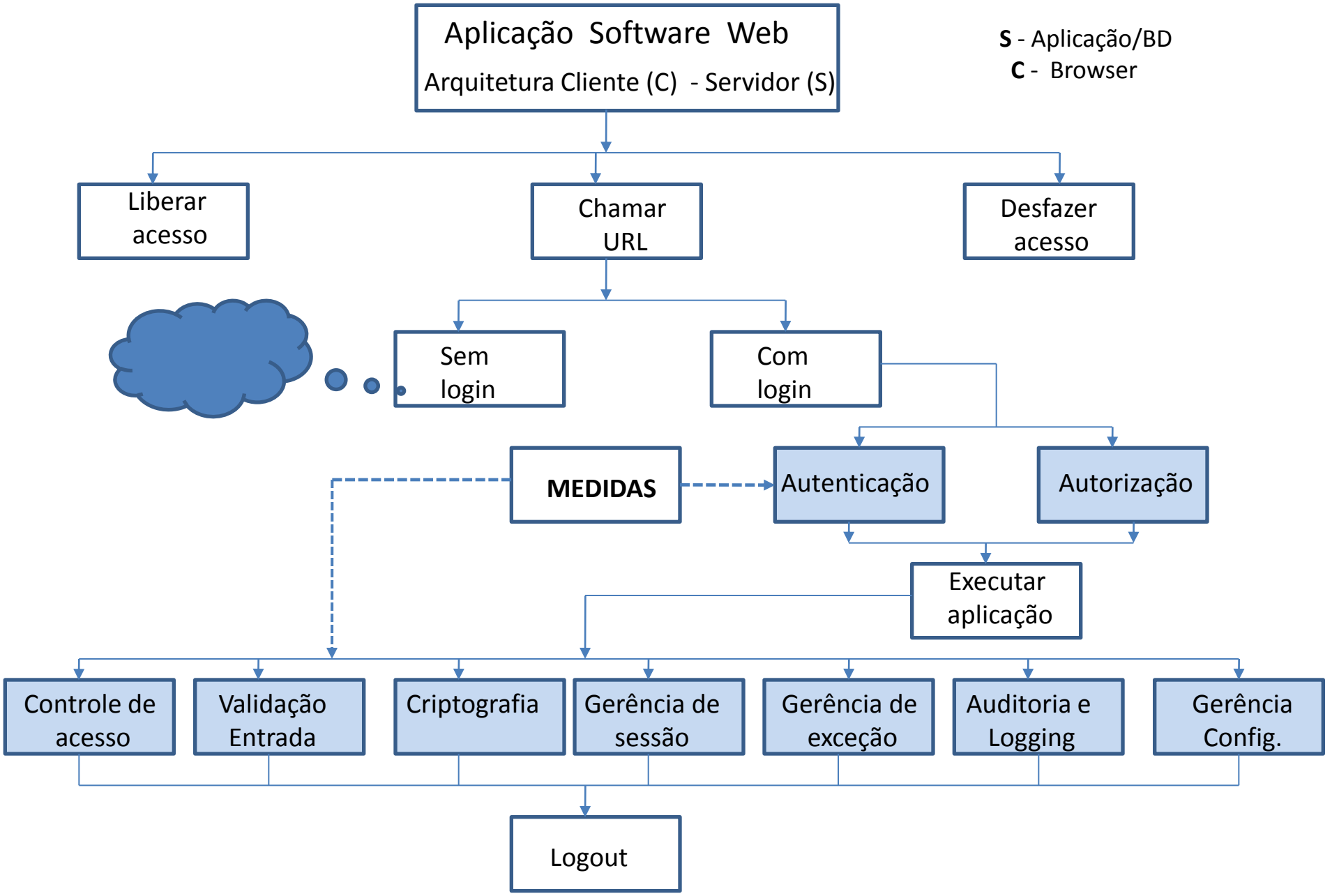
Propriedades da Segurança

Confidencialidade
Integridade
Disponibilidade
Não - Repúdio
Responsabilidade
Autenticidade

Aplicação Executável


Categorias de Requisitos de Segurança
Técnica
Lista de verificação
Ferramentas
MEDIDAS
Autenticação
Autorização
Gestão de Sessão
Controle de Acesso
Validação de Entrada
Criptografia
Gestão de Configuração
Gestão de Exceção
Auditoria e Logging
Gestão
Riscos
MÉTRICAS
$B = \frac{\sum_{m=1}^{M} qE}{\sum_{m=1}^{M} q}$
M
q B
Aplicação Executável

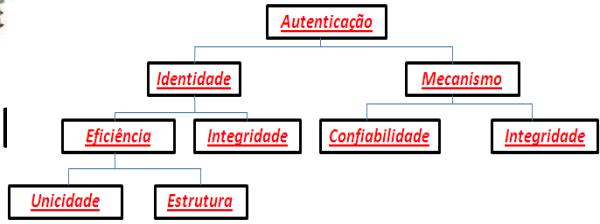
ROTEIRO DE AVALIAÇÃO



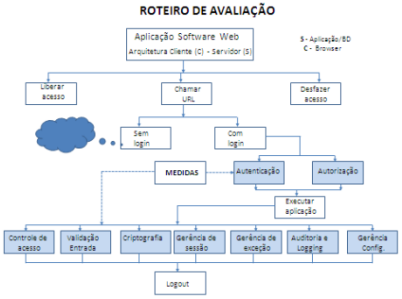
Resultados esperados

- Levantamento bibliográfico

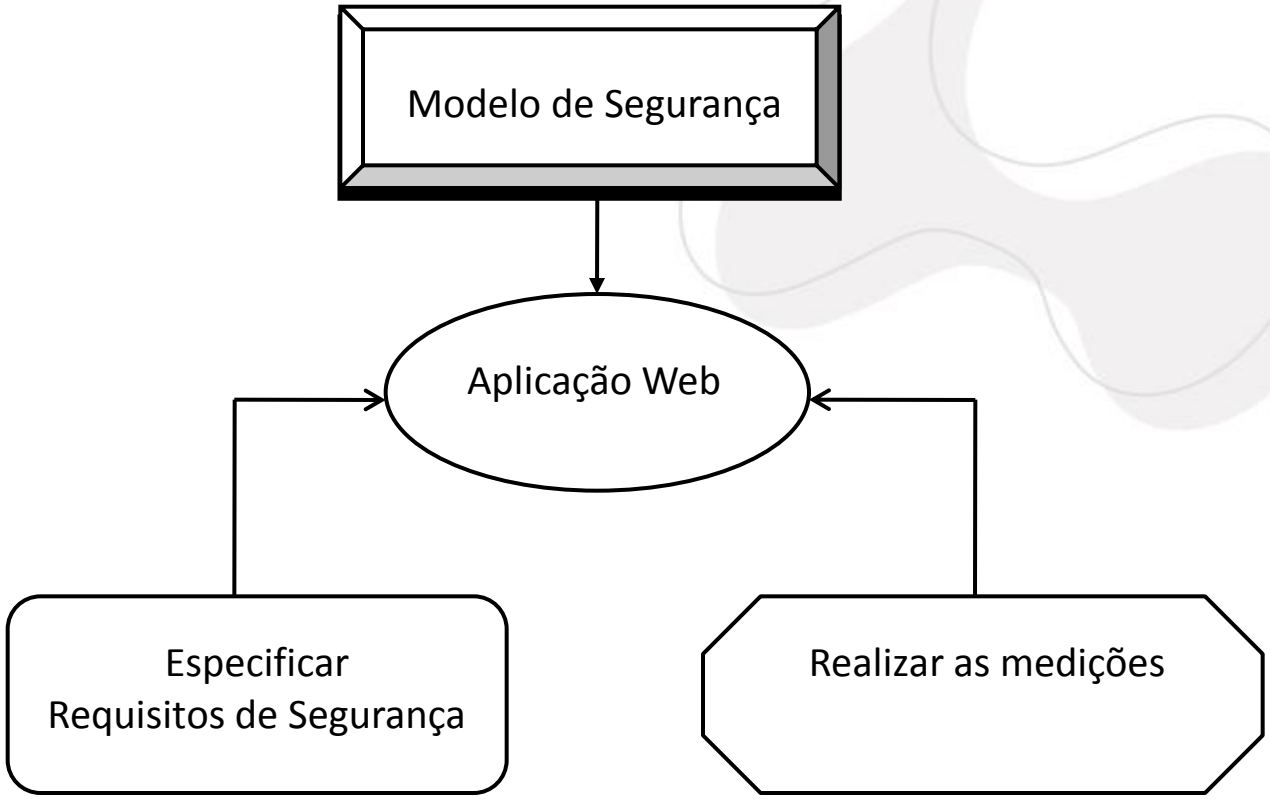
- Modelo de Requisitos de Segurança



- Roteiro de Avaliação



- Aplicação piloto da avaliação em um aplicativo web



Objetivo – Promover a Segurança de Aplicação Web

Cronograma 2011

Janeiro-Março	- Levantamento e estudo bibliográfico
Abril-Junho	- Elaboração do Modelo de Requisitos
Julho-Setembro	- Roteiro de avaliação e Medidas
Outubro-Dezembro	- Aplicação piloto, Artigo

Referências

ISO/IEC 27002:2005 – Gestão de SI

ISO/IEC 15408:2005 – Common Criteria

- ISO/IEC 25010 - Qualidade de produto - Modelo de qualidade
- ISO/IEC 25040 - Processo de Avaliação de software

Nancy Mead 

 Reijo Savola

 Karen Goertzel

Michael Howard

ASP - ASVS

Características

Relevância

Impacto

Abrangência

Inovação

Obrigada!

Regina Maria Thienne Colombo

MCTI - Ministério da Ciência, Tecnologia e Inovação
CTI - Centro de Tecnologia da Informação Renato Archer
Divisão de Sistema de Segurança da Informação

e-mail: regina.thienne@cti.gov.br
Telefone +55 (19) 3746-6107