Segurança de dados e Auditoria de Sistemas

COMO AVALIAR A SEGURANÇA?

ISO/IEC 15.408

- Padronizando a segurança de sistemas

ISO/IEC 15.408

- Padronizando a segurança de sistemas

BOMPRATODOS

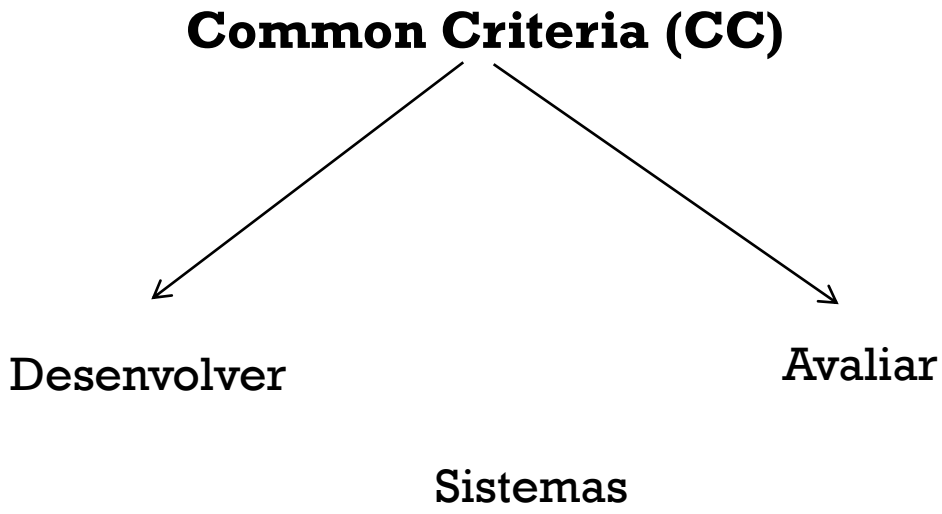
ISO/IEC 15.408

- Objetivo:

O objetivo da norma é fornecer um conjunto de critérios objetivos que permitam especificar a segurança de uma aplicação de forma clara, a partir de características do ambiente da aplicação e definir formas de garantir a segurança da aplicação para o cliente final.

ISO/IEC 15.408

- Também apelidado de :



COMMON CRITERIA

http://www.commoncriteriaportal.org/products/

ZTE Base Station Controller Series
ZTE Corporation

Certification Report | Security Target

ZTE Access System Series
ZTE Corporation

Certification Report | Security Target

IBM Tivoli Access Manager for e-business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2
IBM Corporation

Certification Report | Security Target

Atenção na versão!

SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7
Utimaco Safeware AG

Certification Report | Security Target

Active Directory Federation Services 2.0

COMMON CRITERIA

- Garantias

Certificação →

Ameaça Específica

Ambiente Específico

COMMON CRITERIA

- Partes Interessadas

PP

Desenvolvedor/Vendedor

Avaliador/Testador

Consumidor
(Define o "Perfil de Proteção (PP)")

Aprovador

COMMON CRITERIA DOCUMENT

- Parte 1 - Introdução e Modelo Geral
- Parte 2 – Requisitos Funcionais de Segurança
- Parte 3 - Requisitos de Garantia da Segurança

COMMON CRITERIA DOCUMENT

- Parte 1 - Introdução e Modelo Geral
  - Conceitos Gerais
  - Como expressar os objetivos de segurança
  - Expressar a utilidade para cada interessado

COMMON CRITERIA DOCUMENT

- Parte 2 – Requisitos Funcionais de Segurança
  - Padrão de expressar requisitos de segurança

COMMON CRITERIA DOCUMENT

- Parte 3 - Requisitos de Garantia da Segurança
  - Apresenta os sete níveis do Evaluation Assurance Leves (EALs)

EVALUATION ASSURANCE LEVELS (EALS)

- EAL1 – Testado Funcionalmente
- EAL2 – Testado Estruturalmente
- EAL3 – Metodologicamente Testado e checado
- EAL4 - Metodologicamente Desenhado, Testado e Revisado
- EAL5 – Semi-Formalmente Desenhado
- EAL6 - Semi-Formalmente Desenho verificado
- EAL7 – Formalmente Desenhado, verificado e Testado.

EVALUATION ASSURANCE LEVELS (EALS)

- EAL1 – Testado Funcionalmente
  - Ameaças não sérias
  - Alguma confiança é necessária
  - Sem assistência do desenvolvedor do "TOE"
  - Requisitos
    - Teste de desenvolvedor,
    - Análise de Vulnerabilidades

EVALUATION ASSURANCE LEVELS (EALS)

- EAL2 – Testado Estruturalmente
  - Ver o código
  - Cooperação do desenvolvedor
  - Requisitos
    - Gestão de Configuração
    - Entrega e Operação
    - Desenvolvimento,
    - Documentos GUia
    - Testes Gerais

EVALUATION ASSURANCE LEVELS (EALS)

- EAL3 – Metodologicamente Testado e checado
  - Precisa de cooperação do Desenvolvedor
  - Adiciona requisitos de testes, controle de ambiente de execução e gestão de configuração

EVALUATION ASSURANCE LEVELS (EALS)

- EAL4 - Metodologicamente Desenhado, Testado e Revisado
  - Quando as práticas de desenvolvimento inclui engenharia de segurança
  - Requisitos
    - Gestão de Configuração
    - Desenho
    - Desenvolvimento,
    - Análise de Vulnerabilidades

EVALUATION ASSURANCE LEVELS (EALS)

- EAL5 – Semi-Formalmente Desenhado e Testado
  - Rigorosas práticas de desenvolvimento comercial
  - Moderado uso de especialistas

EVALUATION ASSURANCE LEVELS (EALS)

- EAL6 - Semi-Formalmente Desenhado Verificado e Testado
  - Produto valioso
  - Onde os riscos são altos

EVALUATION ASSURANCE LEVELS (EALS)

- EAL7 – Formalmente Desenhado, verificado e Testado.
  - Produto altamente valioso
  - Riscos extremamente altos

- Seguir o modelo Common Criteria é fácil?

ALBUQUERQUE 2002 PROPÔS OUTRO PROCESSO:

- Em caso de desenvolvimento
  - Especificar a aplicação na fase de análise gerando um doc de especificação com base no ISO/IEC 15.408
  - Tentar atingir apenas o EAL3 mantendo o ambiente de desenvolvimento e testes seguro
  - Usar boas práticas de programação seguindo req. de segurança
  - Testar o sistema internamente

ALBUQUERQUE 2002 PROPÔS OUTRO PROCESSO:

- Em caso de aplicação já desenvolvida
  - Levantar a especificação de segurança usando o ISO/IEC 15.408
  - Levantar os requisitos existentes e o necessário
  - Verificar se os requisitos implementados atendem à necessidade de segurança da especificação inicial
  - Escolha um nível de garantia de segurança (até EAL3!)

ESPECIFICAÇÃO DA SEGURANÇA DESEJADA

PORQUE PRECISAMOS DE SEGURANÇA NOS SISTEMAS ?(SEGUNDO ALBUQUERQUE)

Por conta de legislações ou políticas de segurança

Pela existência de ameaças

PASSOS GERAIS

Levantar as **necessidades legais** e as **políticas** de segurança.

Verificar que tipo de **ameaças** o sistema está sujeito.

Consolidar os **objetivos de segurança**

ASPECTOS A SEREM CONSIDERADOS

- **Políticas de Segurança**: Diretrizes, normas, regulamentos, padrões e legislação.
- **Ameaças**: Mecanismos de ataque a ativos a serem controlados.
- **Objetivos de Segurança**: Formalização das necessidades de seg. do usuário.
- **Premissas**: Fatos sobre o uso do sistema e seu ambiente.

ATENÇÃO AO FOCO DAS ETAPAS

- Levantamento das ameaças
  - Objetividade

ATENÇÃO AO FOCO DAS ETAPAS

- Objetivos de segurança (ser explícito)
  - O sistema deve ser capaz de rastrear uma ação e ligá-la ao responsável.
  - Manter a capacidade de rastreamento de ações mesmo que essas sejam do administrador do sistema.
  - O sistema deve ser capaz de se recuperar de uma perda completa por desastre natural.
  - O sistema deve fornecer meios de ser auditado para seguir a legislação vigente.