**ISO IEC 15.408**

A ISO/IEC 15408, uma norma de produtos em TI, mas também faz a avaliação de requisitos de segurança de produtos tratando definições de componentes de segurança e mostra como avaliar sistemas frente aos requisitos de segurança. A norma conhecida como Common Critéria é formada por um conjunto de três níveis:

* Primeiro - discute definições e metodologia
* Segundo - lista requisitos de segurança
* Terceiro - lista metodologias de avaliação

A norma avalia produtos do tipo de gerenciamento de configuração, entrega e instalação do software, desenvolvimento e documentação.

**Common Criteria (CC)** é um padrão internacional (ISO/IEC 15408) para segurança de computadores. Este padrão é voltado para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras. Ele define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas.

Common Criteria é um framework em que os usuários de sistemas computacionais podem especificar seus requisitos funcionais de segurança e garantia. Dessa forma os fornecedores podem, então, implementar e/ou fazer alegações sobre os atributos de segurança de seus produtos, enquanto que os laboratórios de teste podem avaliar os produtos para determinar se eles realmente cumprem as reivindicações. Em outras palavras, Common Criteria fornece uma garantia de que o processo de especificação, implementação e avaliação de um produto de segurança computacional foi conduzido de uma maneira rigorosa e padronizada.

**Perfil de Proteção (Protection Profile – PP):**consiste de um documento tipicamente criado por um usuário, ou comunidade de usuários, o qual identifica requisitos de segurança para uma classe de dispositivos de segurança (por exemplo, smart cards utilizadas para prover Assinatura Digital, ou firewalls de rede) relevantes para aquele usuário ou grupo de usuários. Desenvolvedores de software podem escolher desenvolver os seus produtos de acordo com um ou mais PPs e, então, validar estes produtos de acordo com estes documentos. Neste caso, o PP pode servir como template para o ST (Security Target);

**Security Target** (ST) pode ser definido como uma "declaração de **aplicação específica** das necessidades de segurança de um alvo identificado específico de avaliação (TOE)”.

**Alvo de Avaliação (Target of Evaluation – TOE):** consiste do produto ou sistema que é alvo da avaliação. A análise tem por intuito validar afirmações feitas a cerca do alvo. Em termos práticos, a avaliação deve verificar as características de segurança do produto ou sistema.

**15408 - terminologia**

A ISO/IEC 15408 define uma serie de termos e abreviações que são necessárias para entender a norma.

**Alvo de avaliação (TOE - target of evaluation)** - um conjunto de software, firmware e(ou) hardware;  
**Perfil de proteção (PP - protection profile)** - uma classe de dispositivos;

**Alvo de segurança (ST - security target)** - um objeto a ser avaliado.  
requisitos funcionais de segurança (SFR - security funcional requirements)  - uma declaração de necessidades de segurança;   
**Requisitos funcionais de segurança (SFR - security funcional requirements)**  - uma declaração de necessidades de segurança;

Pessoal, com uma definição clara dos objetivos da norma ISO/IEC 15.408 pode-se matar a questão. A norma acima é um framework que visa especificar os requisitos de segurança para produtos e serviços computacionais. Com essa especificação é possível guiar o desenvolvimento e avaliação de atributos de segurança dos produtos de software.   
Vejam que o foco é guiar o **desenvolvedor e o avaliador** quanto aos critérios de segurança previstos na norma, detalhados nas ST (Security Targets). Assim, a alternativa A é a correta, pois fala esses dois perfis: desenvolvedor e avaliador.