## 1-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Assembleia Legislativa do Estado de Goiás (AL-GO) - Analista - Datacenter (2019)](https://www.questoesestrategicas.com.br/provas/ver/assembleia-legislativa-do-estado-de-goias-al-go-analista-datacenter-iades-2019)

Donos de informação podem requisitar que a disponibilidade, disseminação e modificação de qualquer informação seja estritamente controlada e que os ativos sejam protegidos de ameaças por meio de contramedidas.  
  
International Organization for Standardization. *ISO/IEC 15408-1*: Introduction and general mode, 2009. Tradução livre.

Segundo a ISO/IEC 15408, existem dois elementos principais que devem ser demonstrados para se poder defender a escolha de contramedidas. Esses elementos determinam que as contramedidas devem ser

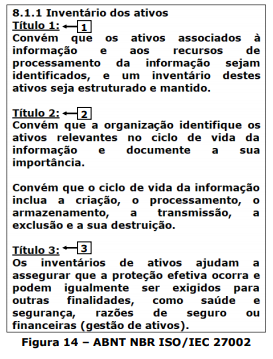
* **A** corretas, ou seja, capazes de fazer o que afirmam, e suficientes, ou seja, caso corretas, devem neutralizar as ameaças.
* **B** corretas, ou seja, capazes de fazer o que afirmam, e imprevisíveis, ou seja, devem ser difíceis de prever.
* **C** imprevisíveis, ou seja, devem ser difíceis de se prever, e suficientes, ou seja, caso corretas devem neutralizar as ameaças.
* **D** complexas, ou seja, difíceis de se compreender, e suficientes, ou seja, caso corretas devem neutralizar as ameaças.
* **E** imprevisíveis, ou seja, devem ser difíceis de se prever, e complexas, ou seja, difíceis de se compreender.

2-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Consórcio de Informática na Gestão Pública Municipal de Santa Catarina (CIGA-SC) - Analista de Sistemas (2018)](https://www.questoesestrategicas.com.br/provas/ver/consorcio-de-informatica-na-gestao-publica-municipal-de-santa-catarina-ciga-sc-analista-de-sistema)

**Para responder à questão, considere a Figura 14 que mostra apenas parte de um texto retirado da ABNT NBR ISO/IEC 27002 Tecnologia da informação — Técnicas de segurança, no qual as palavras originais existentes nos locais apontados pelas setas nº 1, 2 e 3, foram substituídas, intencionalmente, por "Título 1", "Título 2" e "Título 3".**



Nesse caso, os títulos apontados pelas setas nº 1, 2 e 3, devem ser substituídos, respectivamente, pelos seguintes textos:

I. **Título 1**: Controle.

II. **Título 2**: Diretrizes para implementação.

III. T**ítulo 3**: Informações adicionais.

Quais estão corretos?

* **A** Apenas I.
* **B** Apenas II.
* **C** Apenas III.
* **D** Apenas I e II.
* **E** I, II e III.

3-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Contas do Estado do Rio Grande do Norte (TCE-RN) - Tecnologia da Informação - Cargo 5 (2015)](https://www.questoesestrategicas.com.br/provas/ver/tribunal-de-contas-do-estado-do-rio-grande-do-norte-tce-rn-tecnologia-da-informacao-cargo-5-cespe)

Com base nas disposições das normas NBR ISO/IEC 15408 e ISO 38500, julgue o próximo item.  
  
A Common Criteria estabelece que um produto de software implementa determinado conjunto de funcionalidades de segurança, garantindo que este conjunto seja seguro.

* Certo
* Errado

4-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Justiça do Estado de Sergipe (TJ-SE) - Analista Judiciário (2014)](https://www.questoesestrategicas.com.br/provas/ver/tj-se-analista-judiciario-2014-cespe)

Julgue os seguintes itens, com base na NBR ISO/IEC 15408.  
  
O TSF (TOE (*target of evaluation*) security functions) representa as funções de segurança de um TOE que serão avaliadas.

* Certo
* Errado

5-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Justiça do Estado de Sergipe (TJ-SE) - Analista Judiciário (2014)](https://www.questoesestrategicas.com.br/provas/ver/tj-se-analista-judiciario-2014-cespe)

Julgue os seguintes itens, com base na NBR ISO/IEC 15408.  
  
O PP (*protection profile*) compõe os requisitos de auditoria para a avaliação do sistema.

* Certo
* Errado

6-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Agência Nacional do Cinema (ANCINE) - Analista Administrativo - Área 2 (2013)](https://www.questoesestrategicas.com.br/provas/ver/ancine-analista-administrativo-area-2-2013-cespe)

Julgue o próximo item , acerca de segurança da informação.  
  
O principal objetivo da norma ISO/IEC 15.408 é especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

* Certo
* Errado

7-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Agência Nacional de Transportes Terrestres (ANTT) - Analista Administrativo - Desenvolvimento de Sistemas da Informação (2013)](https://www.questoesestrategicas.com.br/provas/ver/antt-analista-administrativo-desenvolvimento-de-sistemas-da-informacao-2013-cespe)

Julgue os itens seguintes, a respeito de segurança da informação.  
  
A falta de rotina de substituição periódica e a destruição de um equipamento, ocasionada pela inexistência dessa rotina, são consideradas ameaças no gerenciamento de risco e devem ser tratadas, após a identificação dos equipamentos de*hardware*possivelmente afetados, por meio da utilização de ações descritas na NBR ISO/IEC n.º 15.408.

* Certo
* Errado

8-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [Segurança de sistemas de informação](https://www.questoesestrategicas.com.br/questoes/busca/assunto/seguranca-de-sistemas-de-informacao) | [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Justiça do Estado de Minas Gerais (TJ-MG) - Ciências da Computação (2012)](https://www.questoesestrategicas.com.br/provas/ver/tribunal-de-justica-do-estado-de-minas-gerais-tj-mg-tecnico-de-nivel-superior-ciencias-da-computac)

Em relação às normas relacionadas a segurança da informação, julgue os itens a seguir, marcando com (**V**) a assertiva verdadeira e com (**F**) a assertiva falsa.  
  
( ) A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.  
( ) A elaboração de uma política de segurança da informação deve ser o primeiro passo de uma organização que deseja proteger seus ativos e estar livre de perigos e incertezas.  
( ) Autenticidade refere-se a propriedade de salvaguarda da exatidão e completeza da informação.  
( ) A norma ISO/IEC 15408 (*Common Criteria*) é a versão brasileira da bS 7799 (*British standard*) e especifca os requisitos para implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.  
  
Assinale a opção com a sequência **CORRETA.**

* **A** V, F, V, V.
* **B** F, F, F, V.
* **C** F, V, V, F
* **D** V, V, F, F.

9-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Justiça do Estado de Pernambuco (TJ-PE) - Analista Judiciário - Análise de Sistemas (2012)](https://www.questoesestrategicas.com.br/provas/ver/tj-pe-analista-judiciario-analise-de-sistemas-2012-fcc)

De acordo com a ISO/IEC 15408,*Security Targets*(ST) especificam, antes e durante a fase de avaliação, o que deve ser avaliado. Neste papel, as ST servem de base de acordo para definição das propriedades exatas de segurança do alvo da avaliação, bem como do escopo exato de avaliação negociados entre o

* **A** desenvolvedor e o avaliador.
* **B** avaliador e o consumidor.
* **C** consumidor e o desenvolvedor.
* **D** auditor e o consumidor.
* **E** avaliador e o auditor.

10-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Tribunal de Justiça do Estado de Pernambuco (TJ-PE) - Analista Judiciário - Análise de Sistemas (2012)](https://www.questoesestrategicas.com.br/provas/ver/tj-pe-analista-judiciario-analise-de-sistemas-2012-fcc)

Sobre o padrão ISO/IEC 15408, considere:  
  
I. Este padrão é flexível em relação ao que deve ser avaliado, e portanto não está restrito aos limites de produtos de tecnologia da informação comumente utilizados.  
  
II. Um alvo de avaliação é definido pelo padrão co-mo um conjunto de *softwares, firmwares*e/ou*hardwares*.  
  
III. Em certos casos, um alvo de avaliação definido pelo padrão pode consistir de um produto de TI, uma parte de um produto de TI ou uma tecnologia única que talvez não se torne um produto.  
  
IV. Em relação aos produtos de TI, o padrão define que o alvo de avaliação de parte de um produto de TI deverá ser representado como o alvo de avaliação de todo o produto.  
  
Está correto o que se afirma em

* **A** I e II, apenas.
* **B** I, II e III, apenas.
* **C** I, II, III e IV.
* **D** II, III e IV, apenas.
* **E** III e IV, apenas.

11-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO) - Analista Executivo em Metrologia e Qualidade - Desenvolvimento de Sistemas (2009)](https://www.questoesestrategicas.com.br/provas/ver/inmetro-analista-executivo-em-metrologia-e-qualidade-desenvolvimento-de-sistemas-2009-cespe)

 ESCONDER TEXTO ASSOCIADO

A respeito dos conceitos de políticas, de normas e de modelos de  
segurança em TI, julgue os seguintes itens.

Na norma ISO/IEC 15408, os termos: alvo de avaliação (*TOE - target of evaluation*); perfil de proteção (*PP - protection profile*); alvo de segurança (*ST - security target*) e requisitos funcionais de segurança (*SFR - security funcional requirements*) podem ser respectivamente descritos como: um conjunto de *software, firmware e(ou) hardware*; uma classe de dispositivos; uma declaração de necessidades de segurança; um objeto a ser avaliado.

* Certo
* Errado

12-

## [Segurança da Informação](https://www.questoesestrategicas.com.br/assuntos/seguranca-da-informacao) [ISO-IEC 15408](https://www.questoesestrategicas.com.br/questoes/busca/assunto/iso-iec-15408)

### [Serviço Federal de Processamento de Dados (SERPRO) - Analista - Desenvolvimento de Sistemas (2008)](https://www.questoesestrategicas.com.br/provas/ver/serpro-analista-desenvolvimento-de-sistemas-2008-cespe)

 ESCONDER TEXTO ASSOCIADO

A respeito das normas de segurança da informação, julgue os  
itens subseqüentes.

A norma ISO/IEC 15408, também conhecida por common criteria, é recomendada para a avaliação de aspectos de segurança de sistemas e produtos de tecnologia da informação em geral.

* Certo
* Errado

GABARITO

1-A 2-E 3-ERRADO 4-CERTO 5-ERRADO

6-ERRADO 7-ERRADO 8-D 9-A 10-B