

# ABNT NBR ISO/IEC 27002:2005

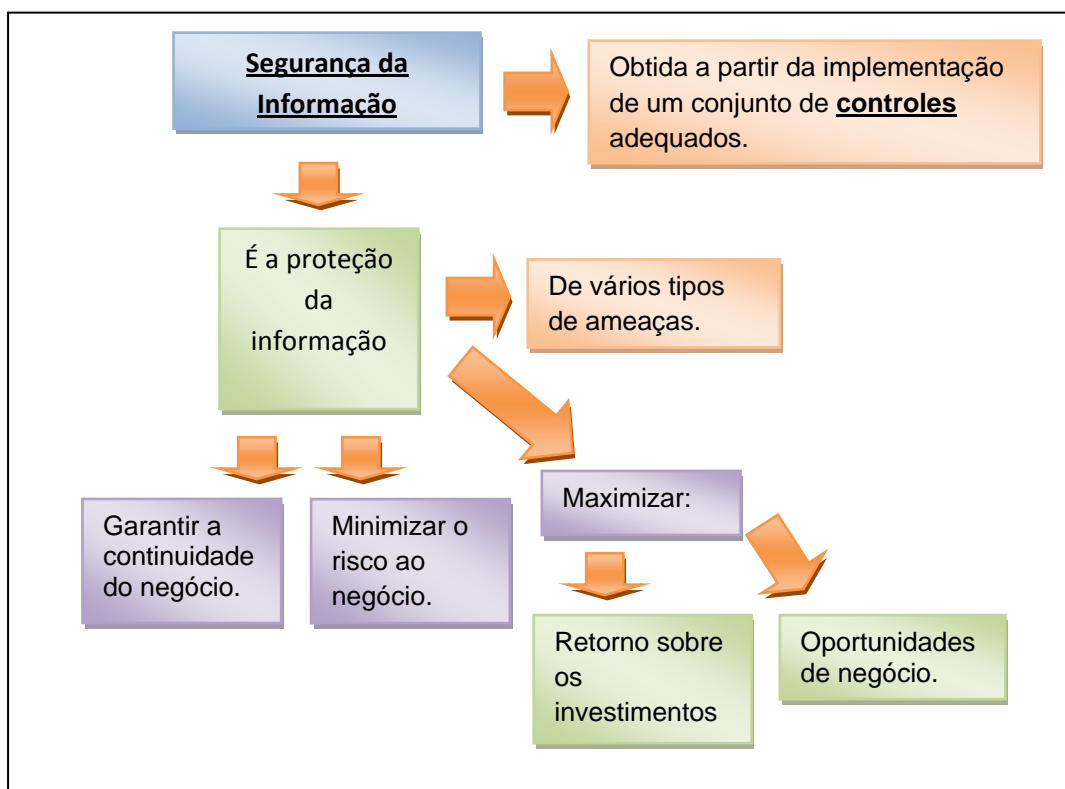
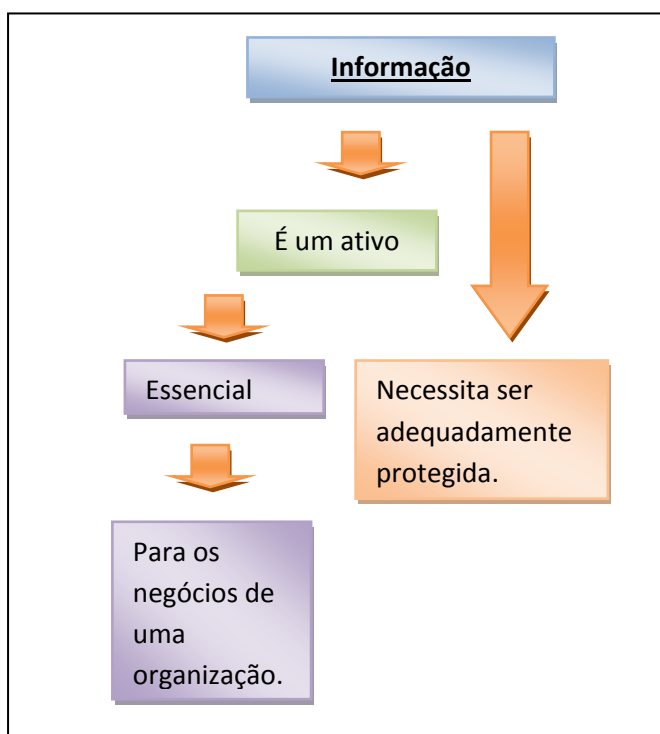
## Código de prática para a gestão da segurança da informação

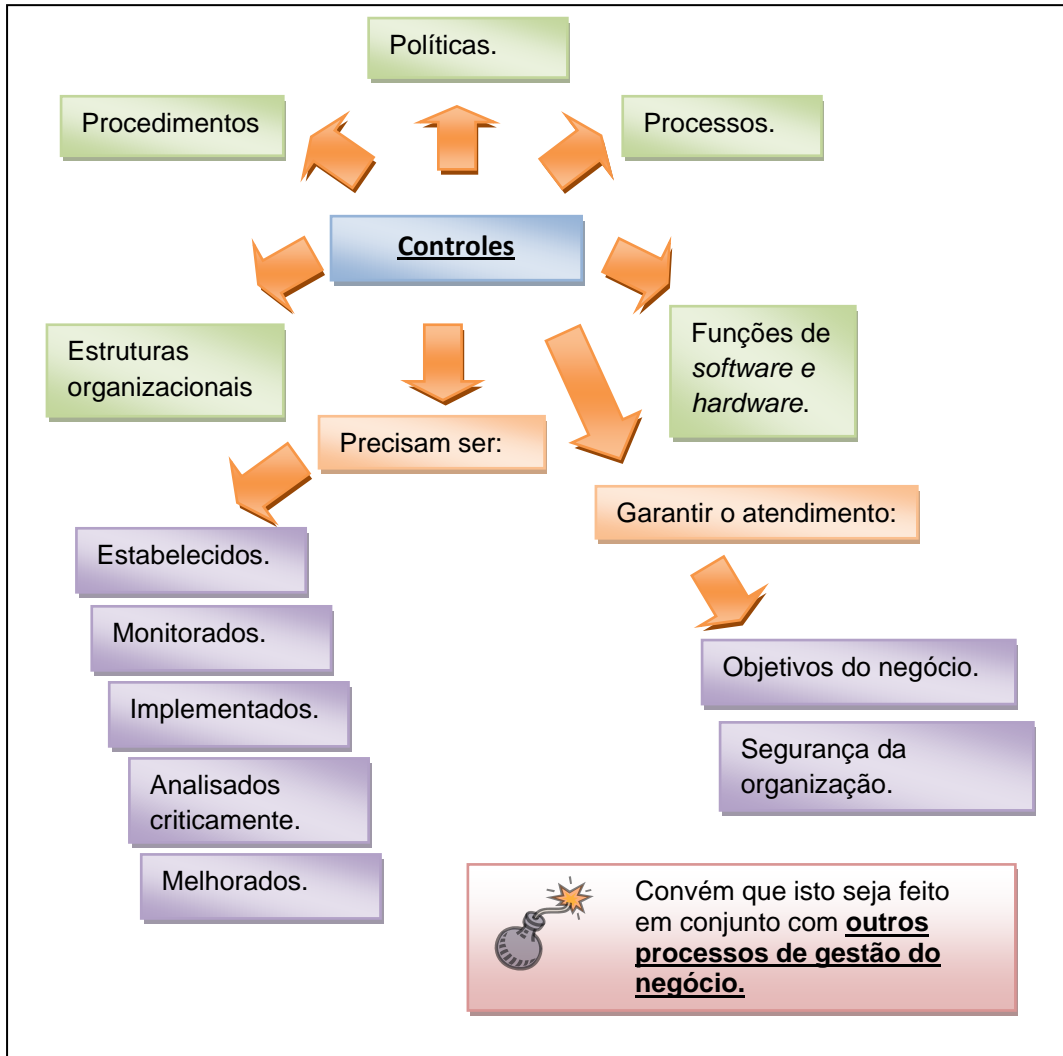


A partir de 2007, a nova edição da ISO/IEC 17799 será incorporada ao novo esquema de numeração como ISO/IEC 27002.

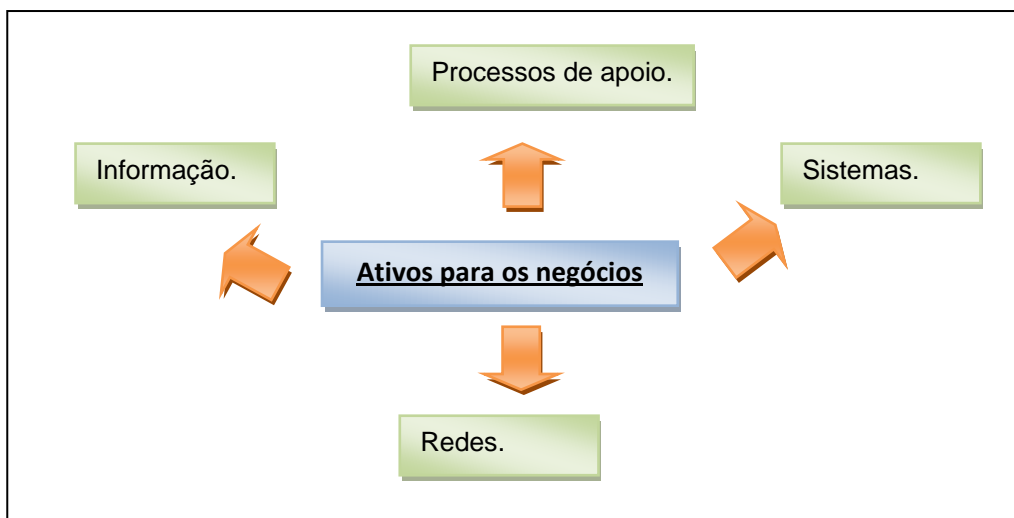
### 0 Introdução

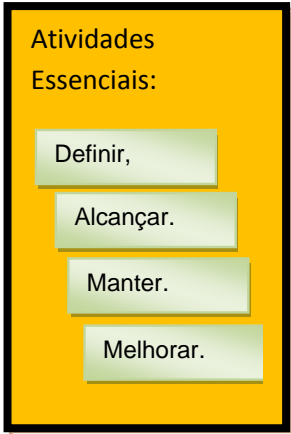
#### 0.1 O que é segurança da informação?





## 0.2 Por que a segurança da informação é necessária?





Segurança da informação

Asseguram



Importante para o negócio (setores público / privado).

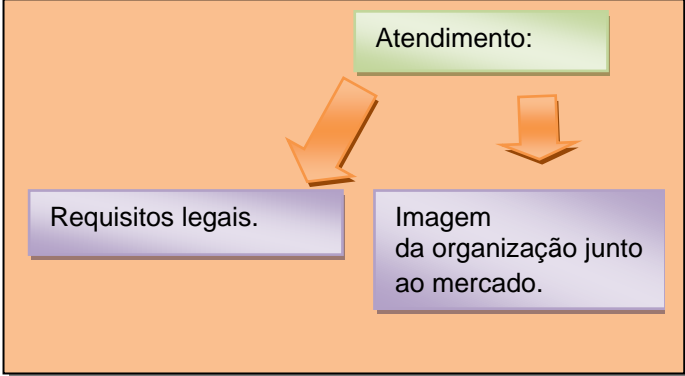
Evitar ou reduzir os **riscos**.



Competitividade.

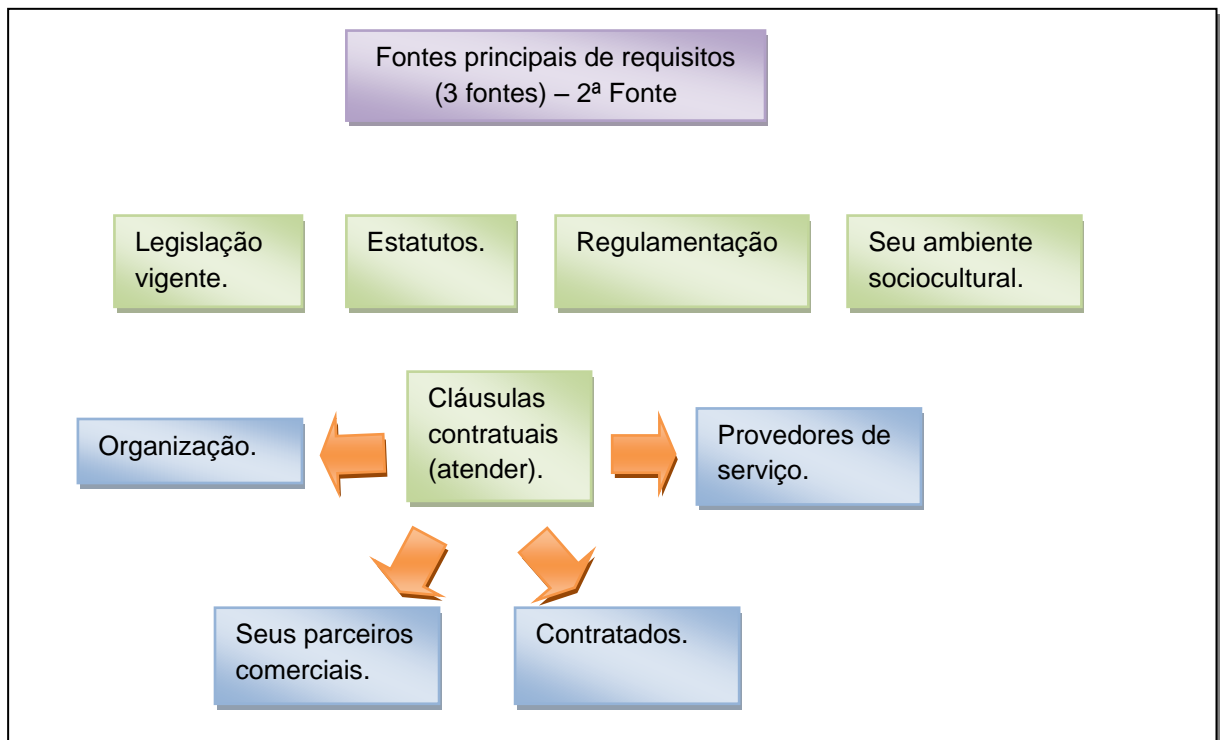
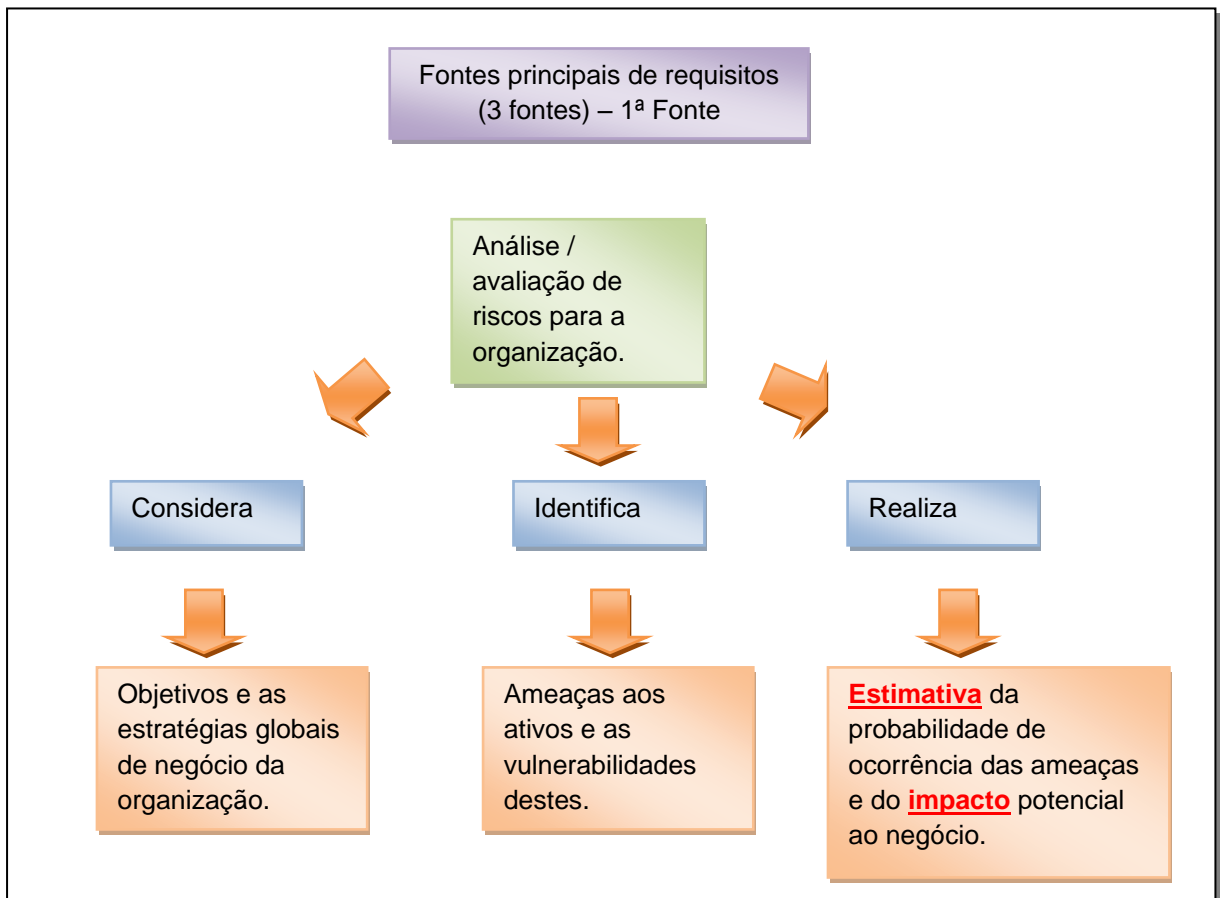
Fluxo de caixa.

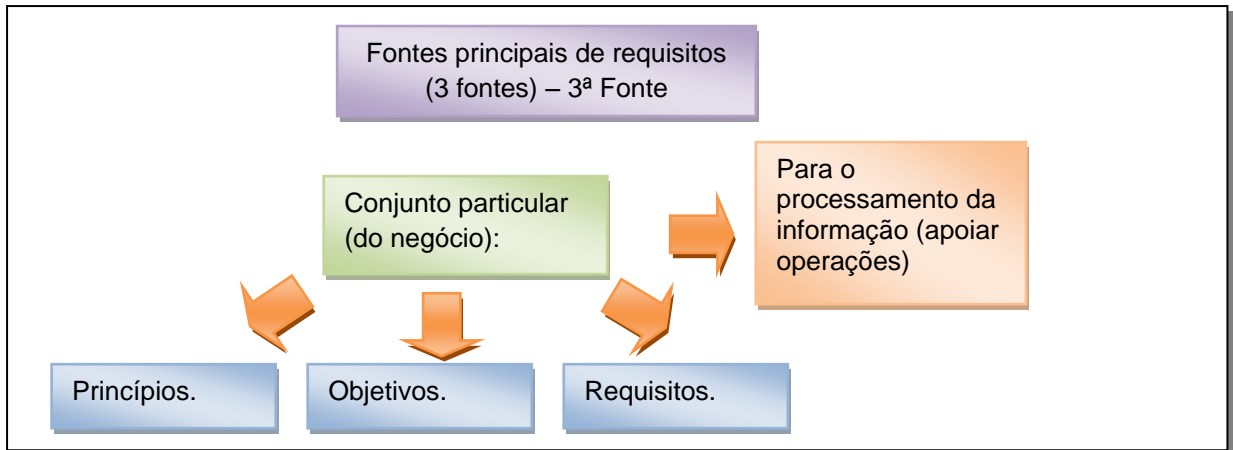
Lucratividade.



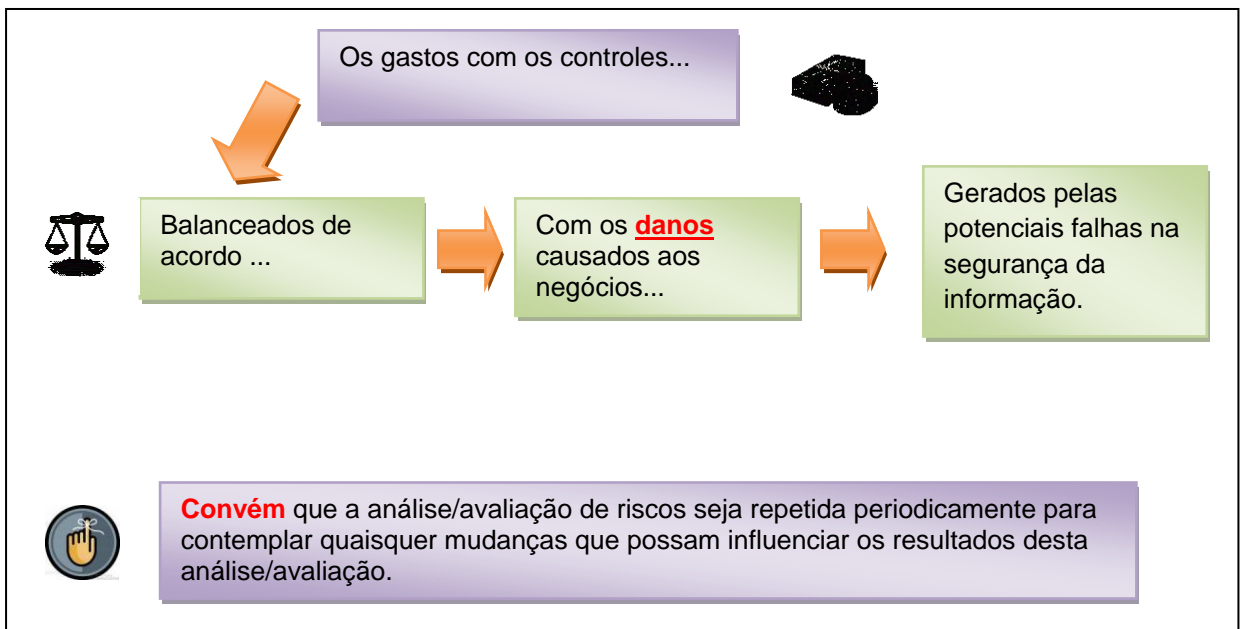
A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

### 0.3 Como estabelecer requisitos de segurança da informação

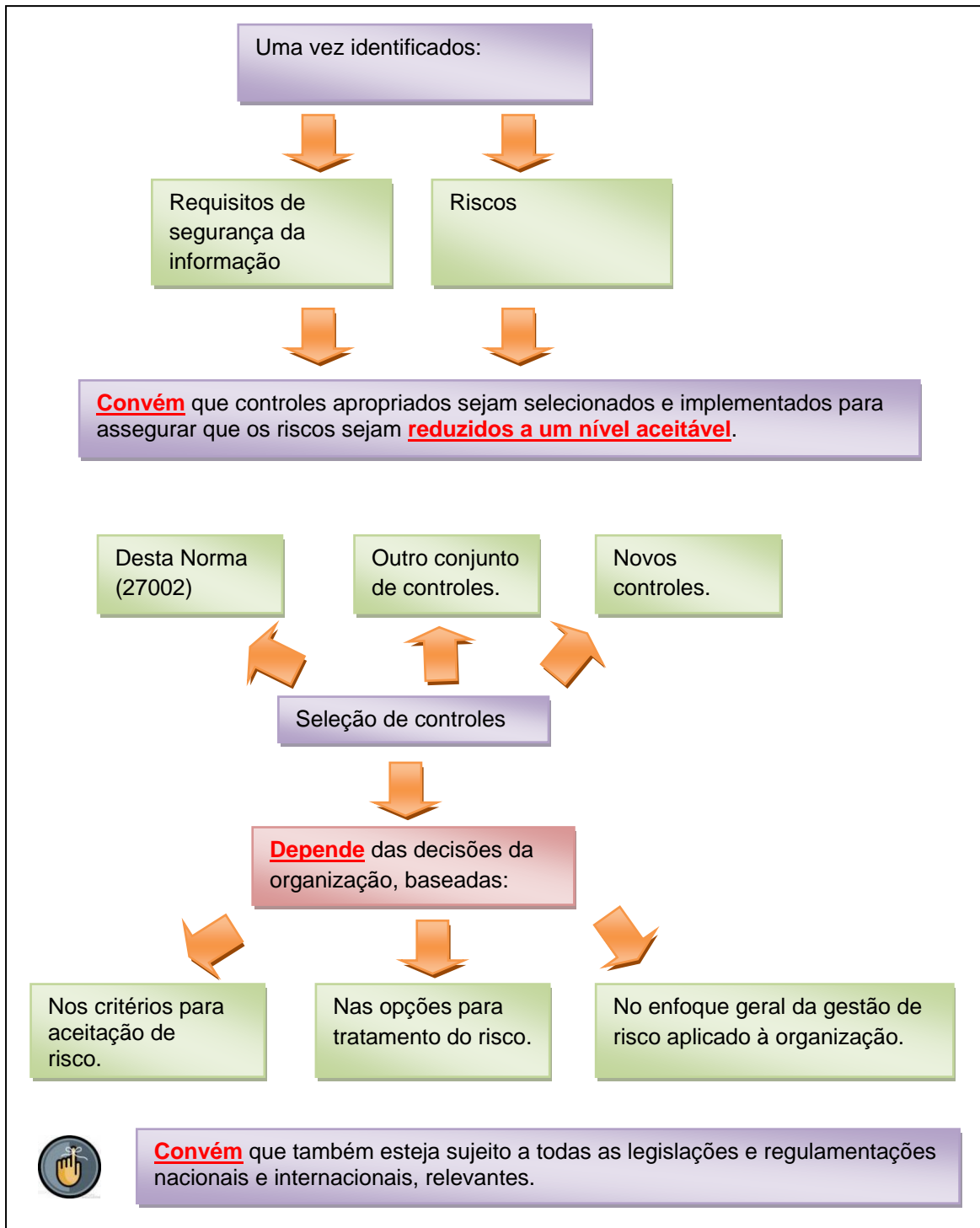




#### 0.4 Analisando/avaliando os riscos de segurança da informação



## 0.5 Seleção de controles



## 0.6 Ponto de partida para a segurança da informação

Sob o ponto de vista legal:

- a) Proteção de dados e privacidade de informações pessoais (ver 15.1.4);
- b) Proteção de registros organizacionais (ver 15.1.3);
- c) Direitos de propriedade intelectual (ver 15.1.2).

Práticas para a segurança da informação

- a) Documento da política de segurança da informação (ver 5.1.1);
- b) Atribuição de responsabilidades para a segurança da informação (ver 6.1.3);
- c) Conscientização, educação e treinamento em segurança da informação (ver 8.2.2);
- d) Processamento correto nas aplicações (ver 12.2);
- e) Gestão de vulnerabilidades técnicas (ver 12.6);
- f) Gestão da continuidade do negócio (ver seção 14);
- g) Gestão de incidentes de segurança da informação e melhorias (ver 13.2).



Embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos.

## 0.7 Fatores críticos de sucesso

Política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

- a) Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação **que seja consistente com a cultura organizacional**;
- b) Comprometimento e apoio visível de **todos** os níveis gerenciais;
- c) Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;
- d) Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;
- e) Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;
- f) Provisão de recursos financeiros para as atividades da gestão de segurança da informação;
- g) Provisão de conscientização, treinamento e educação adequados;
- h) Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;
- i) Implementação de um sistema de **medição**, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.



As **medições** de segurança da informação estão fora do escopo desta Norma.

## 0.8 Desenvolvendo suas próprias diretrizes



Nem todos os controles e diretrizes contidos nesta Norma podem ser aplicados.

Controles adicionais e recomendações não incluídos nesta Norma podem ser necessários.