# **Gestão do risco e adopção de medidas**
Aspectos económicos da cibersegurança

# Gestão do risco e adopção de medidas

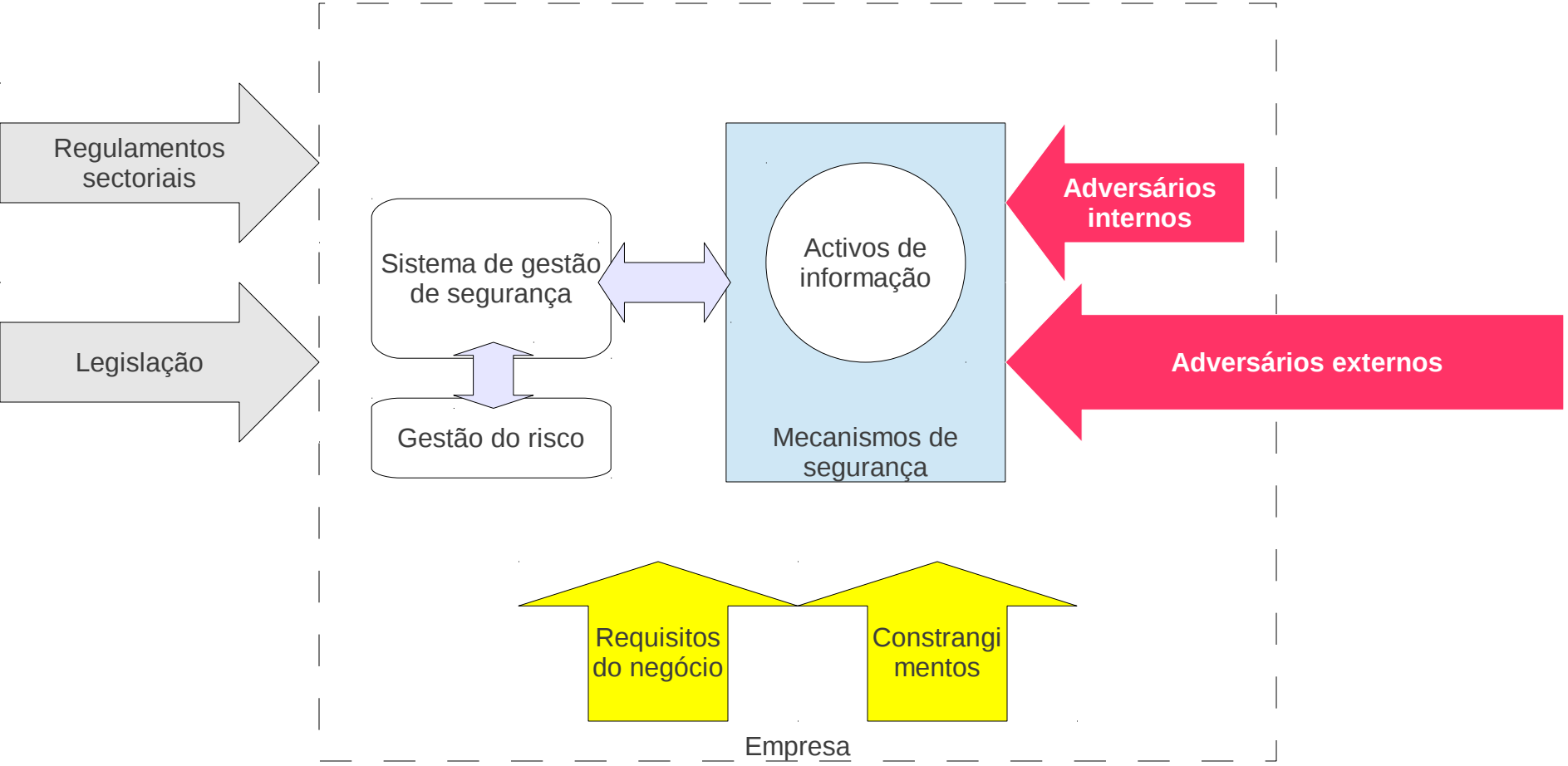
- **Colaboração para a segurança das redes e da informação**
- Ambiente micro
- Ambiente macro
- Desafios

# Colaboração para a segurança das redes e da informação

**Desafio**

**Partilha de informação entre organizações**

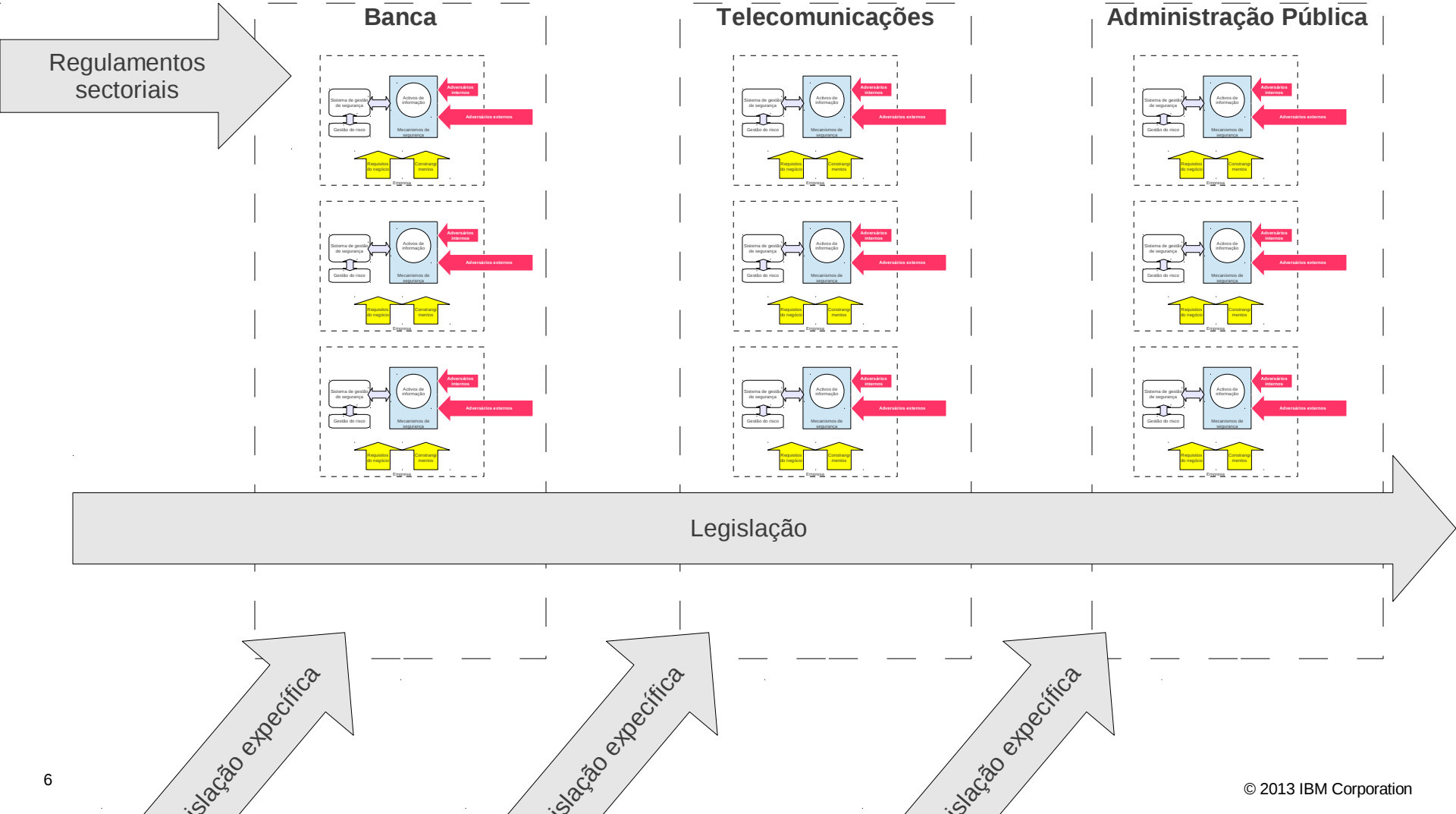
# Cada organização tem uma forma própria de gerir a sua segurança orientada por requisitos internos e pela interpretação que faz do seu ambiente.



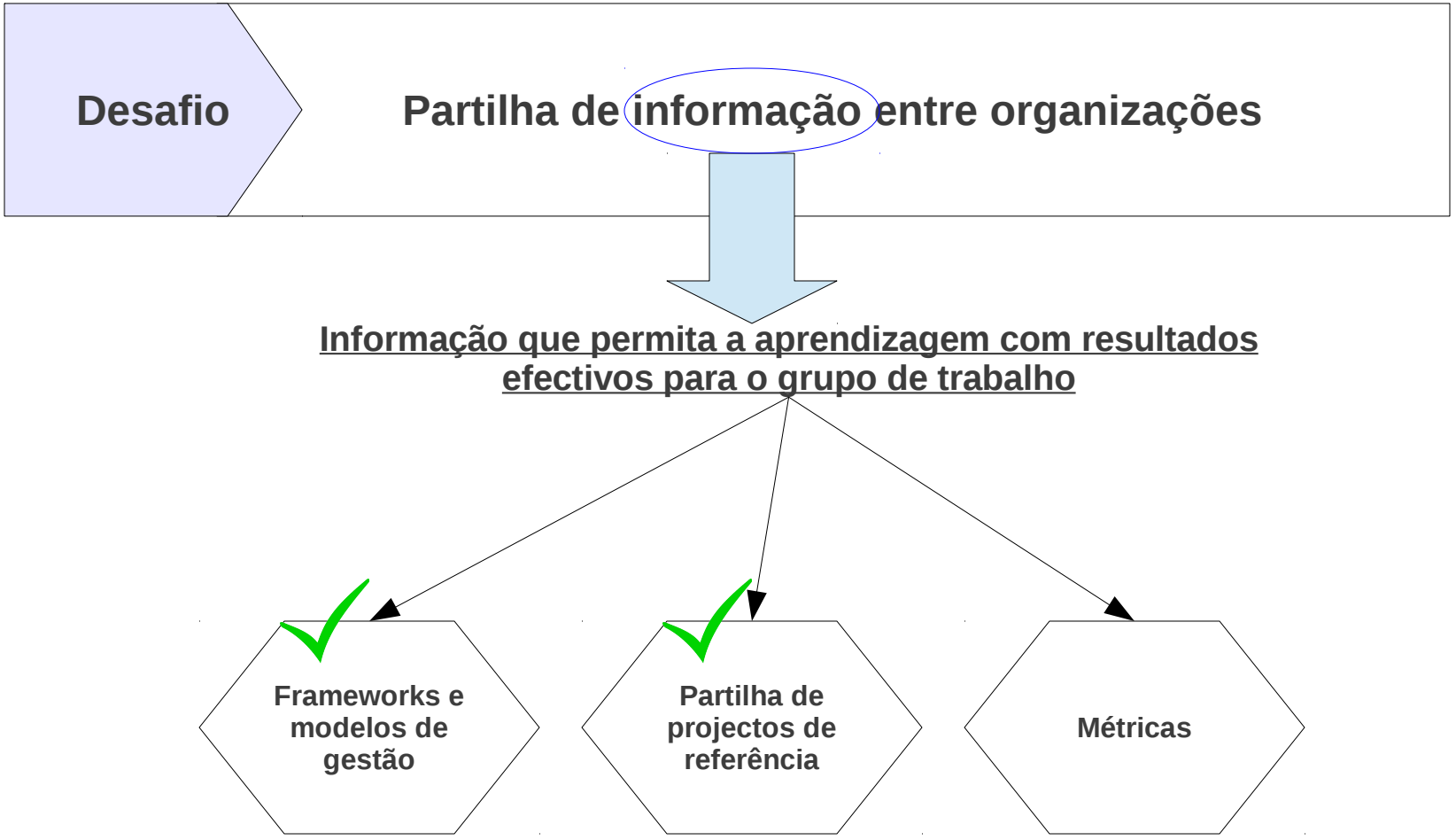
# As opções tomadas por cada empresa têm impacto na forma com mede a segurança (e a reporta interna e externamente)

- Interpretação do ambiente envolvente
  - Regulamentos
  - Legislação
  - Ameaças / adversários
- Postura de risco
- Orçamento
- Experiência da equipa de segurança
- Selecção de modelos de gestão de segurança
- Implementação e gestão dos mecanismos de segurança

# Num modelo de colaboração intra- e inter-sector o desafio de partilha de informação está em encontrar uma linguagem que permita “realmente” aprender.



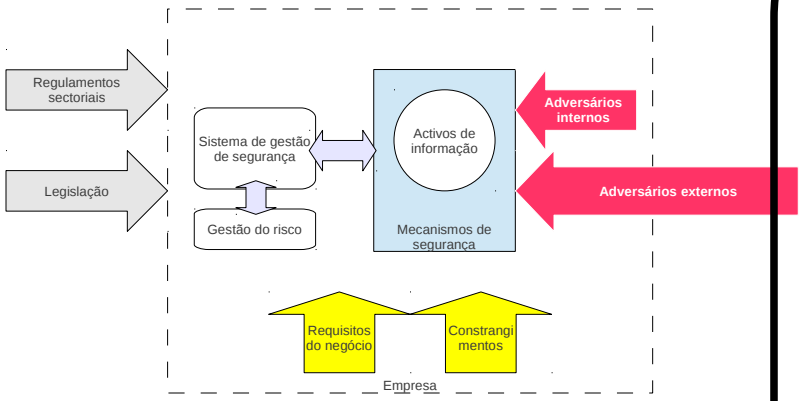
# Colaboração para a segurança das redes e da informação



# Métricas de segurança

- Métricas de segurança e subsequentes decisões de risco tendem a melhorar com o aumento da recolha e da análise de informação relevante sobre a operação do sistema de gestão de segurança.
- A segurança de uma organização depende em grande parte das acções individuais de cada um. Métricas de segurança têm necessariamente de envolver o factor humano.

# Exemplo prático




**Métricas**
Benchmarking intra- e inter-sector com base na identificação clara dos componentes do programa de segurança.

- **Activo de informação**: Dados residentes numa base de dados;
- **Risco**: Acesso indevido a dados de negócio por utilizadores priviligiados;
- **Regra de segurança**: Utilizadores priviligiados podem usar as suas credenciais apenas para realização de acções de administração de sistemas (e de bases de dados);
- **Mecanismo de segurança:**
  - Database activity monitoring and control
  - Configurado para registar detalhes de todos as acções realizados por utilizadores não pertencentes a uma lista de acessos permitidos;
- **Métrica**
  - Quantas vezes e qual a justificação de acesso a dados de negócio por utilizadores priviligiados;
- **Construção da métrica:**
  - Quantos registos de acesso indevido foram criados pelo mecanismo de segurança;
  - Quantas transacções foram realizadas na totalidade (acessos indevidos + acessos normais);
  - Onde estão os registos de investigação / aprovação das acções dos utilizadores priviligiados.