

Potenciar a maturidade de SI/TI em Hospitais do SNS

Desafios “Actuais”

Rui Gomes
Hospital Fernando Fonseca E.P.E.
(Amadora/Sintra)



Hotel Tivoli Vitoria, Vilamora, 22 a 24 Maio 2009

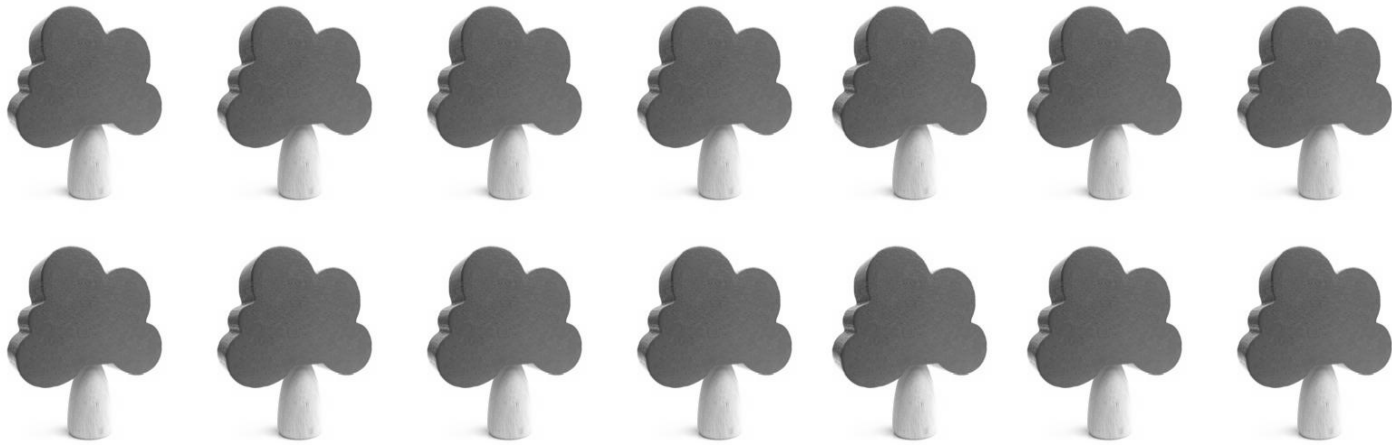
- ✓ **Onde “estamos” (ciclo eterno)**
- ✓ **O que não “queremos”**
- ✓ **O que podemos cultivar**
- ✓ **Resultados expectáveis**
- ✓ **Conclusões**

Onde “estamos” (ciclo eterno)



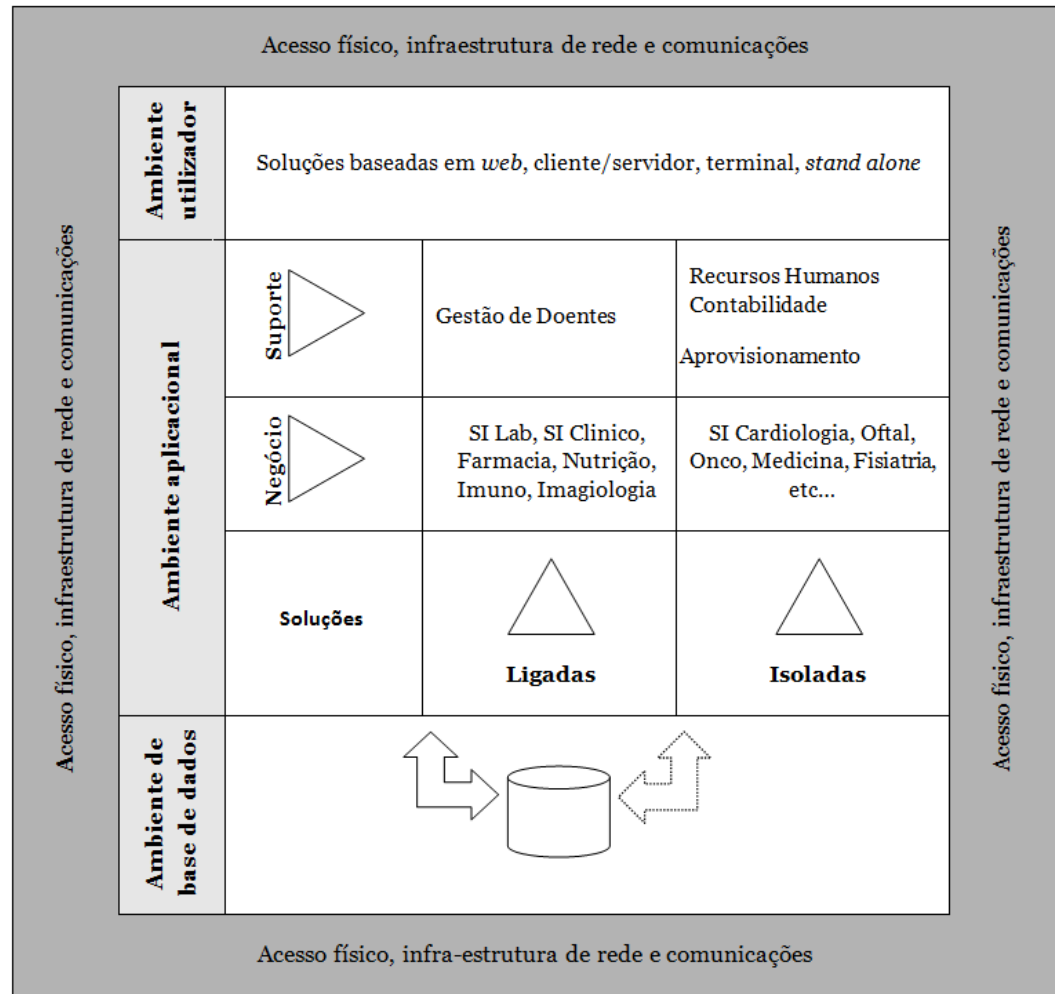
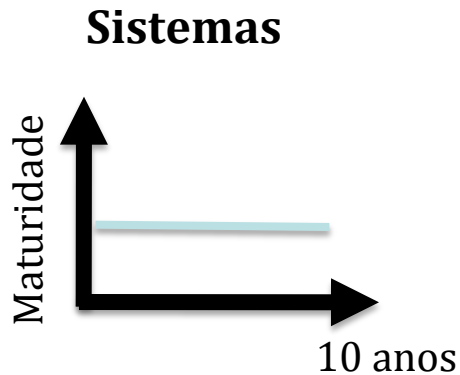
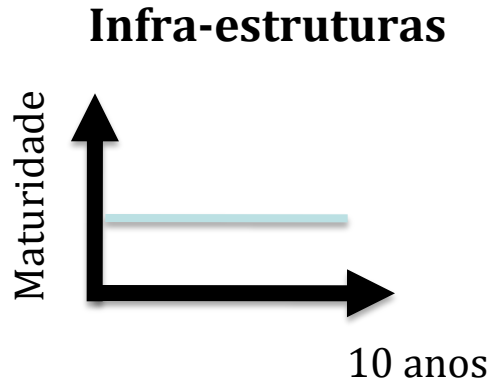
Árvore

Onde “estamos” (ciclo eterno)



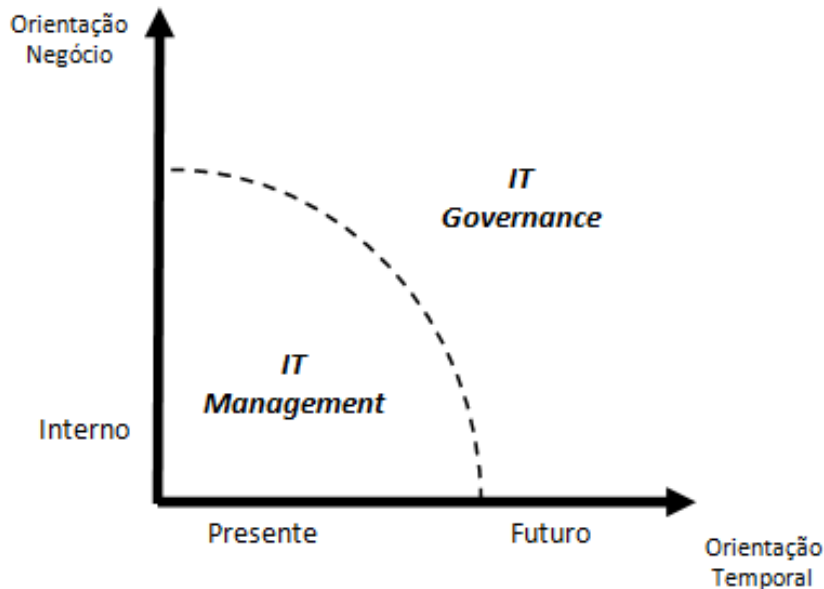
Floresta

Onde “estamos” (ciclo eterno)



Onde “estamos” (ciclo eterno)

Porquê?



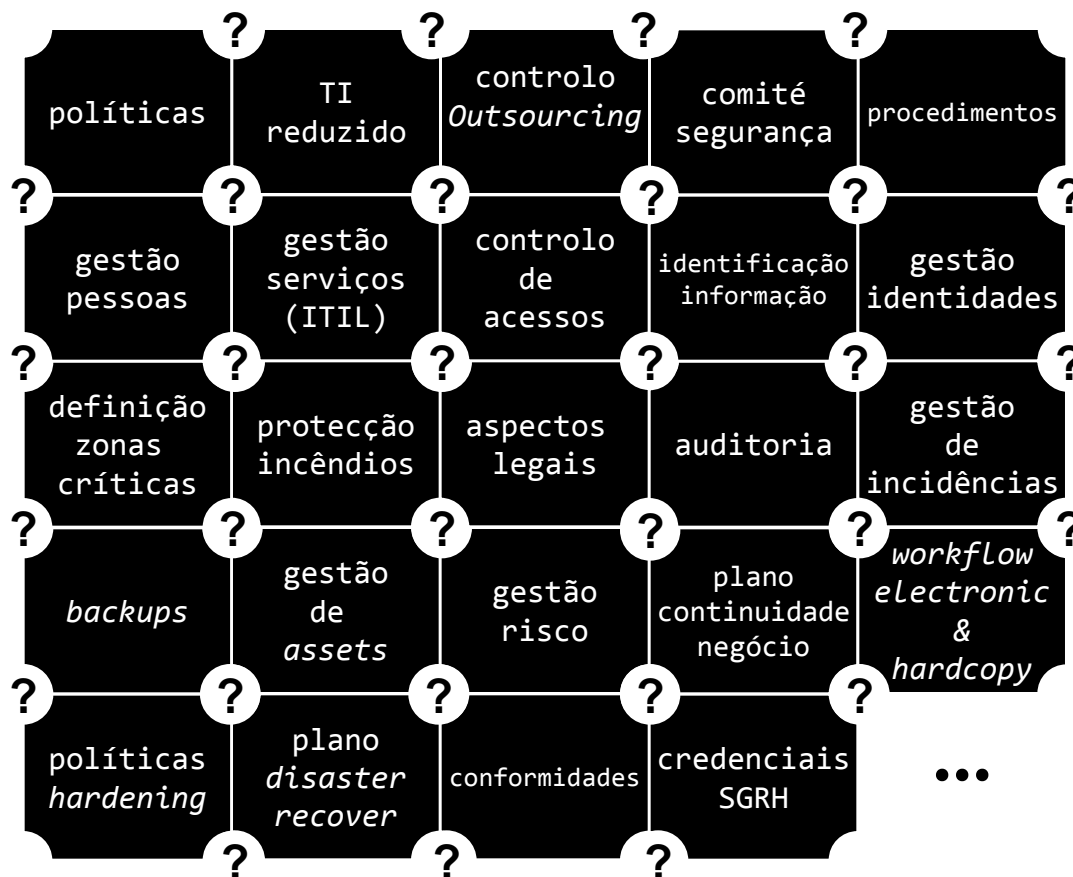
Adaptado a partir de ISACA

Ausência de uma estratégia que permita fazer crescer a componente de SI/TI ao nível do IT Governance

- ✓ Pensar no futuro
- ✓ Orientada ao negócio

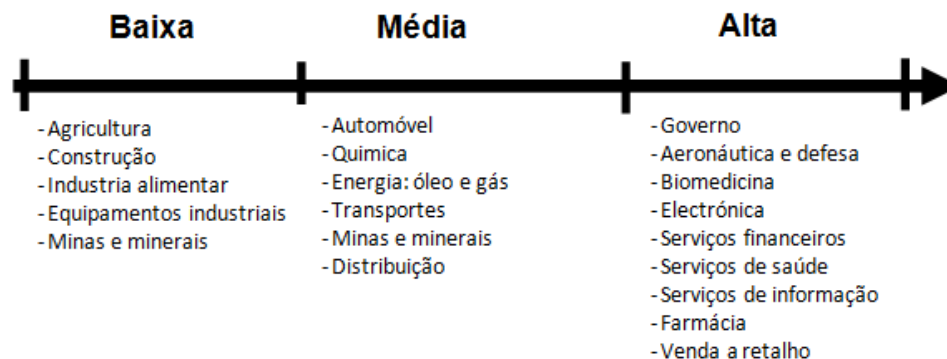
O que não “queremos”

Estado de “sítio” hospitais



O que não “queremos”

Controlo do Risco

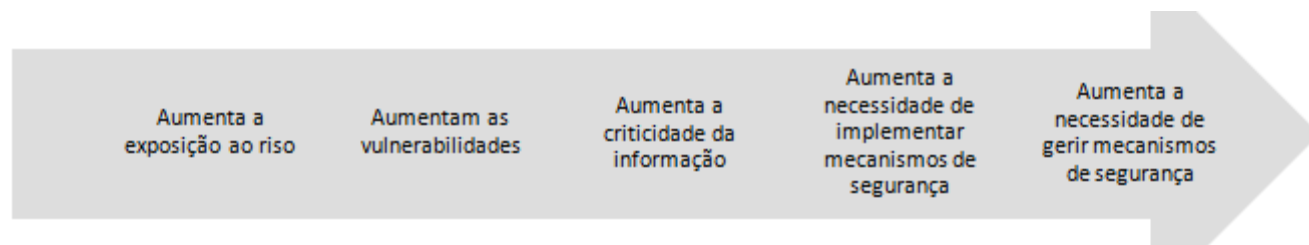
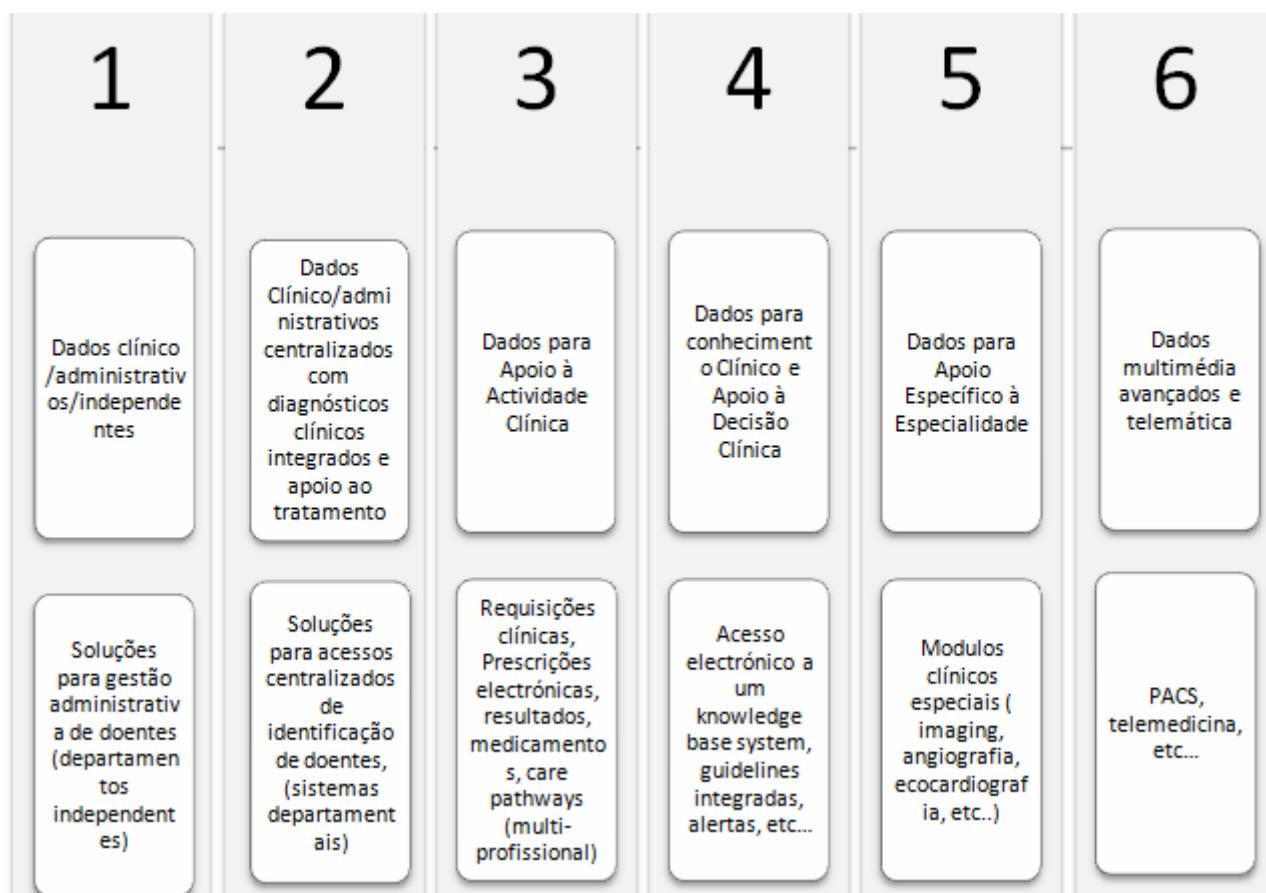


Nível de risco pela exposição de um sistema de informação por sector de actividade

O que não “queremos”

Com o aumento da exposição ao risco

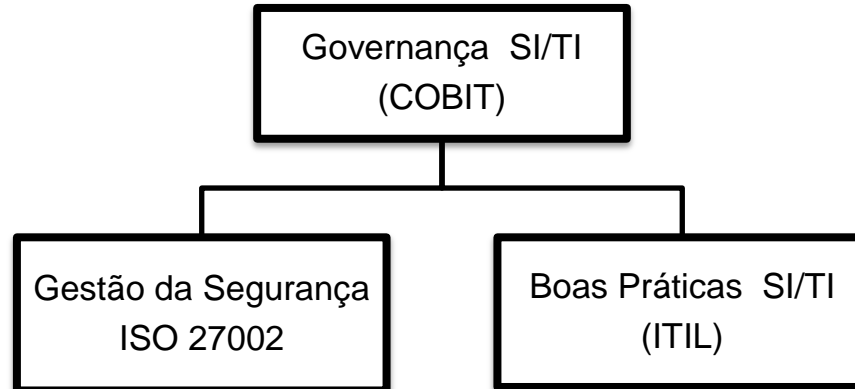
- ✓ Aumenta complexidade dos riscos
- ✓ Aumenta a complexidade na protecção riscos



Os 6 níveis de maturidade da informação clínica, adaptado de segundo ICT Strategy 2007-2011 Trust board

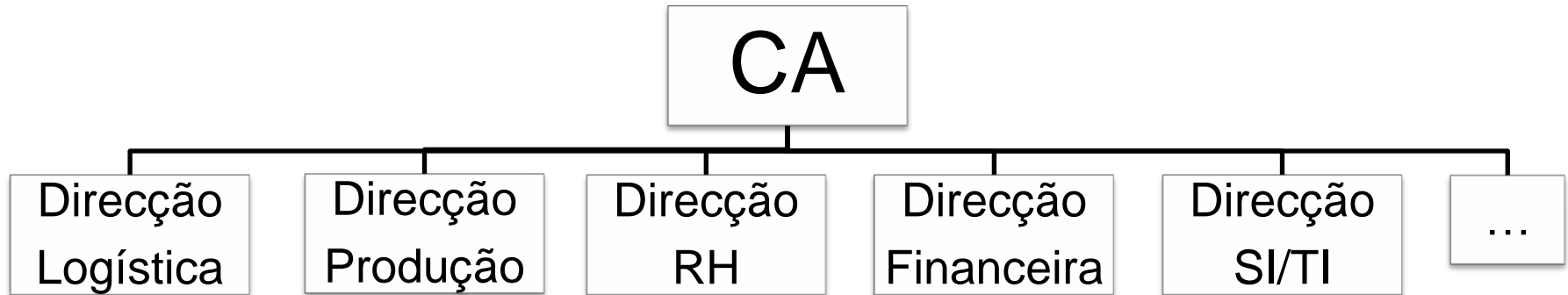
O que podemos cultivar

Esses objectivos podem ser alcançados se for implementada uma estrutura organizacional onde estejam bem definidas os papéis e as responsabilidades pela informação, os processos de negócio, aplicações, infra-estrutura, etc.



O que podemos cultivar

Qual o alinhamento da Gestão dos hospitais com os SI/TI?



O que podemos cultivar

Aplicação do *IT Governance* garante pelo menos...

- ✓ Assegurar que os investimentos em TI geram valor de negócio;
- ✓ Atenuar os riscos associados à introdução e investimentos das TI.

O “segredo” está nas **pessoas** e nas suas responsabilidades

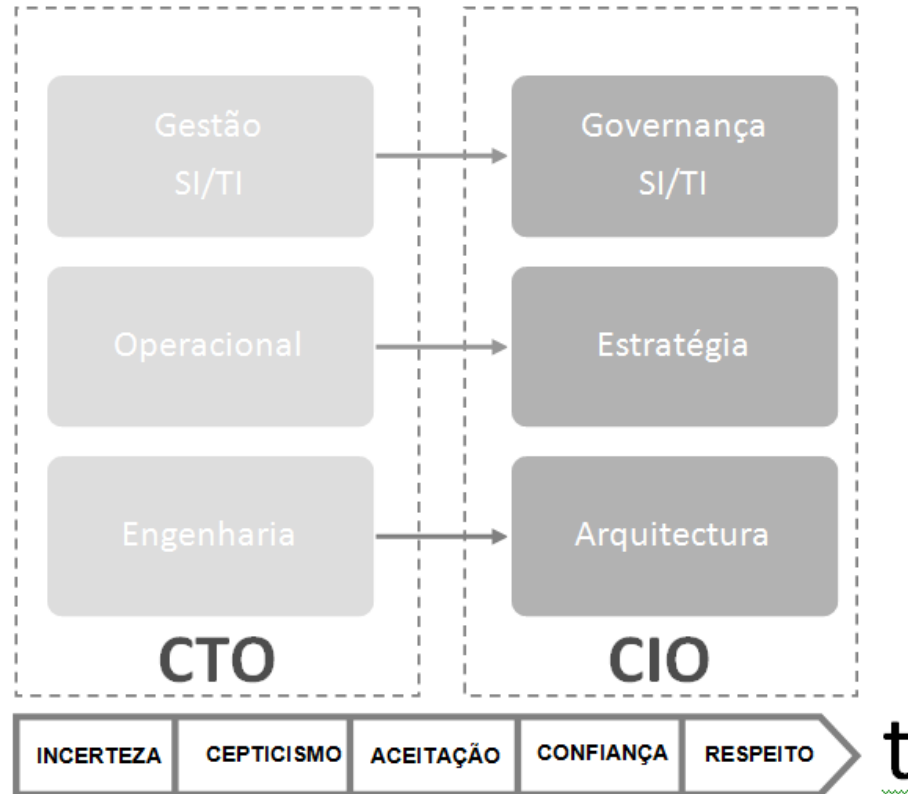
O que podemos cultivar

Controlo do Risco

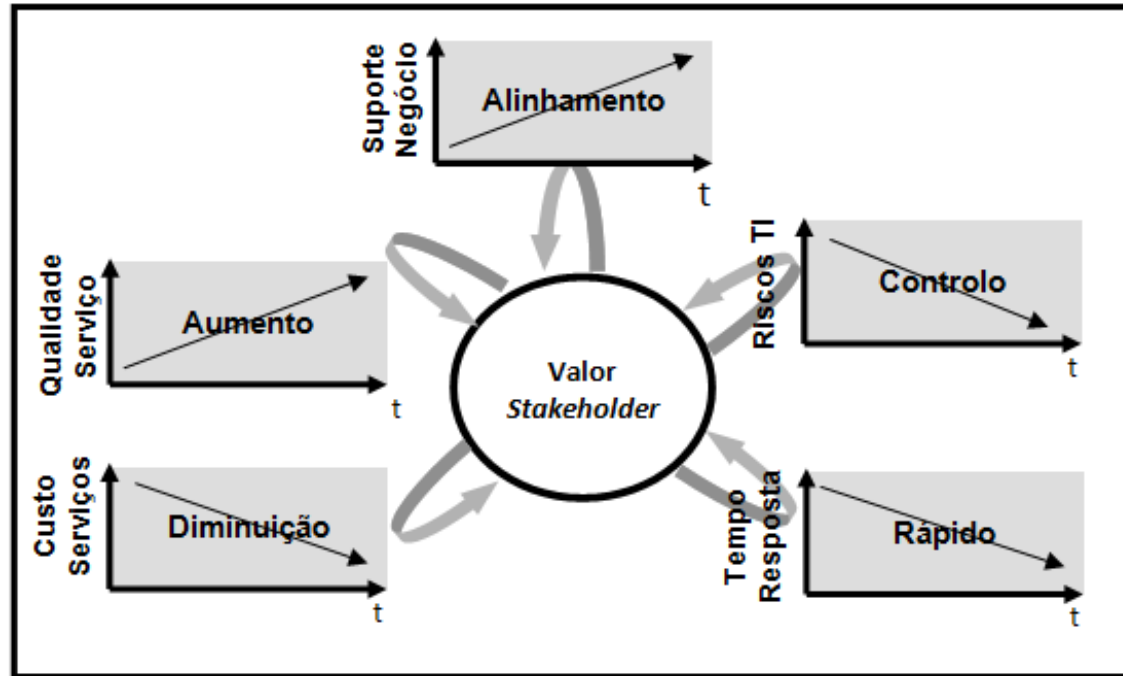
Transferir o risco Aquisição de seguros ou Outsourcing	Evitar o risco Decidir não avançar ou não implementar
Aceitar o Risco Decidir que o nível de risco identificado está dentro do limiar de tolerância das capacidades da organização	Mitigar o risco Implementar controlos técnicos de mitigação de risco (por exemplo uma firewall)

O que podemos cultivar

Qual o alinhamento da Gestão dos hospitais com os SI/TI?

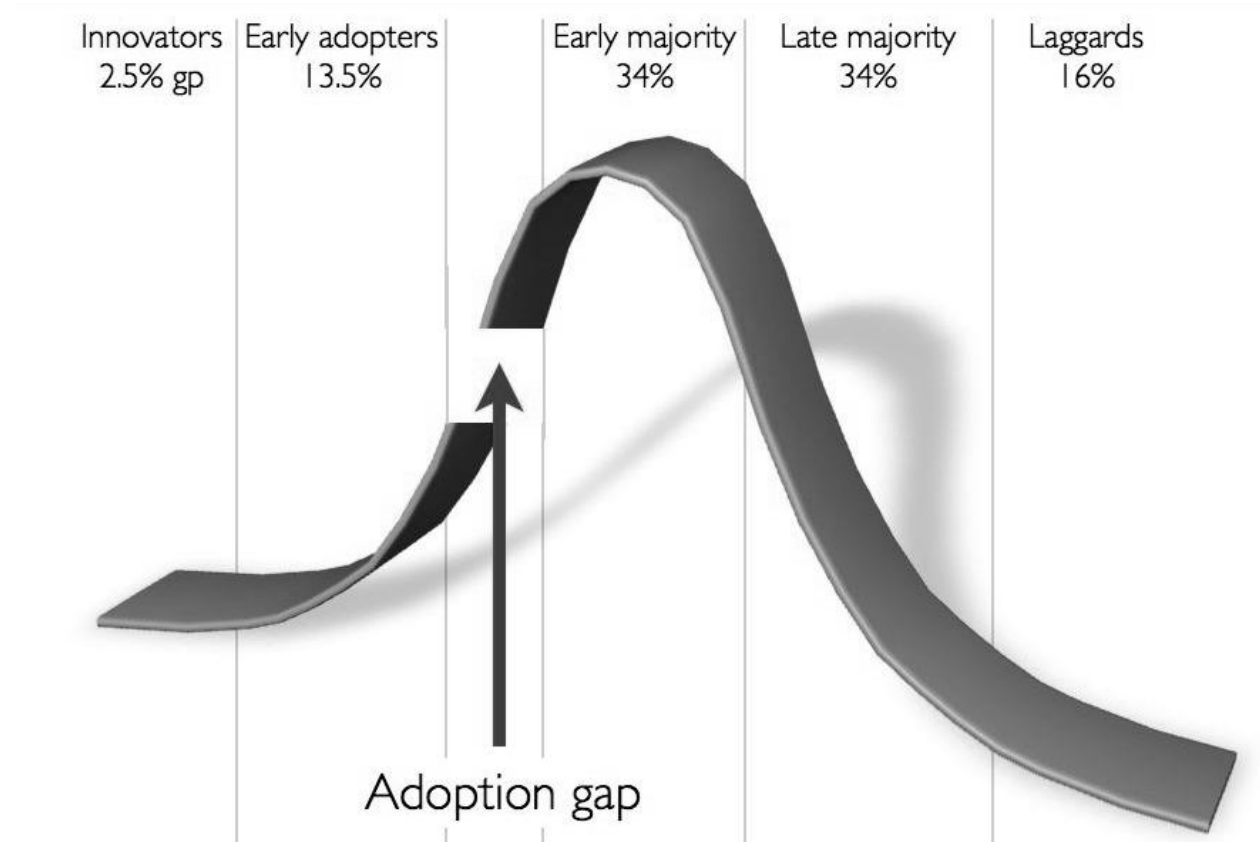


O que podemos cultivar



O que podemos cultivar

Qual o alinhamento dos profissionais de saúde com a introdução dos SI/TI?



Rogers Innovation Adopters Curve

O que podemos cultivar

Gestão da Mudança



O que podemos cultivar

Gestão da Mudança

Por exemplo

ISO 27799:2008

**Health informatics — Information security
management in health using ISO/IEC 27002**

O que podemos cultivar

Gestão da Mudança

Segurança de TI	Segurança da Informação
<ul style="list-style-type: none">. Firewall. Vírus, worms. Intrusão. Detecção. Gestão S.O. (hardening). Encriptação	<ul style="list-style-type: none">. Propriedade intelectual. Integridade no negócio. Integridade financeira. Aspectos legais. Abuso por infiltração. Privacidade. Confidencialidade
Problema de tecnologia	Problema de negócio

Resultados expectáveis

“Sensibilizar para a segurança da informação é um processo contínuo de aprendizagem proveitoso para os destinatários e se traduz em benefícios quantificáveis, não só na segurança, mas para a organização a todos os níveis, em resultado de uma mudança comportamental duradoura”

Autor: não é Rui Gomes

Resultados expectáveis

- ✓ Organização Processos,
- ✓ Mitigação do Risco;
- ✓ Visibilidade;
- ✓ Qualidade;
- ✓ Confiança stakeholders

País	Total
Japan	2280
UK	352
India	305
Taiwan	128
Germany	73
China	67
Hungary	58
Korea	50
Australia	53
USA	52
Italy	44
Netherlands	31
Hong Kong	30
Singapore	28
Czech Republic	26
Malaysia	20
Brazil, Ireland	17
Poland	16
Austria	15
Finland, Norway	14
Mexico, Switzerland, Turkey	12
Spain	11
Philippines, Saudi Arabia	9
Sweden, UAE,	8
Iceland	7
Kuwait, Russian Federation	6
Greece	5
Bahrain, Canada, Indonesia...	4
Argentina, France...	3
Croatia, Denmark, Portugal...	2
Armenia, Bulgaria, Egypt...	1
Relative Total	3792
Absolute Total	3890

Número de certificados ISO/IEC 27001 emitidos⁷

Hotel Tivoli Vitoria, Vilamora, 22 a 24 Maio 2009

Conclusões

1. Não é possível manter a segurança sem planear a sua gestão;
2. Os organismos estão muito atrasados neste sector;
3. Não existe “*such thing*” segurança total;
4. Implementar controlos permite minimizar riscos
5. Só o ISO 27001 permite certificar a gestão da segurança;
6. Implementar a norma exige grandes mudanças estruturais no âmbito das tecnologias e dos comportamentos;
7. Pode ter custos de investimentos elevados mas com retorno visível