apdsi
associação para a promoção e desenvolvimento da sociedade da informação

A Gestão do Risco nos Grandes Hospitais

Eng.º Rui Gomes

Director das Tecnologias e Informação do HPFF

Conferência
As TIC e a Saúde no Portugal de 2011

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

15 de Dezembro de 2011
Auditório do Centro Hospitalar Psiquiátrico de Lisboa
Av. Brasil, Lisboa

A Gestão do Risco nos grandes Hospitais

Rui Gomes
Hospital Professor Doutor Fernando Fonseca

15 de Dezembro 2011

Só a existência de uma arquitectura pode responder às questões da **complexidade** e da **mudança**. É a única forma que a Humanidade tem de lidar com elas. **Ao caos opõe-se à estrutura**. *Zachman*

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

INTRODUÇÃO

Esta apresentação nada tem a ver com…

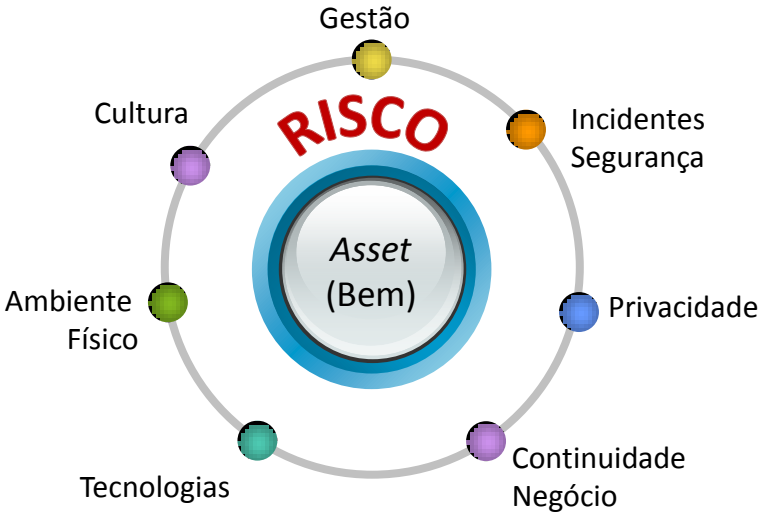
os computadores, os servidores, as bases de dados, os tablets, o wifi, as larguras de banda, a internet, a cloud, os processos clínicos, as firewalls, os antivirus, as empresas, a ACSS, a microsoft, o licenciamento, a virtualização, os thin clients, etc… e nenhum problema de Tecnologias.

Esta apresentação tem tudo a ver com…

Problemas de gestão (desde o nível estratégico ao operacional), falta de estratégia, ausência de visão, desalinhamento, desordem, incapacidade, passividade, esmorecimento, resignação, intolerância, obtusidade, indefinição de prioridades, e outras *borboletas* que tais que nos guiam ao CAOS e limitam na nossa capacidade de crescer.

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

Definição de *asset* no ambiente



- Aumento da exposição ao Risco
- Complexidade dos Riscos
- Complexidade na Protecção Riscos

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- **CICLO ETERNO?**
- O QUE NÃO QUEREMOS
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

CICLO ETERNO

Quem somos e o que vemos?

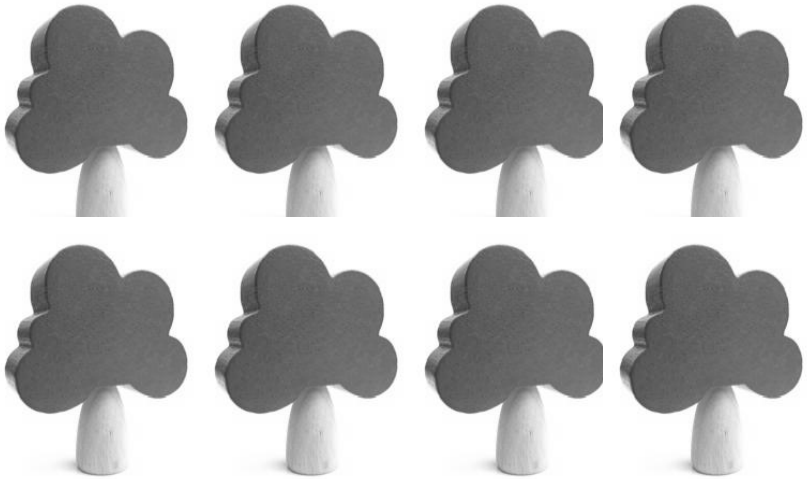
Árvore

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- **CICLO ETERNO?**
- O QUE NÃO QUEREMOS
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

CICLO ETERNO

Quem somos e o que vemos?



Floresta

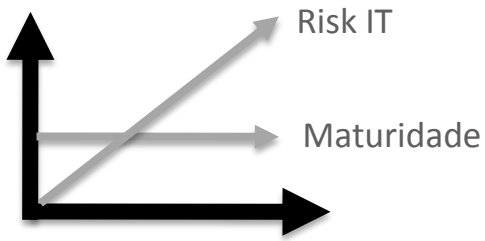
apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- **CICLO ETERNO?**
- O QUE NÃO QUEREMOS
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

CICLO ETERNO

Onde estamos ?

Infra-estruturas



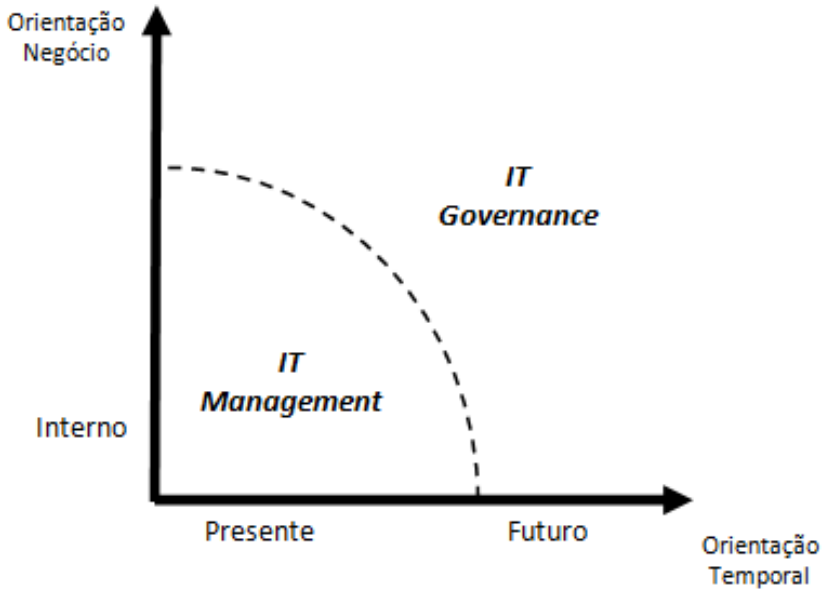
Sistemas Informação

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- **CICLO ETERNO?**
- O QUE NÃO QUEREMOS
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

CICLO ETERNO

Porquê?



Adaptado a partir de ISACA

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

CICLO ETERNO

As equipas dos Departamentos de Sistemas de Informação têm pouca participação ou motivação em grupos… Governance, Qualidade, Gestão de Risco, Segurança, etc..

- "Comité Olímpico"

Os Departamentos de Sistemas de Informação vivem sujeitos a imensa adversidade e incertezas - vulgarmente Riscos - contantes, que algures no tempo, senão forem tratados criam impacto.

- "Teoria do Caos"

Exemplo de uma paragem por completo num hospital publico durante aproximadamente 12 horas devido a uma alteração de denominação de rede de um equipamento que não era possível identificar no meio.

apdsi

associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- **CICLO ETERNO?**
- O QUE NÃO QUEREMOS
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

Exemplo de uma paragem por completo num hospital publico durante aproximadamente 12 horas devido a uma alteração de denominação de rede de um equipamento que não era possível identificar no meio.

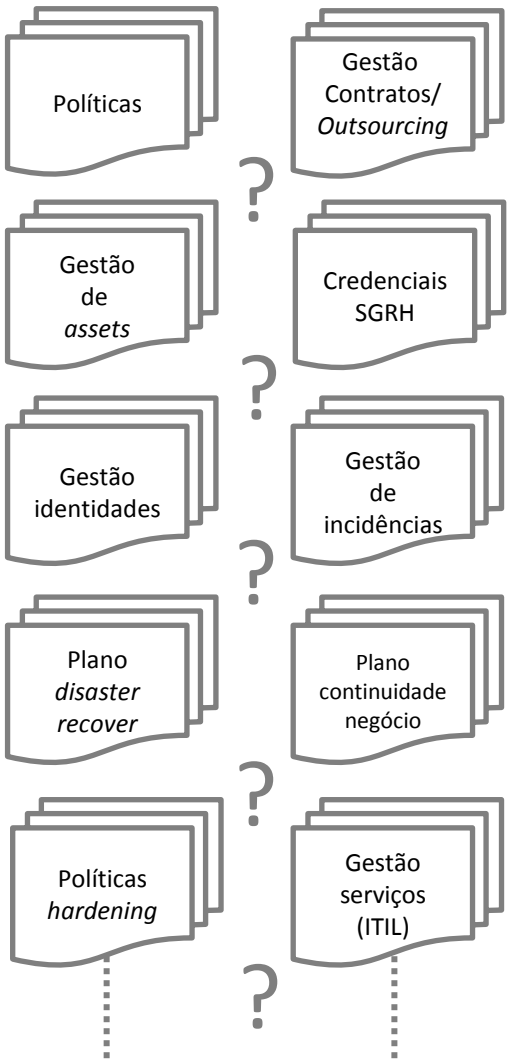
CICLO ETERNO

Exemplo

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

O QUE NÃO QUEREMOS

Ausência de…



apdsi
associação para a Promoção e desenvolvimento da Sociedade da Informação

- INTRODUÇÃO
- CICLO ETERNO?
- **O QUE NÃO QUEREMOS**
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

Muitas vezes as questões de proteção para as empresas inclinam-se unicamente em ajudar os clientes a protegerem-se das ameaças externas ao nível da circulação de informação electrónica (anti-virus, certificados digitais, firewall, etc…)

O QUE NÃO QUEREMOS

O Elo Mais Fraco

Pessoas

- Desmotivação (esmorecimento)
- Negligência dos colaboradores;
- Falta de capacidades compatíveis funções;
- Desconhecimento ou ignorância;

apdsi

associação para a Promoção e desenvolvimento da Sociedade da Informação

- INTRODUÇÃO
- CICLO ETERNO?
- **O QUE NÃO QUEREMOS**
- O QUE PODEMOS CULTIVAR
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

O QUE NÃO QUEREMOS

Níveis de maturidade da informação clínica e a sua relação com o RISCO

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

O QUE NÃO QUEREMOS

Os mecanismos de protecção não são suficientes.

- é necessário vigiar os Riscos
- e melhorar mecanismos de protecção

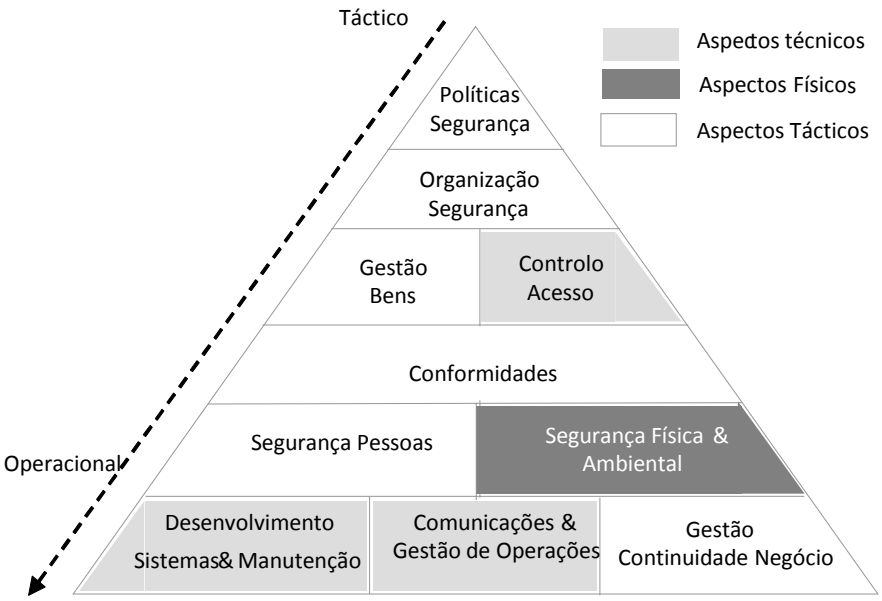
Ou seja, é necessário…

Gerir a Segurança

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

O QUE PODEMOS CULTIVAR

Claúsulas de abrangência



apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- CICLO ETERNO?
- O QUE NÃO QUEREMOS
- **O QUE PODEMOS CULTIVAR**
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

O QUE PODEMOS CULTIVAR

Cláusulas da ISO/IEC 27002:2005

1	Política de Segurança da Informação
2	Organização da Segurança da Informação
3	Gestão de Recursos
4	Gestão de Recursos Humanos
5	Gestão da segurança física e ambiental
6	Gestão das Comunicações e Operações
7	Controlo de acessos
8	Aquisições, manutenções e desenv. de sistemas
9	Gestão de incidentes de segurança da informação
10	Plano de gestão da continuidade de negócio
11	Conformidade com os aspectos legais

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

O QUE PODEMOS CULTIVAR

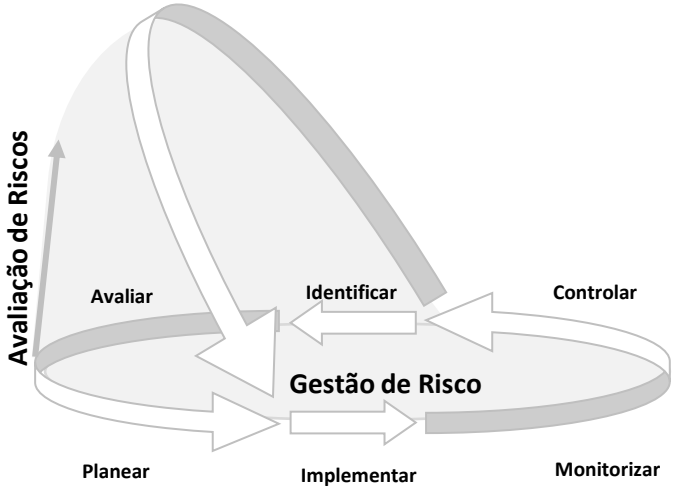
Formas de abordar do Risco

Mitigar o risco Implementar controlos técnicos de mitigação de risco (por exemplo uma *firewall*)	**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	**Transferir o risco** Aquisição de seguros ou *outsourcing*

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

O QUE PODEMOS CULTIVAR

Gestão do Risco



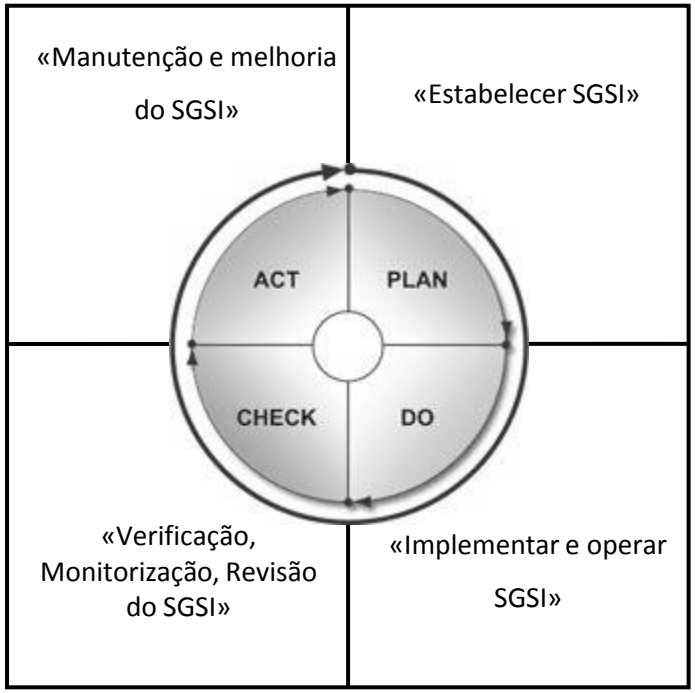
A implementação de mitigação de riscos envolve tipicamente as Pessoas, os Processos e as Tecnologias.

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

- INTRODUÇÃO
- CICLO ETERNO?
- O QUE NÃO QUEREMOS
- **O QUE PODEMOS CULTIVAR**
- RESULTADOS EXPECTAVEIS
- CONCLUSÕES

O QUE PODEMOS CULTIVAR

Implementação de um SGSI



apdsi
associação para a promoção e desenvolvimento da sociedade da informação

Estrutura de um SGSI

ISO/IEC 27000 - vocabulário e definições utilizadas

27005
Gestão de Risco
(ISO 13335)

- 27001 - requisitos para um SGSI
- 27002 - Boas Práticas para um SGSI
- 27003 - Guia de Implementação SGSI
- 27004 - Métricas e Medidas avaliar SGSI

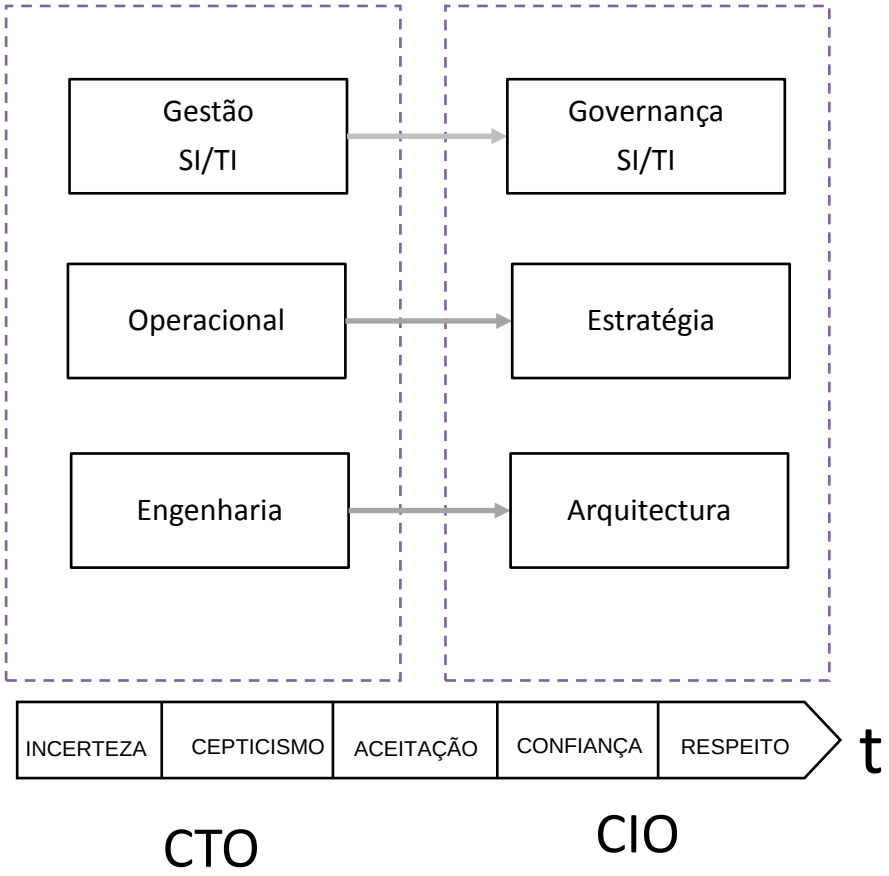
Família TC 215 - ISO 27000 também conhecida como ISO 27k

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

Só a existência de uma arquitectura pode responder às questões da **complexidade** e da **mudança**. É a única forma que a Humanidade tem de lidar com elas. **Ao caos opõe-se à estrutura**. *Zachman*

RESULTADOS EXPECTAVEIS

- Do Caos à Estrutura
- Lidar com a Complexidade
- Papel do CEO, CFO, CMIO, CIO, CISO e CTO



apdsi
associação para a promoção e desenvolvimento da sociedade da informação

CONCLUSÕES

- Não é possível manter a segurança sem planear a sua gestão
- Nenhuma organização vai estar um dia totalmente protegida das ameaças que põem em risco a sua Informação de negócio.
- Investir num nível de protecção que se considere próximo do ideal atingiria custos muito elevados ou bloquearia de forma não aceitável os processos desenvolvidos pelo hospital.

No entanto….

As utilização do modelo de boas práticas possibilitaria uma abordagem sistemática dos riscos (que pode ser realizada numa forma gradual e com custos controlados) de modo a implementar controlos com o objectivo de os minimizar.

apdsi
associação para a promoção e desenvolvimento da sociedade da informação

OBRIGADO

rui.gomes@hff.min-saude.pt