Estrutura e Governo das TI para a Saúde

Rui Gomes
Director de Gestão das Tecnologias e da Informação
Hospital Fernando Fonseca E.P.E.
Rui.Gomes@hff.min-saude.pt

Resumo
Num mercado em crescimento e sempre competitivo, só mesmo as organizações que tiram partido do melhor da informação que utilizam, como base para a decisão, podem beneficiar de lucros e crescer. As instituições que recolhem, manipulam e gerem dados de saúde são responsáveis pela informação sensível que utilizam de tal modo que a devem reconhecer como um recurso valioso que deve ser protegido e utilizado com conveniência. A utilização de um governo para as TI, com base nas melhores práticas da indústria para a gestão e protecção da informação de saúde, são o melhor critério para a preservação da informação contra extravios, exposição ou destruição, mas também para garantir a gestão de continuidade de negócio, minimizando em simultâneo o impacto de incidentes de segurança, e a garantia de consistência nas melhores características de confidencialidade e integridade da informação.

1. Introdução

Durante mais de uma década da era da informação que cada vez mais se tem acentua a necessidade de utilização da informação para a extracção de conhecimento que permita acções de decisão de negócio. A informação é reconhecida, para algumas organizações, como um dos mais importantes bens mais importantes utilizados na gestão estratégica. Os Sistemas de Informação e os serviços que lhe estão associados desempenham um papel indispensável para a persecução do negócio pelo que são recursos que necessitam de ser favorecidos de uma gestão apropriada. O conceito de governo relaciona-se geralmente com elementos originais da relação social, designadamente as regras, processos e os comportamentos através dos quais os interesses se articulam, os recursos são geridos e o poder é exercido no seio da sociedade.

2. Governo empresarial (*Corporate Governance*)

A generalidade das pessoas prefere trabalhar em organizações estáveis e produtivas e no qual o controlo dos processos seja rigoroso mas estável. O governo ou governança empresarial é o sistema pelo qual as organizações são dirigidas e controladas e está directamente relacionado com a capacidade de tomada de decisões e no qual assume um grande potencial de realização associado a uma constante verificação da performance das medidas correntes. Tipicamente estará relacionado com uma gestão consistente, com políticas organizadas. O facto de algumas organizações apostarem no governo é porque preferem projectos de governação com processos sempre controlados e alinhados com os objectivos de negócio. E essa é uma das características que se lhes permite dar forma e terem personalidade suficiente para se protegerem do caos. A dependência dos negócios nas tecnologias de informação resulta no facto de que as matérias do governo empresarial já não podem ser resolvidas sem termos em consideração as tecnologias da

informação e isso significa que o *Corporate Governance* deve conduzir e estabelecer um governo de Tecnologias e da Informação (*IT-Governance*).

3. Governo das TI (*IT-Governance*)

De acordo com o dicionário de Oxford, o termo *Governance* é o acto de controlar, dirigir ou regular as acções de uma entidade, como uma empresa ou o estado, e portanto o *IT-Governance*, será o acto de regular os processos das TI dessa entidade. Implementar um modelo de Governo de TI significa utilizar um conjunto de práticas e normas, delineados pela gestão, técnicos e utilizadores de uma organização, com o propósito de garantir controlo efectivo de processos, melhorando a segurança, minimizando riscos, aumentando o desempenho, optimizando recursos, reduzindo custos, sustentando as melhores decisões e em consequência esperar o melhor alinhamento entre as TI com os negócios.

A 26 de Maio de 2008 foi lançada a norma internacional dedicada à gestão das TI (a ISO 38500) [1] - que é baseada na norma australiana AS8015 2005 [2]. Esta norma é composta por três grandes áreas: Avaliar, Gerir e Monitorizar no qual se estabelece um guia baseado em seis princípios: 1) estabelecer responsabilidades, 2) planear as TI de suporte às organizações, 3) adquirir valor das TI, 4) assegurar desempenhos adequados das TI sempre e onde é necessário, 5) assegurar a conformidade formal das TI com as regras internas e externas e como 6) assegurar que o uso das TI respeitam o factor humano. Esta é a chave para as linhas de convergência que garantem que os nossos sistemas estão a trabalhar de forma conveniente, e no qual temos a capacidade de investir e aplicar sobre eles novas capacidades. Como podemos dar prioridade e gerir o desenvolvimento de aplicações, alocar capital para novas aquisições e saber quando está na altura de descartar dos sistemas legados. Estas são as questões que devem ser respondidas em qualquer programa de *IT-Governance*. Um projecto de Governança efectiva pode ajudar uma organização a assegurar que os seus recursos de TI permanecem focados nas prioridades de modo que os compromissos com o nível de serviço são preenchidos e as decisões são tomadas com a informação necessária. Em resumo o *IT-Governance* para além de garantir ferramentas de suporte à gestão das TI também procura obter o alinhamento das TI com os objectivos estratégicos e financeiros da instituição. As TI por seu lado podem influenciar oportunidades estratégicas definidas pela empresa fornecendo informação vital para planos estratégicos. É assim que o *IT-Governance* garante às empresas capacidade em tirar o máximo partido da informação.

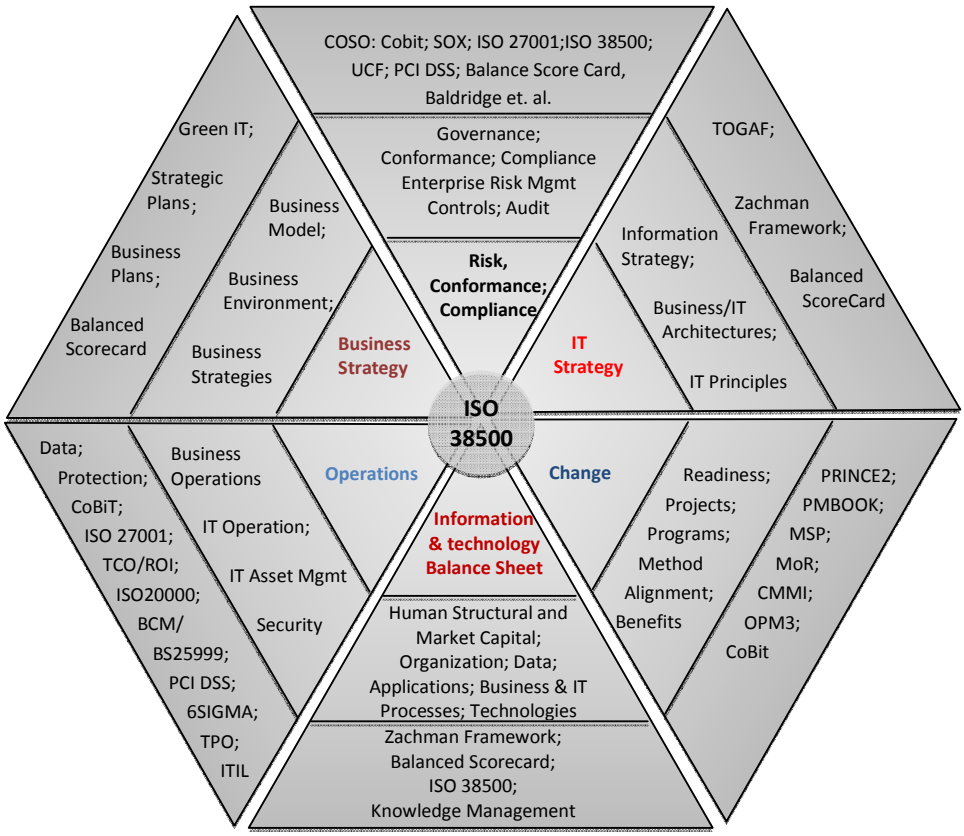

Fig. 1 : Adaptado do *Framework IT-Governance* (*Alan Calder*)

Os 10 princípios do Governo das TI

A partir de uma compilação da *Harvard Business School* [3], segue uma versão adaptada dos 10 princípios para a boa governação da Tecnologias da Informação, no qual podemos retirar orientações para a criação de valor para as organizações.

*1 – **Desenhe activamente um modelo de governo:** O departamento das Tecnologias e dos Sistemas de Informação deve estar envolvido directamente com a estratégia da organização e os seus objectivos de desempenho. A estratégia de "tapar buracos" e resolver problemas pontuais limita o impacto estratégico das TI.*

*2 – **Procurar saber quando se deve reformular a estratégia**. Um modelo desenhado só é válido enquanto for eficiente. Não se exige definir tempos de duração, mas uma atenção particular à necessidade de um dia ter de remodelar a estratégia.*

*3 – **Envolva gestores séniores**: OS CIOs devem estar activamente envolvidos na gestão das TI para que a governação tenha sucesso, mas é necessário envolver gestores de topo de outras áreas nos comités e processos de aprovação.*

*4 – **Faça escolhas.** Não é possível cumprir todos os objectivos e por isso devem ser identificados os que geram conflitos de execução e começar por aqueles que são mais simples de concluir e que ao mesmo tempo sejam estratégicos para o negócio da empresa.*

*5 **– Clarifique o processo de gestão de excepções:** Para acompanhar mudanças numa unidade de negócio é preciso saber abrir excepções em relação à arquitectura de TI e à infra-estrutura. Avalie se estas fazem sentido e defina critérios para a sua aceitação.*

*6 – **Forneça os incentivos certos:** Muitas vezes os sistemas de incentivos e recompensas não estão alinhados. É um problema que ultrapassa a governação de TI mas que também a afecta.*

*7 – **Defina responsabilidades na governação das TI:** Em última análise a administração é responsável por toda a governação, mas a delegação da responsabilidade individual ou de grupo normalmente recai no CIO, que assume o desenho, implementação e desempenho desta área. É preciso encontrar a pessoa certa mas não a separar do resto dos objectivos do negócio e garantir que esta crie uma equipa sustentável que apoie a implementação do projecto de governação.*

*8 **– Implemente a governação aos vários níveis organizacionais:** Em grandes empresas, com vários níveis funcionais, é preciso considerar a governança de TI a vários níveis. O ponto de partida são sempre os objectivos e estratégias globais, comuns às múltiplas empresas do mesmo grupo e diferentes geografias.*

*9 – **Assegure transparência e formação:** Quanto mais transparente e mais conhecido for o processo de governação mais fácil é a sua implementação e o cumprimento das directivas por parte de toda a organização.*

*10 – **Implemente mecanismos comuns para as áreas fundamentais:** Vale a pena pensar de forma estruturada os recursos humanos, as relações com clientes e fornecedores, produtos, vendas, finanças e informação e TI. A coordenação destes bens fundamentais da empresa parece óbvia mas nem sempre é implementada.*

A dependência que no momento os negócios têm das TI está implícito que não é possível assegurar a implementação e controlo de medidas de *Corporate Governance* sem ter em linha de conta o *IT-Governance*.

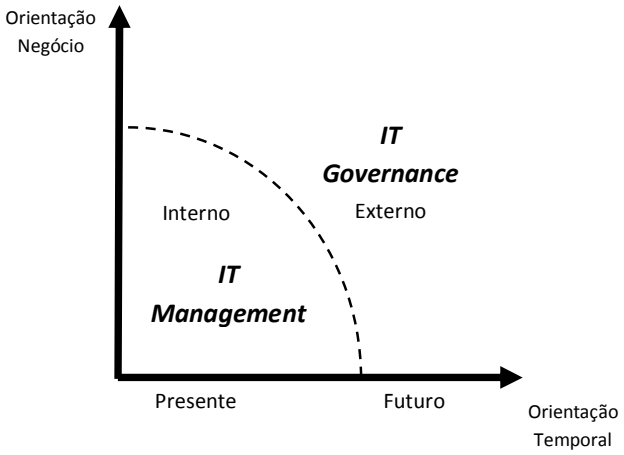

Figura 2 - *IT-Governance* e Negócio, Adaptado a partir de modelo da ISACA [4]

As empresas mais despertas já estarão a mover-se pela consciência de que isto reforça a sua credibilidade, segurança e solidez. Ao cumprirem os requisitos de conformidades, as organizações podem tomar melhores decisões, pois partem de informação com melhor qualidade, que permite melhorar os processos de negócio.

4. Gestão das TI (*IT Management*)

O conceito de *Governance* está subjacente na capacidade de se criarem mecanismos no qual outros possam vir a gerir eficazmente algum recurso, enquanto o *Management* é a actividade para se conseguir operacionalizar esses mecanismos. Para que o *IT-Governance* seja situado numa perspectiva prática é importante saber qual a orientação deste para o negócio e qual é o universo de relacionamento que este tem de ter com a componente de tecnologias. Segundo a figura 2 [adaptada a partir da ISACA], é possível ver que na relação entre o *IT-Governance* e o *IT Management*, o *IT-Governance* é muito mais abrangente e concentra-se na performance e na transformação das TI para irem ao encontro no presente e no futuro das necessidades do negócio. Por outro lado o *IT Management* está focado na eficiência do fornecimento interno efectivo de serviços e produtos e na gestão das operações de TI para responder num curto prazo.

5. Governo nas organizações em geral

Segundo um inquérito da DTI [4] (Departamento de Comércio e Indústria Britânico), 30% das organizações a nível mundial, não reconhecem que a informação relativa ao seu negócio pode conter características sensíveis ou críticas que lhes confiram o estatuto de serem um bem de negócio. Segundo a norma ISO 38500 existem ciclos distintos de controlo que podem ser aplicados a qualquer infra-estrutura de tecnologias de informação de uma organização, baseado em IT-Governance para acções de definir e implementar processos, políticas e regras para o governo das actividades.

- **Projectos de desenvolvimento de aplicações:** Adicionam estrutura e disciplina à prática no desenvolvimento de aplicações. Controlo do código fonte, repositórios de dados,

monitorização de tarefas, e planeamento de projectos e a gestão de *software* e a análise e as ferramentas de testes podem ser muito úteis para a implementação de projectos de *IT-Governance*.

- **Operação de sistemas em tempo real:** As aplicações de *software* para a monitorização das actividades de negócio podem ter neste cenário o papel de sensores. As aplicações de gestão das regras de negócio podem ter um papel importante para o gestor enquanto o *software* de segurança pode ser considerado como um actuador que protege os acessos de utilizadores não autorizados.

- **Gestão de portfólio:** Nesta componente é onde se decide fazer versus comprar; substituir *versus upgrade*, *in-house versus outsourcing*, etc. São algumas das decisões consideradas como parte das gestão do portfólio das TI, e estas decisões podem ser consideradas utilizando uma aplicação de gestão do portfólio de *assets* que providenciam informação sobre as dependências do suporte necessário e o impacto de custos. Um programa efectivo de *IT-Governance* pode ajudar uma organização a manter os seus recursos de TI focados nas prioridades, mantendo os compromissos com o nível de serviço assegurados e decidir com base em informação precisa. É de crucial importância que as direcções das organizações conheçam na integra a arquitectura global do seu portfólio de aplicações de TI, conheçam os recursos de informação que se encontram disponíveis e em que condições e qual o papel que devem desempenhar para produzirem valor.

O principal objectivo da aplicação do *IT-Governance* numa organização é:

1. assegurar que os investimentos em TI geram valor de negócio e
2. atenuar os riscos associados à introdução e investimentos das TI (figura 3).

Pelo que estes 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.

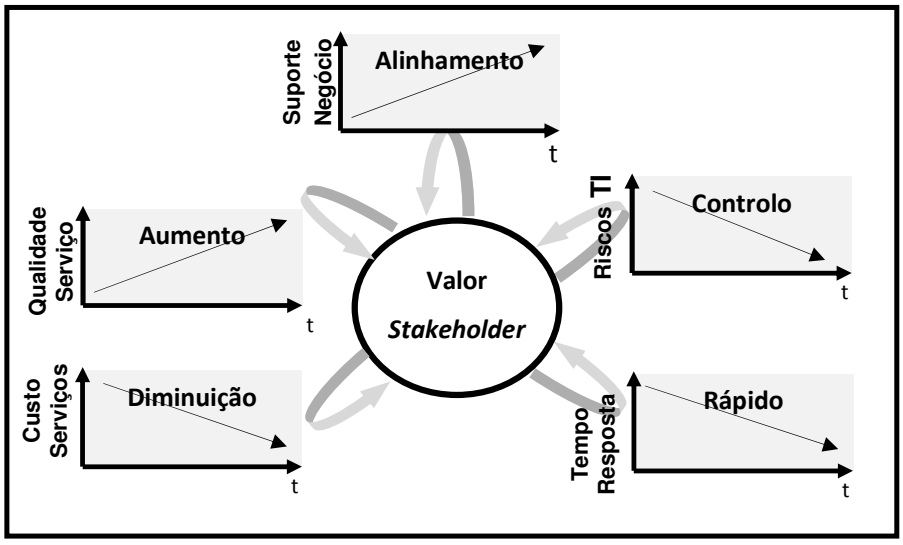

Figura 3 – *IT-Governance* como habilitador negócio

6. Governo nas organizações de saúde

Nos organismos de saúde, nomeadamente nos hospitais onde se encontre alguma maturidade que diga respeito à necessidade de gestão dos acessos aos recursos de informação, aguarda-se com ansiedade por orientações objectivas, provenientes de uma entidade de regulação, de como pode e deve ser gerido o seu conjunto de peças de informação em matéria de política que siga padrões de gestão do risco e da segurança de informação. A indefinição de regras e orientações e a falta de um repositório legal de documentação com as normas e conceitos mínimos que possam ser adoptados, na área das tecnologias informáticas e nas infra-estruturas de comunicação, redes e energia para que do ponto de vista funcional seja possível e acessível a pesquisa de informação que permita uma gestão operacional adequada (ex. implementação de directórios LDAP, servidores de comunicações, tecnologias *thin client*, *service desk* com qualidade, centros de dados energicamente eficientes, medidas a ter na implementação de equipamento informático nos blocos operatórios, etc… Não esquecer porém o enfoque nas arquitecturas de sistemas de informação, interoperabilidade, desenvolvimento, comunicação, arquivo, e até mapeamentos da informação de negócio. No âmbito do Serviço de Saúde seria valioso a promoção de:

- um repositório central e actualizado com todas as regulações nacionais e internacionais com relevo para a Saúde;
- um directório com vários actores ligados à gestão das TI onde pudessem ser acompanhados com a divulgação de trabalhos relacionados que estejam a decorrer nas instituições de saúde;
- a divulgação de trabalhos relacionados que estejam a decorrer na academia;
- a criação de um espaço em que sejam propostos à academia novos estudos de avaliação, sistemas avançados, etc.;
- formação relacionada com a interoperabilidade (ITIL, HL7, DICOM, openEHR, ...)

7. A Segurança das TI como habilitador de negócio

Segundo Eugene Spafford [5] a segurança não é um problema mas uma ferramenta que protege o nosso emprego e ajuda a impulsionar o negócio. Uma aposta numa plataforma ágil e integrada para a segurança da informação pode garantir uma serie de oportunidades. Configure-se o exemplo na imagem (da CA) onde podemos constatar como quatro oportunidades se podem estender no seguinte posicionamento (figura 4). A oportunidade mais abrangente e a longo prazo é aquela que terá mais impacto para além do seu âmbito. Por exemplo as actividades de conformidades podem ter benefícios significativos para além de meramente ajustar conformidades com os requisitos de cada uma regulação.

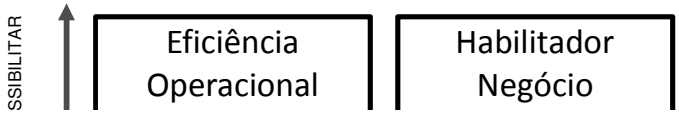

Figura 4 – A adopção do *IT-Governance* como habilitador negócio [7]

Eficiência Operacional

O desafio para os gestores da segurança das TI é reduzir o custo total das operações em TI e em infra-estruturas e melhorar a produtividade de quem as utiliza. Do ponto de vista operacional uma plataforma integrada de segurança pode criar eficiência se:

1. Centralizar a gestão das identidades dos utilizadores de modo que IDs e perfis dos utilizadores não tenham de ser criados e geridos em múltiplos sistemas;
2. Centralizar toda a gestão de acessos de forma que a segurança não necessite de ser gerida em cada aplicação ou cada sistema operativo;
3. Automatizar o acesso ou a inibição de todos os direitos de acesso das aplicações de cada utilizador de forma a eliminar que os administradores de sistemas tenham de dar acesso manualmente a cada sistema;
4. Automatizar a gestão das vulnerabilidades de modo que os sistemas possam ser actualizados mais facilmente com *patches* para as últimas vulnerabilidades;
5. Permitir aos utilizadores que possam criar e gerir alguma da informação do seu perfil (por exemplo *passwords*) e evitar assim que isso tenha de ser realizado pelos administradores de sistemas ou pela equipa de *helpdesk*;
6. Automatização e filtro de eventos na análise da gestão da segurança da informação. Permitir que os *logs* sejam agrupados e correlacionados de modo a ficarem mais visíveis os eventos mais importantes permitindo redução de tempo no esforço necessário pelos gestores da segurança, tal como a redução da probabilidade de ignorar as quebras de segurança.

Mitigação do Risco

Uma das oportunidades que a segurança da informação nos oferece é a capacidade de delimitar os riscos operacionais tal como as ameaças de *hackers*, *malware*, acesso não autorizados a recursos, tempo de latência até a desactivação de perfis de utilizadores que deixaram a organização, contas abandonadas, etc. São necessários planos para a delimitação dos riscos de modo a garantir que estes se encontram a um nível baixo aceitável. Estas ameaças não só têm impacto na criticidade da segurança dos bens da organização, como também tornam qualquer iniciativa de regulamentar e garantir a conformidade mais difícil. Existem duas áreas principais

no qual uma efectiva gestão da segurança pode fazer beneficiar uma significante delimitação do risco: a protecção de bens de forma a assegurar que os recursos valiosos da organização se mantêm seguros e acessíveis só a quem de direito; e a garantia da continuidade de Serviço de forma a garantirmos que os serviços disponibilizados a empregados, parceiros e clientes estão disponíveis quando necessários, sem degradação de qualidade ou nível de serviço. Uma solução integrada para a gestão das ameaças pode ajudar a assegurar a continuidade de serviços críticos de TI.

Conformidades & Auditoria

A gestão da segurança é o coração de muitas regulações das indústrias e dos governos, especialmente aqueles que lidam com requisitos relativos à privacidade de informação. Sem um infra-estrutura robusta de segurança que proteja sistemas, aplicações, dados e processos de acessos ou uso não autorizado, obter a conformidade das *regulations* é muito difícil. A chave para a *compliance* com estas regulações é garantir a implementação de um robusto conjunto de controlos de segurança. Esses controlos devem não só assegurar a validação e eficácia dos processos críticos de informação, mas também permitir que sejam facilmente auditáveis de modo a provar a *compliance* a auditores internos e externos.

Habilitador de Negócio

Existe um grande oportunidade - normalmente desprezada - relacionada com um sistema de segurança integrado no qual a aposta é em deixar entrar com segurança quem pretende fazer o bem permitindo o estabelecimento de iniciativas de negócio. Uma gestão efectiva da segurança permite que a infra-estrutura seja gerida de uma forma que mais facilmente faça crescer o negócio. Fortalece também a relação entre clientes e parceiros de uma forma que cria oportunidade de vendas de produtos e serviços adicionais seja com uma diversificação de serviços, melhoria do relacionamento com os clientes, melhorar a reputação (pode ser muito prejudicial para o negócio o conhecimento público de uma simples quebra de segurança), criação de um ecossistema robusto para partilha de aplicações e capacidade de reagir rapidamente à mudança das condições de mercado.

8. Conclusões

As equipas de gestão nos *boards* das instituições de saúde deverão estar sensíveis às questões da segurança das TI, mesmo que não estejam confiantes que um investimento nesse sector possa ser habilitador de negócio. Isto porque, investir nessa área tecnológica vai no mínimo assegurar um ambiente seguro e proteger os bens da organização tal como a reputação desta na indústria da saúde. Normalmente é obrigatório que estas actividades sejam implementadas a um custo mais baixo do que no passado. O *IT-Governance* é visto como um aliado nesta preocupação estratégica pois ajuda a potenciar a introdução de nova tecnologia com método e investimento controlado e identifica os principais riscos que as infra-estruturas críticas podem estar sujeitas. É importante considerar que qualquer mudança pode ter riscos reais associados e infinitos, pelo que a estabelecer um caminho para um programa de segurança da informação deve considerar-se que o ambiente da informação é altamente dinâmico e os seus recursos são finitos. A implementação de uma solução terá sempre de incluir de base as pessoas, os processos e as tecnologias e assumir que o maior problema serão sempre as pessoas. A grande parte dos

ataques surge devido a erro ou iniciativa humana, falha de sistemas e *software* malicioso. Quer sejam as pessoas que desenham o *software*, as que instalam, as que abusam dos sistemas e muitas vezes as que é suposto estarem a guardar o sistema, a verdade é que o elemento humano é sempre considerado o elo mais fraco.

Bibliografia

[1] ISO/IEC 38500:2008, JTC 1 Information technology, Corporate governance of information technology

[2] Australian Standard for Corporate Governance of Information and Communication Technology)

[3] Weill, Ross. (2004) In Governance - How Top Performers Manage It Decision Rights For Superior Results , Harvard Business Press.

[4] The Information Systems Audit and Control Association (ISACA), http://www.isaca.org/

[5] DTI (Departamento de Comércio e Indústria Britânico)

[6] Eugene Spafford, (perito internacional da segurança - the executive director of Purdue University's Center for Education and Research in Information Assurance and Security (Cerias)

[7] Whitman, Mattord. (2009). Risk Management: Controlling Risk. Chap 9. Management of Information Security. 3th edition. USA, Course Technology.