



Universidade do Minho

**Departamento de Sistemas de Informação**

**Escola de Engenharia**

José Luís da Rocha Sousa

# **MODELO DE PLANEAMENTO DE SISTEMAS DE INFORMAÇÃO PARA A ERA DA COLABORAÇÃO, A ERA WEB 2.0**

Dissertação de Mestrado

**Mestrado em Sistemas de Informação**

**Trabalho efectuado sobre a orientação do**

**Professor Doutor Henrique Santos**

**Junho de 2008**



Universidade do Minho

**Departamento de Sistemas de Informação**

**Escola de Engenharia**

José Luís da Rocha Sousa

**MODELO DE PLANEAMENTO DE SISTEMAS DE  
INFORMAÇÃO PARA A ERA DA COLABORAÇÃO, A ERA  
WEB 2.0**

**DISSERTAÇÃO DE MESTRADO**

**Junho 2008**

À Susana, ao Luís e á Margarida

*"It is not the strongest of the species that survive, or the most intelligent, but  
the one most responsive to change."*

Charles Darwin (1809 - 1882)

*"Se vamos ficar expostos, pelo menos estejamos em forma"*

Don Tabscott (2006)

*"Não me importo de perder, apenas não quero ser surpreendido"*

Alexandre, o Grande

*This is our future – this how we must fight in the age of small, the fast and the  
many"*

(Arthur Cebrowski)



## AGRADECIMENTOS

Um agradecimento especial, á minha esposa Susana, pelo apoio na criação das condições para tornar possível a concretização do mestrado.

Aos meus filhos, Luís e Margarida, pela compreensão quando as horas de disponibilidade e de brincadeira não foram as pretendidas.

Ao Professor Doutor Henrique Santos pela forma como aceitou este desafio e contribuiu para que o mesmo fosse possível.

Ao IBMC, por ter criado as condições para que este resultado fosse possível e por ter valorizado a obtenção deste mestrado.

A todos os outros, um muito obrigado.

## RESUMO

Suportado pela WEB 2.0, o paradigma actual dos sistemas de informação é a colaboração em rede com a criação do conhecimento em rede. Confrontada com este conhecimento as organizações estão a convergir para a sua adopção, estamos na era da WEB 2.0 . Esta WEB não é apenas tecnologia mas uma nova forma de utilização dessa tecnologia para produção de conhecimento.

As organizações enfrentam novos desafios na adopção e integração de soluções e metodologias, colocando na linha da frente sistemas actualmente protegidos pelos limites físicos das organizações. A arquitectura destes sistemas não foi desenvolvida com a colaboração ou mesma a partilha em mente, sendo usados no seu planeamento modelos tradicionais, incapazes de gerir os novos limites das organizações.

Esta evolução está a criar a uma economia em rede e a alterar o forma como as organizações interagem com os seus recursos. Estando a evoluir do computador em rede para o utilizador em rede.

Os modelos tradicionais definem a forma como os sistemas de informação devem suportar as actividades das organizações. Este é um aspecto chave, mas o novo paradigma coloca um novo desafio, saber como os sistemas de informação devem ser desenvolvidos de forma a serem capazes de garantir o efeito da informação.

Nesta dissertação é apresentado um modelo de planeamento, cujo objectivo é garantir que a organização irá alcançar os efeitos pretendidos quando os mesmos forem suportados pelo ecossistema correcto. O modelo identifica as vulnerabilidades críticas, as capacidades críticas e as necessidades críticas que suportam determinado efeito no ecossistema.

De forma a serem obtidos os efeitos correctos é usada a prioritização e a interdependência, dois elementos da engenharia de software, permitindo assim a correcta caracterização dos mesmos no ecossistema.

Apenas um modelo baseado em efeitos, em que a segurança da informação é uma parte integrante do objecto informação torna possível o planeamento de sistemas na era das organizações colaborativas.

O planeamento baseado na procura dos efeitos da informação, enquanto característica da mesma, é uma forma de obter uma visão clara desde as primeiras fases de criação do ecossistema colaborativo, suportado pela WEB 2.0.

**Palavras chave:**

Planeamento, segurança, WEB 2.0, efeitos, informação, ecossistema, interdependência, priorização, necessidades críticas, vulnerabilidades críticas

## ABSTRACT

Supported by WEB 2.0 today information systems paradigm is networked collaboration with networked knowledge creation. Confronted with the network knowledge, organizations are trying to converge to the adoption of that knowledge, we are in the web 2.0 era. Web 2.0 is not only technology but about the way that technology is used for knowledge production.

This enrollment of organizations in the new WEB puts new challenges in the adoption and integration of solutions and methodologies putting in the front line systems that are today protected behind the organizations structures. These systems architectures weren't developed with collaboration or even sharing in mind, they use the traditional information systems planning models that are incapable of managing the new organizations boundaries.

This new way of organizations interacting with resources is defined as the networked economy.

In this economy we have a networked user, not only a networked computer.

The traditional models define the way information systems should support organizations activities, this is a key aspect, but the new collaboration paradigm creates a new challenge that is to know how information systems should be develop in order to guarantee the organization information effect.

In this paper is presented a model to give information systems planning a way to guarantee that organization will achieve the effects they want when supported with the correct information system ecosystem. The model identifies the critical vulnerabilities, critical capacities, critical needs that support the critical center of the ecosystem. In order to get the correct effects is used prioritization and interdependency two well know words of software engineering, in order to define effects relation in the ecosystem.

Only a model based on information effects and with the integration of security as part of the information object makes information systems planning possible in this organization collaboration era. The collaboration supported by WEB 2.0 is a challenge for organizations and the planning of information, as ecosystem, using effects based planning, is a way to give a clear view of the development since the early stage of the ecosystem creation.

**Keywords:**

Planning, security, WEB 2.0, effects, information, ecosystem, interdependency and prioritization, critical needs, critical capabilities, critical vulnerabilities

# INDICE

INDICE DE FIGURAS.....	XII
INDICE DE TABELAS .....	XIII
1. INTRODUÇÃO .....	16
1.1. OBJECTIVOS .....	19
1.2. ESTUDO REALIZADO.....	21
1.3. ESTRUTURA DA DISSERTAÇÃO.....	21
2. MODELOS DE PLANEAMENTO DE SISTEMAS DE INFORMAÇÃO .....	23
2.1. INTRODUÇÃO .....	23
2.2. CADEIA DE VALOR.....	25
2.3. FACTORES CRITICOS DE SUCESSO (FCS) .....	27
2.4. PLANEAMENTO DE SISTEMAS DE NEGÓCIO (PSN) .....	28
2.5. PLANEAMENTO ESTRATÉGICO DE SISTEMAS (PES).....	31
2.6. PLANEAMENTO DA ENGENHARIA DA INFORMAÇÃO (PEI) .....	32
2.7. METHOD 1.....	33
2.8. PLANEAMENTO ESTRATEGICO DE SISTEMAS DE INFORMAÇÃO (PESI) .....	33
2.9. LEARN.....	35
2.10. CONCLUSÕES.....	36
3. PARADIGMA DA COLABORAÇÃO .....	38
3.1. CARACTERIZAÇÃO .....	38
3.2. A WEB 2.0 .....	40
3.3. CONCLUSÕES.....	44
4. A SEGURANÇA DE INFORMAÇÃO.....	45
4.1. CARACTERIZAÇÃO .....	45
4.2. IMPACTO DA WEB 2.0 .....	48

4.3. CONCLUSÕES.....	54
5. MODELO PROPOSTO .....	57
5.1. PLANEAMENTO ORIENTADO AOS EFEITOS .....	58
5.2. CARACTERIZAÇÃO DOS EFEITOS .....	61
5.3. PRIORITIZAÇÃO .....	62
5.4. INTERDEPENDÊNCIA .....	63
5.5. CONCLUSÕES.....	65
6. CASO PRÁTICO .....	67
6.1. INFRAESTRUTURA DE SERVIDORES E ARMAZENAMENTO .....	67
6.1.1. EFEITOS .....	67
6.1.2. PONTO DA SITUAÇÃO .....	68
6.1.3. CAPACIDADES CRITICAS .....	68
6.2. INFRAESTRUTURA DE REDE.....	69
6.2.1. EFEITOS .....	69
6.2.2. PONTO DA SITUAÇÃO .....	70
6.2.3. CAPACIDADES CRITICAS .....	70
7. CONCLUSÕES.....	72
BIBLIOGRAFIA.....	77
INDEX .....	79
ANEXO A .....	80
ANEXO B.....	83

## INDICE DE FIGURAS

FIGURA 1 - DUAS VISÕES DOS MODELOS DE PLANEAMENTO DE SISTEMAS DE INFORMAÇÃO .....	24
FIGURA 2 – MODELO DA CADEIA DE VALOR DE PORTER (PORTER 1984) .....	25
FIGURA 3 - HIERARQUIA DOS FACTORES CRÍTICOS DE SUCESSO .....	27
FIGURA 4 - PASSOS DO MÉTODO DE PLANEAMENTO DE SISTEMAS DE NEGOCIO .....	30
FIGURA 5 - MÉTODO ASSOCIADO AO DESENVOLVIMENTO DO MODELO PES .....	31
FIGURA 6 - PIRÂMIDE DA ENGENHARIA DA INFORMAÇÃO (MARTIN 1989).....	32
FIGURA 7 - MODELO DE PLANEAMENTO ESTRATÉGICO DE SISTEMAS DE INFORMAÇÃO .....	34
FIGURA 8 – MÉTODO LEARN .....	36
FIGURA 9 – O EFEITO WEB 2.0 - ADAPTADO DE(ROMAN HOEGG 2007) .....	40
FIGURA 10 – EXEMPLOS DE FERRAMENTAS DA ERA DA COLABORAÇÃO.....	42
FIGURA 11 – CARACTERIZAÇÃO DE ALGUMAS DAS APLICAÇÕES DISPONIBILIZADAS NA WEB 2.0 (HAMMOND 2007) .....	43
FIGURA 12 – ANÉIS ESTRATÉGICOS.....	58
FIGURA 13 – ARQUITECTURA DO MODELO .....	60
FIGURA 14 – CARACTERÍSTICAS FUNDAMENTAIS DA INTERDEPENDÊNCIA.....	64



## INDICE DE TABELAS

TABELA 1 - PERÍODOS DE DESENVOLVIMENTO DOS SISTEMAS DE INFORMAÇÃO (Hsu 1995) .....	17
TABELA 2 - MÉTODOS DE PLANEAMENTO DE SISTEMAS DE INFORMAÇÃO .....	24
TABELA 3 - MÉTODO ASSOCIADO AO MODELO DA CADEIA DE VALOR .....	26
TABELA 4 - MÉTODO PARA O PSN (ALBERT L. LEDERER 1998).....	29
TABELA 5 – MÉTODO ASSOCIADO AO MODELO DE PLANEAMENTO DE ENGENHARIA DA INFORMAÇÃO (MARTIN 1989) .....	32
TABELA 6 – DOIS EXEMPLOS DE ATAQUES Á ERA WEB 2.0 .....	49
TABELA 7 – CARACTERÍSTICAS DO MYSPACE E EXPLORAÇÃO DE VULNERABILIDADES.....	49
TABELA 8 – VULNERABILIDADES E FORMA DE ATAQUE ASSOCIADAS .....	50
TABELA 9 – EXEMPLO DE FUNCIONAMENTO DO JITKO .....	51
TABELA 10 - LISTA DAS APLICAÇÕES MAIS COMUNS DE 2007 E SUAS VULNERABILIDADES .....	52
TABELA 11 – DEFINIÇÃO DOS ANÉIS ESTRATÉGICOS DE UM ECOSISTEMA DE INFORMAÇÃO .....	59

## SIGLAS

IT	Information and Tecnhology
FCS	Factores críticos de sucesso
PSN	Planeamento de sistemas de negócio
PES	Planeamento estratégico de sistemas
EI	Engenharia da informação
PESI	Planeamento estratégico de sistemas de informação
LEARN	Nome para o método de planeamento retirado da palavra inglesa Learning
HTTP	Hyper Text Transmition Protocol
SMTP	Simple Mail Transfer Protocol
XML	Extended Markup Language
P2P	Peer to Peer
TCP	Transmission Control Protocol
IP	Internet Protocol
AJAX	Asynchronous JavaScript
XML	Extended Markup Language
SISP	System Information Strategic Planning
DFD	Data Flow Diagram
BPM	Business Process Modeling
RIA	Rich Interface Access
XSS	Cross-Site-Scripting
DoS	Denial of Service
SPAM	E-mail não solicitado ou indesejado
JITKO	Aplicação de código malicioso com o objectivo de transformar o browser infectado parte de redes de bots
SOAP	Simple Object Access Protocol
LDAP	Light Data Access Protocol
VOIP	Voice over IP

XPATH	XML path language
UI	User interface
RSS	Real Simple Syndication
CMS	Content Management System

### 1. INTRODUÇÃO

As organizações têm crescido de uma forma acelerada desde o início da década de 90, tornando-se cada vez mais complexas de gerir. Este crescimento comprimiu o ciclo de negócio e desenvolvimento das organizações e conduziu (e conduz) a elevadas exigências no acesso à informação.

Face a esta exigência central, as organizações têm vindo a definir a informação como o seu bem mais precioso, o que dada a sua grande diversidade, volatilidade e quantidade, tornou necessária a adopção de tecnologias de informação para a sua gestão. Estas tecnologias de informação foram evoluindo conforme as necessidades organizacionais. Se no início, a sua utilização poderia ser uma vantagem competitiva, dado o seu elevado investimento e complexidade funcional, sendo necessário a utilização de recursos humanos consideráveis, hoje é possível, com um pequeno investimento, conseguir tecnologia com as mesmas funcionalidades dos grandes sistemas.

Esta banalização das tecnologias de informação torna pois claro que exigências ao nível do acesso à informação, apenas podem ser suportadas com a qualidade e eficiência adequadas, através da correcta definição dos sistemas de informação da organização (André Vasconcelos 1999), abordando não apenas a recolha e processamento como acontecia nos primórdios dos sistemas de informação, mas traçando um caminho de desenvolvimento paralelo ao desenvolvimento organizacional, sendo capaz, de em cada altura disponibilizar a informação adequada.

Definir este mapa da informação organizacional, em que as necessidades de informação das organizações se traduzem na adopção correcta de tecnologias de informação, tem sido o objectivo do planeamento de sistemas de informação.

De forma a que em cada momento do desenvolvimento organizacional esta tenha os meios adequados, têm vindo a ser desenvolvidos modelos de forma a criar um referencial de caracterização organizacional e subsequente tradução na tecnologia a adoptar. Como é natural,

o desenvolvimento destes modelos tem estado associado às características e necessidades das organizações em determinada fase do seu desenvolvimento estando ainda alinhados com os períodos de desenvolvimento dos sistemas de informação.

Tabela 1 - Períodos de desenvolvimento dos sistemas de informação (Hsu 1995)		
	PERÍODO	CARACTERÍSTICAS
60s	Processamento de dados (PD)	Computadores isolados, longe dos utilizadores, função de redução de custos
70s & 80s	Gestão de Sistemas de Informação (GSI)	Processos distribuídos, interligados, suportar o negócio, orientados ao utilizador
80s & 90s	Sistemas de informação estratégicos (SIE)	Rede, sistemas integrados, disponíveis e funcionais para os utilizadores, relacionados com a estratégia do negócio, orientado para o desenvolvimento do negócio.
Sec. XX/XXI	Segurança da Informação (SI)	Gestão dinâmica de todo o fluxo de informação, orientado à segurança

A tabela 1 apresenta as diversas fases do desenvolvimento dos sistemas de informação e as suas preocupações principais, permitindo identificar os diversos desafios para o planeamento de sistemas de informação e mostrando a sua capacidade de dinamicamente se ajustar.

Tendo já comprimido a sua dinâmica de ciclo de vida, as organizações enfrentam agora uma alteração profunda na forma como é efectuada a sua interacção com os elementos que determinam o seu desenvolvimento.

Tendo sofrido um primeiro impacto com o aparecimento da internet e possibilidade de disponibilização de informação de formas perfeitamente inovadoras, conhecida por *World Wide Web*, e que podemos abreviar para WEB 1.0. No entanto, o desenvolvimento continuado de tecnologia permitiu a internet crescer em potencialidades levando a que a WEB desenvolve-se novas formas de “*information availability*”. Nos últimos três anos, esta evolução têm-se centrado em torno do novo paradigma WEB, a WEB 2.0 (Reilly 2005). Com este paradigma o mundo da informação migra de uma visão de “*network is the computer*” para o “*networked user*”.

Este utilizador em rede, munido-se das ferramentas ubíquas de tecnologia e interagindo com as mesmas de diversas formas produz um conhecimento centrado em rede de acordo com determinadas preferências e objectivos. Assiste-se no presente a um crescimento acelerado

deste conhecimento, podendo ser apontados exemplos como o *Facebook*, o *Flick* ou o mais mediático em Portugal, o *Youtube*.

No entanto o conhecimento em rede demonstrou realmente o seu valor naqueles que podem ser os dois ex-libris do desenvolvimento na WEB 2.0, o software *open-source* e a *Wikipedia*, que na sua forma reflectem a nova forma de desenvolvimento informacional e apontam a direcção para a criação do ecossistema colaborativo.

Atentas a este novo ecossistema as organizações estão a tentar criar valor com recurso a este novo paradigma. Este ecossistema colaborativo coloca á prova as organizações e a sua capacidade para adoptarem esta nova realidade funcional de forma a poderem potenciar e integrar o seu desenvolvimento numa economia centrada em rede (Tapscott 2007). Para as organizações a integração neste novo ecossistema coloca novos desafios ao nível da segurança da informação, dado que neste ecossistema em rede, a garantia das características da informação é fundamental, já que a disponibilização da informação organizacional assenta num pressuposto fundamental a credibilidade. A segurança da informação deixa de ser apenas uma gestão de acesso, tendo por base garantir disponibilidade, integridade e confidencialidade, mas passa a ter de ser uma característica intrínseca dessa mesma informação e fazendo parte da forma como a mesma se desenvolve dentro do ecossistema.

Assim como a informação tem de ser segura para ser credível, pretende-se que a disponibilização da mesma possa permitir a obtenção de determinado efeito organizacional.

As organizações têm assim de ter condições para garantir a obtenção do efeito pretendido.

Permitir que as organizações integrem este novo paradigma e que consigam garantir segurança na informação e obtenham os efeitos pretendidos com a disponibilização da informação, só é possível com a correcta caracterização do seu ecossistema informacional. Só existe um forma de o fazer, planeando.

O correcto planeamento do ecossistema de informação, é hoje, como era no passado o planeamento de sistemas de informação, o maior desafio para a correcta gestão da informação organizacional (Hsu 1995).

## 1.1. OBJECTIVOS

Os modelos de planeamento de sistemas de informação actuais ainda se preocupam apenas com os aspectos internos das organizações e com a forma como os sistemas os podem implementar, desenvolver ou melhorar, tendo por objectivo central o desenvolvimento das organizações. O conceito de ecossistema permite a evolução para a integração de novos elementos nos sistemas existentes, que ao interagirem com estes potenciem o efeito organizacional.

Os modelos actuais pretendendo efectuar um alinhamento estratégico entre a organização e o IT, orientam-se para a criação de valor, desenvolvimento dos processos organizacionais, ou integração de tecnologia diferenciadora.

A palavra corrente, quando se fala em planeamento de sistemas de informação é “*alinhamento*” estratégico. Este alinhamento estratégico é difícil de definir num sistema de informação cujo ambiente funcional está em constante mudança, traduzindo em problemas de completa disfunção entre os sistemas e as organizações.

Os modelos de planeamento de sistemas de informação debruçam-se frequentemente apenas sobre o ciclo de vida de determinada informação, seja ela, financeira, produtiva, etc. No entanto a realidade colaborativa a que assistimos exige a criação de um sistema de informação com uma arquitectura capaz de criar um fluxo de informação, desde o mundo físico (dados) até ao domínio cognitivo (conhecimento), tendo pelo meio o processo de criação de informação.

As organizações vivem de forma concorrente num mundo global onde a frase “*think global act local*” (Anna H. Perrault 2000) foi substituída pela “*think global act global*”. (Tapscott 2007)

Torna-se pois necessário que o planeamento de sistemas de informação passe de um alinhamento estratégico para um ecossistema colaborativo, sendo capaz de, em cada momento, fornecer as condições de arquitectura adequadas ao funcionamento da organização, ou seja, sendo capaz de caracterizar as relações existentes no processo informacional de cada fase do desenvolvimento da organização.

Perante estas observações, surgiu a necessidade de desenvolver um modelo de planeamento que incorporasse esta nova realidade, o ecossistema informacional. O planeamento deverá pois ser capaz de, neste contexto,, tratar do produto informação sendo capaz de gerir o seu fluxo, desenvolvendo o planeamento do ecossistema de informação. Este planeamento tem de garantir

o efeito pretendido para a informação, sem o qual esta não tem valor, bem como a confidencialidade, integridade e disponibilidade da informação, traduzindo uma garantia da segurança da informação, sem a qual esta não pode criar valor, nem a obtenção do efeito pode ser garantida.

Tratando-se do bem mais precioso das organizações, este bem deverá ser protegido de acordo com a sua importância, e o que se assiste nos modelos de planeamento actuais, é que a tarefa de segurança da informação é essencialmente um problema tecnológico e desenvolvido após a implementação do sistema de informação.

Nesta dissertação de mestrado apresenta-se um novo modelo para planeamento, orientado ao ecossistema de informação, que pretende ser capaz de endereçar as necessidades de funcionamento actual das organizações integrando como característica da informação o efeito e a segurança.

É proposta uma mudança de paradigma, passando do alinhamento estratégico para o efeito da informação e da segurança do acesso à informação para a integração da segurança como característica da informação. Nesse sentido, este modelo caracteriza os efeitos que a organização pretende obter com o seu funcionamento, tentando, a partir daí, caracterizar quais as implicações que esses efeitos têm ao nível dos elementos de suporte ao desenvolvimento, recriando o ecossistema.

Centrado no elemento principal das organizações, a informação, e aplicando conceitos da guerra da informação, apresenta-se a capacidade do modelo para adequar a segurança da informação aos efeitos pretendidos, integrando a segurança no fluxo informacional.

É efectuada uma caracterização do modelo que absorvendo as necessidades de informação e segurança da mesma traduz a complexidade e volatilidade desse processo de modelação. Assim, recorrendo ao planeamento militar da guerra da informação do modelo orientado aos efeitos (Nunes 2006) e acrescentando dois elementos da engenharia do software para gerir esses mesmos efeitos, priorização (Leffingwell D. 2000) e interdependência (Robertson 1999), pretende-se obter um modelo que recrie o ecossistema organizacional e que potencie a obtenção de determinado efeito sendo fundamental a garantia da segurança do fluxo informacional, sem a qual o efeito pretendido para o ecossistema pode ser comprometido.



Cada organização é assim vista como parte de um ecossistema relacional através do processo causa/efeito em que a informação de que é proprietária será sempre um elemento do ecossistema e cujo objectivo será garantir a sobrevivência da organização no ecossistema.

## **1.2. ESTUDO REALIZADO**

O trabalho realizado partiu de uma revisão de literatura sobre os modelos de planeamento de sistemas de informação e a sua adequação ao novo paradigma da WEB 2.0, em que o utilizador em rede potencia a criação de uma economia em rede, criando um ecossistema de informação em rede.

Foram assim analisados os modelos de planeamento tradicionais e atendendo às características do novo ambiente organizacional, foram definidas como características da informação o seu efeito, segurança, interdependência e prioritização elementos normalmente usados em análise conceptuais.

Esta integração traduziu-se no modelo aqui apresentado, em que o ecossistema da informação é o seu elemento central.

## **1.3. ESTRUTURA DA DISSERTAÇÃO**

A presente dissertação encontra-se organizada em sete capítulos.

È de seguida apresentado um breve resumo de cada capítulo.

O segundo capítulo caracteriza os modelos de planeamento de sistemas de informação mais frequentes e cuja orientação é a produção de sistemas de informação.

O terceiro capítulo faz uma abordagem ao paradigma colaborativo introduzido pela WEB 2.0, e as implicações que a mesma acarreta para o desenvolvimento das organizações.

No quarto capítulo é efectuado o desenvolvimento do tema da segurança da informação face aos desafios colocados pelo desenvolvimento das tecnologias que suportam a WEB 2.0.

O quinto capítulo apresenta o modelo de planeamento do ecossistema da informação apresentando as suas bases teóricas fundamentais.

No sexto capítulo, é apresentado um projecto como caso prático de construção de um ecossistema de informação, levado a cabo numa instituição de investigação científica, desenvolvido com o recurso ao modelo de planeamento aqui apresentado.

No sétimo capítulo são apresentadas as conclusões.

Existem ainda o anexo A, com o método LEARN e o anexo B com a instanciação do modelo com elementos do caso prático apresentado.

# 2. MODELOS DE PLANEAMENTO DE SISTEMAS DE INFORMAÇÃO

## 2.1. INTRODUÇÃO

Em todas as áreas de desenvolvimento humano existe sempre uma necessidade de criar um conjunto de elementos que permitam endereçar a resolução de determinados problemas. Os sistemas de informação e mais concretamente o planeamento associado à sua implementação, não são excepção.

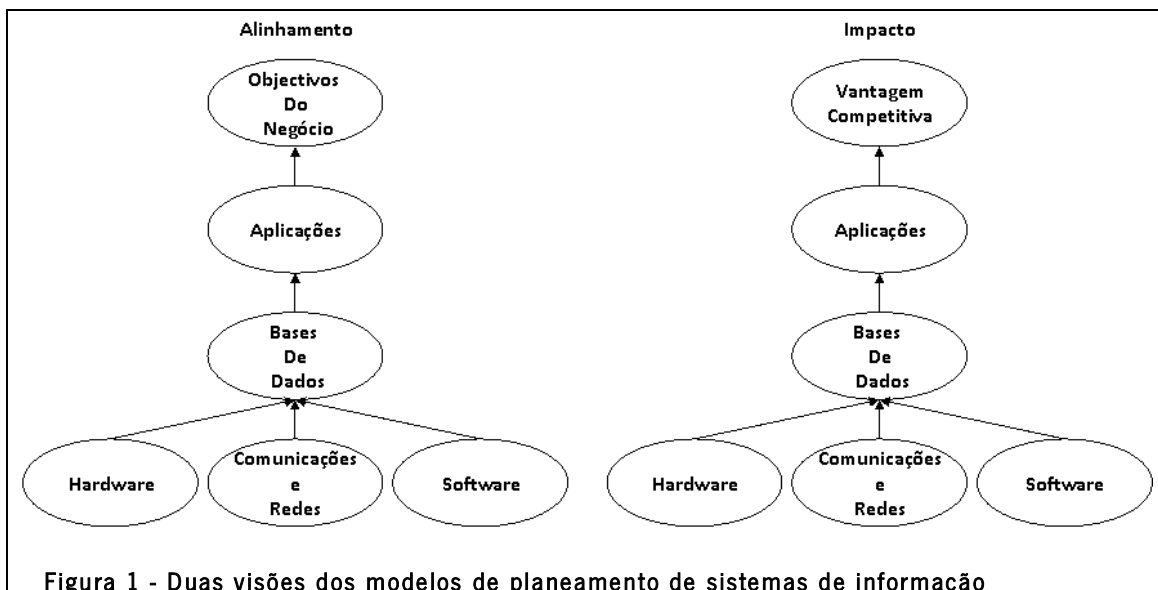
Este planeamento de sistemas de informação pode ser visto como *“a actividade da vida das organizações onde se define o futuro desejado para o seu sistema de informação, para o modo como este deverá ser suportado pelas tecnologias da informação e comunicação, de forma a concretizar esse suporte”* (Amaral 1994).

Numa perspectiva permanente de mudança frequente do contexto organizacional o planeamento de sistemas de informação vê-se obrigado a ter a capacidade de se adaptar (Carvalho 1997). Garantir a sobrevivência e o sucesso de um sistema de informação nesta realidade constitui uma tarefa verdadeiramente difícil.

Porque se considera que *“pensar antes de fazer”* constitui uma atitude racional, fundamental quando se pretende alcançar o melhor resultado com a realização de uma determinada tarefa. *“O plano não é nada, o planeamento é tudo”*, determina que esta é uma actividade dinâmica.

Existem de forma preponderante duas classificações relativamente a modelos de planeamento de sistemas de informação. Os modelos podem ser classificados segundo duas categorias: impacto e alinhamento (Hsu 1995).

Temos modelos de alinhamento quando se procura um alinhamento estratégico com a organização e de impacto quando são se pretende obter alguma vantagem usando a integração de soluções centradas na tecnologia (Carvalho 1997).



Na figura 1 são identificados os dois modelos centrais de planeamento assim como os elementos que integram cada uma das visões.

Estas visões encontram-se representadas pelos modelos apresentados na tabela 2.

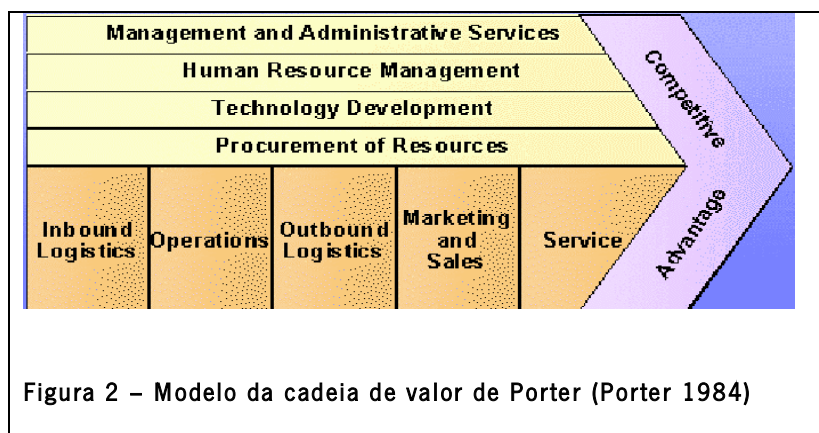
Tabela 2 - Modelos de planeamento de sistemas de informação	
Impacto	Alinhamento
Cadeia de valor (Porter 1984)	Method/1 (Hsu 1995)
Factores críticos de sucesso (FCS) (Rockart 1979)	Planeamento estratégico de Sistemas de informação para construção de flexibilidade e sucesso (PESI) (Palanisamy 2005)
Planeamento de sistemas de negócio (PSN) (Jachman 1982)	LEARN (Coelho 2003)
Planeamento estratégico de sistemas (PES) (Sethi 1988)	
Planeamento da engenharia da informação (PEI) (Martin 1989)	

Na tabela 2, são apresentados os modelos analisados neste trabalho, encontrando-se os mesmos classificados de acordo com a visão do modelo definido para o planeamento de sistemas de informação.

## 2.2. CADEIA DE VALOR

A cadeia de valor é talvez, um dos exemplos mais marcantes, da ligação entre os sistemas de informação e a necessidade de o mesmo criar valor.

Esta criação de valor é muitas vezes confundida com valor financeiro, perfeitamente tangível, sendo notada esta ligação frequentemente nos organogramas das organizações em que o departamento de informática depende da direcção financeira.



A figura 2 caracteriza a modelo da cadeia de valor de Porter identificando as suas componentes e áreas associadas, decorrendo da análise da figura que a vantagem competitiva cresce fundamentalmente do valor que uma organização é capaz de criar para os seus compradores que exceda os custos de a criar (Porter 1994).

A cadeia de valor é portanto, uma das formas de análise da actividade de negócio. Qualquer empresa executa um conjunto de actividades para levar a cabo um desenho, produzir, colocar no mercado ou entregar e suportar um produto. Essas actividades são descritas usando uma cadeia de valor, focando-se no valor chave adicionado às actividades de negócio e processos. Actividades essas que podem ser efectuados de forma mais eficiente usando IT.

<b>Tabela 3 - Método associado ao modelo da cadeia de valor</b>		
<b>Actividades</b>	<b>Medidas</b>	<b>Objectivos</b>
Avaliar as necessidades de informação	Potencialmente muita informação na cadeia de valor Potencialmente muita informação no produto	Identificar as unidades de negócio prioritárias para investimentos em IT
Determinar o papel da tecnologia de informação na estrutura da industria		Implementação de medidas tecnológicas revolucionárias, tais como processamento automático de transacções para o sistema bancário.
Identificar e classificar as formas nas quais a tecnologia de informação possa criar vantagem competitiva	Pode a tecnologia da informação ajudar a companhia a chegar a novos segmentos de mercado? Pode a tecnologia da informação fornecer a capacidade para expandir o negócio? Pode os gestores esperar da tecnologia de informação a capacidade de explorar as relações com outras industrias?	
Determinar se a tecnologia da informação pode gerar novos negócios	Pode a informação gerada na organização ser vendida? Que capacidade existe interna de processamento de informação para um novo negócio? Pode a tecnologia de informação tornar possível a produção de novos itens relacionado com o produto da organização?	
Desenvolver um plano para obter vantagem da tecnologia da informação		

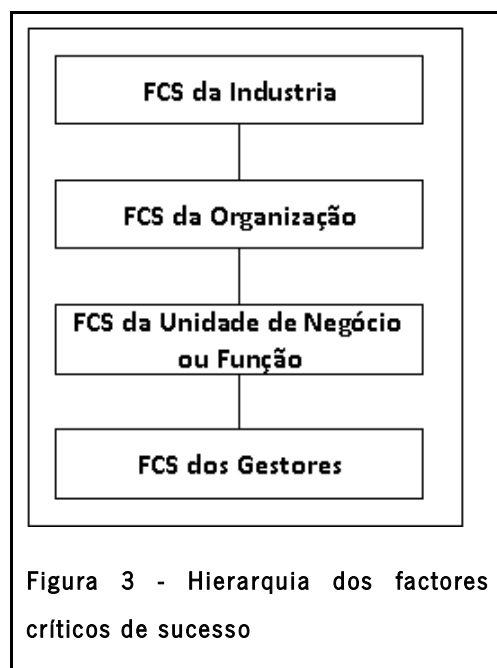
Na tabela 3 são apresentadas as actividades e de que forma as mesmas deverão ser desenvolvidas bem como quais os objectivos a serem alcançados. Esta tabela tem por base

orientar os utilizadores do modelo no sentido de conseguirem extrair os elementos para a escolha das soluções tecnológicas adequadas.

Este modelo é demasiado abstracto e não aborda os elementos dos sistemas de informação nem a sua implementação, focando-se no impacto fornecido pelas tecnologias. Tem por base os dados e define a arquitectura de dados a ser desenvolvida.

### 2.3. FACTORES CRITICOS DE SUCESSO (FCS)

Podemos considerar que são os “*elementos que em dado momento e em determinado contexto podem por em causa o normal funcionamento das organizações*” (Rockart 1979), podendo ser hierarquizados de acordo com a estrutura apresentada na figura 3.



Os factores críticos de sucesso são usados para identificar as necessidades críticas de informação, necessárias para o sucesso da organização e dos seus gestores. O modelo centra-se nas necessidades de informação crítica para os gestores seniores e constrói os sistemas de informação tendo por base essas necessidades. Centrado nas necessidades críticas de informação dos utilizadores internos, ignora o valor acrescentado que pode ser introduzido pelo sistema de informação.

Os factores críticos de sucesso são assim para cada negócio, um conjunto limitado de áreas, cujos resultados, se forem satisfatórios, asseguram o sucesso da performance competitiva da organização (Rockart 1979). Devem ser identificados os factores críticos de sucesso para cada tipo de organização, tendo em atenção (Rockart 1979):

- a particularidade da estrutura da industria;
- a competitividade estratégica, posição da industria e localização geográfica;
- o ambiente organizacional.

Este modelo pode ter efeitos ao nível do impacto e ao nível do alinhamento, tendo o seu enfoque na decisão sobre a informação, não definindo a arquitectura dos dados.

## **2.4. PLANEAMENTO DE SISTEMAS DE NEGÓCIO (PSN)**

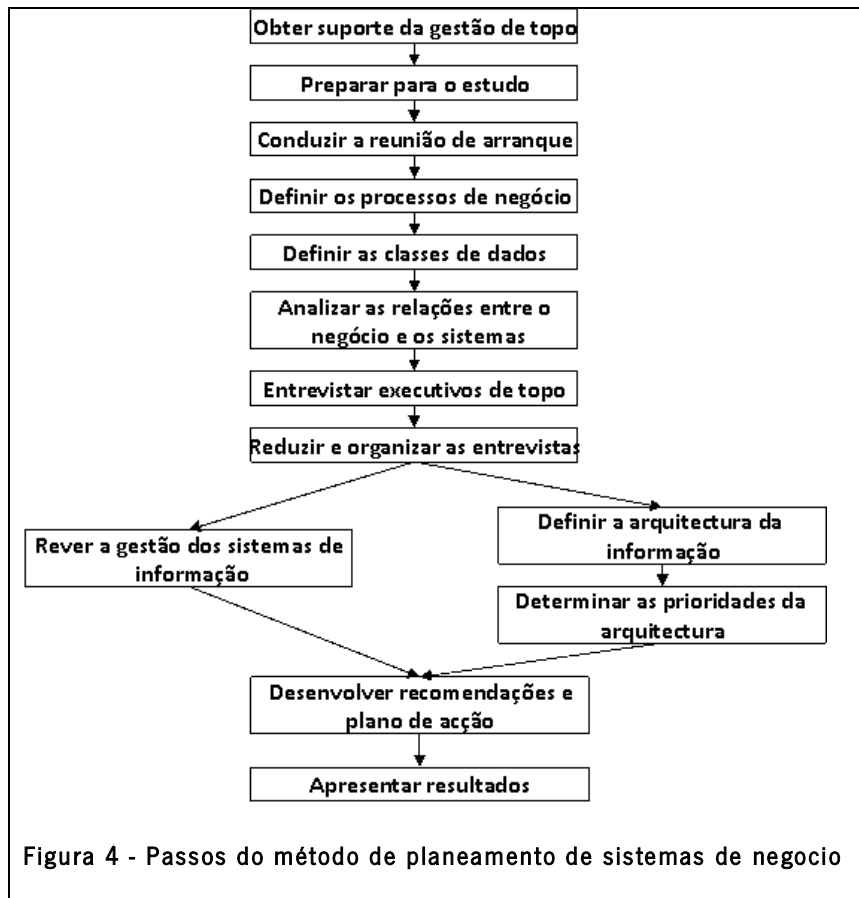
Neste modelo de planeamento as características da informação são derivadas dos processos de negócio, em que a organização reconhece a sua missão de negócio, objectivos e funções e a forma como esses determinam os seus processos de negócio.

Os processos são analisados á luz das necessidades de informação sendo de seguida identificadas as classes de dados. As bases de dados são desenvolvidas através da combinação de classes similares. O plano final descreve uma visão global da arquitectura de sistemas de informação, bem como o calendário de instalação dos sistemas individuais (Jachman 1982).

A tabela 4 descreve os passos do método para implementação do modelo.



<b>Tabela 4 - Método para o PSN (Albert L. Lederer 1998)</b>	
<b>Obter o comprometimento dos executivos</b>	Um executivo de topo e outros executivos interessados são considerados como as maiores fontes de informação do estudo
<b>Preparação do estudo</b>	São compilados os dados das funções de negócio e o suporte actual fornecido pelo sistema de informação
<b>Início do estudo</b>	O patrocinador revê a proposta do estudo, e o líder da equipa revê os elementos recolhidos
<b>Definindo os processos de negócio</b>	São identificados os processos de negócio que serão a base para as entrevistas aos executivos
<b>Definindo as classes de dados</b>	Os dados são agrupados em categorias denominadas classes de dados baseadas nas suas relações com os processos de negócio identificadas acima
<b>Analisando o suporte fornecido pelos sistemas actuais</b>	É identificada a forma como o sistema de informação suporta actualmente a organização.
<b>Determinando a perspectiva dos executivos</b>	As entrevistas aos executivos comprometem os intervenientes com as funcionalidades futuras do sistema
<b>Definindo resultados e conclusões</b>	Os problemas são classificados em categorias
<b>Definindo a arquitectura da informação</b>	São definidas as prioridades de desenvolvimento baseada no potencial financeiro e não financeiro, na possibilidade de sucesso, e a necessidade desse serviço para a organização
<b>Reverendo a gestão de recursos de informação</b>	A equipa avalia as potencialidades e fraquezas do sistema actual
<b>Desenvolvendo recomendações e plano de acção</b>	É preparado um plano de acção com recomendações sobre o hardware, software, ajustes no sistema actual, e métodos para fortalecer a gestão de sistemas de informação
<b>Relatório com os resultados</b>	É elaborado um relatório com os resultados



A figura 4 estrutura os passos a serem executados e o objectivo associado.

O PSN coloca muita ênfase no envolvimento e comprometimento da gestão de topo. O patrocínio da gestão de topo é considerada como critica. A informação necessária deriva dos processos de negócio tendo como fraqueza o facto de consumir muito tempo, ter um custo elevado e não incluir uma metodologia para o desenho de software, sendo ainda necessário que a equipa de planeamento tenha um elevado grau de experiência em tecnologias de informação (Palanisamy 2005).

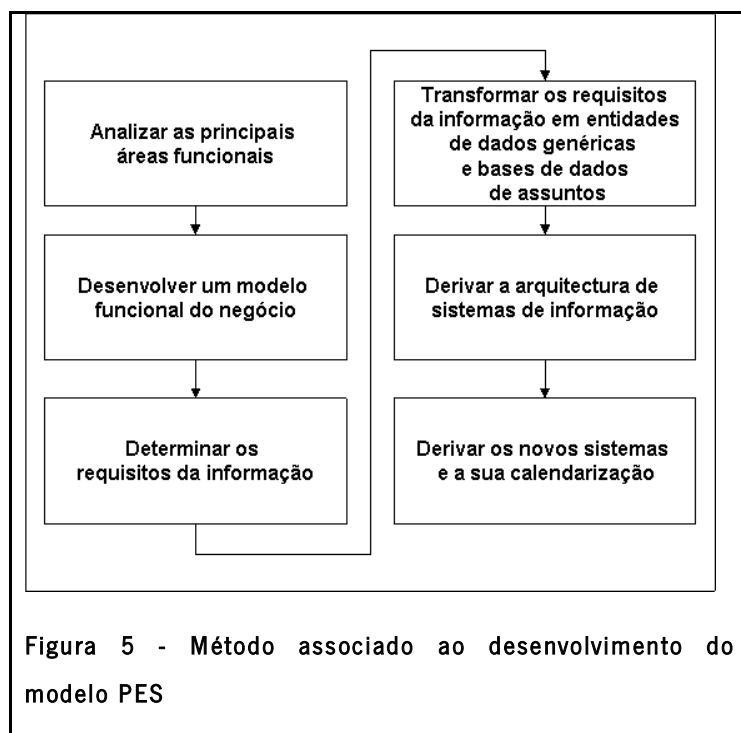
Apresenta como principal objectivo o alinhamento , tendo um enfoque nos dados e definindo a arquitectura dos mesmos.

## 2.5. PLANEAMENTO ESTRATÉGICO DE SISTEMAS (PES)

Foca-se nas áreas funcionais do negócio e na arquitectura dos dados. A arquitectura de dados é usada para identificar e desenhar novas aplicações.

Técnicas de pensamento estruturado são definidas como as resposta para todos os problemas de desenvolvimento. Desenvolvido por Robert Holland (Hsu 1995), define um modelo funcional de negócio através da análise das áreas funcionais maiores. Uma arquitectura de dados é derivada do modelo funcional do negócio, através da combinação dos efeitos de informação com entidades genéricas e bases de dados de assuntos. Uma arquitectura de sistemas de informação identifica de seguida novos sistemas e os seus calendários de implementação.

Embora a linguagem utilizada seja diferente do PSN os procedimentos são similares. A maior diferença é a capacidade automática de armazenar, manipular e apresentar as informações recolhidas durante o processo (Albert L. Lederer 1998).



A figura 5 apresenta a estrutura do método. É claramente identificado, como no PSN, que se trata de um método organizacional, com o objectivo de criar os sistemas adequados ao seu desenvolvimento funcional.

## 2.6. PLANEAMENTO DA ENGENHARIA DA INFORMAÇÃO (PEI)

Este modelo é mais orientado para os dados, fornecendo métodos para construção de dados empresariais, modelos de processos e bases de conhecimento. A base de conhecimento fornece as indicações para criar e manter os sistemas de informação. Desenvolvida por James Martin a engenharia da informação, no âmbito do presente contexto é definida como *“a aplicação de um conjunto de técnicas formais para o planeamento, análise, desenho e construção de sistemas de informação tendo por base a organização ou agrupando em sectores de organização”* (Martin 1989).

Este modelo adopta a abordagem apresentada na figura 6.



O desenvolvimento deste modelo assenta num método em quatro passos, conforme apresentado na tabela 5.

Passos	Preocupação
Planeamento estratégico dos sistemas de informação	Preocupado com os objectivos da gestão de topo e factores críticos de sucesso. Preocupado em como a tecnologia pode ser usada para criar novas oportunidades ou vantagens competitivas, é criada uma visão de alto nível da organização, as suas funções, dados e necessidades de informação
Análise da área de negócio	Preocupada com quais os processos a serem executados para suportar determinada área , e como esses processos ser relacionam, e qual a informação necessária
Desenho do sistema	Preocupado com como são implementados os procedimentos e como funcionam para os processos da área de negócio seleccionados.

<b>Construção</b>	Implementação de procedimentos usando geradores de código, quando prático, linguagens de quarta geração e outras ferramentas finais, sendo desejável a ligação à construção usando protótipos.
-------------------	--

Apesar do modelo conter uma metodologia bem estruturada, esta é bastante longa e o seu sucesso depende bastante do líder da equipa.

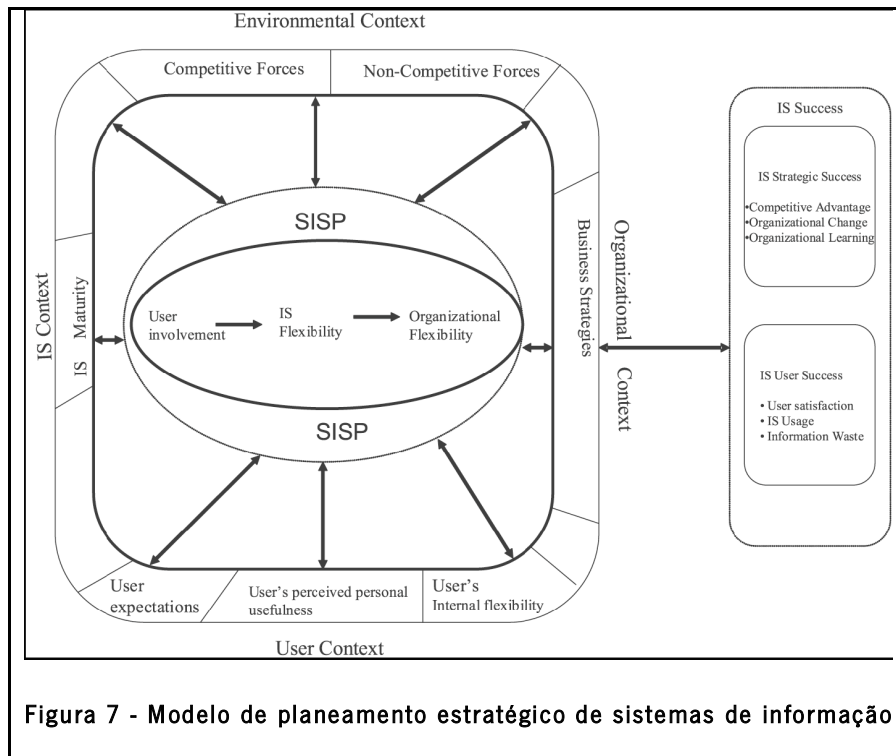
## **2.7. METHOD 1**

É um modelo cuja abordagem é baseada em níveis, tendo uma metodologia no nível de topo, técnicas no meio, e ferramentas suportando técnicas no nível inferior tendo sido desenvolvido pela empresa de consultoria, da área das tecnologias de informação, Andersen Consulting.

Apresenta como características fundamentais o facto de ser um modelo de alinhamento estratégico, com um enfoque nos projectos, não definindo contudo a arquitectura dos dados.

Esta abordagem pretende estruturar as diversas fases de desenvolvimento do projecto tendo também como objectivo gerir o desenvolvimento desse mesmo projecto, através da incorporação da relação entre trabalho e resultados.

## **2.8. PLANEAMENTO ESTRATEGICO DE SISTEMAS DE INFORMAÇÃO (PESI)**



O modelo sugere que a flexibilidade organizacional e sucesso, figura 7, devem ser as variáveis, sendo a flexibilidade do sistema de informação o “meio” para alcançar o sucesso dos sistemas de informação e flexibilidade organizacional. Este modelo assume variáveis de controlo baseadas num conjunto de conhecimentos e habilidades necessárias á organização. Dessa forma o modelo assume variáveis de controlo da tecnologia dos sistemas de informação, organizacional e do utilizador. A estratégia de negócio é considerada no contexto da organização, a maturidade do sistema de informação é considerada no contexto dos sistemas de informação, as expectativas do utilizador, a percepção de utilidade e a flexibilidade interna do utilizador é considerada no contexto do utilizador(Palanisamy 2005).

Este modelo parte dos seguintes elementos:

- envolvimento dos utilizadores no planeamento de sistemas de informação;
- flexibilidade dos sistema de informação;
- flexibilidade organizacional;
- sucesso do sistema de informação;
- satisfação do utilizador;
- utilização do sistema de informação;

- desperdício de informação;
- vantagem competitiva;
- alterações organizacionais;
- aprendizagem organizacional;
- expectativas do utilizador;
- percepção de utilidade por parte do utilizador;
- flexibilidade interna do utilizador;
- maturidade do sistema de informação;

Neste modelo o utilizar é parte activa de todo o processo.

## 2.9. LEARN

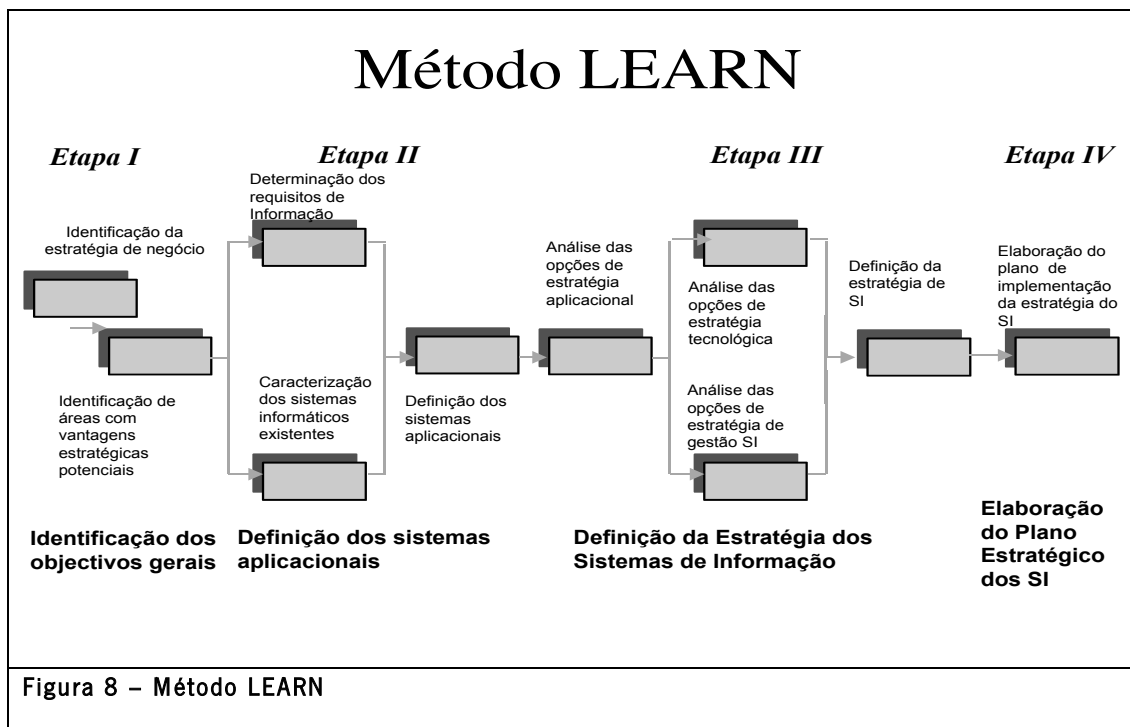
Este modelo usa uma abordagem baseada num método composto por um conjunto de passos e estruturas rígidas.

Assenta nos seguintes princípios (Joao Alvaro Carvalho 2005):

- os efeitos de informação não devem ser identificados nem definidos pelos utilizadores;
- os efeitos de informação devem ser identificados no contexto dos processos de negócio;
- os processos de negócio devem ser definidos numa perspectiva sistémica;
- os processos de negócio devem ser enquadrados numa arquitectura da empresa centrada nos processos;
- A implementação de aplicações informáticas deverá ser sempre enquadrada por projecto de mudança organizacional.

O modelo LEARN assenta numa abordagem integrada á organização, encontrando-se organizado segundo a estrutura apresentada no anexo A.

Esta abordagem aos sistemas de informação é substancialmente diferentes das abordagens tradicionais já que não estuda a organização para produzir um sistema alinhado com a estratégia de negócio, aborda antes os processos da organização e especifica as necessidades de informação, para depois dar inicio ao planeamento dos sistemas de informação.



Na figura 8, onde é apresentado o método para desenvolvimento do modelo, fica claro que o plano estratégico é a ultima fase e que a tecnologia de suporte é que define esse mesmo plano ou seja a solução tecnológica é central ao desenvolvimento do modelo.

Esta é uma das implementações que auxilia as abordagens BPM em arquitectura de processos. Esta abordagem por processos normalmente designada por BPM, surge como uma nova oportunidade para resolver problemas antigos das organizações, nomeadamente também no que respeita aos sistemas de informação.

Este modelo adopta uma abordagem estratégica e integrada ás organizações, proporcionando as condições para uma eficaz implementação da estratégia e garantindo um adequado alinhamento estratégico dos sistemas de informação. (Luís Amaral 2005)

O objectivo não é melhorar os processos em si mesmos com a ajuda ou não dos sistemas de informação.

## 2.10. CONCLUSÕES

Os modelos de planeamento de sistemas de informação descritos apresentam diversos tipos de abordagens aos sistemas de informação. O modelo da cadeia de valor, factores críticos de



sucesso, planeamento de processos de negocio, planeamento estratégico de sistemas, planeamento da engenharia da informação e planeamento estratégico de sistemas de informação focalizam a sua actividade no sistema de informação, não considerando a visão organizacional, sendo possível identificar uma tentativa de desenvolver métodos com objectivo de provocarem impacto com a adopção de tecnologias de informação. O Method 1 cobre todas as áreas mas não tem a flexibilidade adequada para os objectivos de conhecimento organizacionais específicos, dado que o factor humano na implementação será extremamente forte.

O modelo LEARN implementado pelo método LEARN, com a sua grande amplitude promove um comprometimento dos elementos envolvidos e pode garantir um modelo viável para planeamento de sistemas de informação. É de notar o facto de no modelo LEARN ser-se contra a intervenção do utilizador e no modelo PESI se advogar a intervenção activa do utilizador como elemento preponderante do sucesso.

São aqui caracterizadas duas visões, suportadas por diversos modelos cujos métodos associados têm por objectivo planear o sistema de informação de uma organização mas nada dizendo sobre a forma como essa mesma informação flui no ecossistema organizacional.

### 3. PARADIGMA DA COLABORAÇÃO

#### 3.1. CARACTERIZAÇÃO

O ambiente dos sistemas de informação, tem vindo a ser alvo, desde a sua génese, de desafios constantes. Desafios estes que assentaram, numa primeira abordagem, no suporte à automatização de processos, tendo de seguida evoluído para o suporte organizacional e depois para a criação de valor estratégico.

A sociedade moderna encontra-se assente sobre o pilar tecnológico e sobre o qual coloca uma pressão funcional e estrutural constante. As tecnologias e modelos de desenvolvimento de sistemas de informação existentes actualmente são a caracterização clara do processo evolutivo, suportado pelo desenvolvimento das tecnologias.

As tecnologias de informação disponibilizam hoje ferramentas e arquitecturas que permitem a criação simples de ecossistemas funcionais, onde a informação é disseminada e colocada à consideração de todos os interessados, para sobre ela reflectirem e desenvolverem algum tipo de actividade. Estamos a transformar-nos numa sociedade “*wikinomics*” (Tapscott 2007).

Esta sociedade, centrada em utilizadores em rede e plataformas colaborativas, é hoje para as organizações um desafio de utilização, no sentido em que cada organização tem “*às suas portas*” um elevado numero de potenciais colaboradores.

Estes potenciais colaboradores cresceram já na “*net-generation*” (Tapscott 2007), assumem a Internet como uma “*commodity*” sendo o e-mail já uma ferramenta do passado, centrando assim cada vez mais a comunicação no “*instant messaging*” e nas ferramentas de P2P.

Atrair novos colaboradores e a sua integração obriga as organizações a expor a sua estrutura de sistemas de informação a novos desafios. Agora, os sistemas de informação encontram-se integrados numa realidade externa que não controlam e da qual dependem. As empresas são levadas a integrar estes sistemas, que não foram definidos com a segurança, partilha ou colaboração como objectivo, nesta nova realidade colaborativa.

As organizações têm pois de mudar a forma como se relacionam com essa realidade. Acostumadas a definir políticas ao nível local, usando a máxima, “*think global act local*” (Anna H.

Perrault 2000) as empresas tentam agora conciliar regulamentos complexos que variam de país para país, centradas no pensamento "*think global act global*".

As redes colaborativas, quando possível a sua integração, permitem pegar no repositório institucional e partilhá-lo, de forma a que utilizadores motivados possam avaliar as possibilidades contidas na informação disponibilizada e aí acrescentar valor.

Estamos a usar a internet, não como um meio de publicação suportada pela WEB 1.0, mas como um meio computacional, a WEB 2.0. A internet transformou-se numa infra-estrutura passível de programação, criando o espaço para o desenvolvimento de novas aplicações, novos modelos de negócios e diferenciação competitiva.

Podemos notar que as organizações têm de mudar, e algumas delas já o fizeram, os seus conceitos de gestão de informação.

A informação tem de ser fornecida pela organização, não apenas aos seus colaboradores, mas também aos limites da organização para que seja possível motivar as redes de conhecimento que se encontram nos limites da organização.

Estas redes de conhecimento, quando transformadas em redes colaborativas, aumentam a forma como as organizações, pessoas e coisas podem interagir, usando como meio a internet.

Os departamentos tradicionais serão os guardiões de standards, como centro do treino e de especialistas, não serão os locais onde o trabalho será feito. O trabalho será essencialmente executado em grandes equipas especializadas(Drucker 2001).

O que as ferramentas da WEB 2.0 permitem é a integração de equipas distribuídas pelo mundo, de forma a que os departamentos das organizações serão tão só os gestores dessas mesmas equipas. Um dos exemplo embrionários desta nova colaboração foi o Lótus Notes, que nos princípios dos anos noventa apresentava ferramentas essencialmente de workflow, assentes num servidor aplicacional de e-mail, que adicionava novas formas de gestão aos processos dentro das organizações. Em 2005, com o advento do P2P, surgiam novas ferramentas que tornaram partilhável todo o tipo de informação, assim como fomentaram o desenvolvimento de redes de conhecimento.

Apesar desta necessidade de mudança, a competitividade continua no centro do objectivo das organizações. A colaboração exige pois uma correcta apreciação da estratégia, no contexto do negócio. Dado que é necessário pensar a estratégia, como num ecossistema, em que o

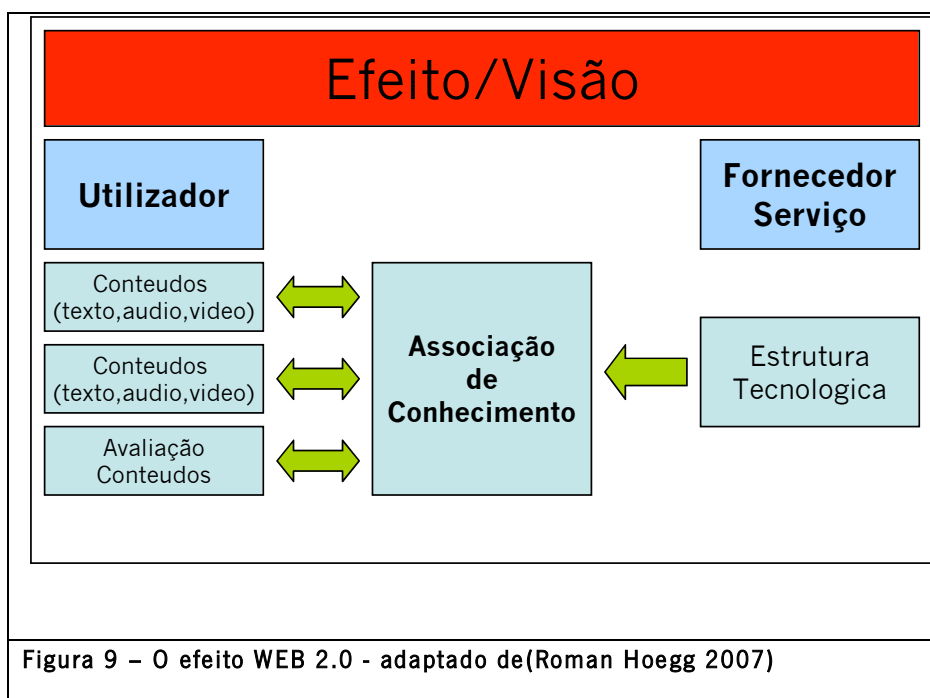
resultado não depende apenas das acções das organizações mas também dos seus competidores, é pois um sistema dinâmico com resultados não lineares.

É notório que a WEB 2.0, suportada numa internet com disponibilidade e características que permitem a integração de novos tipos de funcionalidades, tornando possível a implementação do novo paradigma colaborativo, mas esta colaboração exige algo completamente novo para as organizações, a abertura. Esta abertura é, de facto, o elemento mais importante do desenvolvimento actual das organizações.

Esta nova plataforma e as suas características são definidas de forma clara por aquele que é considerado o pai desta nova WEB, Tim O'Reilly. "*A WEB 2.0 não é uma tecnologia, mas sim o emergir de uma atitude colaborativa agregando tecnologia, atitude e filosofia*" (Reilly 2005) (Roman Hoegg 2007).

### 3.2. A WEB 2.0

A WEB 2.0, tem vindo a ganhar consistência tendo realmente efectuado o seu desenvolvimento após a conferencia de Tim O'Reilly sobre a Media Web, em 2004.



A arquitectura da WEB 2.0 pode ser representada de forma simples pelo modelo apresentado na figura 9. Daqui se pode perceber que se trata de uma filosofia e não uma tecnologia, tendo por

objectivo maximizar o conhecimento colectivo dos participantes. A WEB 2.0 é assim uma filosofia de maximização da inteligência colectiva e que adiciona valor por cada participante, através da partilha e criação de conhecimento, de forma informal (Roman Hoegg 2007).

Esta inteligência colectiva associa-se em comunidades e não se encontra associada a uma tecnologia inovadora e específica. Do ponto de vista técnico a WEB 2.0 é apenas uma combinação de protocolos e linguagens de computação combinadas de uma forma única.

As funcionalidades disponibilizadas, bem como as comunidades associadas, permitem a seguinte classificação ao nível funcional (Panada 2007):

- *Blogs e blogosphere;*
- *Wikis;*
- *Podcasts;*
- *Redes sociais;*
- *Social bookmarking e Folksonomies;*

Estas comunidades criam conhecimento de acordo com diversas áreas de interesse, podendo, quando correctamente integradas nas necessidades organizacionais, criar valor para a evolução e mudança (Mikroyannidis 2007).

Migramos definitivamente do conceito de uma internet, que suportava uma WEB de publicação, que podemos considerar de WEB 1.0, para uma estrutura dinâmica e colaborativa, a WEB 2.0 .

De acordo com Tim O'Reilly (Reilly 2005), "***A WEB 2.0 é a revolução de negócio na indústria dos computadores provocada pela mudança para a utilização da Internet como plataforma, e uma tentativa de compreender as regras para o sucesso nessa nova plataforma.***"

Esta plataforma suporta um conjunto de ferramentas de software que a caracterizam a WEB 2.0, conforme apresentado na figura 10.



Figura 10 – Exemplos de ferramentas da era da colaboração

Deste conjunto de aplicações, figura 10, bem como web sites que se encontram em plena fase de consolidação do conceito da WEB 2.0, a WIKIPEDIA, é talvez aquela que melhor traduz a potencialidade do paradigma colaborativo e as vantagens que advêm para as organizações, caso sejam capaz de o traduzir no seu desenvolvimento do negócio.

Outros exemplos de aplicações que obrigaram a indústria a repensar a sua interacção com o consumidor, são representadas pelo Napster e o pelo Bittorrent. Na área da comunicação tradicional, a voz, o Skype permitiu ao VOIP ter um rápido crescimento junto do utilizador, colocando pressão na sua utilização e desenvolvimento para utilização nas organizações.

O paradigma colaborativo e as ferramentas disponibilizadas, estão assim a criar condições para as organizações usufruírem de forças produtivas que não se encontram dentro das mesmas. Os limites das organizações são assim esbatidos.

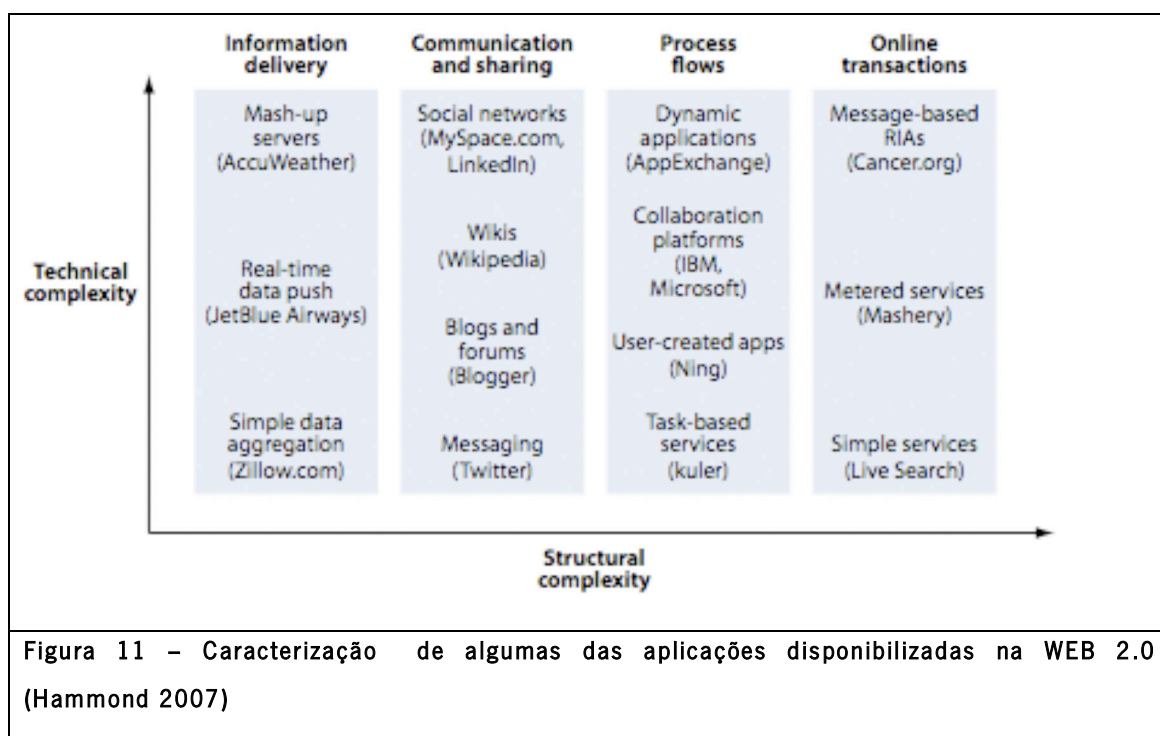
No entanto, desde que a WEB 2.0 foi apresentada por Tim O'Reilly, a forma como os intervenientes se relacionam com ela tem sido bastante irracional e deveras exuberante. Apesar disso, esta nova WEB pode acrescentar valor de três formas:

- a criação comunidades empenhadas, baseadas em computação social, que não procuram directamente valorização financeira;
- o acesso a conteúdos e dados expande as redes de inovação, que assentes em redes de conhecimento permitem pesquisas complexas de dados;
- o comprometimento efectivo como o elemento diferenciador para a competitividade, pelo que a informação da organização deverá ser segura.

De forma a conseguir acrescentar desta forma valor e realizar esta integração transparente das comunidades, a WEB 2.0 utiliza ferramentas tecnológicas assentes em:

- integração da informação focadas na disponibilização;
- computação social disponibilizando a comunicação e partilha;
- suporte aos fluxos de processos através de plataformas colaborativa.

A WEB 2.0, tem assim á sua disposição um conjunto de soluções cujo objectivo é otimizar e cativar os utilizadores para a colaboração.



No entanto esta diversidade de soluções apresenta também relações de complexidade estrutural e técnica bastante diversas, conforme apresentado na figura 11.

Mas as organizações devem ter a noção que a WEB 2.0 não é a panaceia para todas necessidades de desenvolvimento organizacional, dado que :

- a WEB 2.0 não está preparada para as aplicações mais complexas;
- a disponibilização dos serviços é uma proposição do tipo tudo ou nada;
- é difícil esconder processos e aplicações fracas.

Assim, a informação residente nos sistemas computacionais das organizações têm de ser exposta de forma a colmatar estas fragilidades.

Da mesma forma que não conseguem endereçar todas as necessidades organizacionais, e tendo sido desenvolvidas de forma a tornarem a experiência do utilizador o mais interessante possível, existem aspectos como a segurança, que não estão na linha da frente.

No entanto, a integração das organizações na WEB 2.0 tem de garantir os conceitos fundamentais da segurança da informação que são a confidencialidade, a disponibilidade e a integridade, ao longo de todo o fluxo da informação neste ecossistema.

É pois determinante que as organizações consigam integrar nestas redes de conhecimento a sua informação mas que o façam de forma adequada às necessidades organizacionais.

Neste novo desafio existem um conjunto de elementos, que têm de ser repensados como sejam os copyright, autoria, identidade, ética, gostos, retórica, gestão, privacidade, comércio, amor, família e no limite, nós mesmos.

### **3.3. CONCLUSÕES**

As mudanças criam oportunidades e a mudança para o paradigma colaborativo, centrado no modelo de desenvolvimento da WEB 2.0, trará um desenvolvimento sustentado e disruptivo do negócio, alterando a forma e técnica de relacionamento entre todas as formas de interação organizacional.

As organizações que consigam criar valor com esta integração serão capazes de atrair comunidades de conhecimento vibrantes e entusiastas, acelerando a inovação. Estas organizações terão assim condições para ganharem a corrida da WEB 2.0 organizacional.

As máquinas passam a ser os indivíduos, o texto digital e o “*hypertext*” deixaram de ser apenas informação associada. A WEB 2.0 não associa apenas informação, associa pessoas nas relações pessoais, nos negócios e na colaboração.



### 4. A SEGURANÇA DE INFORMAÇÃO

#### 4.1. CARACTERIZAÇÃO

A WEB 2.0, a ser implementada amanhã, apresenta diversos problemas de segurança hoje. Esta poderia ser um frase estritamente comercial para um problema demasiadamente complexo, que é a segurança da informação. No entanto, ela traduz na integra aquilo que os sistemas de informação têm como desafio estrutural e funcional.

Sendo claro que as organizações só poderão integrar o paradigma colaborativo se o fizerem de forma segura, a segurança é um elemento completamente transversal ao desenvolvimento deste novo ecossistema colaborativo.

Apesar da segurança da informação ser tema recorrente na abordagem aos sistemas de informação, é fundamental efectuar uma contextualização do problema da segurança e a sua caracterização, sendo usada como fonte principal o relatório de 2007 do Computer Security Institute (CSI), unidade do governo norte americano responsável pela análise e caracterização do crime e segurança de sistemas de informação(CSI 2007).

No relatório do CSI de 2007 fica claro que a segurança é um dos elementos do sistema de informação das organizações em que o investimento é constante. Sendo também patente o valor dos investimentos que os gestores de informação e tecnologia atribuem á segurança, tendo subido de forma assinalável nos valores intermédios de investimento, de 3 e 5%.

É perceptível que a segurança continua a ser considerada uma questão tecnológica. No entanto, a manter-se esta perspectiva não irá ser possível a protecção das organizações colaborativas, dado que estas se centram no utilizador. E este utilizador interage com a informação de uma forma completamente ubíqua.

A incapacidade das organizações gerirem a segurança é associada frequentemente á inexistência de mão de obra que tenha reais qualificações para efectuar essa gestão, devido á falta de especialistas nessa área. De forma a colmatar essa dificuldade aponta-se o *outsourcing* das soluções tecnologias a organizações especializadas, fazendo a segurança parte desse pacote, como uma das abordagens(CSI 2007) .

No entanto as organizações continuam a considerar que tal tarefa deve ser executada por pessoal da organização. Assim sendo, as organizações têm de conseguir garantir a formação complementar dos seus funcionários, ou contratar especialistas, que lhe permitam manter segura a sua informação.

A segurança da informação pode ser analisada, usando uma métrica simples, podemos por exemplo considerar, o numero de ataques identificados. No que respeita aos meios de ataque, são identificáveis um conjunto de indicadores que determinam as características da segurança:

- 59 % dos ataques são efectuados do interior, centrados no utilizador;
- 52% devem-se a vírus (muito embora não se identifica a origem do vírus, de uma forma geral admite-se que a Internet é a sua origem mais frequente);
- 50% foram o roubo de equipamentos portáteis, centrados no utilizador;
- 26% devem-se a *phishing*, centrados no utilizador;
- 25% ficaram a dever-se á má utilização das mensagens instantâneas, centrados no utilizador

Apesar do centro da preocupação ser a segurança e os investimentos associados estarem orientados para as tecnologias, verifica-se, conforme apresentado em cada um dos pontos anteriores, que os riscos têm um denominador comum, o utilizador, que parece não ser objecto da devida atenção. Não estamos a falar dos utilizadores externos da organizações mas os que se encontram integrados na própria organização. É pois então possível verificar que a segurança deverá acrescentar ao seu âmbito de análise o âmbito do comportamento humano, e na forma como o mesmo interage com o seu ecossistema informacional.

Característico é também o aumento do numero de casos em que é desconhecido o número de ataques, podendo aqui mais uma vez estar presente o desconhecimento de métodos de análise de segurança, ou o facto das organizações protegerem essa informação pelas mais diversas razões. Mais um vez não deixa de ser importante que o investimento em segurança aumenta mas o conhecimento do estado da segurança diminui, aparecendo ainda a fraude no topo da lista, enquanto que as alterações dos WEB sites aparecem num lugar do fundo da lista.

Se numa primeira fase a exploração de vulnerabilidades passava por uma auto valorização, as organizações sentem agora que o objectivo é a fraude. Esta fraude tem-se materializado, por exemplo, na utilização de *pop-up boxes* com código maléfico assim como de *phishing*, que tem

sido o mais mediático. No entanto, as vulnerabilidades introduzidas pelos vírus continuam no topo da lista no valor das perdas, e o roubo de identidades nas suas mais diversas vertentes têm assumido a liderança. Torna-se necessário mais uma vez enfatizar que o vírus é o problema que mais atenção tem tido por parte das políticas de segurança, no entanto o valor associado, relativo a perdas, aumenta anualmente.

Apesar do investimento, não existe um decréscimo assinalável nas ocorrências de incidentes de segurança, e o investimento tem-se centrado essencialmente soluções de antivírus, firewalls, VPN e anti-spyware. O investimento de segurança continua a ser efectuado no perímetro e como este perímetro está cada vez mais amplo e mais difícil de definir, essas soluções revelam cada vez mais as suas fragilidades na protecção segura da informação.

Tecnologias como o NAC, que poderiam proteger os acessos dentro da infra-estrutura da organização, onde ocorrem os maiores danos, são relegadas para os últimos lugares da lista de investimento e inclusive sofrem um desinvestimento.

A normalização tem sido também defendida como uma das formas de aumentar a segurança. Pode-se constatar que 25%(CSI 2007) dos que responderam discordam em absoluto, que a normalização aumenta a segurança. Este valor é mais do dobro dos que concordam plenamente, o que faz acreditar que os responsáveis pelas organizações quando implementam a norma, a implementam com o objectivo de obedecer às regras de normalização e não para efectivamente obterem uma mais valia para a segurança.

A normalização é também apresentada como o elemento capaz de potenciar a gestão tecnológica das organizações, traduzida na palavra inglesa *governance* ou *e-governance*, conforme o contexto em que a mesma seja implementada. No entanto o número de inquiridos que discordam em completo com o facto de que a normas, tomando como exemplo a Sarbanes-Oxley, aumenta o *governance*, é três vezes superior ao daqueles que concordam plenamente.

Assim sendo, a normalização, pelo menos a norma analisada e neste momento a mais significativa, e sobre a qual se tem escrito bastante, não se afigura capaz de gerir a integração da segurança nos moldes que ela deve hoje assumir.

Este relatório traduz o estado da arte na segurança da informação e identifica os caminhos que estão a ser seguidos para dotar as organizações de segurança da informação. Mas enquanto diversos problemas do passado se mantêm, como os vírus e a compreensão de que segurança é

tecnologia, as necessidades de informação das organizações evoluem e aos seus sistemas de informação exige-se que se adequem a novas realidades.

## **4.2. IMPACTO DA WEB 2.0**

Aos problemas actuais do desenvolvimento da segurança dos sistemas de informação acresce agora o desenvolvimento e integração da WEB 2.0, que, no limite, pode levar á eliminação do perímetro colaborativo traduzido na passagem de sistemas de informação para ecossistema de informação.

A integração da WEB 2.0, assente em comunidades de conhecimento, nos sistemas actuais, de forma a criar um ecossistema organizacional, agrava a segurança da informação. A WEB 2.0 usa ferramentas que têm por objectivo a facilidade de utilização, sendo muitas vezes uma agregação de diversas soluções e devido ao contexto em que são desenvolvidas padecem dos mesmos problemas das soluções desenvolvidas actualmente, que promovem a funcionalidade em detrimento da segurança.

Assim, a segurança deste novo perímetro da organização, traduzido no seu ecossistema, enfrenta problemas que podem por em causa o desenvolvimento das próprias sociedades. Pode ser apresentado como exemplo, os ataques que exploram o XSS, através da injeção de código malicioso e a sua execução no WEB browser dos outros utilizadores.

A internet continua a ser saturada e ameaçada através de blogs e aplicações de e-mail. Os ataques de DoS, SPAM e explorações de bugs nos browser e nas mais diversas aplicações, continuam a ser possíveis.

Na tabela 6 são apresentados dois exemplos de ataques a dois dos sites actualmente mais representativos da WEB 2.0, demonstrando assim a sua vulnerabilidade e insegurança.

<b>Tabela 6 – Dois exemplos de ataques á era WEB 2.0</b>	
<b>Yamanner</b>	<b>Samy&amp;Spaceflash</b>
tem como objectivo o e-mail do Yahoo  associa código malicioso javascript a um tag de imagem standard do HTML  o utilizador não tem de efectuar um click em qualquer tipo de anexo para ficar infectado  auto-propaga-se enquanto obtém os endereços de e-mail	objectivo o Myspace

Na tabela 7 são apresentadas explorações de vulnerabilidades de um dos sites mais populares e de que forma isso é conseguido.

<b>Tabela 7 – Características do MySpace e exploração de vulnerabilidades</b>	
<b>Myspace</b>	<b>Samy, Spaceflash</b>
o sexto WEB site em lingua inglesa mais popular do mundo	Alterado o perfil do utilizador de forma a adicionar o autor como amigo
o sexto WEB site mais popular em qualquer linguagem	redireccionamento para um URL com um ficheiro Macromedia flash com código malicioso
o terceiro mais popular WEB site nos Estados Unidos	Ficheiros Quicktime maliciosos alteram o perfil do utilizador de forma a auxiliarem o phishing

Sendo a WEB 2.0 o paradigma colaborativo assente no individuo, atingir o utilizador e descobrir o caminho de acesso á informação existente no ecossistema, desde o seu interior, passou a ser o objectivo (CIOInsight 2007; Insight 2007), o que fica claro nas tabelas 6 e 7.

A exploração das vulnerabilidades de segurança aparece assim, não direccionada aos sistemas que suportam o ecossistema, mas sim aos utilizadores desse mesmo ecossistema, que depois de comprometidos, ou melhor, os seus recursos computacionais comprometidos, permitem aceder ao ecossistema desde o seu interior. Este acesso do interior é sempre mais permeável á utilização de outras formas de ataque e com um potencial destrutivo muito superior, quando comparado com os ataques efectuados do exterior.

Fica também claro, que existe uma exploração tradicional de vulnerabilidades, e estas são exploradas de acordo com a visibilidade do elemento a comprometer, o que na WEB 2.0 pode

ser medida pelo numero de utilizadores. Como qualquer ferramenta, as soluções da WEB 2.0 apresentam diversas vulnerabilidades, que neste caso afectam o utilizador, das quais algumas são apresentadas na tabela 8, revelando a relação entre vulnerabilidade e consequências da exploração dessa mesma vulnerabilidade.

<b>Tabela 8 – Vulnerabilidades e forma de ataque associadas</b>	
<b>Vulnerabilidade</b>	<b>Consequências</b>
cross-site scripting usando AJAX e XML	o AJAX é executado do lado do cliente permitindo o comprometimento através de um script escrito de forma maliciosa
envenenamento por XML	pode levar a um DoS ou quebra de lógica funcional
execução maliciosa de código AJAX usando XMLHttpRequest	os cookies podem levar a uma perda de informação confidencial
RSS/Atom Injection (baseado no XML 1.0)	injecção de javascript em feeds de forma a permitir ataques usando o browser do cliente
enumeração e pesquisa WSDL	a definição da linguagem de web services pode ter abertas funções ou métodos desnecessários  este ficheiro fornece informação chave sobre os serviços, protocolos, portas, funções e métodos expostos, padrões de execução, etc
validação de rotinas de AJAX do lado do cliente	é possível efectuar um bypass às validações e efectuar novos pedidos á aplicação (i.e. SQL Injection, LDAP Injection, etc...)
problemas de routing nos WEB services	se os nós de routing forem comprometidos o acesso às mensagens de SOAP pode ser possível
manipulação de parâmetros usando SOAP	os serviços usam variáveis que podem ser manipuladas
XPATH injection numa mensagem SOAP	XPATH é uma linguagem para efectuar perguntas a documentos XML sendo frequente as aplicações aceitarem inputs que podem levar á injection
manipulação binária do cliente RIA thick client (usando reverse engineering)	O RIA usa funcionalidade UI tais como flash, controlos activex ou applets como interface primário para as aplicações web o que pode conduzir a problemas de segurança

Estas vulnerabilidades são introduzidas pela utilização de tecnologias da plataforma WEB 2.0. No entanto os sistemas tradicionais mantêm as suas vulnerabilidades, também críticas, às quais a utilização de tecnologias como o AJAX vem trazer uma nova dimensão.

O refinamento das tecnologias e metodologias cria condições para a melhoria das técnicas de ataque. Por exemplo, o Javascript permite ao atacante enviar determinada informação através da rede, que resulta na escrita pelo browser de algo completamente diferente na página, isto é tudo executado através do browser, que depois de infectado não necessita de ligação á rede para a execução do código, ou seja, este script pode ser instalado no browser.

Explorando estas novas características funcionais aparecem um conjunto de aplicações maliciosas que as exploram. O JITKO é o exemplo de uma dessas aplicações. Aparecendo como uma aplicação para pesquisa de vulnerabilidades WEB pode ser integrado no site do atacante, ou injectado em sites de confiança. Pode descobrir diversos buracos comuns de segurança e ligar-se ao seu controlador remoto para obter instruções sobre quais os WEB sites a atacar e quais as variáveis a procurar. Um exemplo de pesquisa de vulnerabilidades usando o JITKO, é apresentado na tabela 9.

Tabela 9 – Exemplo de funcionamento do JITKO	
Exemplo	Resultado
<pre> var encodedText = "dW5lc2NhcGUoliV1OTA5MCV1OTA5MCIp..."; var decodedText = decode(encodedText); document.write(decodedText); decode(input) { ... } </pre>	<pre> var shellcode = unescape("%uyadd%uayad%udaya%uddaa"); var          nop_sled          = unescape("%u9090%u9090"); while(nop_sled.length &lt;= 40000) nop_sled += nop_sled; var myArray = new Array(); for(var i=0; i&lt;300; i++) myArray[i] = nop_sled+shellcode; </pre>

À integração dos sistemas tradicionais neste novo paradigma acresce uma outra vertente, a exploração dos documentos compostos, ou seja documentos standard conhecidos por serem

gerados por aplicações ERP ou outras e que usam nomes standard para os relatórios, foram transformados no melhor ataque estruturado visto até á data, estando a ser usados tanto nomes de relatórios actuais e válidos bem como a utilização de endereços de e-mail obtidos de forma não autorizada(Panada 2007).

Quando surgem problemas com aplicações que são completamente transversais, dado o seu nível de utilização, temos um problema difícil de abordar , afectando virtualmente, todos os WEB sites do mundo.

Como por exemplo, refira-se a vulnerabilidade do software Adobe Reader a um ataque usando XSS, no qual, ao fornecer um link para um pdf local, permite a execução de um javascript, na zona local. Este ataque surpreende na sua simplicidade assentando no seguinte formato:

***http://www.xzy.com/whatup.pdf#javascript:alert('test');***

Na tabela 10 são apresentadas algumas das aplicações, as mais populares em 2007, disponíveis para a WEB 2.0 e algumas das suas vulnerabilidades.

Tabela 10 - Lista das aplicações mais comuns de 2007 e suas vulnerabilidades				
Software	Versão	Solução do Fornecedor	Natureza das vulnerabilidades	ID CVE
Yahoo! Messenger	8.1.0.239 e posteriores	Actualização para 8.1.0.419	Buffer overflow permite aos ataques remotos executar código arbitrário através de vectores não especificados.	<a href="#">CVE-2007-4515</a> <a href="#">CVE-2007-4391</a> <a href="#">CVE-2007-3148</a> <a href="#">CVE-2007-3147</a> <a href="#">CVE-2007-1680</a>
Apple QuickTime	7.2	Correcção	Diversas vulnerabilidades permitem aos ataques remotos a execução de comandos arbitrários e codificar URL e applets Java	<a href="#">CVE-2007-4673</a> <a href="#">CVE-2007-2397</a> <a href="#">CVE-2007-2396</a>



				<a href="#">CVE-2007-2393</a>
Mozilla Firefox	2.0.0.6	Actualização para 2.0.0.7 para algumas correcções	Permite aos ataques remotos executar comandos arbitrários através de codificações especiais de URIs.	<a href="#">CVE-2007-5045</a> <a href="#">CVE-2007-4841</a> <a href="#">CVE-2007-3845</a>
Microsoft Windows Live (MSN) Messenger	7.0, 8.0	Actualização para 7.0.0820 ou 8.1	Heap-based buffer overflow permite aos ataques remotos assistidos pelos utilizadores executar código arbitrário usando vectores não especificados envolvendo a conversação vídeo geridas em sessões de Web Cam.	<a href="#">CVE-2007-4579</a> <a href="#">CVE-2007-2931</a>
EMC Vmware Player (e outros produtos)	2.0, 1.0.4	Actualização para 2.0.1 ou 1.0.5	Permite aos atacantes remotos a execução de código arbitrário através de um pacote DHCP mal formado que active um stack-based buffer overflow ou corrompa uma stack memory.	<a href="#">CVE-2007-0063</a> <a href="#">CVE-2007-0062</a> <a href="#">CVE-2007-0061</a>
Apple iTunes	7.3.2	Actualização para 7.4	Buffer overflow permite aos ataques remotos terminar a aplicação ou executar código arbitrário usando um ficheiro de musica com alterações ao nível da arte da capa	<a href="#">CVE-2007-3752</a>
Intuit QuickBooks Online Edition	9 e posterior	Actualização para 10 ou correcção	Múltiplos stack-based buffer overflows no controlo ActiveX permite aos atacantes remotos executar código arbitrário via vectores não especificados	<a href="#">CVE-2007-4471</a> <a href="#">CVE-2007-0322</a>
Sun Java Runtime Environment (JRE)	1.6.0_X	Não disponível	O Buffer overflow no Java Web Start permite aos atacantes remotos ter um impacto desconhecido através do uso de chamadas de argumentos dentro de um método.	<a href="#">CVE-2007-5019</a>
Yahoo! Widgets	4.0.5 e anteriores	Actualização	Stack-based buffer overflow permite aos atacantes executar código arbitrário através da de argumento inesperados na chamada de um método	<a href="#">CVE-2007-4034</a>

Ask.com Toolbar	4.0.2.53 e anteriores	Não disponível	Stack-based buffer overflow no controlo ActiveX e Ask Toolbar permite aos atacantes remotos executar código remoto	<a href="#">CVE-2007-5107</a>
Broadcom wireless device driver conforme usado no Cisco Linksys WPC300N Wireless-N	3.50.21.10	Actualização do driver	Stack-based buffer overflow permite aos atacantes executar código arbitrário num frame de resposta do 802.11 contendo um longo campo SSID	<a href="#">CVE-2006-5882</a>
Macrovision (formalmente InstallShield) InstallFromTheWeb	Unversioned	Não suportado	Multiple buffer overflows permite aos atacantes a execução de código arbitrário usando documentos HTML	<a href="#">CVE-2007-0320</a>

Fica visível na tabela 10, que as vulnerabilidades afectam diversas soluções de software, e têm um desenvolvimento contínuo. A segurança de um ecossistema deverá assim assumir-se como um processo dinâmico, incluindo a possibilidade de continuamente rever, reformular e modificar todos os aspectos do modelo do ecossistema, de forma a tratar as necessidades de segurança (CSI 2007).

### 4.3. CONCLUSÕES

Existe uma clara orientação para uma cultura de segurança centrada na tecnologia e não nos utilizadores. A complexidade tecnológica aumenta diariamente e a convergência dos diversos mundos, como sejam o fixo – móvel, fundamento da computação ubíqua, são um bom exemplo.

No entanto as organizações estão a reformatar as suas aplicações para uma arquitectura orientada aos serviços, suportados na WEB 2.0, tentando criar vantagens competitivas, mas criando simultaneamente um pântano de novas vulnerabilidades, bastante difícil de controlar (CSI 2007).

No passado, a luta tem sido entre os profissionais de IT e os criminosos que atacam as suas redes, tendo por denominador comum a tecnologia. O problema na WEB 2.0 é mais grave, dado que os atacantes centram as suas atenções nos utilizadores. Limitando-se a segurança da

informação ao status quo das *firewalls* e anti-virus, irá assistir-se a uma corrosão da segurança das organizações.

A tarefa de criação de um ecossistema de informação para gerir o fluxo da informação, que se traduza na construção de um ecossistema colaborativo dentro da organização, é uma tarefa complexa. Gerir a segurança dessa mesma informação faz elevar ainda mais a complexidade.

A normalização, apresentada frequentemente como a panaceia e, nomeadamente, a lei Sarbanes-Oxley, não é vista como estando a endereçar o planeamento da segurança dos sistemas de informação.

Apesar da segurança ser um problema na mente de todos os intervenientes no processo de criação do ecossistema, a clara aposta de investimento em tecnologia tem-se mostrado perfeitamente incompleta, ainda mais agora com o pressuposto da colaboração e eliminação das barreiras das organizações.

Esta eliminação das barreiras vem trazer aos três pilares da segurança da informação (confidencialidade, integridade e disponibilidade) uma dimensão humana, cujo envolvimento é desejável, mas cujo controlo, se possível, ameaça tornar-se disfuncional. Ecossistemas integrados levam a problemas integrados, que se propagam de camada em camada exigindo um conhecimento completo do fluxo de informação no ecossistema.

Garantir pois, os três pilares da segurança numa organização esbatida, confrontada com desenvolvimentos cada vez mais rápidos e crescentes pirâmides de funcionalidades, é o desafio dos novos ecossistemas de informação.

Alguns números ajudam a perceber a dimensão desta plataforma colaborativa e em face das vulnerabilidades apresentadas na tabela 10 perceber a dimensão do problema:

- 74% dos CIO consideram que a WEB 2.0 acrescenta insegurança (CIO 2006);
- 67,000 é o numero de entradas de *blogs* em cada hora (Technorati 2006);
- 12% é o numero de consumidores on-line norte americanos que usam RSS (Juniper 2006);
- 12 Milhões é o numero de subscrições de *podcasts* (Forrester 2006);
- 52.4 Milhões foi o numero de *podcasts* identificados em Agosto de 2006 (Technorati 2006).

A segurança não deve ser algo que inibe a inovação mas sim uma base que suporta a inovação sustentada.

### 5. MODELO PROPOSTO

Com o advento da tecnologia como elemento integrante das organizações e com a possibilidade de facilmente serem adquiridos pequenos sistemas, com o mesmo nível de funcionalidades dos grandes sistemas, mas com custos substancialmente mais baixos, bem como com a disponibilização de sistemas operativos com maior facilidade de utilização, o argumento de que a tecnologia era um elemento diferenciador caiu por terra.

Torna-se pois imperioso reformular a forma como a organização se relaciona com a tecnologia, não o que pode a tecnologia fazer pelas organização, mas que tecnologia precisa para implementar o desenvolvimento organizacional, quais os efeitos pretendidos pela organização ao utilizar os elementos de informação.

Com a reformulação do paradigma da tecnologia para a colaboração e existindo diversos modelos de planeamento de sistemas de informação, conforme apresentado no Capítulo 2, estes não constituem uma ferramenta que permita uma visão global da informação, capaz de cobrir todo o seu ciclo de vida, incorporando a segurança em todo o fluxo informacional, ou seja, tornando visíveis as interações com a informação efectuadas pelo ecossistema. A segurança do fluxo da informação do ecossistema não pode ser analisada com uma metodologia própria, deve sim ser considerada como características da informação, que deverá tentar garantir a outra característica da informação, o efeito.

A utilização destas duas características da informação, a segurança e o efeito, obriga á definição de um modelo de planeamento que trate o fluxo de vida da informação no ecossistema organizacional.

Pretende-se com este modelo desenvolver uma abordagem de planeamento, que possibilitando a integração dos modelos tradicionais na concepção dos sistemas, possa desenvolver a concepção do fluxo da informação, garantindo a obtenção da relação informação -> efeito.

O modelo desenvolvido assenta na noção de efeito da informação, conceito desenvolvido na guerra da informação. De forma a ser possível caracterizar o papel do efeito no ecossistema, foram integradas no modelo duas variáveis adicionais, a interdependência e a priorização.

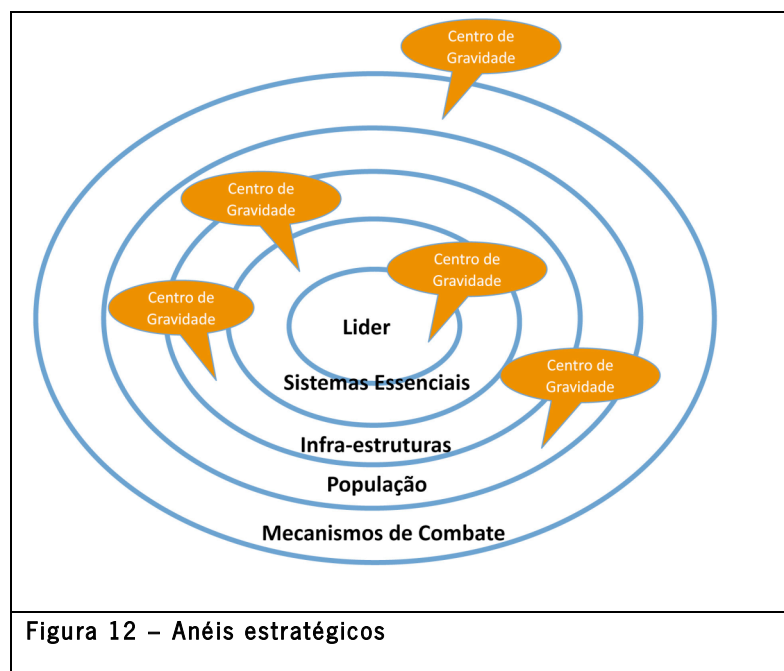
Estando os limites da organização completamente esbatidos, torna-se fundamental que a segurança da informação não seja apenas uma implementação tecnologia no perímetro, mas sim algo que faz parte da informação. Ao ser integrado como característica da informação, esta pode e deverá mudar ao longo do ciclo de vida da mesma. O controlo de segurança mais comum é o controlo de acessos, que é estático ao longo de todo o ciclo de vida da organização, em que cada utilizador tem um conjunto de privilégios que lhe permitem aceder aos dados. Isto controla a disponibilização da informação e não o seu fluxo, e uma vez essa informação libertada pela autenticação, pode ser comprometida.

No desenvolvimento actual da WEB 2.0, este controlo de acessos é manifestamente insuficiente e não fornecem mecanismos confiáveis de protecção dos sistemas de computação.

O ecossistema organizacional tem de ser correctamente caracterizado de forma a garantir o patamar da colaboração e o desejável grau de confiança no fluxo da informação.

## 5.1. PLANEAMENTO ORIENTADO AOS EFEITOS

O modelo assenta na construção de cinco anéis estratégicos caracterizados de acordo com a organização apresentada na figura 12.



Cada um dos anéis estratégicos pode ser caracterizado da seguinte forma:

- **Líder:** é o recurso disponibilizado para a obtenção de determinado tipo de efeito;
- **Sistemas essenciais:** são os elementos necessários para que determinado efeito se possa desenrolar;
- **Infra-estruturas:** são o conjunto de elementos físicos que permitem o funcionamento dos sistemas essenciais;
- **População:** é o conjunto de todas as entidades que podem ser alvo do efeito ou que podem interagir com o mesmo;
- **Mecanismos de combate:** são o conjunto de elementos que podem garantir que determinado efeito será executado sem ser comprometido.

No ecossistema de informação e quando comparado com outras formas de organização, podem ser identificados os elementos de acordo com a tabela 11.

<b>Tabela 11 – Definição comparativa dos anéis estratégicos de um ecossistema de informação</b>			
<b>Anéis estratégicos</b>	<b>Individuo</b>	<b>Organizações</b>	<b>Ecossistema de Informação</b>
<b>Líder</b>	Cérebro	Conselhos de administração	Informação
<b>Sistemas essenciais</b>	Olhos, coração, pulmões	Área financeira, recursos humanos, sistemas produtivos	Protocolos
<b>Infra-estruturas</b>	Vasos sanguíneos	Sistemas produtivos	Hardware, Software, Sistemas de comunicação
<b>População</b>	Células	Mercados	Equipamentos periféricos
<b>Mecanismos de combate</b>	Sistema imunitário	Sistemas de regulação	Modelos de planeamento de sistemas de informação

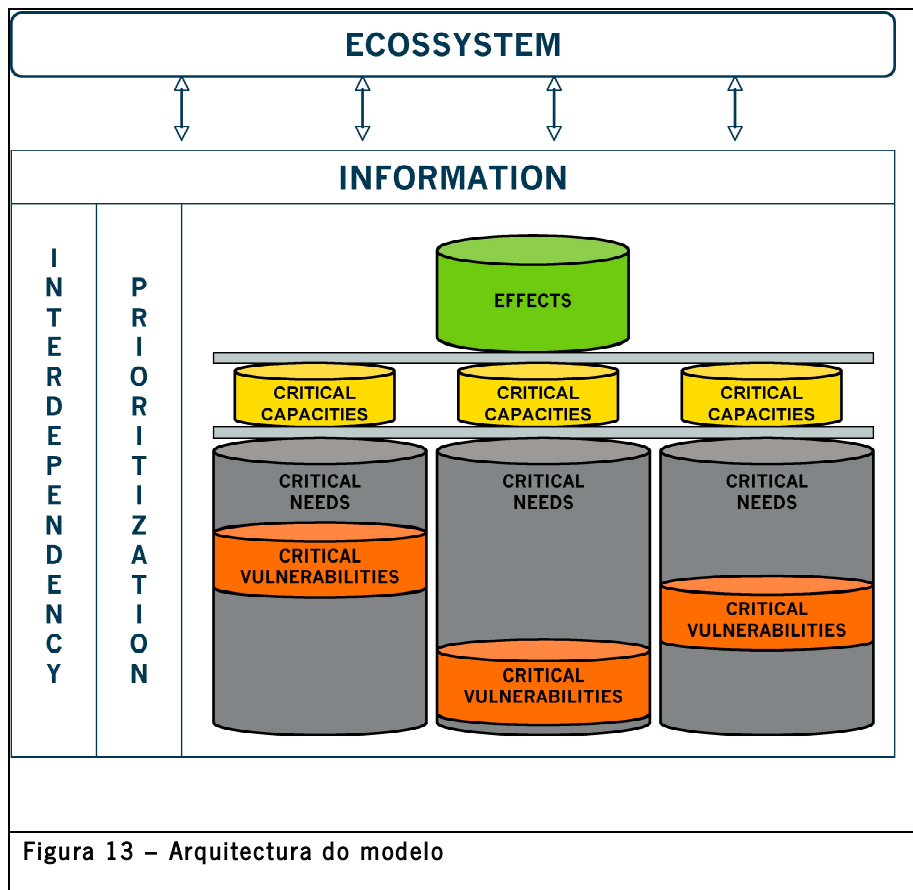
Cada anel é desenvolvido tendo por base a análise de três elementos, de forma a permitir identificar as necessidades associadas á obtenção do efeito.

Assim temos:

- **Capacidades Críticas (CC):** como sendo as capacidades fundamentais associadas a determinado efeito;

- **Necessidades Críticas (NC):** são os recursos que permitem a realização das capacidades;
- **Vulnerabilidades Críticas (VC):** são as vulnerabilidades intrínsecas aos próprios recursos;

A arquitectura obtida é definida na figura 13.



A figura 13, ilustra de forma clara os elementos que suportam a disponibilização da informação assente em efeitos. A segurança, que permitirá garantir a correcta obtenção do efeito pretendido encontra-se integrada nas necessidades críticas, identificadas para cada efeito. A implementação de cada elemento de suporte ao efeito e o próprio efeito em si, é mais ou menos relevante e depende ou não de outros elementos do ecossistema. Assim a prioritização e a interdependência surgem integradas de uma forma transversal abarcando todos os elementos que permitem o desenvolvimento do efeito.



## 5.2. CARACTERIZAÇÃO DOS EFEITOS

A orientação aos efeitos não é um conceito novo. O que é novo, é a forma como se estende este conceito ao desenvolvimento sustentável de uma arquitectura de ecossistemas, onde o desenvolvimento de cada um depende fortemente da interacção em rede, caracterizada pelo ecossistema informacional, permitindo desta forma um salto qualitativo, de uma estratégia centrada no suporte operacional para uma estratégia suportada em ecossistema.

É difícil escolher uma única definição para esta abordagem, devido à origem desta temática, essencialmente de origem militar e centrada na forma de fazer a “guerra”. A definição base de modelo orientado para os efeitos foi apresentada em (Vicente 2007), como sendo: ***“o conjunto de acções coordenadas que procuram condicionar o estado de um sistema através da aplicação integrada de instrumentos de poder, de forma transversal ao espectro do efeito, considerando os efeitos das acções na conquista dos objectivos. As acções são planeadas, executadas, avaliadas e adaptadas utilizando um conhecimento holístico do problema e do espaço em que o mesmo se desenvolve, orientadas para condicionar os comportamentos dos intervenientes”***.

Pode assim considerar-se que o planeamento deve efectuar uma análise transversal do ecossistema, percebendo capacidades ou fontes de poder, vulnerabilidades e fraquezas, fazendo emergir os nós vulneráveis assim como as formas ideais de aplicação de acções, tendentes a alterar o comportamento do efeito.

Os efeitos referem-se assim ***“a uma gama de resultados, eventos, ou consequências de acções, que podem advir de qualquer instrumento. Os efeitos são uma consequência cumulativa transversal ao ambiente estratégico de uma ou mais acções”*** (Vicente 2007).

Com maior detalhe e para melhorar a compreensão, importa distinguir os tipos de efeitos: directos e indirectos. A diferença básica entre eles é que um efeito directo ***“resulta de acções sem nenhum mecanismo interveniente entre o acto e o resultado”***. Os efeitos indirectos são de difícil previsão e arrastam-se no tempo, contribuindo ou não para a obtenção do resultado pretendido.

Os efeitos directos podem ser:

- **físicos:** alteração física no objecto de aplicação;
- **funcionais:** efeito na capacidade de funcionamento, degradando o seu funcionamento;
- **psicológicos:** resultado de acções que influenciam emoções, motivos e em última análise o comportamento dos sistemas;
- **colaterais:** resultados ocorridos para além das intenções, com consequências positivas ou negativas relativamente à obtenção do objectivo.

Os efeitos indirectos podem ser:

- **psicológicos;**
- **colaterais;**
- **funcionais;**
- **cumulativos:** o resultado dos efeitos directos e indirectos contra um sistema;
- **em cascata:** um efeito indirecto transversal a vários sistemas;
- **sistémicos:** efeito na operação específica de sistemas.

Para obter a compreensão dos efeitos decorrentes de uma possível acção, é necessário ter um conhecimento holístico, considerando as teias de relacionamento entre os sistemas que constituem o ecossistema. Durante o processo de planeamento são identificados em primeiro lugar os efeitos desejados.

### 5.3. PRIORITIZAÇÃO

De forma a caracterizar a importância do efeito e conseqüentemente a sua implementação, foi adoptada neste modelo a prioritização da engenharia de software.

O papel da prioritização é estabelecer uma relação de criticidade entre os efeitos a desenvolver.

*“O desafio é seleccionar os efeitos “certos” de um conjunto de efeitos candidatos de forma a que os diversos interesses, limitações técnicas e preferências dos diversos intervenientes sejam salvaguardadas”* (Ruhe G. 2002).

Esta prioritização é desenvolvida tendo por base a caracterização das seguintes variáveis (Berander et al. 2005):

- **importância;**
- **penalizações;**
- **custo;**
- **tempo;**
- **risco;**
- **volatilidade.**

O estabelecimento destas variáveis deverá considerar ainda:

- **nível de abstracção;**
- **reprioritização;**
- **funcionalidade.**

A quantificação destas variáveis deve ser tão objectiva quanto possível, podendo ser usados diversos métodos para a obtenção desse objectivo (Berander et al. 2005).

- **AHP (Analytical Hierarchy Process);**
- **100 dollar test;**
- **agrupamento;**
- **classificação;**
- **top-ten;**

O resultado da priorização sugere quais os efeitos que devem ser implementados e em que ordem. Tal como todos os métodos de avaliação, o resultado deverá ser interpretado e possivelmente ajustado pelos decisores detentores do conhecimento e não simplesmente aceites.

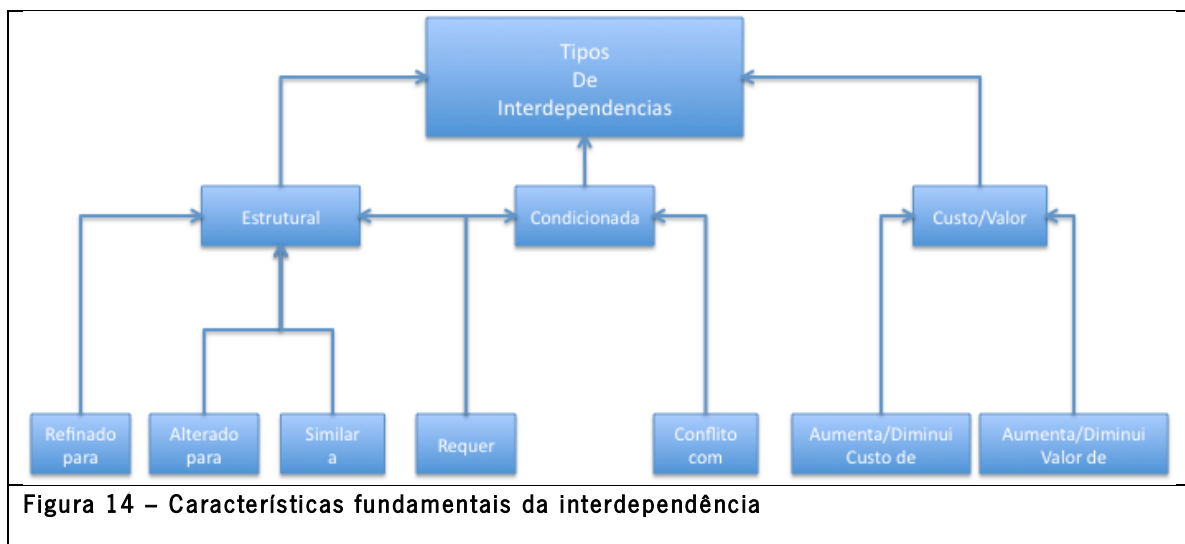
## **5.4. INTERDEPENDÊNCIA**

Os efeitos podem afectar-se mutuamente de diversas formas, sendo a sua influência diversa, como seja o facto de condicionarem o desenvolvimento de outros efeitos, afectarem o custo de implementação de outros efeitos ou aumentarem/diminuírem o grau de satisfação relativamente a outros efeitos (Dahlstedt et al. 2005).

Não sendo um problema, a interdependência de efeitos pode influenciar um conjunto de actividades de desenvolvimento e decisões durante um projecto, na fase de planeamento, alterações de gestão, características de desenho e implementação, teste e reutilização de efeitos.

O conhecimento sobre a existência e consequência da interdependência de efeitos é portanto essencial de forma a evitar potenciais erros aos quais podem estar associados custos elevados, ou mesmo vulnerabilidades adicionais que põem em risco o próprio efeito. A identificação das características da interdependência permite ainda garantir a rastreabilidade do efeito ao longo do ciclo de vida do mesmo. Ou seja, para determinado efeito, permite identificar o seu percurso de desenvolvimento e o papel que o mesmo tem no desenvolvimento dos restantes efeitos.

A interdependência apresenta um conjunto de características esquematizadas na figura 14.



As interdependências estruturais, relacionam-se com facto de, dado um conjunto específico de efeitos, estes possam ser organizados numa estrutura, onde as relações são de natureza hierárquica bem como transversal, sendo dividida em três categorias:

- **refinado para:** o efeito é detalhado para um determinado número de efeitos mais específicos;
- **alterado para:** alteração de um efeito para outro efeito se uma nova versão desse efeito substitui o mais antigo;
- **similar a:** um efeito declarado é similar ou sobreposto por um ou mais efeitos.

Na figura 14 identificam-se ainda as interdependências condicionadas, que definem a forma como alguns efeitos podem condicionar outros. Este condicionamento é caracterizado por:

- **requer**: a execução de um efeito depende da execução de outro efeito. Depende, neste sentido, significa que um ou mais efeitos detalhados são necessários, isto é, não são opcionais, de forma a completar um efeito de mais alto nível;
- **Conflito com**: um efeito está em conflito com outro se não podem existir simultaneamente ou se a satisfação de um efeito diminui a satisfação de outro.

O terceiro tipo de interdependência identificado na figura 14, é a interdependência de custo/valor. As interdependências do tipo custo/valor estão relacionadas com o custo envolvido na implementação de efeitos e o valor que a implementação desse efeito irá trazer, classificando-se da seguinte forma:

- **Aumentam/Diminuem o custo de**: Se um efeito for escolhido para implementação, então o custo de implementação de outro efeito diminui ou aumenta;
- **Aumenta/Diminui o valor de**: se um efeito for escolhido para implementação então o valor para o outro efeito irá aumentar ou diminuir.

## 5.5. CONCLUSÕES

O crescimento exponencial do uso das tecnologias de informação, crescimento de acordo com a Lei de Moore (Kopp 2002; Moore 1965) e o paradigma actual da colaboração, com as ferramentas da WEB 2.0, actuam como multiplicadores da força do conhecimento colectivo em proveito do indivíduo e das organizações. Os conceitos fluem através das fronteiras como se elas não existissem. Hoje, mais do que nunca, os fusos horários são mais importantes do que as fronteiras (Wriston 1997). Os Estados, as empresas e os indivíduos, estão agora ligados por um comércio global, pelos media, pelos transportes e tecnologias de comunicação. Estamos a viver uma era de economia em rede, centrada no ecossistema da informação, em que o efeito informacional é cada vez mais importante.

Desta perspectiva benigna, o “nivelar” do mundo permite que qualquer indivíduo, em qualquer parte do globo possa aceder ao conhecimento (Alberts 2003). A relevância da função hardware foi substituída pela do software.

Na perspectiva do paradigma colaborativo, suportado pelas ferramentas da actual WEB 2.0, o perímetro da informação não tem limites, tornando-se por isso num espaço multi-dimensional, onde prevalece a dimensão espacial catalisada pelos aspectos tempo/velocidade. O tempo e o espaço foram sempre preponderantes na informação, no entanto, hoje, o tempo é mais importante, procurando-se executar um ciclo de decisão mais rápido.

É neste ambiente complexo que amadurece o conceito de ecossistema de informação baseado em efeitos, como modelo para alcançar também a segurança da informação do ecossistema organizacional, obtendo uma arquitectura capaz de suportar o ciclo de vida da informação, criando assim um ecossistema mais saudável.

Ao integrar os conceitos da guerra da informação, sistematizando o seu desenvolvimento de níveis estratégicos para um ecossistema de informação, o modelo fornece a caracterização dos diferentes anéis, fornecendo uma visão integrada do ecossistema.

Este modelo integra ainda os conceitos actuais da partilha da informação, permitindo a caracterização dos elementos fundamentais deste desenvolvimento, as ligações fiáveis em rede e a consciência partilhada do estado informacional.

Ao identificar na fase de desenvolvimento do ecossistema os efeitos pretendidos, caracterizando os três elementos que os suportam, está a realizar-se uma análise que será capaz de acompanhar todo o desenvolvimento da organização.

A integração das vulnerabilidades críticas permite garantir que a análise de segurança não é um processo de avaliação do acesso á informação mas sim uma característica de suporte ao efeito pretendido, reflectindo a relevância associada ao efeito.

A sistematização do modelo foi efectuada numa matriz que traduz a integração das diversas vertentes agora propostas. O modelo sistematizado é apresentado no anexo B.

Este modelo foi instanciado no dimensionamento de um ecossistema de informação de uma instituição de investigação científica, IBMC – Instituto de Biologia Molecular e Celular – ligada á Universidade do Porto.

Ficou claro que este modelo foi a solução adequada para o desenvolvimento pretendido, tendo demonstrado toda a sua relevância quando confrontado com novas necessidades, como seja por exemplo o efeito pretendido com a criação de um repositório da informação institucional de investigação.

### 6. CASO PRÁTICO

O caso prático de aplicação foi efectuado tendo como objectivo a remodelação dos sistemas de informação do IBMC – Instituto de Biologia Molecular e Celular, uma instituição de investigação científica ligada á Universidade do Porto. Desta remodelação resultou a criação de um ecossistema de informação.

O projecto foi estruturado em duas dimensões, uma ao nível da infra-estrutura de servidores e armazenamento, outra ao nível da infra-estrutura passiva de rede.

#### 6.1. INFRAESTRUTURA DE SERVIDORES E ARMAZENAMENTO

##### 6.1.1. EFEITOS

A identificação dos efeitos não foi efectuada por inquéritos formais aos utilizadores, tendo-se no entanto recolhido informação formal relativamente a satisfação e qualidade do serviço. A decisão sobre a utilização de um método deste tipo, não estruturado, teve por base, por uma lado, a inexistência de metodologias reconhecidas para tal e por lado a necessidade de agilizar esta fase envolvendo o menos possível a organização no desenvolvimento dos efeitos. Assim foram definidos os seguintes efeitos:

- criação de políticas de autenticação, segurança e salvaguarda de dados;
- implementação de uma gestão centralizada, simplificada e profissional dos sistemas de informação;
- implementação de soluções de administração remota para suporte e *helpdesk*;
- definição e implementação de soluções de *disaster recovery*;
- criação de uma solução de alta disponibilidade para os serviços essenciais (www, e-mail, acesso internet, etc.);

Além disso, pretende-se preparar a instituição para os desafios futuros, ao nível dos sistemas de informação, nomeadamente com a criação de intranets e integração da informação na era da WEB 2.0.

### 6.1.2. PONTO DA SITUAÇÃO

O estado da arte dos sistemas de informação no IBMC, em Junho de 2005, reflecte o que ainda hoje acontece em muitas organizações:

- nos últimos anos, os sistemas de informação do IBMC sofreram um crescimento não planeado, com soluções pouco consistentes;
- tipicamente existe um servidor por aplicação com desperdício de espaço de armazenamento;
- é comum a utilização de equipamento inadequado para as funções de suporte funcional da organização (exemplo: máquinas concebidas como computadores de secretária utilizadas como servidores departamentais);
- a maior parte dos grupos de trabalho apresentava gestão autónoma de recursos e equipamentos;
- as soluções de backup instaladas eram escassas e ineficientes;
- todos os servidores de suporte ao funcionamento estavam instalados numa DMZ;
- não existiam políticas de autenticação e segurança;
- o serviço de *helpdesk* tinham uma capacidade de resposta limitada.

Destes problemas resultaram as seguintes consequências imediatas e visíveis:

- perda de controlo sobre as soluções tecnológicas implementadas;
- falta de capacidade de resposta aos desafios de evolução e desenvolvimento;
- gestão ineficiente da informação;
- gestão ineficiente dos recursos;
- falta de controlo sobre o acesso (quem, onde, quando) à informação ou às infra-estruturas;
- elevada vulnerabilidade a ataques de DoS;
- elevados custos de funcionamento.

### 6.1.3. CAPACIDADES CRITICAS

Para suportar os efeitos anteriores, foram identificadas as seguintes capacidades críticas:



- consolidação dos servidores do departamento de sistemas de informação, criando um *data center*;
- criação de um serviço geral de autenticação e segurança, incluindo uma distribuição centralizada de espaço de armazenamento;
- implementação de uma solução centralizada de armazenamento de dados para repositório seguro de toda a informação;
- criação de uma arquitectura com elevada disponibilidade (mín. 95%) e versatilidade de utilização, com redundância de equipamentos;
- implementação de uma intranet baseada num CMS de *opensource* sobre plataforma *opensource*;
- reconfiguração das políticas de segurança e criação de um manual de segurança;

## 6.2. INFRAESTRUTURA DE REDE

### 6.2.1. EFEITOS

A infra-estrutura de rede é o elemento central de um sistema de informação, pelo que deve permitir o crescimento da organização, facilitar alterações funcionais e garantir a fiabilidade, tudo isto obviamente procurando otimizar o investimento. Uma má infra-estrutura consome recursos muitas vezes necessários para outras tarefas.

À análise da infra-estrutura existente, incluiu a verificação visual da instalação, bem como a análise da tecnologia utilizada, da organização e da distribuição do equipamento.

Em face disto, para o presente projecto foram identificados os seguintes efeitos:

- a criação de uma infra-estrutura capaz de suportar os desafios presentes e futuros, devidamente estruturada e organizada;
- integração de voz e dados;
- garantir QoS;
- proceder à certificação da cablagem, com a concomitante garantia de 20 anos da solução instalada.

### 6.2.2. PONTO DA SITUAÇÃO

A solução tecnológica existente em Junho de 2005 evidenciava as seguintes características:

- um elevado grau de desorganização da infra-estrutura de rede;
- crescimento não planeado;
- soluções e tecnologias heterogéneas;
- separação das infra-estruturas de voz e dados.

Como consequência, existia:

- perda de controlo sobre a natureza e localização dos equipamentos ligados;
- impossibilidade de gestão da infra-estrutura;
- impossibilidade de (re)organização dos meios instalados;
- impossibilidade de garantir QoS.

### 6.2.3. CAPACIDADES CRITICAS

De forma a atingir os efeitos propostos foram definidas as seguintes capacidades críticas:

- criar um data center para colocação da infra-estrutura central de distribuição e serviços;
- implementar uma infra-estrutura passiva estruturada em gigabit ethernet;
- criar anéis de comunicação funcionando a 10 Gb sobre fibra óptica ou cobre (sempre que seja possível); (interligação dos armários de distribuição e o Data Center)
- criar *backbones* robustos entre os diversos armários da mesma zona bem como entre *data center* e cada um dos armários;
- instalar dois armários de serviço por piso criando uma infra-estrutura redundante em estrela;
- reutilização dos equipamentos activos existentes.

Foram assim identificadas as forças e as fragilidades existentes no sistema de informação actual e a forma como as mesmas deveriam ser desenvolvidas em direcção á criação do ecossistema colaborativo.

Seguindo o processo preconizado no modelo obtiveram-se diversas matrizes, sendo apresentada em anexo B a referente á solução de *anti-spam* e que permitiram estabelecer a ordem de implementação das capacidades críticas que condicionaram a escolha da solução adequada.

Com a aplicação do planeamento apresentado neste documento conseguiu-se desenvolver o projecto de forma integrada e estabelecer uma relação de credibilidade e desenvolvimento com os fornecedores de cada uma das soluções.

Na área da infra-estrutura de servidores e serviços teve como resultado a escolha de uma solução de *Blade Center* da IBM, tendo dado origem a um caso de sucesso publicado na imprensa nacional e internamente ao nível da IBM (Sousa 2007a).

A infra-estrutura de serviços de rede, ao nível do equipamento activo de rede, deu origem a apresentação publica em dois eventos nacionais, o *Directions 2007* (Sousa 2007c) e o *SIAP 2007* (Sousa 2007b).

A infra-estrutura passiva de rede deu origem á publicação em Espanha de um artigo em conjunto com a SIEMON (Sousa 2008b), parceiro de projecto para a infra-estrutura passiva de rede.

### 7. CONCLUSÕES

Torna-se claro que está a acontecer uma alteração profunda na forma como as organizações se relacionam com o seu meio ambiente. O IT é o elemento fundamental para esta alteração, e a WEB 2.0 em particular, fornece o conceito que permite potenciar essa alteração.

Apesar desta constatação assiste-se frequentemente a títulos do tipo “*IT doesn't matter*” assente no pressuposto que estando o IT tão banalizado, ou seja, fazendo parte integrante do desenvolvimento actual das organizações, é completamente incapaz de ser um elemento diferenciador e de aumento de competitividade.

Esta visão leva a que nos últimos anos os Departamento de Sistemas de Informação tenham sido pressionados, quer para reduzir o valor do investimento quer para efectuar mais com menos. No entanto o IT tem demonstrado a sua importância de forma inovadora e não pelo tradicional suporte organizacional mas como potenciador da incorporação de novas formas de pensar as organizações.

O *Myspace* apresenta um desenvolvimento de 2 Milhões de novos utilizadores por mês, o *Facebook* é utilizador por 85% de todos os estudantes nos Estados Unidos e um *blog* é criado a cada segundo.

Não se trata agora de colocar apenas a informação on-line, trata-se isso sim da utilização das ferramentas da colaboração em massa como meio de produção, estando a provocar uma mudança fundamental na forma como inovamos.

No modelo tradicional das organizações temos uma hierarquia fechada, no novo modelo temos uma organização aberta e fundamentalmente centrada em rede e nas pessoas, não no capital. Esta reorganização assenta na liderança e não na gestão.

No entanto esta alteração do modelo das organizações apesar de já existente á várias décadas só agora tem reunidas as condições para se desenvolver, como sejam:

- **tecnologia adequada;**
- **demografia;**

- **economia;**
- **sociedade;**

A tecnologia capaz de suportar esta nova dinâmica tem o nome de WEB 2.0 e não é mais um conjunto de *links* estáticos e acessível apenas de um PC, usa todos os equipamentos capazes de algum tipo de comunicação.

É uma solução ubíqua e dinâmica, permitindo a integração de variadíssimos formatos e soluções que tornam a experiência do utilizador cada vez mais interactiva. Esta nova dinâmica permite uma computação baseada no ambiente. O elemento que interage com os ecossistemas organizacionais é a “coisa”.

Perante este cenário, o desenvolvimento do planeamento de um sistema de informação é uma tarefa que tem vindo a tornar-se cada vez mais complexa, sendo esta complexidade derivada da forma como os fabricantes entendem a tecnologia, como as empresas a integram e por último como os recursos humanos as desenvolvem, integram e utilizam.

Os sistemas de informação têm demonstrado as suas capacidades de suportar as estruturas organizacionais. Foram assim desenvolvidas soluções para aplicação da integração de sistemas na área dos processos e produtividade, centradas dentro dos limites físicos das organizações.

Com o aparecimento da internet, fornecendo um novo meio de comunicação e de desenvolvimento, as organizações desenvolveram um conjunto de ferramentas para potenciar esse novo canal, como sejam o comércio electrónico.

O correio electrónico chegou de forma massiva às organizações integrando-se com os sistemas existentes desenvolvendo os sistemas on-line de encomendas, métodos de *workflow* e fomentou a evolução de plataformas móveis de comunicação.

As comunicações evoluíram permitindo a ligação ubíqua à organização, a organização disponibilizava aos seus colaboradores ferramentas para acederem on-line às ferramentas empresariais usando tradicionalmente soluções de VPN.

As condições fornecidas pelas comunicações permitiram a integração de soluções cada vez mais interactivas, o desenvolvimento aplicativo, não tinha agora de se preocupar com a optimização da velocidade, não sendo necessários conhecimentos tão profundos de comunicação para desenvolvimento de uma aplicação funcional.

Surgiram cada vez mais aplicações desenvolvidas para a WEB, com ambientes gráficos bem desenvolvidos e interactivos e que implementavam soluções para estabelecimento de relações que iam das simples relações pessoais á partilha de conhecimento.

No advento deste desenvolvimento tecnológico, suportado na WEB 2.0, os sistemas de informação foram ficando cada vez mais expostos á necessidade de partilha de informação, de forma a fomentar o desenvolvimento da inovação organizacional e no limite, garantir que as organizações serão capazes de sobreviver.

No entanto, os modelos de planeamento tradicionais continuam a fornecer apenas visões internas das organizações, ou seja, continuam a fechar a organização dentro das suas quatro paredes.

Esta estrutura reflecte-se na forma como as organizações pensam a segurança da sua informação. Tipicamente temos uma *firewall* que protege o perímetro e disponibiliza o acesso a determinadas funcionalidades da organização e no entanto os comprometimentos da organização acontecem com maior complexidade e prejuízo no interior da LAN organizacional.

Este problema é agravado com a necessidade de integração da filosofia WEB 2.0, movendo o centro do conhecimento em LAN para um conhecimento em WAN.

A única forma das organizações se prepararem para que este ecossistema seja o suporte da inovação e desenvolvimento é garantirem que têm conhecimento do estado da informação organizacional e de que forma esta flui.

Este modelo efectua uma abordagem que permite, desde a fase de desenvolvimento do primeiro efeito até á criação do ecossistema organizacional, obter as condições para minimizar os problemas e o impacto da volatilidade do desenvolvimento organizacional.

A informação é o elemento que circula neste ecossistema e as organizações têm de ser capazes de criar as condições que permitam a integração das comunidades de conhecimento de forma a potenciarem o seu desenvolvimento e sobrevivência neste novo mundo de competitividade global.

As organizações têm de perceber que a sua agilidade depende cada vez menos da forma como protegem a informação que produzem, mas sim como disponibilizam informação garantindo a sua confiabilidade.

A informação não é o produto final mas sim a matéria-prima para o desenvolvimento das organizações, que todas pretendem tornar em conhecimento. Assim, a cada noção elementar de informação torna-se necessário traduzir o efeito pretendido para a sua utilização.

É pois fundamental que as organizações se apercebam das consequências e capacidades da utilização dessa informação ao longo de todo o processo de transformação.

Este modelo de planeamento é apresentado como uma abordagem a esse problema, criando as condições para o conhecimento organizacional e desenvolvendo o conceito de ecossistema organizacional.

Se ao modelarmos criarmos uma realidade dinâmica do ecossistema, apesar de este ser dinamicamente complexo, teremos as condições para compreender essa complexidade.

Os desafios da nova WEB são claros, cada vez mais colaboração para as organizações. A adopção deste paradigma apenas é possível se garantir a troca confiável de informação e para isso foram apresentadas algumas características fundamentais.

Foi apresentado que esta integração, para potenciar o desenvolvimento organizacional, extremamente complexo, dado que expõe sistemas estruturais da organização, disponibiliza novas ferramentas desenvolvidas para fornecerem uma boa experiência de utilização.

Ora os sistemas existentes e os problemas associados a estas novas ferramentas vêm potenciar ainda mais os problemas de criação deste ecossistema de informação seguro, como se demonstrou na apresentação das vulnerabilidades associadas a cada um dos intervenientes nesta nova forma de interacção.

Este modelo pretende integrar aqueles que são os desafios da WEB 2.0, apresentando uma forma de conseguir uma orientação adequada a esta realidade de utilizadores em rede.

Considerado o pontapé de saída, no sentido de criar um desenvolvimento integrado, consistente e dinâmico, capaz de garantir que a inovação será cada vez mais rapidamente integrada nas organizações, onde quer que ela esteja.

A WEB 2.0 será o tesouro de desenvolvimento e inovação das organizações, e o modelo de planeamento será o mapa para o ponto X.

Trata-se de uma abordagem que ainda carece de diversas validações, mas no entanto, pelo caso prático apresentado, pelas diversas conferências onde foi apresentado, como sejam, *Directions*

2007, SIAP 2007, SIS 2008 e aceite para apresentação e publicação na conferência EUNIS 2008 (Sousa 2008a), já demonstrou o seu elevado potencial e condições para cumprir o efeito pretendido.

Saliente-se ainda que a síntese deste trabalho será integrada como capítulo de um livro sobre *“Enterprise Information Systems for Business Integration in SME's”*.

“Toda a gente está a falar sobre isso, no entanto ninguém está a fazer nada”

Mark Twain

“Devemos aceitar o futuro, pois rapidamente será passado. Mas devemos respeitar o passado pois era o humanamente possível.”

Saint-Exupery



## BIBLIOGRAFIA

- Albert L. Lederer, V.S. "The implementation of strategic information systems planning methodologies," *MIS Quartely* (12:3), Setembro de 1988 1998, pp 445-461.
- Alberts, D.S.H., Richard E. "Power to the Edge: Command...Control...in the Information Age,") 2003.
- Amaral, L. "PRAXIS - Um referencial para o planeamento de sistemas de informação," in: *Departamento de Sistemas de Informação*, Universidade do Minho, 1994.
- André Vasconcelos, A.C., Pedro Sinogas, Ricardo Mendes, José Tribolet "Arquitectura de Sistemas de Informação: A Ferramenta de Alinhamento Negócio / Sistemas de Informação?," 1999.
- Anna H. Perrault , V.L.G. "THINK GLOBAL, ACT LOCAL: THE CHALLENGES OF TAKING THE WEBSITE GLOBAL\*," in: *INSPEL*, 2000.
- Berander, P., and Andrews, A. "Requirements Prioritization," in: *Engineering and Managing Software Requirements*, 2005, pp. 69-94.
- Carvalho, J.A., Luis Amaral e Rui D. Sousa "Business Process Models for Process Management," EURO/INFORMS 1997, Universidade do Minho, Barcelona, Espanha 1997.
- CIO, I. "Research Study,") 2006.
- CIOInsight "Security in the world of web 2.0,") 2007.
- Coelho, J.S. "Método LEARN – Um Contributo para a Definição das Necessidades de Informação de Acordo com a Estratégia do Negócio," *CAPSI* 2003.
- CSI, C.S.I. "2007 - CSI COMPUTER CRIME AND SECURITY SURVEY," Computer Security Institute.
- Dahlstedt, Å., and Persson, A. "Requirements Interdependencies: State of the Art and Future Challenges," in: *Engineering and Managing Software Requirements*, 2005, pp. 95-116.
- Drucker, P.F. "The coming of the new organization," (Harvard Business review on Knowledge, Management), 31 July 2001 2001, pp 1-19.
- Forrester, R.) 2006.
- Hammond, J. "Developing Enterprise Web 2.0 Applications," *Forrester Research*) 2007.
- Hsu, S.P.a.C. "Strategic Information Systems Planning: A Review," in: *Information Resources Management Association International*, Atlanta, Georgia, 1995.
- Insight, C. "Security in the world of web 2.0,") 2007.
- Jachman, J.A. "Business Systems Planning and Business Information Control Study: A comparison," *IBM Systems Journal* (21:1), 1982 1982.
- Joao Alvaro Carvalho, C.Z., Luis Amaral Jorge S. Coelho et al *Sistemas de Informação Organizacionais*, (1ª Edição ed.) Silabo, 2005.
- Juniper, R. "Research,") 2006.
- Kopp, C. "Moore's Law and its implications for information warfare,") 6 Janeiro de 2002 2002.
- Leffingwell D., W.D. *Managing Software Requirements – A Unified Approach* Addison-Wesley, Upper Saddle River, NJ, 2000.
- Luis Amaral, R.M., Carlos Campos Morais, António Serrano, Carlos Zorrinho "Sistemas de informação organizacionais," *Edições Silabo* (Capitulo 6) 2005.
- Martin, J. *Information Engineering*, 1989.
- Mikroyannidis, A. "Toward a Social Semantic Web,") 2007.
- Moore, G. "Cramming more componentes onto integrated circuits," *Electronics* (38:8), 19 Abril 1965 1965.

- Nunes, P.V. "Planeamento operacional baseado em efeitos (PEBE)," in: *Sociedade em rede: competição e conflito no domínio da informação*, Universidade do Minho, Universidade do Minho, 2006.
- Palanisamy, R. "Strategic information systems planning model for building flexibility and success," in: *Industrial Management & Data*, 2005, pp. 63-81.
- Panada, F. "The Emerging Thread,") 2007.
- Porter, M.E. "Competitive Advantage," in: *Free Press*, 1984.
- Porter, M.E. *Creating and sustaining superior performance*, 1994.
- Reilly, T.O. "What is web 2.0,") 2005.
- Robertson, S., and Robertson J. *Mastering the Requirements Process* ACM Press, London, UK, 1999.
- Rockart, J.F. "Chief executives define their own data needs," *Harvard Business Review* (57:2) 1979, pp 81-93.
- Roman Hoegg, R.M., Miriam Meckel, Katarina Stanoevska-Slabeva "Overview of business models for Web 2.0 communities," in: *Universität St. Gallen*, Institute of Media and Communication Management, 2007.
- Ruhe G., E.A., Pfahl D. "Quantitative WinWin – A New Method for Decision Support in Requirements Negotiation," Proceedings of the 14th International Conference on Software Engineering and Knowledge Engineering (SEKE'02), Ischia, Italy, 2002, pp. 159-166.
- Sethi, A.L.L.a.V. "The Implementation of Strategic Information Systems Planning Methodologies," *MIS Quartely* (12:3), September, 1988 1988, pp 445-461.
- Sousa, J. "Information Systems Planning in WEB 2.0, a new model approach," *Eunis 2008*, Junho 2008 2008a.
- Sousa, J.L. "IBM reestrutura sistemas de informação com tecnologia IBM,") 2007a.
- Sousa, J.L. "Planeamento de sistemas de informação orientado aos efeitos,") 2007b.
- Sousa, J.L. "Planeamento Orientado aos Efeitos, interdependencia e priorização,") 2007c.
- Sousa, J.L. "IBM reestrutura su arquitectura de sistemas de información con cableado Siemon,") 2008b.
- Tapscott, D. (ed.) *Wikinomics*, 2007.
- Technorati 2006.
- Vicente, J. "Operações baseadas em efeitos : o paradigma da guerra do século XXI,") 2007.
- Wriston, W.B. "Bits, Bytes, and Diplomacy,") Setembro de 1997 1997.

## INDEX

ambiente .....**19 , 28 , 38 , 61 , 66**  
colaboração .....**39**  
contexto .....**27 , 34 , 35 , 39 , 80**  
criticas..... VI, VII, 27, 51, 59, 60, 66, 68, 70  
ecossistema. VI, VII, XIII, 18, **19**, 20, 21, 22, 37, **39**, 44,  
45, 46, 48, **49**, 54, 55, 57, 58, 59, 60, 61, 62, 65,  
66, 67, 70, 74, 75  
efeitosVI, VII, 18, 20, 28, 31, 35, 57, 60, 61, 62, 63, 64,  
65, 66, 67, 69, 70, 81  
FCS ..... **XIV, 24, 27**  
informaçãoVI, VII, XIII, XIV, **16 , 17 , 18, 19 , 20 , 21, 22,**  
**23, 24, 25, 26, 27, 28, 29, 30, 31, 32,** 33, 34,  
**35, 36, 37, 38, 39, 42, 43, 44, 45, 46, 47, 48, 49,**  
**50, 51, 55, 57, 58, 59, 60, 65, 66, 67, 68, 69, 70,**  
72, 73, 74, 75, **81, 82**  
interdependência .....VI, VII, **20, 21, 57, 60, 64, 65**  
IT **XIV, 19, 25, 26, 54**

LEARN.....**XIV, 35**  
modelos ..... **VII, 16, 17, 19, 21, 32, 39, 40**  
Planeamento VII, XIV, **16, 17, 18, 19, 20, 21, 24, 30,**  
**32, 34, 35, 55, 57, 59, 64,** 81, 82  
prioritização.....VI, VII, **20, 21, 57, 60, 62, 63**  
PSN .....**XIV, 24, 28, 29, 30**  
segurança ... **VII, 17, 20, 21, 38, 45, 49, 51, 54, 55,**  
**66**  
SISP .....**XIV, 24, 33**  
sistemas.....**16, 17, 19, 21, 24, 25, 27, 28, 29, 31,**  
**32, 34, 35, 38, 45, 49, 55, 57, 59, 62, 81**  
WEB 2.0...I, II, VI, VII, VIII, IX, X, XIII, 17, 18, **21, 39, 40,**  
**41, 42, 43, 44, 45, 48, 49, 51, 52, 54, 55, 58, 65,**  
66, 67, 72, 73, 74, 75

## ANEXO A

### Etapa 1 Clarificação da estratégia do negócio

- Fase 1 Clarificação da estratégia a médio prazo
  - o Passo 1 Clarificar missão
  - o Passo 2 Clarificar visão
  - o Passo 3 Traduzir a estratégia em objectivos e indicadores a médio prazo
- Fase 2 Identificação dos processos de 1º nível
  - o Passo 1 Definição do método de contexto externo (stakeholders)
  - o Passo 2 Definição do método de processos do 1º nível
- Fase 3 Clarificação da estratégia a curto prazo
  - o Passo 1 Identificação das preocupações a curto prazo
  - o Passo 2 Definição dos objectivos e indicadores a curto prazo
  - o Passo 3 Refinamento da consistência dos objectivos
- Fase 4 Definição das prioridades de intervenção
  - o Passo 1 Elaboração da matriz de cruzamento objectivos/processos
  - o Passo 2 Identificação das prioridades de intervenção nos processos
  - o Passo 3 Definição das prioridades dos projectos e acções

### Etapa 2 Definição da arquitectura dos processos de negócio

- Fase 1 Definição de cada processo de 1º nível
- Fase 2 Decomposição dos processos de 1º nível em sub-processos
- Fase 3 Diagnóstico dos processos aos vários níveis
  - o Passo 1 Identificação das preocupações do processo
  - o Passo 2 Definição de objectivos e indicadores do processo
  - o Passo 3 Refinamento da consistência dos objectivos

### Etapa 3 Modelação dos processos elementares

- Fase 1 Definição de cada processo elementar
- Fase 2 Identificação das actividades
- Fase 3 Diagnóstico do processo elementar
  - o Passo 1 Identificação das preocupações do processo
  - o Passo 2 Definição de objectivos e indicadores do processo
  - o Passo 3 Refinamento da consistência dos objectivos

### Etapa 4 Diagnóstico das actividades

- Fase 1 Definição das actividades
- Fase 2 Levantamento e definição das tarefas
  - o Passo 1 Levantamento das operações das tarefas
  - o Passo 2 Redefinição das tarefas
- Fase 3 Identificação, discussão e aprovação das melhorias
  - o Passo 1 Diagnóstico das tarefas
  - o Passo 2 Identificação das melhorias
  - o Passo 3 Discussão alargada e aprovação das melhorias

### Etapa 5 Planeamento e controlo da implementação do método de melhoria contínua

- Fase 1 Definição do método de melhoria contínua
- Fase 2 Definição dos gestores e coordenadores de melhoria dos processos
- Fase 3 Definição do plano de melhoria
- Fase 4 Implementação e controlo do plano de melhoria

### Etapa 6 Planeamento dos sistemas de informação

- Fase 1 Identificação dos efeitos de informação
- Fase 2 Especificação de sistemas aplicacionais
- Fase 3 Selecção de aplicações informáticas

#### Etapa 7 Controlo da implementação de aplicações informáticas

- Fase 1 Parameterização das aplicações informáticas
- Fase 2 Aceitação das aplicações informáticas
- Fase 3 Manutenção do sistema de informação
- Fase 4 Formação dos utilizadores

#### Etapa 8 Recursos Humanos

- Fase 1 Definição de competências e funções
- Fase 2 Definição dos critérios de avaliação de desempenho
- Fase 3 Definição das necessidades de formação

#### Etapa 9 Referenciais de qualidade e risco

- Fase 1 Diagnóstico de melhorias face às normas da qualidade e do risco
- Fase 2 Planeamento e controlo da implementação de melhorias
- Fase 3 Adequação do manual de gestão

## ANEXO B

Item	Informação	Efeito	Prioritização							Interdependencia									
			Importância	Penalizações	Custo	Tempo	Risco	Volatilidade	Classificação	Ordenação	Estrutural			Condicionada		Custo/Valor			
											Refinado para	Alterado para	Semelhante a	Requer	Conflito com	Diminui o custo de	Aumenta o custo de	Diminui o valor de	Aumenta o valor de
<b>R2.</b>	<b>SOLUÇÃO DE ANTI-SPAM</b>																		
R2.1	Instalação de	Numero de falsos positivos entre 0 e 1 por cada 100 Mensagens	6	6	5	6	6	6	35	1					2.2				2
R2.2	uma solução e	Numero de falsos negativos entre 0 e 1 por cada 100 Mensagens	6	6	5	6	6	6	35	1					2.1				2
R2.3	anti-spam	Robustez e facilidade de integração na infraestrutura	5	5	6	5	6	4	31	2							2		2
R2.4	redundante e	Facilidade de gestão	5	5	5	5	5	4	29	4									2
R2.5		Capacidade técnica de evolução acompanhando as ameaças	5	5	5	5	5	5	30	3							2		2
R2.6	funcional	Eficiencia de captura	6	6	5	6	6	6	35	1	2.1,2.2			2.1,2.2					2