Continuidade do Negócio e *Cloud Computing*

Sumário da lição de síntese, nos termos da alínea c) do artigo 5º do Decreto-Lei nº 239/2007 de 19 de Junho

Candidatura ao título de **Agregado** em **Ciências da Informação**

Especialidade em

Sistemas e Tecnologias da Informação

apresentado à

Universidade Fernando Pessoa

por

Maria Leonilde dos Reis

2014

Índice

1. Introdução

A lição cujo sumário pormenorizado se apresenta neste documento intitula-se Continuidade do negócio e *Cloud Computing*.

A lição enquadra-se numa unidade de ensino subordinada Sistemas de Informação Organizacionais a leccionar no âmbito da Unidade Curricular Auditoria e Continuidade do negócio, Unidade Curricular que integra o Mestrado em Sistemas de Informação Organizacionais, em funcionamento na Escola Superior de Ciências Empresariais (ESCE) do Instituto Politécnico de Setúbal (IPS), desde 2008.

Esta Unidade Curricular é apresentada no relatório com o título "Auditoria e Continuidade do negócio: Relatório de Unidade Curricular contendo os Conteúdos e Métodos de Organização Científica e de Execução Pedagógica", que, em conjunto com este documento da Lição de Síntese, constituiu requisito exigido aos candidatos ao título de agregado.

Para além do sumário pormenorizado, este documento inclui um enquadramento da lição na Unidade Curricular e na unidade de ensino em que se insere e ainda uma descrição dos seus objectivos específicos e conteúdo.

2. Enquadramento da Unidade Curricular

2.1. A Unidade Curricular de Auditoria e Continuidade do negócio

A Unidade Curricular de Auditoria e Continuidade do negócio (ACN) integra o plano de estudos do Mestrado em Sistemas de Informação Organizacionais (MSIO) da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal. A Unidade Curricular supracitada é de carácter obrigatório, leccionada no 2º semestre do 1º ano, com uma tipologia lectiva teórico-prática, incluindo 162 horas de tempo de trabalho, sendo 45 horas de aulas de contacto, totalizando 6 ECTS[1].

A Unidade Curricular tem como principais objectivos:

- Sensibilizar os estudantes para a importância dos sistemas de informação e tecnologias de informação e comunicação em contexto organizacional.

- Sistematizar um conjunto de conceitos que permita aos estudantes compreender a relevância da auditoria de sistemas de informação em contexto organizacional.

- Sistematizar um conjunto de conceitos que permita aos estudantes compreender a relevância da continuidade do negócio em contexto organizacional.

[1] *European Credit Transfer and Accumulation System*, designado pela sigla ECTS

Especificamente os objectivos da Unidade Curricular são [Reis 2014]:

00 – Conhecer o contexto e os objectivos da Unidade Curricular assim como o seu conteúdo programático, referências e sistema de avaliação.

01 – Conhecer e compreender os principais conceitos e mais-valias associados à auditoria de sistemas de informação nas organizações.

02 - Conhecer e compreender os principais métodos e ferramentas de suporte à actividade de auditoria de sistemas de informação nas organizações.

03 - Conhecer e compreender as práticas instituídas nas organizações na actividade de auditoria de sistemas de informação.

04 - Conhecer e compreender normas internacionais de suporte à actividade de auditoria de sistemas de informação.

05 – Saber analisar e interpretar os problemas que ocorram em contexto organizacional.

06 – Saber realizar e/ou colaborar num processo de auditoria de sistemas de informação.

07 – Conhecer e compreender os principais conceitos e mais-valias associados à continuidade do negócio nas organizações.

08 - Conhecer e compreender os principais métodos e ferramentas de suporte à actividade de continuidade do negócio nas organizações.

09 - Conhecer e compreender as práticas instituídas nas organizações na actividade de continuidade do negócio.

10 - Conhecer e compreender normas internacionais de suporte à actividade continuidade do negócio.

11 – Saber analisar e interpretar os problemas que ocorram em contexto organizacional.

12 – Saber propor e implementar medidas de continuidade do negócio face aos riscos a que a organização está exposta.

13 – Saber identificar e recomendar propostas de optimização das práticas organizacionais.

14 – Apresentar e discutir as temáticas abordadas na Unidade Curricular utilizando um discurso rigoroso e coerente.

2.2. A Unidade de ensino Sistemas de Informação Organizacionais

De acordo com o planeamento definido em Reis (2014) a leccionação da Unidade Curricular está prevista para a sessão S3 da unidade curricular, o que totaliza 4 horas lectivas. Os seus objectivos incluem os objectivos descritos em O7, O8, O10 e O11 da secção anterior. Os conteúdos a abordar incluem (Reis, 2014):

a. Conceito de Continuidade do negócio
b. Evolução Histórica
c. Dependência das Tecnologias de Informação e Comunicação
d. Análise de Risco
e. Metodologias e Estratégias de Recuperação
f. *Cloud Computing*
g. Desafios do *Cloud Computing* face à Continuidade do negócio.

Sendo esta lista de referências indicativa pelo facto de se entender que a mesma pode ser complementada e analisada, com diferentes prespectivas de detalhe, em função dos temas que cada estudante se propõe desenvolver em contexto organizacional. Como suporte aos conteúdos são sugeridas referências identificadas em Reis (2014):

BCM (2008), *Business Continuity Management - Good Practice Guidelines 2008 – A Management Guide to Implementing Global Good Practice in Business Continuity Management:* Documentos impressos. Business Continuity Institute.

Drewitt, T., (2013), *A Manager's Guide to ISO22301: A Practical Guide to Developing and Implementing a Business Continuity Management System*. Londres. BSI Group Headquarters.

Elliott, D., Swartz, E., Herbane B., (2010), *Business Continuity Management: A Crisis Management Approach*, second edition, Routledge.

Estall, H., (2012), *Business Continuity Management Systems: Implementation and Certification to ISO 22301*, BCS, The Chartered Institute for IT.

Faria, M. L., (1995), *Planos de Contingência e Recuperação em caso de Desastre*, Dissertação de Mestrado, Universidade Católica, Porto.

Faria, M. L., e Amaral, L., (1995), Qualidade e Planos de Contingência e Recuperação em caso de Desastre. *In 2º Encontro Nacional para a Qualidade nas Tecnologias de Informação e Comunicações QUATIC'95*. Lisboa.

Faria, M. L., e Amaral, L., (1998), Planeamento da Contingência e Recuperação, *Revista da Associação Portuguesa de Sistemas de Informação*, 8, 43-51.

Ferreira, D., Reis, L., (2013), Optimização de Práticas de Segurança da Informação – Utilização do Balanced Scorecard Designer, *Revista do Departamento de Inovação, Ciência e Tecnologia*, Universidade Portucalense, vol 3. Porto.

Ferreira, D., Reis, L., (2011), Optimização de práticas no domínio da Segurança da Informação - Balanced Scorecard Designer como ferramenta. *In XXI Jornadas Hispano-Lusas de Gestión Científica*, Universidad de Córdoba, Córdoba, Espanha.

Furht, B., Escalante, A., (2010). *Handbook of Cloud Computing*. New York: Springer.

Goldberg, S. H., Davis S. C. and Pegalis, A. M., (1999), *Y2K Risk Management - Contingency Planning, Business Continuity, and Avoiding Litigation*, Wiley Computer Publishing.

Hotchkiss, S., (2010), *Business Continuity Management: In Practice*, BCS Learning & Development Limited.

Hugos, M., Hulitzky, D., (2011). *Business in the Cloud, what every business needs to know about Cloud Computing*. New York. John Wiley & Sons.

ISO (2008), ISO/IEC 24762:2008 - *Information technology - Security techniques -- Guidelines for information and communications technology disaster recovery services*: Documentos impressos. Geneva: International Organization for Standardization.

ISO (2011), ISO/IEC 27031:2011 - *Information technology -- Security techniques - Guidelines for information and communication technology readiness for business continuity*: Documentos impressos. Geneva: International Organization for Standardization.

Lacey, D.,(2012), *Business Continuity Management for Small and Medium Sized Enterprises. How to Survive a Major Disaster or Failure*, BSI.

Landum, M., Reis, L., (2012), Cloud na Administração Local – Estudo de caso. *In 12ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI2012)*, Universidade do Minho, Guimarães.

Landum, M., Reis, L., (2013), Cloud na Administração Local – Estudo de viabilidade. *Revista do Departamento de Inovação, Ciência e Tecnologia*, Universidade Portucalense, Porto, submetido.

Mainwald, E. and Siegein, W., (2002), *Security Planning & Disaster Recovery - Protect your Organization Resources*, McGraw-Hill Osborne.

Marchão, J., Reis, L., Os Serviços em Cloud na óptica de Utilização Empresarial: Um estudo de viabilidade. *Revista de Ciências da Computação*, vol. 4. Universidade Aberta, Lisboa, 2013.

Marchini, R. (2010). *Cloud Computing: A Practical Introduction to the Legal Issues*. Londres. BSI Group Headquarters.

Reis, L., (2001), *Planeamento de Sistemas de Informação e da Contingência e Recuperação*, Tese de Doutoramento, Universidade do Minho, Braga.

Reis, L., (2001), Manual Electrónico de Apoio ao Desenvolvimento de Planos de Contingência e Recuperação em Sistemas de Informação para PME, *Colecção Investigação*, vol.1, Instituto Politécnico de Setúbal.

Reis, L., e Amaral, L., (2003), Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação. *In 3ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI)*, Universidade de Coimbra, Coimbra.

Reis, M. L., e Amaral, L., (2002), Integrated Planning of Information Systems and Contingency and Recovery. *In International Conference on Enterprise Information Systems*, Universidade de Castilla-La Mancha, Spain.

Reis, M. L., e Amaral, L., (2000), Planeamento da Contingência e Recuperação em Sistemas de Informação. *In Conferência de Sistemas de Informação da Associação Portuguesa de Sistemas de Informação (CAPSI*), Guimarães.

Reis, M. L., e Amaral, L., (2002), Planeamento de Sistemas de Informação e da Contingência e Recuperação. *In Conferência Científica e Tecnológica em Engenharia*, Instituto Superior de Engenharia de Lisboa, Lisboa.

Reis, M. L., e Amaral, L., (2002), Planeamento integrado de Sistemas de Informação e da Contingência e Recuperação. *In XII Jornadas Luso-Espanholas de Gestão Cientifica*, Universidade da Beira Interior, Covilhã.

Trowbridge, B., (2011*). Cloud Sourcing the Corporation*. Austin. Alsbridge.

3. Descrição da Lição

A lição que se apresenta neste documento corresponde a 1 hora lectiva da Unidade Curricular de Auditoria e Continuidade do negócio. Os conteúdos da lição são sobretudo resultado de trabalhos de investigação conduzidos ou orientados pela docente nos últimos anos, os quais se encontram materializados em publicações:

Faria, M. L., (1995), *Planos de Contingência e Recuperação em caso de Desastre*, Dissertação de Mestrado, Universidade Católica, Porto.

Faria, M. L., e Amaral, L., (1995), Qualidade e Planos de Contingência e Recuperação em caso de Desastre. *In 2º Encontro Nacional para a Qualidade nas Tecnologias de Informação e Comunicações QUATIC'95*.

Faria, M. L., e Amaral, L., (1998), Planeamento da Contingência e Recuperação, *Revista da Associação Portuguesa de Sistemas de Informação*, 8, 43-51.

Ferreira, D., Reis, L., (2013), Optimização de Práticas de Segurança da Informação – Utilização do Balanced Scorecard Designer, *Revista do Departamento de Inovação, Ciência e Tecnologia*, Universidade Portucalense, Porto.

Ferreira, D., Reis, L., (2011), Optimização de práticas no domínio da Segurança da Informação - Balanced Scorecard Designer como ferramenta. *In XXI Jornadas Hispano-Lusas de Gestión Científica*, Universidad de Córdoba, Córdoba, Espanha.

Landum, M., Reis, L., (2012), Cloud na Administração Local – Estudo de caso. *In 12ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI2012*), Universidade do Minho, Guimarães.

Landum, M., Reis, L., (2013), Cloud na Administração Local – Estudo de viabilidade. *Revista do Departamento de Inovação, Ciência e Tecnologia*, Universidade Portucalense, Porto, submetido.

Marchão, J., Reis, L., (2013), Os Serviços em Cloud na óptica de Utilização Empresarial: Um estudo de viabilidade. *Revista de Ciências da Computação, vol 4.* Universidade Aberta, Lisboa.

Reis, L., (2001), *Planeamento de Sistemas de Informação e da Contingência e Recuperação*, Tese de Doutoramento, Universidade do Minho, Braga.

Reis, L., (2001), *Manual Electrónico de Apoio ao Desenvolvimento de Planos de Contingência e Recuperação em Sistemas de Informação para PME*, Colecção Investigação, vol.1, Instituto Politécnico de Setúbal, Setúbal.

Reis, L., e Amaral, L., (2003), Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação. *In 3ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI),* Universidade de Coimbra, Coimbra.

Reis, M. L., e Amaral, L., (2002), Integrated Planning of Information Systems and Contingency and Recovery. *In International Conference on Enterprise Information Systems*, Universidade de Castilla-La Mancha, Spain.

Reis, M. L., e Amaral, L., (2000), Planeamento da Contingência e Recuperação em Sistemas de Informação. *In Conferência de Sistemas de Informação da Associação Portuguesa de Sistemas de Informação,* Guimarães.

Reis, M. L., e Amaral, L., (2002), Planeamento de Sistemas de Informação e da Contingência e Recuperação. *In Conferência Científica e Tecnológica em Engenharia*, Instituto Superior de Engenharia de Lisboa, Lisboa.

Reis, M. L., e Amaral, L., (2002), Planeamento integrado de Sistemas de Informação e da Contingência e Recuperação. *In XII Jornadas Luso-Espanholas de Gestão Cientifica*, Universidade da Beira Interior, Covilhã.

Os objectivos específicos da lição são os seguintes:

- Conhecer o conceito Continuidade do negócio.
- Conhecer e compreender o processo de Análise de Risco.
- Conhecer as Metodologias subjacentes à Continuidade do negócio.
- Conhecer e saber propor as Estratégias de Recuperação.
- Conhecer o Conceito *Cloud Computing*.
- Compreender o Modelo de computação, o Modelo de Serviço e o Modelo de Implementação.
- Conhecer os desafios da Continuidade do negócio e do *Cloud Computing*.
- Compreender o *Service Level Agreement* e o Enquadramento Legal.
- Saber aferir quais as Vantagens e Condicionantes da adopção de *Cloud Computing*.

4. Sumário Pormenorizado

4.1. Introdução

Actualmente as organizações dependem dos seus Sistemas de Informação (SI), estando na generalidade dos casos incorrectamente dimensionada essa sua dependência das Tecnologias de Informação e Comunicação (TIC).

As preocupações subjacentes à continuidade do negócio advêm da necessidade de instituir procedimentos que em caso de acidente permitam a continuação da actividade organizacional.

As questões relacionadas com a Segurança dos SI e a problemática dos riscos a que a generalidade das organizações está exposta suscitam só por si preocupações no domínio da Continuidade do negócio, como tal considera-se crucial a definição de estratégias.

A Sociedade de Informação necessita cada vez mais da ubiquidade na disponibilização da informação. Deste modo o *Cloud Computing* tende a propiciá-la, sendo uma forma diferente de prestar e facturar serviços, levantando ao mesmo tempo, novos desafios na sua prestação.

Questões subjacentes aos *Service Level Agreement* (SLA), ou seja os contratos de prestação de serviços, podem não contemplar questões de relevância no sentido da continuidade do negócio. Advoga-se que as questões associadas à portabilidade e interoperabilidade, entre *cloud* e prestadores de serviços, bem como localização dos dados, são factores que devem ser contemplados nos SLA.

Com esta lição propõe-se abordar um conjunto de conceitos subjacentes à temática em estudo tendo sempre como permissa de que as soluções a propor terão em

conta a especificidade do negócio. Assim, nas secções seguintes introduz-se o conceito de continuidade do negócio, análise de risco, metodologias e estratégias de recuperação. Apresentam-se reflexões no que respeita à adopção do *Cloud Computing*, tendo como pressuposto que esse serviço será prestado por uma entidade externa à organização. Como consequência essa prestação de serviço terá enquadramento legal com a formalização de um contrato. Por último, apresentam-se as conclusões.

4.2. Continuidade do Negócio

A actividade de Planeamento da Continuidade do Negócio (PCN) deverá ser uma preocupação vincada nas organizações portuguesas que, em Portugal teve início nos anos 80, quando as primeiras organizações encetaram medidas no sentido de preservarem o seu negócio na eventualidade de acidentes.

A evolução foi extremamente lenta, uma vez que o nosso mercado de serviços estava desprovido de respostas para este novo problema. Estava então detectado um nicho do mercado que necessitava de respostas à altura das necessidades existentes.

As estratégias de recuperação foram outra das preocupações subjacentes. Estas deverão ser em função da especificidade da organização e deverão ter em atenção que, tão importante como ter estratégias de recuperação, é definir estratégias para que a organização possa suportar financeiramente não só a implementação da solução, mas também a sua actualização e manutenção ao longo do tempo.

Considera-se que, actualmente, os negócios estão fortemente dependentes dos SI e das TIC, devendo essa dependência ser equacionada com rigor.

Neste sentido, recuperar rápida e eficientemente a actividade depois de um acidente, minimizando os seus efeitos, deverá ser uma preocupação vincada e real dos decisores.

A análise de cenários de recuperação deve ter como pressupostos os custos de implementação e de manutenção, a complexidade tecnológica e o nível de segurança que podem ser suportados.

4.2.1. Metodologias

Como referido no ponto anterior, a actividade de Planeamento da Continuidade do negócio (PCN) começou a ser vincada nas organizações portuguesas a partir dos anos 80, contudo a sua evolução foi extremamente lenta, uma vez que o nosso mercado de serviços estava desprovido de respostas para este novo problema.

Em resposta a esta necessidade surgem organizações prestadoras de serviços de auditoria que se dedicaram à temática da segurança informática, tendo definido como estratégia apresentar propostas ao mercado no sentido de prestarem serviços no âmbito da auditoria que contemplassem a contingência e recuperação. Deste modo, as organizações passaram a poder optimizar as suas condições de funcionamento prevenindo a ocorrência de acidentes.

Inicialmente estas organizações prestadoras de serviços de contingência e recuperação circunscreveram a sua prestação de serviço às áreas da segurança, especificamente na optimização das condições de segurança dos sistemas e equipamentos. Contudo, perante a necessidade das organizações planearem a recuperação dos acidentes, com preocupações no âmbito do planeamento da continuidade do negócio, as organizações de consultoria passaram a fornecer

serviços mais abrangentes de recuperação. Passamos, então a ter organizações prestadoras de serviços de diferentes ramos: as de auditoria e as prestadoras de serviços na área da recuperação.

As preocupações com o PCN surgem normalmente por imposição legal da organização "mãe", principalmente quando esta estava localizada nos EUA ou na Europa Central, em resultado, por um lado, da percepção e investigação desenvolvida nesta área e, por outro lado, em consequência de imposição legislativa nos países de origem, no que respeita à obrigação da existência de um PCN. Os restantes casos de PCN implementados dizem respeito a organizações cujos accionistas e/ou decisores tomaram consciência da necessidade do PCN como forma de preservar o negócio, em função da consciencialização dos riscos a que estavam expostos.

4.2.2 Estratégias de Recuperação

A definição de estratégias de recuperação no domínio desta actividade deverá ser claramente identificada face à especificidade do negócio da organização e aos resultados da análise de risco.

A análise de risco deve consistir na realização de um ou vários estudos dos riscos subjacentes à actividade do negócio, tendo em conta as suas especificidades. Alguns riscos identificados poderão ser mitigados após debate interno na organização e com o comprometimento do decisor hierárquico responsável por assumir esse tipo de decisões. Este tipo de estudos geralmente evidência riscos que devem ser assumidos como parte de uma normal operação de negócio.

Considera-se, assim, que a realização de uma análise de riscos, utilizando a metodologia que se considere pertinente, potencia benefícios subjacentes a um maior nível de detalhe dos riscos a que uma organização está exposta. Assim, uma análise desta natureza pode potenciar o aumento do conhecimento das fragilidades, uma vez que o debate deste tipo de temáticas pode aumentar o nível geral de interesse e de preocupação entre os colaboradores da organização. Permite também identificar activos, vulnerabilidades e controlos. Algumas organizações desconhecem os seus activos, bem como as vulnerabilidades que lhes estão associadas. Uma análise sistemática pode produzir uma lista actualizada de activos e de riscos. Este tipo de análise pode ainda revestir-se de particular interesse, nomeadamente no que respeita a uma maior consciencialização no que se refere à implementação de mecanismos de segurança que, sendo dispendiosos não apresentam um benefício óbvio para a organização.

Face às fragilidades analisadas em contexto organizacional e face às estratégias do negócio sugere-se que, considerando essas especificidades se analise, no âmbito das soluções tradicionalmente propostas, as opções de recuperação (centro redundante, prestação de serviços, *empty shell*, centros associados) por forma a que a organização encontre a solução mais adequada à recuperação do seu negócio em caso de acidente.

O âmbito do PCN deve ser definido em consonância com a filosofia de gestão dos órgãos decisores da organização, devendo estar circunscrito às áreas consideradas críticas para o negócio. Por os recursos financeiros serem limitados, os órgãos decisores deverão ter como preocupação de centrar a manutenção da solução de recuperação no tempo. Isto é, a solução de recuperação implementada tem associada custos de manutenção a serem suportados ao longo do tempo.

Para proceder à análise dos diversos cenários de processamento alternativo da organização, deve-se fazer uma análise do ponto de vista genérico em que se consideram os diferentes cenários alternativos, devidamente adequados à realidade da organização:

- **Centro próprio** – As instalações e equipamentos do centro de processamento de dados alternativo são definidas, geridas e mantidas pela organização.

- **Acordo comercial** – Se a organização renovar o equipamento com alguma frequência este cenário poderá ser factor facilitador, uma vez que se pretende a formulação de um contrato para proceder à instalação de hardware de acordo com as necessidades da organização, devendo estabelecer-se contratualmente que a organização deverá proceder à instalação de software no centro alternativo.

- **Acordo recíproco** – Estabelecimento de um acordo com outra organização não concorrente no negócio, com características técnicas similares para as funções solicitadas, permitindo a prestação recíproca de serviços. Salienta-se que esta solução poderá ser uma forma de as organizações do tipo Pequena Média Empresa (PME) poderem ter, de forma mais efectiva, planeada a contingência e a recuperação.

A análise de cenários deve ter como pressupostos que os custos de implementação, de manutenção, de complexidade tecnológica e do nível de segurança podem ser suportados e a solução proposta se mantém exequível no tempo. A análise pela adopção de uma solução de *Cloud Computing* no sentido de recuperação em caso de acidente deverá ser precedida de estudo específico, onde

se ponderaram diversos factores no sentido de criar cláusulas de suporte legal a esta prestação de serviço.

4.3. *Cloud Computing*

Apesar da divulgação de serviços de *Cloud Computing*, o significado do conceito não é uniforme nas diversas fontes que permitem reflectir sobre a temática. Contudo, o *National Institute of Standards and Technology* (NIST) tem vindo a analisar esta problemática no sentido da uniformização.

Deste modo, o (NIST, 2011), define que o Cloud Computing "é um modelo para permitir a ubiquidade conveniente, que permite um acesso à rede através da procura para uma *pool* partilhada de recursos de computação configurável (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente fornecidos e disponíveis com um esforço mínimo ou interacção do fornecedor do serviço".

Considera-se que este "novo" paradigma entrou no nosso quotidiano, sensivelmente em 2008 e que está a evoluir gradualmente. As organizações de maior dimensão têm vindo a adoptar o modelo de *cloud* privada. Por outro lado, as Pequenas e Médias Empresas também estão a adoptar este novo paradigma tecnológico, privilegiando, no entanto, a migração dos seus dados para fornecedores externos, no modelo de *cloud* pública, (Hugos, 2011). As preocupações no que se refere ao desempenho e níveis de segurança da informação necessitam de ser avaliados.

4.3.1. Modelo de computação

O modelo de computação do *Cloud Computing* compreende cinco características essenciais, três modelos de serviço e quatro modelos de implementação, segundo as orientações do NIST (2011).

O modelo define a essência do *Cloud Computing* e importantes aspectos, destacando-se de modelos idênticos, pelas suas cinco características essenciais (procura de serviços, amplo acesso à rede ou ubiquidade, recursos computacionais, elasticidade e medição de serviços).

4.3.2. Modelo de Serviço

Os três modelos de serviço definidos pelo NIST (2011), designados por Software *as a Service* (SaaS), *Plataform as a Service* (PaaS), *Infrastructure as a Service* (IaaS). Estes modelos de serviço distinguem-se pela capacidade oferecida pelo prestador de serviços, relativamente a infra-estrutura para o utilizador/cliente colocar as suas aplicações, ou disponibilizar numa plataforma de desenvolvimento com capacidade de processamento, ou disponibilizar serviços de infra-estrutura de armazenamento, rede e outros recursos fundamentais, tudo isto em ambiente *Cloud Computing*.

Considera-se que o que distingue esta tecnologia de outras é a procura de serviços uma vez que qualquer utilizador da *Cloud Computing* pode requerer unilateralmente as capacidades de computação que necessitar. E ainda o amplo acesso à rede ou ubiquidade: **o**s recursos computacionais encontram-se disponíveis através da Internet e podem ser acedidos através de mecanismos padronizados em qualquer ponto. Do ponto de vista do prestador de serviços, os meios sejam eles físicos ou virtuais, são agrupados de modo a servirem vários

utilizadores, sendo alocados e realocados dinamicamente consoante a procura e tipo de utilizador;

As capacidades ou funcionalidades computacionais devem ser prestadas rápida e de forma elástica, assim como também devem ser rapidamente libertadas, numa escala compatível com a procura. A medição dos serviços é considerada fundamental no sentido de os sistemas de gestão utilizados para a *cloud*, controlarem, monitorizarem e optimizarem automaticamente o uso de recursos, em cada tipo de serviço (processamento, armazenamento, largura de banda e activos).

No entanto, a *Cloud Computing* está a evoluir e a especializar-se noutros modelos que funcionam como subfamílias tais como, o *Business Process as a Service* (BPaaS), o qual se pode considerar como uma subfamília de *SaaS*, o *Video Surveillance as a Service* (VSaaS), existindo ainda outras emergentes como o *Security as a Service* (SECaaS), subfamília do *SaaS*, e o *Storage as a Service* (STaaS), subfamília do *IaaS*.

4.3.3 Modelo de Implementação

No que se refere aos modelos de implementação e segundo o NIST (2011), existem quatro modelos que se caracterizam do seguinte modo:

- ***Cloud* pública -** disponibilizada publicamente através do modelo *pay-per-use*, sendo que a infra-estrutura de *cloud* é disponibilizada para uso aberto ao público em geral. Pode ser detida, gerida e operada por um sector empresarial, académico ou organização governamental, ou alguma destas combinações e está localizada nas instalações do fornecedor.

- ***Cloud* privada -** compreende uma infra-estrutura utilizada unicamente por uma organização em que a infra-estrutura de nuvem é disponibilizada para uso exclusivo de uma única organização, que inclui vários consumidores (por exemplo, unidades de negócio). Pode ser detida, gerida e operada pela organização, por um terceiro (*outsourcing*), ou numa destas combinações, e pode existir dentro ou fora das instalações da organização.

- ***Cloud* comunitária -** é partilhada por uma comunidade de organizações com interesses em comum, fornece uma infra-estrutura partilhada, podendo o caso da administração pública ser um bom exemplo.

- ***Cloud* híbrida -** é uma composição de duas ou mais nuvens, em que a infra-estrutura de nuvem é uma composição de duas ou mais infra-estruturas de *cloud* distintas (comunitária, privada ou pública).

Considera-se que a *cloud* comunitária e a *cloud* híbrida podem ser compostas por duas ou mais infra-estruturas de *cloud* comunitária, privada ou pública, conectadas por tecnologias padronizadas ou proprietárias.

Os modelos de implementação a adoptar por cada organização deverão ser factor de ponderação face à especificidade do negócio e às estratégias que lhe estão subjacentes.

4.4. Desafios da Continuidade do negócio e do *Cloud Computing*

Actualmente, a generalidade das organizações têm uma forte dependência dos Sistemas de Informação (SI), sem que essa dependência esteja aferida com rigor. Nesse sentido, e porque existem inúmeras ameaças aos SI, advoga-se que a Continuidade do negócio deverá ser uma preocupação vincada por parte dos

decisores da organização, uma vez que, em caso de acidente, deverão existir estratégias de recuperação da actividade afectada no sentido de dar continuidade às actividades do negócio.

4.4.1. *Service Level Agreement*

Uma das questões de relevância a considerar, quando se pretende migrar dados para a *Cloud Computing*, é o conhecimento do enquadramento legal, principalmente na resolução dos *Service Level Agreement* (SLA).

Os SLA devem ser celebrados de modo que, a resolução de diferendos se consiga fazer unicamente no âmbito do contrato. Considera-se ainda que existem aspectos a precaver, nomeadamente no domínio da implementação de medidas de segurança e no domínio técnico, em que a responsabilidade pela segurança pode passar a ser um problema jurídico.

Advoga-se que deverão também, neste âmbito de preocupações, ser considerados os Planos de Continuidade de Negócio (PCN).

Salienta-se ainda um outro aspecto importante, a legislação do País onde estão situados os *data centers* que contêm os dados ou serviços deve ser tida em conta na preparação e elaboração dos SLA.

4.4.2. Enquadramento Legal

Considera-se assim, importante a existência de legislação adequada a este novo paradigma, que deixou de ser local passando a ser global, estando a ser feito um esforço por parte da União Europeia para criação de legislação adequada, que

abranja a segurança e interoperabilidade dos sistemas nos diferentes Estados Membros.

Assim, considera-se pertinente avaliar a legislação em vigor bem como, eventuais lacunas existentes, por forma a evitar dificuldades na fase de pós-implementação. Em caso de contencioso jurídico devem as organizações ter presente os trâmites da lei, ou a sua ausência, consoante os casos.

Estas são algumas das questões, numa matéria onde se nota ainda a ausência de um quadro legislativo adaptado às novas realidades tecnológicas. O actual quadro jurídico, baseado em legislação nacional, enfrenta o importante desafio de alargar os seus horizontes ao nível global, acompanhando, deste modo, a disseminação global das tecnologias emergentes.

O enquadramento legal difere em função do país em que se está a actuar e pela "natureza da *cloud*, é muito provável que esteja mais que um país envolvido na implementação particular da mesma" (Marchini 2010). Colocam-se desta forma as questões subjacentes à aplicabilidade da legislação onde segundo o autor primeiro necessitamos de identificar qual o sistema legal a aplicar. Na *Cloud Computing* podem existir várias actividades que ultrapassem várias fronteiras, não sendo, por vezes, fácil identificar em que países se realizam determinadas actividades.

Assim, em caso de necessidade de resolução do foro jurídico, a legislação a adoptar será a do país onde se encontra o *data center* com os dados do adquirente do serviço, daí que na contratação de serviços na *Cloud Computing*, ganhe grande relevância o conhecimento da localização dos dados, sendo desejável que os mesmos pudessem ser mantidos no território nacional.

4.4.3. Vantagens e Condicionantes da adopção de *Cloud Computing*

Paralelamente advoga-se, que a problemática deverá ser devidamente equacionada, no sentido de reflectir as questões subjacentes a nível do enquadramento legal, segurança da informação, portabilidade, interoperabilidade, fiabilidade e dependência do fornecedor, sem prejuízo da avaliação de questões como a escalabilidade, flexibilidade, factor económico e meio ambiente.

A adopção do modelo de *Cloud Computing* poderá ser factor potenciador de vantagens competitivas face ao modelo tradicional e impulsionar a inovação em contexto organizacional.

Salienta-se a importância e pertinência da realização de uma análise de riscos que permitam concluir acerca da viabilidade da migração de serviços para a *Cloud Computing*, consideradas as respectivas vantagens e condicionantes da sua utilização.

Recomenda-se que as decisões tomadas sejam alicerçadas na especificidade do negócio, na análise de riscos realizada e não em fundamentação geral que, teoricamente, poderia indiciar vantagens aparentemente aliciantes e que vão no sentido de redução de custos de investimento em hardware e software, custos com os respectivos *upgrades*, e custos de manutenção, permitindo, simultaneamente, libertar os recursos humanos das TIC para actividades *core* do negócio.

4.5. Conclusão

Como conclusão desta lição salienta-se:

a) A continuidade do negócio deverá ser uma preocupação vincada para as organizações;
b) As organizações deverão aferir os riscos inerentes à especificidade dos seus negócios;
c) Deverá ser realizada a análise efectiva do grau de dependência do negócio face aos seus SI;
d) A adopção do modelo de *Cloud Computing* poderá ser factor potenciador de vantagens competitivas face ao modelo tradicional;
e) A inexistência de legislação específica adequada a este novo paradigma na óptica da prestação de serviços deverá constituir factor de reflexão;
f) Salienta-se a importância e pertinência da realização de uma análise de riscos que permitam concluir acerca da viabilidade da migração de serviços para a *Cloud Computing*;
g) Recomenda-se que as decisões tomadas sejam alicerçadas na(s) especificidade(s) do negócio.

5. Referências

BCM (2008), *Business Continuity Management - Good Practice Guidelines 2008 – A Management Guide to Implementing Global Good Practice in Business Continuity Management:* Documentos impressos. Business Continuity Institute.

Dewitt, T., (2013), *A Manager's Guide to ISO22301: A Practical Guide to Developing and Implementing a Business Continuity Management System*. Londres. BSI Group Headquarters.

Elliott, D., Swartz, E., Herbane B., (2010), *Business Continuity Management: A Crisis Management Approach*, second edition, Routledge.

Estall, H., (2012), *Business Continuity Management Systems: Implementation and Certification to ISO 22301*, BCS, The Chartered Institute for IT.

Faria, M. L., (1995), *Planos de Contingência e Recuperação em caso de Desastre*, Dissertação de Mestrado, Universidade Católica, Porto.

Faria, M. L., e Amaral, L., (1995), Qualidade e Planos de Contingência e Recuperação em caso de Desastre. *In 2º Encontro Nacional para a Qualidade nas Tecnologias de Informação e Comunicações (QUATIC'95)*, Lisboa.

Faria, M. L., e Amaral, L., (1998), Planeamento da Contingência e Recuperação. *Revista da Associação Portuguesa de Sistemas de Informação*, 8, 43-51.

Ferreira, D., Reis, L., (2013), Optimização de Práticas de Segurança da Informação – Utilização do Balanced Scorecard Designer. *Revista do Departamento de Inovação, Ciência e Tecnologia*, vol. 3. Universidade Portucalense, Porto.

Ferreira, D., Reis, L., (2011), Optimização de práticas no domínio da Segurança da Informação - Balanced Scorecard Designer como ferramenta. *In XXI Jornadas Hispano-Lusas de Gestión Científica*, In Universidad de Córdoba, Córdoba, Espanha.

Furht, B., Escalante, A., (2010). Handbook of Cloud Computing. New York: Springer.

Goldberg, S. H., Davis S. C. and Pegalis, A. M., (1999), *Y2K Risk Management - Contingency Planning, Business Continuity, and Avoiding Litigation*, Wiley Computer Publishing.

Hotchkiss, S., (2010), *Business Continuity Management: In Practice*, BCS Learning & Development Limited.

Hugos, M., Hulitzky, D., (2011). *Business in the Cloud, what every business needs to know about Cloud Computing*. United States of America. John Wiley & Sons.

ISO (2008), ISO/IEC 24762:2008 - *Information technology - Security techniques -- Guidelines for information and communications technology disaster recovery services*: Documentos impressos. Geneva: International Organization for Standardization.

ISO (2008), ISO/IEC 24762:2008 - *Information technology - Security techniques -- Guidelines for information and communications technology disaster recovery services*: Documentos impressos. Geneva: International Organization for Standardization.

ISO (2011), ISO/IEC 27031:2011 - *Information technology -- Security techniques - Guidelines for information and communication technology readiness for business continuity*: Documentos impressos. Geneva: International Organization for Standardization.

Lacey, D., (2012), *Business Continuity Management for Small and Medium Sized Enterprises. How to Survive a Major Disaster or Failure*, BSI.

Landum, M., Reis, L., (2012), Cloud na Administração Local – Estudo de caso. *In 12ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI2012)*, Universidade do Minho, Guimarães.

Landum, M., Reis, L., (2013), Cloud na Administração Local – Estudo de viabilidade. *Revista do Departamento de Inovação, Ciência e Tecnologia*, Universidade Portucalense, Porto, submetido.

Mainwald, E. and Siegein, W., (2002), *Security Planning & Disaster Recovery - Protect your Organization Resources*, McGraw-Hill Osborne.

Marchão, J., Reis, L., (2013), Os Serviços em Cloud na óptica de Utilização Empresarial: Um estudo de viabilidade. *Revista de Ciências da Computação*, vol 4, Universidade Aberta, Lisboa.

Marchini, R. (2010). *Cloud Computing: A Practical Introduction to the Legal Issues*. Londres. BSI Group Headquarters.

NIST, (2011). *National Institute of Standards and Technology, Computer Security*, Resource Center, Publications.

Reis, L., (2001), *Planeamento de Sistemas de Informação e da Contingência e Recuperação*, Tese de Doutoramento, Universidade do Minho, Braga.

Reis, L., (2001), Manual Electrónico de Apoio ao Desenvolvimento de Planos de Contingência e Recuperação em Sistemas de Informação para PME, *Colecção Investigação*, vol.1, Instituto Politécnico de Setúbal.

Reis, L., e Amaral, L., (2003), Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação. *In 3ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI)*, Universidade de Coimbra, Coimbra.

Reis, M. L., e Amaral, L., (2002), Integrated Planning of Information Systems and Contingency and Recovery. *In International Conference on Enterprise Information Systems*, Universidade de Castilla-La Mancha, Spain.

Reis, M. L., e Amaral, L., (2000), Planeamento da Contingência e Recuperação em Sistemas de Informação. *In Conferência de Sistemas de Informação da Associação Portuguesa de Sistemas de Informaçã (CAPSI)*, Guimarães.

Reis, M. L., e Amaral, L., (2002), Planeamento de Sistemas de Informação e da Contingência e Recuperação. *In Conferência Científica e Tecnológica em Engenharia*, Instituto Superior de Engenharia de Lisboa, Lisboa

Reis, M. L., e Amaral, L., (2002), Planeamento integrado de Sistemas de Informação e da Contingência e Recuperação. *In XII Jornadas Luso-Espanholas de Gestão Cientifica*, Universidade da Beira Interior, Covilhã.

Trowbridge, B., (2011). *Cloud Sourcing the Corporation*. Austin. Alsbridge.