Auditoria e Continuidade do Negócio

Relatório de Unidade Curricular contendo os conteúdos e métodos de organização científica e de execução pedagógica

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

Especialidade em

Sistemas e Tecnologias da Informação

apresentada à

Universidade Fernando Pessoa

por

Maria Leonilde dos Reis

2014

Resumo

Neste relatório apresenta-se uma proposta de programa para a Unidade Curricular Auditoria e Continuidade do Negócio, Unidade Curricular obrigatória do 2º semestre do 1º ano do plano de estudos do curso de Mestrado (2º ciclo) em Sistemas de Informação Organizacionais (MSIO), da Escola Superior de Ciências Empresariais (ESCE) do Instituto Politécnico de Setúbal (IPS), desde o ano lectivo de 2007/2008

O relatório constitui o cumprimento de um dos três requisitos exigidos aos candidatos ao título de Agregado: *apresentação, apreciação e discussão de um relatório sobre conteúdos e métodos de organização científica e de execução pedagógica de uma Unidade Curricular, grupo de unidades curriculares, ou ciclo de estudos, no âmbito do ramo de conhecimento ou especialidade em que são prestadas as provas* (alínea b, do artigo 2, das Normas Regulamentares da Atribuição do Titulo de Agregado pela Universidade Fernando Pessoa, publicadas no DR, 2ª série – Nº 110 – 9 de Junho de 2008).

No relatório, enquadra-se a Unidade Curricular no curso de Mestrado em Sistemas de Informação Organizacionais e apresenta-se a sua finalidade e os seus objectivos gerais e específicos, os conteúdos programáticos e, ainda, o plano de execução pedagógica. Apresentam-se, ainda, as estratégias de ensino-aprendizagem em Sistemas de Informação Organizacionais, o sistema de avaliação, a carga de trabalho e os recursos necessários. Finaliza-se com uma reflexão sobre as características da Unidade Curricular.

Índice

Índice de Quadros e Tabelas

1. Introdução

Neste relatório apresenta-se uma descrição da Unidade Curricular de Auditoria e Continuidade do Negócio, Unidade Curricular obrigatória do Mestrado em Sistemas de Informação Organizacionais, da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal.

O relatório constitui parte da documentação exigida aos candidatos ao título de Agregado nos termos da legislação vigente e das Normas Regulamentares da Atribuição do Titulo de Agregado pela Universidade Fernando Pessoa. A escolha desta Unidade Curricular como objecto do relatório, que inclui " *os conteúdos e métodos de organização científica e de execução pedagógica de uma Unidade Curricular, grupo de unidades curriculares, ou ciclo de estudos, no âmbito do ramo de conhecimento ou especialidade em que são prestadas as provas*", exigido aos candidatos ao titulo de Agregado, justifica-se pelo facto de a candidata ter vindo a ser regente e docente da referida Unidade Curricular desde a sua primeira edição.

Para além desta primeira secção (Introdução), o relatório é constituído por mais onze secções. Na segunda secção (Enquadramento da Unidade Curricular), enquadra-se a Unidade Curricular no curso de Mestrado em Sistemas de Informação Organizacionais, da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, incluindo a sua relação com outras unidades curriculares, bem como o calendário de funcionamento. Na terceira secção (Finalidade e Objectivos), descreve-se a finalidade e enumeram-se os objectivos da Unidade Curricular. Na quarta secção (Conteúdo Programático) apresenta-se o conteúdo programático da

Unidade Curricular. A quinta secção (Plano de Execução Pedagógica) apresenta o plano de execução pedagógica da Unidade Curricular identificando as sessões, a sua tipologia, objectivos e bibliografia de suporte. Na secção seis (Comparação com outras Instituições) são abordadas as questões subjacentes aos referenciais internacionais no que se refere à elaboração de planos de estudo no domínio dos Sistemas de Informação. Na secção sete (Estratégias de Ensino-Aprendizagem) são definidas, por sessão, um conjunto de estratégias para que seja possível alcançar os objectos da Unidade Curricular, incluindo indicação de bibliografia principal e de bibliografia complementar. A secção oito (Sistema de Avaliação) apresenta o sistema de avaliação da Unidade Curricular incluindo a avaliação continua e a avaliação final. A secção nove (Carga de Trabalho) tem por objectivo caracterizar o volume de trabalho subjacente à Unidade Curricular face ao seu enquadramento no ciclo de estudos. A décima secção (Recursos) descreve o conjunto dos recursos necessários ao funcionamento da Unidade Curricular. Na décima primeira secção (Considerações Finais), tecem-se algumas considerações e expõem-se algumas reflexões sobre a Unidade Curricular. Na décima segunda secção (Referências de Suporte), apresenta-se a totalidade das referências subjacentes à Unidade Curricular.

2. Enquadramento da Unidade Curricular

Nesta secção enquadra-se a Unidade Curricular de Auditoria e Continuidade do Negocio, objecto deste relatório, no Mestrado em Sistemas de Informação Organizacionais, da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal (ESCE/IPS).

O Mestrado em Sistemas de Informação Organizacionais, da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, é constituído por dois anos, cada um dividido em dois semestres, o que perfaz um total de quatro semestres. Os dois primeiros semestres são destinados às unidades curriculares lectivas, sendo os dois últimos dedicados à Unidade Curricular de seminário e dissertação, sob a supervisão de um orientador científico.

A Unidade Curricular de Auditoria e Continuidade do Negócio posiciona-se, de acordo com o plano curricular no 2º semestre do 1º ano do Mestrado em Sistemas de Informação Organizacionais, (MSIO) sendo obrigatória. Com uma tipologia lectiva Teórico-Prática, inclui 162 horas de tempo de trabalho, das quais 45 horas são de aulas de contacto, totalizando 6 ECTS. Os quadros apresentados abaixo, retirados do Diário da República, 2.ª série — N.º 122 — 26 de Junho de 2008, enquadram a Unidade Curricular de Auditoria e Continuidade do Negócio, na estrutura curricular do Mestrado em Sistemas de Informação Organizacionais. A sua inclusão como Unidade Curricular é obrigatória.

2.1. Plano de Estudos do Mestrado

Instituto Politécnico de Setúbal — Escola Superior de Ciências Empresariais

Diário da República, 2.ª série — N.º 122 — 26 de Junho de 2008

1º Ano 1º semestre

Unidades curriculares	Área científica	Tipo	Tempo de trabalho (horas)		Créditos	Observações
			Total	Contacto		
Gestão das Tecnologias de Informação e Comunicação	STI	Semestral	162	TP: 45	6	
Comportamento Organizacional	GRH	Semestral	162	TP: 45	6	
Informação Financeira	F	Semestral	162	TP: 45	6	
Inovação, Estratégica e Competitividade	G	Semestral	162	TP: 45	6	
Segurança da Informação	STI	Semestral	162	TP: 45	6	

1º Ano 2º semestre

Unidades curriculares	Área científica	Tipo	Tempo de trabalho (horas)		Créditos	Observações
			Total	Contacto		
Estratégia em Sistemas de Informação	STI	Semestral	162	TP: 45	6	
Gestão do Risco		Semestral	162	TP: 45	6	
Teoria e Gestão da Qualidade em Projectos de Sistemas de Informação	C	Semestral	162	TP: 45	6	
Sistemas de Informação e Organizações		Semestral	162	TP: 45		
Auditoria e Continuidade do Negócio	STI	Semestral	162	TP: 45	6	
	STI				6	

2º Ano 1º semestre

Unidades curriculares	Área científica	Tipo	Tempo de trabalho (horas)		Créditos	Observações
			Total	Contacto		
Seminário	STI	Semestral	135	S: 45	10	
Dissertação Trabalho de Projecto	STI	Semestral	675	OT: 20	20	(*a*)

(*a*) A escolher uma.

2º Ano 2º semestre

Unidades curriculares	Área científica	Tipo	Tempo de trabalho (horas)		Créditos	Observações
			Total	Contacto		
Dissertação Trabalho de Projecto	STI	Semestral	810	OT: 35	30	(*a*)

(*a*) A escolher uma.

2.2. Criação do Mestrado

A proposta de criação do curso de Mestrado em Sistemas de Informação Organizacionais da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal integra-se nos princípios da Declaração de Bolonha e tem por base a legislação produzida, referente à concepção e instrução do processo referente a novos ciclos de estudos. Este curso de 2º Ciclo, em estreita articulação com o curso de Licenciatura em Gestão de Sistemas de Informação (GSI) existente na Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, procura ser um complemento à formação dos licenciados da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal bem como constituir-se como opção de formação no domínio dos Sistemas e Tecnologias de Informação para outros licenciados pelo Instituto Politécnico de Setúbal ou licenciados provenientes de outras Instituições de Ensino Superior.

A formação superior de 2º ciclo integra opções científicas e pedagógicas, não contempladas no 1º ciclo, essencialmente vocacionadas para as actuais exigências de qualificação nas respectivas áreas de formação. A articulação entre as diversas unidades curriculares foi efectuada, tendo como quadro de referência as competências identificadas para os profissionais nesta área, tendo ainda em consideração os requisitos percepcionados no estudo de comparabilidade efectuado com outras Instituições de Ensino Superior.

Esta proposta visa proporcionar aos estudantes, que pretendam continuar a sua formação, um aprofundamento dos conhecimentos específicos no respectivo domínio da especialidade[1], bem como uma consolidação dos

[1] Entidades reconhecidas internacionalmente, nomeadamente a *Association for Information Systems* (AIS), *Association for Computing Machinery* (ACM), bem como sugestões das organizações da região.

conhecimentos gerais de gestão subjacentes a um desempenho profissional de qualidade, de acordo com as exigências do mercado de trabalho, e uma especialização de natureza profissional.

2.3. Objectivos das Unidades Curriculares

Os objectivos de cada Unidade Curricular, descritos no quadro 1, proporcionam um desenvolvimento e aprofundamento dos conhecimentos e competências obtidos ao nível do 1º ciclo nos cursos de licenciatura na área da Gestão dos Sistemas de Informação (GSI). A generalidade das unidades curriculares (de base, e especialidade e de investigação) funcionou em sessões presenciais de natureza teórico-prática onde se procedeu à exposição, desenvolvimento, aprofundamento e discussão de conceitos teóricos, acompanhados pela resolução de exercícios, discussão de casos, apresentação de trabalhos ou outras actividades que implicaram uma participação mais activa por parte dos estudantes.

Quadro 1 – Objectivos das Unidades Curriculares

UNIDADES CURRICULARES	OBJECTIVOS
Gestão das Tecnologias de Informação e Comunicação	Conhecer e compreender a importância das Tecnologias de Informação e Comunicação no contexto organizacional. Conhecer as novas Tecnologias de Informação e Comunicação e a sua inserção nas actividades organizacionais, atendendo às vantagens competitivas.
Comportamento Organizacional	Condicionantes dos comportamentos dos indivíduos, grupos e organizações. Papel da liderança na eficácia das organizações e na gestão de processos de mudança. Poder e política nas organizações e táticas éticas de influência. Como motivar pessoas e aproveitar a dinâmica dos grupos para conseguir melhores decisões e desempenho. Comunicação, gestão de conflitos e negociação, para estimular comportamentos colaborativos. Como influenciar a cultura de uma organização, no sentido de desenvolver nos seus colaboradores um sentimento colectivo de comunhão de interesses.
Informação Financeira	Conhecer a importância da Informação Financeira. Enquadrar a Informação Financeira nos Sistemas de Informação para a Gestão. Relevar a Informação Financeira na tomada de decisão.
Inovação, Estratégia e Competitividade	Analisar a gestão da inovação como componente do sistema de gestão; impacto da inovação tecnológica nas organizações e no seu meio envolvente. A Gestão Estratégica na gestão e no desenvolvimento das organizações. Modelos e instrumentos de análise e formulação estratégica.
Segurança da Informação	Reconhecer a importância da Segurança da Informação organizacional como factor de competitividade. Conhecer o enquadramento normativo e legal da Segurança da Informação. Elaborar políticas de Segurança da Informação enquadradas na estratégia da organização.
Estratégia em Sistemas de Informação	Conhecer os diferentes modelos de definição da estratégia empresarial. Identificar qual a informação estratégica para a definição da estratégia do negócio. Avaliar o Valor Económico da Informação para a Tomada de Decisão Estratégica. Identificar a Cadeia de Valor do Sistema de Informação para a Tomada de Decisão Estratégica. Conceber a Arquitectura do Sistema de Informação para a Tomada de Decisão Estratégica. Identificar qual a informação para a avaliação e o controle da estratégia.
Gestão do Risco	Apresentar conceitos e medidas de Risco. Desenvolver temas relacionados com o processo de Gestão do Risco.

Teoria e Gestão da Qualidade em Projectos de Sistemas de Informação	Conhecer os modelos de referência em Engenharia de Sistemas e processos de realização de produtos de *software* (ISO e IEEE 12207, ISO 15504, CMMi, SPICE, RUP). Compreender os modelos de referência na melhoria da maturidade dos processos e na gestão do risco. Perceber a importância dos modelos de referência no desenvolvimento da aprendizagem organizacional e no desenvolvimento do capital intelectual Analisar o modelo CMMi. Conhecer os Processos do modelo de referência CMMi – "*Standard CMMI Appraisal Method for Process Improvement* (SCAMPISM)". Discutir casos práticos de implantação de modelos de referência.
Sistemas de Informação Organizacionais	Enquadrar os conceitos fundamentais à conceptualização da organização. Compreender os impactos dos sistemas e tecnologias de informação no contexto organizacional. Desenvolver a capacidade de diagnóstico e desenho de soluções organizacionais, tendo por base o respectivo potencial.
Auditoria e Continuidade do Negócio	Conhecer as metodologias subjacentes à actividade das Auditorias Tecnológicas. Conhecer e fomentar a actividade do Planeamento da Contingência e Recuperação no sentido de assegurar a Continuidade do Negócio.
Seminário	Realizar seminários para a apresentação de metodologias/trabalhos de investigação. Organizar seminários com a participação de diversas personalidades tendo por objectivos proporcionar o debate nas diversas temáticas da especialidade.
Dissertação de Mestrado ou Trabalho de Projecto ou Estágio Curricular	Desenvolver um trabalho de investigação aplicada com o objectivo de, utilizando conhecimento científico e tecnológico, resolver problemas. Elaborar uma Dissertação de Mestrado/Trabalho de Projecto que deverá ser original mas sem a obrigatoriedade de ter carácter inovador. Poderá ter um enquadramento profissional/profissionalizante ou académica/científica. Desenvolver competências para realizar trabalho individual. Desenvolver competências para articular trabalho de investigação.

Por esta razão, o programa de formação privilegia contextos de aprendizagem, onde os estudantes são incentivados a aplicar os conhecimentos e a capacidade de análise crítica a problemas concretos, relevantes no domínio organizacional e profissional, e que, pela sua natureza, antes desconhecida pelos estudantes, favoreçam uma efectiva mobilização de conhecimentos e competências de forma inovadora. Para

além do domínio técnico, pretende-se que os estudantes desenvolvam uma perspectiva sistémica e que integrem os problemas apresentados no contexto global das dinâmicas organizacionais e das realidades profissionais. Deu-se relevância às questões de natureza deontológica e a todas as implicações neste domínio das decisões a tomar aquando da resolução dos problemas propostos e que procurarão replicar aquelas com que se depararão quotidianamente ou outras que, pela sua natureza excepcional, representem uma oportunidade de elevado valor heurístico.

Procurou-se também através do incentivo à exposição e discussão e do formato pedagógico participativo, o desenvolvimento de competências na área da comunicação e capacidade argumentativa adoptando terminologia clara e adequada a audiências de especialistas e de não especialistas. Neste domínio é particularmente instrumental a figura dos seminários em que o debate, mais do que a exposição, constitui o principal factor de desenvolvimento destas competências, críticas para o desempenho profissional.

No domínio das atitudes perante a aprendizagem, pretende-se que os valores de aprendizagem contínua, quer técnica, quer não técnica, de constante actualização dos saberes profissionais e de aceitação da natureza transitória dos mesmos, a par da flexibilidade e abertura à mudança, constituíssem valores pessoais e profissionais adoptados pelos estudantes. Da mesma forma, pretende-se que os estudantes compreendam que a empregabilidade depende da sua capacidade de, autonomamente, diagnosticar necessidades formativas pessoais e mobilizar os recursos necessários, próprios ou organizacionais, para assumir essas responsabilidades perante a profissão.

A Unidade Curricular de Seminário visa proporcionar aos estudantes os instrumentos necessários à elaboração de uma Dissertação de Mestrado, um Trabalho de Projecto ou um Estágio Curricular originais e especialmente realizados para a obtenção do grau de Mestre.

O ciclo de estudos correspondente ao Mestrado em Sistemas de Informação Organizacionais teve em atenção os princípios consagrados na Declaração de Bolonha, bem como outros estudos internacionais[2]. O plano de estudos deste 2º Ciclo tem como objectivos curriculares possibilitar ao estudante a actualização e complemento dos conhecimentos adquiridos no curso de graduação detido ao nível do 1º Ciclo, permitindo que o estudante adquira uma especialização profissional nesta área de conhecimento.

Este 2º ciclo encontra-se estruturado em quatro semestres, sendo os dois primeiros semestres (correspondentes ao 1º ano) organizados em 5 unidades curriculares. O 2º ano é dedicado à elaboração da Dissertação de Mestrado, do Trabalho de Projecto ou do Estágio Curricular, estando incluída no início do 3º semestre uma Unidade Curricular de Seminário, com a qual se pretende dotar os estudantes de capacidade de investigação autónoma. A cada Unidade Curricular do 1º ano são atribuídos 6 créditos ECTS, à Unidade Curricular de Seminário são atribuídos 10 créditos ECTS, enquanto que à Dissertação de Mestrado ou Trabalho de Projecto são atribuídos 50 créditos ECTS, correspondendo 1 crédito ECTS a 27 horas de trabalho.

À conclusão e aprovação no 1º ano curricular, com atribuição de 60 créditos, corresponderá uma Pós-Graduação (não conferente a Grau).

[2] MSIS 2006: Model Curriculum and Guidelines for Graduate Degree programs in Information Systems (http://cis.bentley.edu/htopi/MSIS2006.pdf)

Sendo que, para a obtenção do grau de Mestre o estudante deverá realizar um total de 120 créditos com uma duração de 4 semestres lectivos.

O conjunto de áreas científicas e respectivos créditos que integram a estrutura curricular são as apresentadas no quadro 2.

Quadro 2 – Áreas Científicas e Créditos necessários para obtenção do grau/diploma

Áreas Científicas	Sigla	CRÉDITOS	
		Obrigatórios	Optativos
Contabilidade	C	6	-
Finanças	F	6	-
Gestão	G	6	-
Gestão de Recursos Humanos	GRH	6	-
Sistemas e Tecnologias de Informação	STI	96	-
TOTAL		120	-

Distribuição das horas de trabalho por ano curricular e por Unidade Curricular.

Tabela 1 – Distribuição de horas de trabalho

	Horas de contacto (TP)	**Orientação Tutória**	**Investigação**	**Estudo**	**Trabalho (Campo/ Outros)**	**Avaliação**	**Horas de trabalho total**
1º ANO							
…	…	…	…	…	…	…	…
Auditoria e Continuidade do Negócio	45	20	32	40	22	3	162

Nota: Distribuição das horas de trabalho da Unidade Curricular de Auditoria e Continuidade do Negócio para a parte lectiva do Mestrado em Sistemas de Informação Organizacionais

2.4. Plano de Estudos

No 1º ano do curso existem 4 unidades curriculares nas áreas fundamentais de gestão e 6 unidades curriculares da especialidade em STI. Deste modo, procura-se dotar os estudantes no 1º ano de um aprofundamento dos conhecimentos gerais de gestão, designadamente na área de Comportamento Organizacional, Informação Financeira, Inovação, Estratégia e Competitividade e Gestão do Risco, bem como na especialidade com as unidades curriculares de Gestão das Tecnologias de Informação e Comunicação, Segurança da Informação, Estratégia em Sistemas de Informação, Sistemas de Informação Organizacionais, Teoria e Gestão da Qualidade em Projectos de Sistemas de Informação e Auditoria e Continuidade do Negócio.

O 2º ano curricular está totalmente direccionado para a investigação na área da especialidade, possuindo no 3º semestre uma Unidade Curricular de Seminário, destinada a abordar as metodologias de investigação na área dos Sistemas de Informação, com o objectivo de proporcionar o debate e o conhecimento dos paradigmas e tecnologias emergentes, preparando o início dos trabalhos de investigação aplicada que se iniciarão neste semestre e terão continuidade no semestre subsequente na Unidade Curricular de Dissertação de Mestrado, do Trabalho de Projecto ou do Estágio Curricular.

O 4º Semestre será totalmente dedicado ao trabalho de investigação e de desenvolvimento conducentes à elaboração da Dissertação de Mestrado, do Trabalho de Projecto ou do Estágio Curricular, com atribuição de um total de 50 créditos (20 créditos no 3º semestre e 30 créditos no 4º semestre).

2.5. Calendário Escolar

Calendário 2013-14_Impar&Par - MSIO

Mestrado em Sistemas de Informação Organizacionais

7ª Edição - 2013-2015

Calendário Lectivo do 1º ano/2º semestre

Aulas (inclui Avaliação Contínua)

Março de 2014

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª
-	-	-	-	-	-	-	-	-	-	-	-	-	-	P	-	-	P	-	P	-	P	-	-	P	-	P	-	P	-	-

Abril de 2014

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	F	19	P	21	22	23	24	25	26	27	28	29	30
3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª
P	-	P	-	M	-	-	M	-	M	-	P	-	-	P	-	P	F	-	P	-	-	-	-	F	-	-		M	M

Maio de 2014

F	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S
F	-	M	-	-	P	-	P	-	P	-	-	P	-	P	-	P	-	-	P	-	P	-	P	-	-	AC	-	AC	-	AC

Junho de 2014

1	2	3	4	5	6	7	8	9	F	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª
-	-	AC	-	AC	-	AC	-	-	F	P	P	-	P	-	-	P	-	M	-	P	-	-	P	-	P	-	P	-	-

Julho de 2014

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª	6ª	S	D	2ª	3ª	4ª	5ª
M	-	P	-	P	-	-	M	-	P	-	P	-	-	M	-	P	-	P	-	-	AC	-	AC	-	AC	-	-	AC	-	-

Legenda

Estratégia em Sistemas de Informação	Prof. José Rascão	Exame Época Especial	EE	
Gestão do Risco	Prof.ª Teresa Alves	Exame Época Recurso	ER	
Teoria e Gestão da Qualidade em Projectos de SI	Prof.???	Aulas Presenciais	P	
Sistemas de Informação e Organizações	Prof. Francisco Cachatra	Aulas Moodle	M	Acompanhamento de Trabalhos
Auditoria e Continuidade do Negócio	Prof.ª Leonilde Reis	Avaliação Contínua	AC	

Avaliação Final (Época de Recurso e Época Especial)

Setembro de 2014

Exames de Recurso	5	6	7	8	9	10
	6ª	S	D	2ª	3ª	4ª
	ER	ER		ER	ER	ER

Setembro de 2014

Exames de Época Especial	12	16	17	18	19
	6ª	3ª	4ª	5ª	6ª
	EE	EE	EE	EE	EE

Observações

1) As aulas que se realizem aos sábados, iniciam-se às 09h00m e terminam às 13h30m.

2) As aulas que se realizem nos dias úteis, iniciam-se às 18h30m e terminam às 23h00m.

3) Qualquer das aulas presenciais tem previsto um intervalo de 30 m.

4) As datas e horários dos Exames de Época Especial apenas serão divulgados no início de Setembro, dado ser obrigatória a inscrição prévia.

5) Caso exista necessidade, as aulas presenciais podem ser trocadas com as aulas moodle.

3. Finalidade e Objectivos

A Unidade Curricular de Auditoria e Continuidade do Negócio tem por finalidade principal sensibilizar os estudantes para a importância da Auditoria de Sistemas de Informação e do Planeamento da Continuidade do Negócio em contexto organizacional.

Pretende-se dotar os estudantes de conceitos, métodos e ferramentas subjacentes à temática da Auditoria de Sistemas de Informação e ainda de conceitos no domínio da Continuidade do Negócio, bem como, transmitir o conhecimento de Normas/*Standards* de suporte a actividade.

São objectivos específicos da Unidade Curricular:

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 continuidade do negócio nas organizações.

09 - Conhecer e compreender as práticas instituídas nas organizações na actividade 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.

4. Conteúdos Programáticos

Nesta secção apresentam-se os conteúdos programáticos da Unidade Curricular de Auditoria e Continuidade do Negócio. Para a sua determinação considerou-se que os estudantes que frequentarão o Mestrado de Sistemas de Informação Organizacionais não possuirão, na sua generalidade, bases significativas em sistemas e tecnologias de informação, por serem oriundos de diversas licenciaturas. Esta constatação tem vindo a ser reforçada ao longo das edições de mestrado já realizadas.

Neste pressuposto, o programa contém conteúdos sobre os conceitos base de auditoria em sistemas de informação e de continuidade do negócio. Considerando o domínio do mestrado e a opinião dos ex-estudantes sobre as suas necessidades profissionais, decidiu-se refletir práticas organizacionais instituídas, e incluir as práticas utilizadas por parte das prestadoras de serviços no domínio da temática, bem como o estudo das Normas/*Standards*. Abaixo apresenta-se o programa da Unidade Curricular:

1 AUDITORIA
- 1.1 Conceitos
- 1.2 Tipos de Auditoria
- 1.3 Processo de Auditoria
- 1.4 Objectivos e Âmbito
- 1.5 Impacto da Auditoria
- 1.6 Fases de uma Auditoria
- 1.7 Características e competências do Auditor de Sistemas de Informação
- 1.8 Auditoria em Sistemas de Informação
  - 1.8.1 Finalidade
  - 1.8.2 Recursos Utilizados
  - 1.8.3 Técnicas e Ferramentas
  - 1.8.4 Relatórios de Auditoria e Documentação
- 1.9 Normas/*Standards*

2 PLANEAMENTO DA CONTINUIDADE DO NEGÓCIO

2.1 Conceito de Continuidade do Negócio
2.2 Evolução/História
2.3 Importância do Planeamento da Continuidade do Negócio
2.4 Necessidade e Objectivos
2.5 Definição do âmbito do Plano de Continuidade do Negócio
2.6 Caracterização das decisões envolvidas em processos desta natureza
2.7 Características e Componentes
2.8 Equipas e Desenvolvimento
2.9 Fases de Implementação
2.10 Importância dos Testes
2.11 Manutenção do Plano
2.12 Definição de Políticas de Recuperação
2.13 Definição das Estratégias de Recuperação para a organização
2.14 Normas/*Standards*

O ponto 1. do programa tem por objectivo contextualizar a problemática de auditoria de sistemas de informação em contexto organizacional. Pretende-se assim estudar as fases de uma auditoria, caracterizar recursos, técnicas, ferramentas e documentação de suporte. São também objecto de estudo as Normas/S*tandards* de, suporte à actividade.

O ponto 2. do programa tem como objectivo contextualizar a problemática da Continuidade do Negócio, em que são abordados as fases de implementação, testes e manutenção do plano. A definição de políticas e estratégias de recuperação face à especificidade da organização são também abordadas. São também objecto de estudo as Normas/S*tandards* de suporte à actividade.

5. Plano de Execução Pedagógica

Nesta secção, é identificada cada uma das 11 sessões de 4 horas previstas para a Unidade Curricular de Auditoria e Continuidade do Negócio e tipificada a bibliografia principal de suporte aos assuntos abordados. A descrição completa da bibliografia é apresentada em lista própria na última secção deste relatório.

As sessões que constituem o plano sequencial das aulas da Unidade Curricular são apresentadas na tabela abaixo.

Tabela 2: Sessões da unidade curricular Auditoria e Continuidade do Negócio

Sessão	**Título**	**Tipo**	**Bibliografia Principal**
S1	0 - Apresentação I - Auditoria em Sistemas de Informação	Teórica	**[1], [4], [6], [8]**
S2	I - Auditoria em Sistemas de Informação	Teórica	**[7], [9], [24], [41], [43]**
S3	II - Continuidade do Negócio	Teórica	**[10], [11], [20], [35]**
S4	II - Continuidade do Negócio	Teórica	**[21], [26], [27], [28], [45], [55]**
S5	I - Auditoria em Sistemas de Informação	Teórica/Prática	**[24]**
S6	I - Auditoria em Sistemas de Informação	Teórica/Prática	**[24]**
S7	II - Continuidade do Negócio	Teórica/Prática	**[26], [27], [28]**

S8	II - Continuidade do Negócio	Teórica/Prática	**[26], [27], [28]**
S9	I - Auditoria em Sistemas de Informação II - Continuidade do Negócio	Teórica/Prática	**[1], [4], [6], [7], [8], [9], [10], [11], [20], [21], [24], [26], [27], [28], [35], [41], [43], [45], [55]**
S10	I - Auditoria em Sistemas de Informação II - Continuidade do Negócio	Teórica/Prática	**[1], [4], [6], [7], [8], [9], [10], [11], [20], [21], [24], [26], [27], [28], [35], [41], [43], [45], [55]**
S11	I - Auditoria em Sistemas de Informação II - Continuidade do Negócio	Teórica/Prática	**[1], [4], [6], [7], [8], [9], [10], [11], [20], [21], [24], [26], [27], [28], [35], [41], [43], [45], [55]**

Neste plano das sessões da Unidade Curricular é evidente que prevalecem as sessões do tipo teórico/prática sobre as sessões teóricas, pois existe como estratégia subjacente à Unidade Curricular o estudo de casos práticos, bem como o estudo de práticas organizacionais instituídas nas organizações da região, uma vez que é proposto aos estudantes a elaboração de um trabalho individual realizado em contexto organizacional.

Para cada uma das sessões tipificadas apresentam-se os respectivos objectivos.

S1: 0 - Apresentação; I - Auditoria em Sistemas de Informação

a) Conhecer o contexto e os objectivos da Unidade Curricular assim como o seu conteúdo programático, referências e sistema de avaliação;
b) Conhecer e compreender os principais conceitos e mais-valias associados à auditoria de sistemas de informação nas organizações.

S2: I - Auditoria em Sistemas de Informação

a) Conhecer e compreender os principais conceitos da problemática de auditoria de sistemas de informação, estudar as fases de uma auditoria e caracterizar recursos, técnicas, ferramentas e relatório de auditoria, bem como documentação de suporte.
b) Conhecer e saber utilizar as Normas/*Standards* de suporte à actividade.

S3: II - Continuidade do Negócio

a) Conhecer e compreender os principais conceitos da problemática da continuidade do negócio. Pretende-se assim abordar os conceitos que caracterizam a actividade, a avaliação do risco, as aplicações criticas, as estratégias de recuperação e os contratos de prestação de serviço.

b) Conhecer e compreender os principais conceitos e mais-valias associados à continuidade do negócio em contexto organizacional.

S4: II - Continuidade do Negócio

a) Conhecer e compreender os principais conceitos da problemática da Continuidade do Negócio. Pretende-se abordar os conceitos subjacentes ao planeamento, definição do âmbito e caracterização das decisões envolvidas no processo.
b) Conhecer e saber utilizar as Normas/*Standards* de suporte à actividade.

S5: I - Auditoria em Sistemas de Informação

b) Conhecer e saber utilizar as Normas/Standards de suporte à actividade, tendo como objectivo a análise, debate e resolução de um caso prático.
b) Saber definir um plano de auditoria, definir objectivos, estratégias, recursos a utilizar e mencionar as técnicas adoptadas e respectivas ferramentas.

S6: I - Auditoria em Sistemas de Informação

b) Conhecer e saber utilizar as Normas/*Standards* de suporte à actividade, tendo como objectivo a análise, debate e resolução de um caso prático.
b) Saber definir um plano de auditoria, definir objectivos, estratégias, recursos a utilizar, e técnicas a adoptar e respectivas ferramentas.

S7: II - Continuidade do Negócio

a) Conhecer e saber utilizar as Normas/*Standards* de suporte à actividade, tendo como objectivo a análise, debate e resolução de um caso prático.
b) Saber realizar a análise das vulnerabilidades, riscos e ameaças.
c) Saber especificar as decisões envolvidas na definição de políticas de mitigação do risco.

S8: II - Continuidade do Negócio

a) Conhecer e saber utilizar as Normas/*Standards* de suporte à actividade, tendo como objectivo a análise, debate e resolução de um caso prático.
b) Saber delinear e propor estratégias de recuperação.
c) Saber elaborar planos de continuidade do negócio face às especificidades das organizações.

S9: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

a) Realizar um teste teórico abordando as temáticas leccionadas na Unidade Curricular.

S10: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

a) Realizar a apresentação e discussão individual dos trabalhos desenvolvidos em contexto organizacional.
b) Apresentar a caracterização da organização em estudo.
c) Apresentar as Normas/*Standards* de suporte, bem como os controlos a aplicar.
d) A apresentar propostas de solução/optimização face aos problemas diagnosticados.

S11: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

a) Realizar a apresentação e discussão individual dos trabalhos desenvolvidos em contexto organizacional.
b) Apresentar a caracterização da organização em estudo.
c) Apresentar as Normas/*Standards* de suporte bem como os controlos a aplicar.
d) A apresentar propostas de solução/optimização face aos problemas diagnosticados.

6. Comparação com outras Instituições

Nesta secção procura-se analisar e comparar conteúdos de Unidade Curriculares de mestrados relacionadas com Sistemas de Informação, de outras instituições portuguesas e ainda de instituições estrangeiras. Da pesquisa efectuada, seleccionou-se um conjunto de programas para possibilitar a comparação mais detalhada, realçando-se designadamente a similitude das designações e dos respectivos títulos dos conteúdos programáticos. Destes, destacamos, a título de exemplo, além dos dois casos de Instituições de Ensino Superior (IES) nacionais, os casos da Alemanha, Bélgica, Espanha, Grécia, Hungria, Itália, Reino Unido e Suíça, entre outros.

Portuguesas

O Mestrado em Sistemas de Informação Organizacionais tem designação única em Portugal. Esta constatação não depende de pesquisas na Internet. É uma constatação real, a partir da lista completa de Mestrados existentes em Portugal disponível na Direcção-Geral do Ensino Superior (DGES). Contudo foi possível obter alguma similaridade nacional no que se refere aos cursos:

- Universidade do Minho. Portugal. http://• msi.dsi.uminho.pt
- Instituto Politécnico de Santarém. Portugal. http://www.esg.ipsantarem.pt/ensino/mestrados/msig/mestrado_sig_plano.htm

Estrangeiras

Para a comparação do ciclo de estudos realizou-se uma pesquisa no sentido de analisar as unidades curriculares incluídas nessas estruturas.

• *University of Münster*. Alemanha. http://www.is.uni-muenster.de/
• *University of Amsterdam*. Holanda. http://www.english.uva.nl/start.cfm
• *Katholieke Universiteit Leuven*. Bélgica. http://www.kuleuven.be
•*Universidad de Oviedo*. Espanha. http://directo.uniovi.es/postgrado/cabecera_ep.asp?Curso=2006&IdPrograma=2004
• *University of Macedonia – Economic and Social Sciences*. Grécia. http://www.uom.gr/index.php?tmima=103&newlang=eng&categorymenu=3
• *Central European University*. Hungria. http://www.ceubusiness.com
• *Kingston University*. Reino Unido. http://cism.Kingston.ac.uk/mid.htm
• *Cranfield University*. Reino Unido. http://www.cranfield.ac.uk
• *Bournemouth University*. Reino Unido. http://home.bournemouth.ac.uk/
• *Université di Laussane – Hautes Etudes Commerciales* (HEC). Suíça. http://www.hec.unil.ch/hec/masters/msc
• *University of Neuchatel*. Suíça. http://www2.unine.ch/

A criação da estrutura curricular de 2º ciclo do Mestrado em Sistemas de Informação Organizacionais teve também em consideração o modelo de referência apresentado por entidades reconhecidas internacionalmente, nomeadamente a *Association for Information Systems* (AIS) e a *Association for Computing Machinery* (ACM), e contemplou as sugestões emanadas de reuniões com organizações da região, fruto da estreita parceria para com a Escola Superior de Ciências Empresarias do Instituto Politécnico de Setúbal.

Actualmente, e de acordo com Curriculum *Guidelines for Undergraduate Degree Programs in Information Systems* (IS 2010) da *Association for Computing Machinery* (ACM) e da *Association for Information Systems* (AIS) considera-se que os conteúdos programáticos da Unidade Curricular revestem-se de particular interesse no contexto do Mestrado em Sistemas de Informação Organizacionais.

7. Estratégias de Ensino-Aprendizagem

As sessões da Unidade Curricular de Auditoria e Continuidade do negócio são de dois tipos: Teóricas e Teórico/Práticas. As aulas teóricas proporcionaram conhecimento e fomentam a investigação. As sessões Teórico/Práticas permitirão aos estudantes a realização de exercícios práticos no sentido de procurar a resolução de problemas descritos, tendo como suporte a utilização de normas internacionais. Pretende-se ainda o desenvolvimento de um trabalho prático no sentido de fomentar a pesquisa e o sentido crítico dos estudantes face a problemas diagnosticados em contexto organizacional.

Seguidamente, apresentam-se as estratégias de ensino-aprendizagem para cada uma das onze sessões da Unidade Curricular.

S1: Apresentação; Auditoria em Sistemas de Informação

Esta sessão é de cariz teórico e tem dois objectivos. Em primeiro lugar, dar a conhecer aos estudantes uma visão global da Unidade Curricular. Por outro lado, introduzir os principais conceitos e mais-valias associados à auditoria de sistemas de informação nas organizações.

A sessão termina com um debate acerca das temáticas abordadas. O docente sugere que os conceitos abordados devem ser reforçados com a leitura posterior das referências de suporte indicada para esta sessão.

Nesta sessão são ainda apresentadas as regras de apresentação do tema do trabalho a desenvolver em contexto organizacional.

Bibliografia Principal

Amaral, L., Magalhães, R., Morais, C., Serrano, A., Zorrinho, C., (2005), *Sistemas de Informação Organizacionais*, Edições Silabo.

Carneiro, A., (2009), *Auditoria e Controlo de Sistemas de Informação*, FCA.

Cascarino, R., (2012), *Auditor's Guide to IT Auditing*, *Second Edition*, John Wiley & Sons.

Champlain, J., (2003), *Auditing Information Systems, Second Edition*, Jack Champlain editor.

Bibliografia Complementar

Carneiro, A., (2004), *Auditoria de Sistemas de Informação*, 2ª Edição Aumentada, Lisboa, FCA.

IPQ (2003), NP EN ISO 19011:2003 - *Linhas de orientação para auditorias a sistemas de gestão da qualidade e/ou de gestão ambiental*: Documentos impressos. Lisboa: Instituto Português da Qualidade.

ISO (2012), ISO/IEC TS 17021-2:2012 - *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems*: Documentos impressos. Geneva: International Organization for Standardization.

Pathak, J., (2005), *Information Technology Auditing: An Evolving Agenda*, Springer.

Piattini, M., (2000), *Auditing Information Syste*ms, Mario Piattini editor.

S2: I - Auditoria em Sistemas de Informação

Esta sessão também é de cariz teórico e tem como objectivo no contexto da problemática de auditoria de sistemas de informação estudar as fases de uma auditoria e caracterizar recursos técnicos, ferramentas e relatório de auditoria, bem como documentação de suporte. São também objecto de estudo as Normas/S*tandards* nacionais e internacionais de suporte à actividade.

A sessão termina com um debate acerca das temáticas abordadas. A análise das normas em estudo também é objectivo desta sessão. O docente sugere que os conceitos abordados devem ser reforçados com a leitura posterior das referências de suporte indicada para esta sessão.

Bibliografia Principal

Chaplain, J. J., (2000), *Auditing Information Systems*, Wiley - 2nd Edition.

Davis, Chris et al, (2007), *IT Auditing – Using Controls to Protect Information Assets*, McGraw-Hill Osborne.

Musaji, Y. F., (2000), *Auditing and Security: AS/400, NT, UNIX, Networks, and Disaster Recovery Plans*, Wiley.

Pathak, J.,(2005), *Information Technology Auditing: An Evolving Agenda*, Springer.

Piattini, M., (2000), *Auditing Information Systems*, Mario Piattini editor.

Bibliografia Complementar

IIARF (1991), *Systems Auditability and Control - Audit and Control Environment*, Module 2*:* Documentos impressos. Florida: Institute of Internal Auditors Research Foundation.

IIARF (1991), *Systems Auditability and Control - Contingency Planning*, Module 10*:* Documentos impressos. Florida: Institute of Internal Auditors Research Foundation.

IPQ (2003), NP EN ISO 19011:2003 - *Linhas de orientação para auditorias a sistemas de gestão da qualidade e/ou de gestão ambiental*: Documentos impressos. Lisboa: Instituto Português da Qualidade.

ISO (2012), ISO/IEC TS 17021-2:2012 - *Conformity assessment -- Requirements for bodies providing audit and certification of management systems - Part 2: Competence requirements for auditing and certification of environmental management systems*: Documentos impressos. Geneva: International Organization for Standardization.

S3: II - Continuidade do Negócio

Esta sessão também é de cariz teórico e tem como objectivo compreender a problemática da continuidade do negócio, sendo abordados os conceitos subjacentes à actividade bem como a realização de avaliação do risco, a identificação das aplicações críticas, a definição de estratégias de recuperação e a análise de contratos de prestação de serviço.

A sessão termina com um debate acerca das temáticas abordadas. O docente sugere que os conceitos abordados devem ser reforçados com a leitura posterior das referências de suporte indicada para esta sessão.

Bibliografia Principal

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

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

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

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

Bibliografia Complementar

BCM (2008), *Business Continuity Management - Good Pratice 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.

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

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.

Hugos, M., Hulitzky, D., (2011). *Business in the Cloud, what every business needs to now 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 (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.

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

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

Trowbridge, B., (2011). *Cloud Sourcing the Corporation*. Estados Unidos da América e Reino Unido. Alsbridge.

S4: II - Continuidade do Negócio

Esta sessão também é de cariz teórico e tem como objectivo, no contexto da problemática da continuidade do negócio, abordar as fases de implementação, testes e manutenção do plano. Pretende-se assim abordar os conceitos subjacentes ao planeamento, definição do âmbito e caracterização das decisões envolvidas no processo. São também objecto de estudo as Normas/*Standards* nacionais e internacionais de suporte à actividade.

Nesta sessão procede-se à apresentação do tema do trabalho a realizar. Serão apresentadas as organizações que são objecto de estudo bem como os principais problemas subjacentes à temática seleccionada. Esta caracterização terá uma ponderação de 20%.

Bibliografia Principal

Preen, J., (2012), *Business Continuity Exercises and Tests. Delivering Successful Exercise Programmes with ISO 22301*. Second Edition, Jim Preen, BSI.

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

Snedaker, S., (2013), *Business Continuity and Disaster Recovery Planning for IT Professionals*, Second Edition, Susan Snedaker.

Wallace, M., Webber, L., (2011), *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, Michael Wallace and Lawrence Webber.

Watters, J., (2010), *The Business Continuity Management Desk Reference: Guide to Business Continuity Planning, Crisis Management and IT Disaster Recovery*, Business Leverage.

Bibliografia Complementar

Ferreira, D., Reis, L., 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, Cordoba, Espanha, 2011.

Ferreira, D., Reis, L., 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, 2013.

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.

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

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

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.

Parker, T. R., (2001), *Information Security Risk Analysis*, Auerbach Publications.

S5: I - Auditoria em Sistemas de Informação;

Esta é a primeira sessão de cariz prático, tendo como objectivo a análise, debate e resolução de um caso prático. Para a estruturação do caso prático os estudantes deverão definir um plano de auditoria, definindo objectivos, estratégias, recursos a utilizar e mencionar as técnicas adoptadas e respectivas ferramentas.

O caso será realizado por cada estudante dentro da sessão, com acompanhamento do docente. Considera-se fundamental a participação de cada estudante neste exercício de resolução e análise de um problema organizacional, uma vez que o trabalho final realizado em contexto organizacional poderá versar sobre esta temática.

Bibliografia Principal

IPQ (2012), NP EN ISO 19011:2012 - *Linhas de orientação para auditorias a sistemas de gestão*: Documentos impressos. Lisboa: Instituto Português da Qualidade.

Bibliografia Complementar

ISO (2012), ISO/IEC TS 17021-2:2012 - *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems*: Documentos impressos. Geneva: International Organization for Standardization.

S6: I - Auditoria em Sistemas de Informação

Esta sessão de cariz prático, tem como objectivo a resolução do caso prático. Nesta sessão debatem-se em conjunto a forma como foi estruturada a resolução do caso prático, nomeadamente nas vertentes de plano de auditoria, objectivos, estratégias, recursos, técnicas e respectivas ferramentas. A proposta de resolução do caso terá como suporte orientador a utilização de Normas/*Standards*.

O caso continua a ser realizado por cada estudante dentro da sessão, com acompanhamento do docente. Antes da sessão estar concluída é criado um espaço de debate onde são discutidas as diversas abordagens e soluções.

Bibliografia Principal

IPQ (2012), NP EN ISO 19011:2012 - *Linhas de orientação para auditorias a sistemas de gestão*: Documentos impressos. Lisboa: Instituto Português da Qualidade.

Bibliografia Complementar

ISO (2012), ISO/IEC TS 17021-2:2012 - *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems*: Documentos impressos. Geneva: International Organization for Standardization.

S7: II - Continuidade do Negócio

Esta é a primeira sessão de cariz prático, no domínio da temática de continuidade do negócio e tem como objectivo a análise, debate e resolução de um caso prático. Para a estruturação do caso prático os estudantes deverão definir o âmbito da área em estudo, efectuar uma avaliação dos riscos, analisar as aplicações críticas, definir estratégias de recuperação e, analisar contratos de prestação de serviço.

O caso será realizado por cada estudante dentro da sessão, com acompanhamento do docente. Considera-se fundamental a participação de cada estudante neste exercício de resolução e análise de um problema organizacional, uma vez que o trabalho final realizado em contexto organizacional poderá versar sobre esta temática.

Bibliografia Principal

ISO (2006), BS 25999-1:2006 – *Business continuity management – part 1: Code of practice*: Documentos impressos. Geneva: International Organization for Standardization.

ISO (2007), BS 25999-2:2007 – *Business continuity management – part 2: Specification*: Documentos impressos. Geneva: International Organization for Standardization.

ISO (2013), ISO/IEC 27002:2013 *Information Technology – Security Techniques – Code of Practice for Information Security Management*: Documentos impressos. Geneva: International Organization for Standardization.

Bibliografia Complementar

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 (2005), ISO/IEC 27001:2005(E) – *Information Technology - Security Techniques - Information Security Management Systems - Requirements*: 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.

ISO (2007), ISO/PAS 22399:2007 - *Societal security - Guideline for incident preparedness and operational continuity management*: 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 (2008), ISO/IEC 27005:2008(E) – *Information Technology - Security Techniques - Information Security Risk Management*: Documentos impressos. Geneva: International Organization for Standardization.

S8: II - Continuidade do Negócio

Esta sessão de cariz prático, tem como objectivo a resolução do caso prático. Nesta sessão, em conjunto debatem-se a forma como foi estruturada a resolução do caso prático, nomeadamente nas vertentes de análise das vulnerabilidades, riscos e ameaças. Considera-se fundamental especificar as decisões envolvidas e definir políticas e estratégias de recuperação. A proposta de resolução do caso terá como suporte orientador a utilização de Normas/*Standards*.

O caso continua a ser realizado por cada estudante dentro da sessão, com acompanhamento do docente. Antes de a sessão estar concluída é criado

um espaço de debate onde são discutidas as diversas abordagens e soluções.

Bibliografia Principal

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*, vol.8, 43-51.

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

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.

ISO (2007), ISO/PAS 22399:2007 - *Societal security - Guideline for incident preparedness and operational continuity management*: 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.

ISO (2013), ISO/IEC 27001:2013 - *Information technology -- Security techniques - Information security management systems -- Requirements*: Documentos impressos. Geneva: International Organization for Standardization.

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

Reis, M. 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, M. 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., Integrated Planning of Information Systems and Contingency and Recovery. *In International Conference on Enterprise Information Systems*, Universidade de Castilla-La Mancha, Spain, 3-6, April de 2002.

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.

Bibliografia Complementar

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, Cordoba, 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, 2012.

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

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

S9: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

É objectivo desta sessão a realização de um teste teórico abordando as temáticas leccionadas na Unidade Curricular. O teste teórico aborda a totalidade das temáticas da Unidade Curricular e terá uma ponderação de 20%. Um exemplo de Exame Teórico está disponível no Anexo 2 deste documento.

A segunda componente da sessão destina-se à realização de um ponto de situação dos trabalhos que estão a ser desenvolvidos em contexto organizacional. O docente explicita a importância do cumprimento das regras subjacente à elaboração do relatório de acordo com a estrutura e os tópicos definidos em documento elaborado para o efeito. O relatório deverá ser entregue em papel e o ficheiro deverá ser submetido numa área criada para o efeito no *Moodle*. As datas foram previamente acordadas e agendadas.

Bibliografia Principal

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

Bibliografia Complementar

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

S10: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

Nesta sessão, inicia-se a apresentação e discussão individual dos trabalhos desenvolvidos em contexto organizacional. Na sequência das regras previamente apresentadas considera-se fundamental, no que se refere à informação a apresentar no domínio da caracterização da organização em estudo, a inclusão dos seguintes parâmetros: caracterização da actividade da organização, estratégia de negócio, e caracterização dos sistemas de informação e comunicação. No domínio da problemática em estudo considera-se que se deve definir a temática a estudar, o âmbito, as Normas/*Standards* de suporte, bem como os controlos a aplicar. A apresentação de proposta de solução/optimização face aos problemas diagnosticados devem ser suportados em *template* das Normas/*Standards*. O desempenho dos estudantes no trabalho prático terá uma ponderação de 60% na sua classificação final da Unidade Curricular.

Bibliografia Principal

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

Bibliografia Complementar

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

S11: I - Auditoria em Sistemas de Informação; II - Continuidade do Negócio

Nesta sessão conclui-se a apresentação e discussão individual dos trabalhos desenvolvidos em contexto organizacional. Na sequência das regras previamente apresentadas considera-se fundamental, no que se refere à informação a apresentar no domínio da caracterização da organização em estudo a inclusão dos seguintes parâmetros: caracterização da actividade da organização, estratégia de negócio, e caracterização dos sistemas de informação e comunicação. No domínio da problemática em estudo considera-se que se deve definir a temática a estudar, o âmbito, as Normas/*Standards* de suporte, bem como os controlos a aplicar. A apresentação de proposta de solução/optimização face aos problemas diagnosticados devem ser suportados em *template* das Normas/*Standards*. O desempenho dos estudantes no trabalho prático terá uma ponderação de 60% na sua classificação final da Unidade Curricular.

Bibliografia Principal

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

Bibliografia Complementar

Nesta sessão a bibliografia de suporte é a totalidade abordada na Unidade Curricular e anteriormente exposta.

8. Sistema de Avaliação

O método de avaliação da Unidade Curricular de Auditoria e Continuidade do Negócio assenta no modelo de avaliação continua e, em caso de insucesso consistirá num exame de recurso, desde que satisfeitos os requisitos estipulados no Regulamento Pedagógico da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal.

Avaliação Continua

Nesta Unidade Curricular, a presença às aulas é obrigatória em, pelo menos 60% das aulas leccionadas, de acordo com o regulamento pedagógico da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal.

Avaliação

A avaliação de conhecimentos é constituída por:

- Apresentação do Tema do Trabalho Prático (AT)
- Apresentação e Discussão do Trabalho Prático (TP)
- Realização de Teste (T)

Nota Final = 0,20 AT + 0,60 TP + 0,20 T

As provas ocorrem de acordo com o calendário escolar estipulado para o efeito. A prova escrita incide sobre a totalidade da matéria leccionada e descrita no programa da Unidade Curricular. A duração máxima é de 120 minutos.

Este momento de avaliação destina-se aos estudantes que não obtiveram aprovação na componente de avaliação contínua. Podem também realizar avaliação de recurso os estudantes que não tenham obtido aprovação em avaliação contínua na componente do teste teórico e/ou trabalho prático.

A avaliação de recurso/época especial é constituída pela realização de um Exame Teórico e/ou Trabalho Prático.

$$\text{Nota Final} = 0{,}20\ AT + 0{,}60\ TP + 0{,}20\ T$$

9. Carga de Trabalho

A distribuição das horas de trabalho por ano curricular e por Unidade Curricular é apresentada na tabela 1.

Tabela 1 – Distribuição de horas de trabalho

	Horas de contacto (TP)	**Orientação Tutória**	**Investigação**	**Estudo**	**Trabalho (Campo/ Outros)**	**Avaliação**	**Horas de trabalho total**
1º ANO							
Gestão das Tecnologias de Informação e Comunicação	45	20	32	40	22	3	162
Comportamento Organizacional	45	20	22	40	32	3	162
Informação Financeira	45	20	22	40	32	3	162
Inovação, Estratégia e Competitividade	45	20	22	40	32	3	162
Segurança da Informação	45	20	32	40	22	3	162
Estratégia em Sistemas de Informação	45	20	32	40	22	3	162
Gestão do Risco	45	20	22	40	32	3	162
Teoria e Gestão da Qualidade em Projectos de Sistemas de Informação	45	20	32	40	22	3	162
Sistemas de Informação Organizacionais	45	20	32	40	22	3	162
Auditoria e Continuidade do Negócio	**45**	**20**	**32**	**40**	**22**	**3**	**162**

Nota: Distribuição das horas de trabalho apenas para a parte lectiva do Mestrado em Sistemas de Informação Organizacionais

A Unidade Curricular tem previstas 4 horas de aulas por sessão, de acordo com o Calendário Escolar apresentado em 2.5., num total de 45 horas. As

sessões são leccionadas de acordo com as estratégias previstas na secção de Estratégias de Ensino-Aprendizagem apresentadas na secção sete.

10. Recursos

Nesta secção consideram-se os recursos necessários para a Unidade Curricular, categorizados como recursos humanos, espaços físicos, equipamentos pedagógicos, software e meios documentais.

Recursos Humanos

A leccionação da Unidade Curricular é assegurada pela docente, a candidata ao título de Agregado. Paralelamente deverá estar disponível um funcionário não docente para apoio, nomeadamente para entregar e registar a solicitação da chave da sala.

Espaços Físicos

A leccionação da Unidade Curricular tem por base requisitos que facilite a interligação entre o docente e os estudantes. Assim será mais vantajosa a utilização de uma sala com mesas de trabalho do que um anfiteatro. A sala deverá ter um computador, videoprojector, quadro e marcadores e os exemplares das Normas/*Standards*. Devendo ainda esta sala possuir tomadas eléctricas, de modo a permitir a utilização de computadores portáteis.

Equipamentos Pedagógicos

Os equipamentos pedagógicos necessários na sala de aula incluem um quadro de escrita com marcador, computador e videoprojector.

Software

A leccionação da Unidade Curricular não exige a disponibilidade de qualquer software específico.

Meios Documentais

Os meios documentais necessários para apoio à Unidade Curricular de Auditoria e Continuidade do Negócio são livros, Normas/*Standards*, teses, dissertações, relatórios técnicos, artigos periódicos, e apontamentos da área dos sistemas e tecnologias de informação, disponíveis quer em papel, quer em suporte electrónico.

A docente disponibiliza alguns destes recursos na plataforma *Moodle* da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal. Outros documentos podem ser obtidos disponíveis no centro de documentação da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal. O acesso à *Web*, permitirá obter por exemplo teses, dissertações, Normas/*Standards* e relatórios técnicos.

11. Considerações finais

Nesta secção tecem-se algumas considerações finais e expõem-se algumas reflexões sobre a Unidade Curricular de Auditoria e Continuidade do Negócio do Mestrado em Sistemas de Informação Organizacionais da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, objecto deste relatório.

A Unidade Curricular de Auditoria e Continuidade do Negócio pretende proporcionar conhecimentos genéricos aos estudantes de auditoria em sistemas de informação e de continuidade do negócio, tendo em consideração as formações de base dos potenciais estudantes (diversas), o nível de ensino em que se insere (mestrado) e o domínio do curso (Sistemas de Informação).

Neste sentido, faz-se uma introdução relativamente abrangente em aspectos que se consideram relevantes para o contexto referido no parágrafo anterior: Tipos de Auditoria, Processo de Auditoria; Impacto da Auditoria; Fases de uma Auditoria; Características e competências do Auditor de Sistemas de Informação; Auditoria em Sistemas de Informação; Normas/Standards. Conceito de Continuidade do Negócio; Importância do Planeamento da Continuidade do Negócio; Definição do âmbito do Plano de Continuidade do Negócio; Caracterização das decisões envolvidas em processos desta natureza; Definição de Políticas de Recuperação; Definição das Estratégias de Recuperação para a organização; Normas/*Standards*.

Após o funcionamento de 7 edições da Unidade Curricular de Auditoria e Continuidade do Negócio é-se de opinião que a supracitada Unidade

Curricular constitui um importante contributo para o papel dos Sistemas e Tecnologias de Informação nas organizações. O estudo e análise das Normas/*Standards* têm constituído factor diferenciador no sentido de os estudantes terem oportunidade de reflectirem acerca das práticas organizacionais. Tem sido considerado valor acrescentado quer por parte dos estudantes, quer por parte dos responsáveis das organizações a realização de trabalhos em contexto organizacional neste domínio de conhecimento.

12. Referências de Suporte

Nesta secção apresenta-se a totalidade das referências de suporte aos conteúdos programáticos da Unidade Curricular de Auditoria e Continuidade do Negócio, incluindo quer a bibliografia principal, quer a bibliografia complementar indicada para cada uma das sessões Estratégias de Ensino-Aprendizagem. A lista da bibliografia está ordenada pelo nome dos autores.

[1] Amaral, L., Magalhães, R., Morais, C., Serrano, A., Zorrinho, C., (2005), *Sistemas de Informação Organizacionais*, Edições Silabo.

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

[3] Carneiro, A., (2004), *Auditoria de Sistemas de Informação*, 2ª Edição Aumentada, Lisboa, FCA.

[4] Carneiro, A., (2009), *Auditoria e Controlo de Sistemas de Informação*, FCA.

[5] Cascarino, R., (2007), *Auditor's Guide to Information Systems Auditing*, John Wiley Publishers.

[6] Cascarino, R., (2012), *Auditor's Guide to IT Auditing,* Second edition, John Wiley & Sons.

[7] Chaplain, J., (2000), *Auditing Information Systems*, Second Edition, John Wiley & Sons.

[8] Chaplain, J., (2003), *Auditing Information Systems*, Second Edition, Jack Champlain editor.

[9] Davis, Chris et al, (2007), *IT Auditing – Using Controls to Protect Information Assets*, McGraw-Hill Osborne.

[10] Drewitt, T., (2013), *A Manager's Guide to ISO22301: A Practical Guide to Developing and Implementing a Business Continuity Management System*.

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

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

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

[14] 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.

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

[16] 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. 4. Universidade Portucalense, Porto, 2013.

[17] 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, Cordoba, Espanha.

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

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

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

[21] 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.

[22] IIARF (1991), *Systems Auditability and Control - Audit and Control Environment, Module 2:* Documentos impressos. Florida: Institute of Internal Auditors Research Foundation.

[23] IIARF (1991), *Systems Auditability and Control - Contingency Planning, Module 10:* Documentos impressos. Florida: Institute of Internal Auditors Research Foundation.

[24] IPQ (2003), NP EN ISO 19011:2003 - *Linhas de orientação para auditorias a sistemas de gestão da qualidade e/ou de gestão ambienta*l: Documentos impressos. Lisboa: Instituto Português da Qualidade.

[25] ISO (2005), ISO/IEC 27001:2005(E) – *Information Technology - Security Techniques - Information Security Management Systems - Requirements*: Documentos impressos. Geneva: International Organization for Standardization.

[26] ISO (2005), ISO/IEC 27002:2005(E) *Information Technology – Security Techniques – Code of Practice for Information Security Management*: Documentos impressos. Geneva: International Organization for Standardization.

[27] ISO (2006), BS 25999-1:2006 – *Business continuity management – part 1: Code of practice*: Documentos impressos. Geneva: International Organization for Standardization.

[28] ISO (2007), BS 25999-2:2007 – *Business continuity management – part 2: Specification*: Documentos impressos. Geneva: International Organization for Standardization.

[29] ISO (2007), ISO/PAS 22399:2007 - *Societal security - Guideline for incident preparedness and operational continuity management*: Documentos impressos. Geneva: International Organization for Standardization.

[30] 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.

[31] ISO (2008), ISO/IEC 27005:2008(E) – *Information Technology - Security Techniques - Information Security Risk Management*: Documentos impressos. Geneva: International Organization for Standardization.

[32] 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.

[33] ISO (2012), ISO/IEC TS 17021-2:2012 - *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems*: Documentos impressos. Geneva: International Organization for Standardization.

[34] ISO (2013), ISO/IEC 27001:2013 - *Information technology -- Security techniques - - Information security management systems - Requirements*: Documentos impressos. Geneva: International Organization for Standardization.

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

[36] 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.

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

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

[39] 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.

[40] Marchini, R. (2010). *Cloud Computing: A Pratical Introduction to the Legal Issues*. 1st edition. Londres. BSI Group Headquarters.

[41] Musaji, Y. F., (2000), *Auditing and Security: AS/400, NT, UNIX, Networks, and Disaster Recovery Plans*, John Wiley & Sons.

[42] Parker, T. R., (2001), *Information Security Risk Analysis*, Auerbach Publications.

[43] Pathak, J., (2005), *Information Technology Auditing: An Evolving Agenda*, Springer.

[44] Piattini, M., (2000), *Auditing Information Systems*, Mario Piattini editor.

[45] Preen, J., (2012), *Business Continuity Exercises and Tests. Delivering Successful Exercise Programmes with ISO 22301* (Second Edition), Jim Preen, BSI.

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

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

[48] 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.

[49] 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.

[50] 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.* Universidade do Minho. Guimarães.

[51] 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.

[52] 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.

[53] Sandhu, R., (2002), *Disaster Recovery Planning*, Premier Press.

[54] Serrano, A., Jardim, N., (2007), *Disaster Recovery – Um Paradigma na Gestão da Continuidade,* FCA**.**

[55] Snedaker, S., (2013), *Business Continuity and Disaster Recovery Planning for IT Professionals*, Second Edition, Susan Snedaker.

[56] Toigo, J. W., (2003), *Disaster Recovery Planning – Preparing for the Unthinkable,* Third Edition, Prentice Hall.

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

[58] Wallace, M., Webber, L., (2011), *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, Michael Wallace and Lawrence Webber.

[59] Watters, J., (2010), *The Business Continuity Management Desk Reference: Guide to Business Continuity Planning, Crisis Management and IT Disaster Recovery*, Business Leverage.

Anexos

Anexo 1

Exemplo de Caso de

Continuidade do Negócio

Escola Superior de Ciências Empresariais
Instituto Politécnico de Setúbal

Curso: Mestrado em Sistemas de Informação Organizacionais

Ano: 1º Semestre: 2º

Objectivo: Análise da Norma ISO/IEC 27005:2008

Descrição: Para cada um dos exercícios apresentados nas alíneas seguintes tente responder tendo em conta as indicações da norma.

Notas: No caso de não possuir informação que considere ser suficiente para responder as questões apresente pressupostos.

Exercícios Específicos

1. A organização onde exerce funções na área dos sistemas de informação pretende implementar uma Gestão de Riscos na Segurança da Informação.

a) Definição do Contexto
- **i)** Objectivo
- **ii)** Defina o critério para impacto na organização
- **iii)** Defina o critério para a avaliação do risco
- **iv)** Defina o critério para a aceitação do risco
- **v)** Defina as funções e as responsabilidades

b) Avaliação do Risco na Segurança da Informação
- **i)** Identifique os activos existentes, os processos relacionados com os activos e a sua relevância
- **ii)** Identifique as ameaças, respectivos tipos e origens
- **iii)** Identifique os controlos existentes, a sua forma de implementação e estado
- **iv)** Identifique as vulnerabilidades relativas a cada activo, ameaça e controlo existente
- **v)** Identifique os cenários de incidentes com as respectivas consequências nos activos e nos processos de negócio
- **vi)** Defina o valor do impacto para cada uma das ameaças
- **vii)** Defina o valor da probabilidade para cada uma das ameaças
- **viii)** Defina o nível de risco tendo em conta o impacto e a probabilidade para cada uma das ameaças
- **ix)** Defina uma lista de riscos (por prioridades) tendo em conta o critério de avaliação

c) Tratamento do Risco na Segurança da Informação
- **i)** Defina qual o tratamento a dar aos principais riscos tendo em conta o critério de aceitação

d) Aceitação do Risco na Segurança da Informação
- **i)** Identifique quem deve ser informado e quando das actividades existentes

e) Comunicação do Risco na Segurança da Informação
- **i)** Identifique quem deve ser informado e quando das actividades existentes

f) Revisão e monitorização e melhoria do Risco na Segurança da Informação
- **i)** Identifique quais actividades e quando que devem ser revistas, monitorizadas e melhoradas

Nota: As respostas devem ser justificadas tendo em conta a sua organização. Deve dar nomes concretos (independentemente de serem reais ou não) à organização, departamentos, pessoas, responsabilidade, etc.

Anexo 2

Exemplo

de

Exame Escrito

Escola Superior de Ciências Empresariais
Instituto Politécnico de Setúbal

Curso: Mestrado em Sistemas de Informação Organizacionais

Ano: 1º Semestre: 2º Docente: Leonilde Reis

Duração do Exame: 120 minutos

O exame é individual e sem consulta. Pretende-se respostas sucintas e claras. A duração da prova é de 120 minutos. As cotações encontram-se junto às questões.

Exame Escrito

[2,0 v.] **1.** Qual a relevância de uma Auditoria de Sistemas de Informação face ao seu contexto organizacional?

[2,0 v.] **2.** Na qualidade de responsável pela realização de uma Auditoria de Sistemas de Informação, enumere justificando quais os instrumentos que utilizaria?

[2,0 v.] **3.** Enumere os factores que considera com maior relevância perante a necessidade da elaboração de um Plano de Continuidade do Negócio no contexto de uma organização internacional em que o negócio é essencialmente suportado nas TIC.

[2,0 v.] **4.** Especifique e justifique quais as estratégias de recuperação que proporia implementar tendo como pressuposto o funcionamento da organização mencionadas na questão anterior?

5. Leia atentamente o caso abaixo apresentado e responda às questões propostas, de uma forma organizada e sucinta.

Se considerar que o caso não apresenta, em sua opinião, dados suficientes para responder a determinada questão poderá ser indicado/sugerido algum pressuposto.

"A organização Biblioteca Lusa S.A. tem como objectivo permitir a divulgação de informação relacionada com Portugal, Europa e o Mundo nas mais diversas áreas.

A organização com cinco anos de existência, tem espalhado pelas principais cidades portuguesas um espaço (inferior ao que existe na sede em Lisboa) que tem as mesmas valências no que toca a documentação digital, o mesmo não se verifica na documentação não digital.

Os serviços administrativos estão centralizados na sede. Nos outros espaços apenas existe o serviço prestado aos utentes.

Alguns deste espaços não se encontram nas melhores condições, uns por estarem em edifícios mais antigos (sem as condições que seriam espectáveis), alguns no rés-do-chão, sem ar condicionado, …

Em termos de Sistemas, existe uma plataforma baseada nas soluções Microsoft.

. Máquinas - Servidores – *Windows 2003 Server* - aplicações (IBM) e correio electrónico e site web (HP) e de ficheiros ("Linha Branca");

. Máquinas - Clientes – *Windows XP/Windows* 2007 – aplicações colaborativas ("Linha Branca");

Em termos de hardware, para além dos computadores há fotocopiadoras, impressoras, impressoras de cartões e etiquetas e leitores de códigos de barras (utentes e empréstimos).

Em termos de assistência técnica esta é suportada por uma organização externa, existindo um SLA. Este nunca foi revisto e a renovação do contracto é efectuada de forma automática. Também não existem registos das intervenções efectuadas quer na sede, quer nos outros espaços.

No que se refere à infra-estrutura de rede, existe uma rede *Ethernet* (em todos os computadores) com ligação à internet a 50 Mbps e respectiva *Firewall* com o principal objectivo de providenciar à comunidade o acesso quer à internet que a base de dados de conhecimento. Existem protocolos específicos renovados todos os anos com as respectivas entidades. No entanto, nos últimos tempos tem havido queixas, nomeadamente acessos lentos e serviços indisponíveis.

Salienta-se que existem outros serviços fundamentais, como o empréstimo de documentação, livros, revistas; a possibilidade de impressão e fotocópia de documentos.

Em termos de *layout* dos espaços, estes podem ser considerados *open space* estes estão divididos (em termos funcionais) em duas grandes áreas: pública (de consulta e estudo) em que os utentes têm acesso e uma área administrativa que é de acesso restrito (reservada somente a funcionários). A divisão física é feita através de biombos.

Os funcionários na sua maioria trabalham em computadores *desktop* sem controlo de acesso ao computador.

Existe uma política de *backups*, mas não existe documentação."

[7,0 v.] **a)** Na qualidade de responsável pelo Departamento de Sistemas de Informação, foi-lhe solicitado pela administração a elaboração de um Plano de Auditoria aos Sistemas de Informação.

Descreva o Plano de Auditoria, justificando as opções, tendo em conta os seguintes aspectos: objectivo, âmbito, critérios, auditoria interna/externa, equipa, metodologia (técnicas/ferramentas) e cronograma.

[5,0 v.] **b)** Na qualidade de responsável pelo Departamento de Sistemas de Informação, foi-lhe solicitado pela administração a elaboração de um Plano de Continuidade do Negócio (PCN).

Identifique os aspectos fundamentais que um PCN deve endereçar, justificando as opções.