

PROJETO FINAL DE CURSO

APLICAÇÃO DA NORMA ISO/IEC 27002:2005 NA ISS FACILITY SERVICES PORTUGAL

INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - CODE OF PRACTICE

FOR INFORMATION SECURITY MANAGEMENT



Resumo

Atualmente, a generalidade das organizações, independentemente do sector onde atuam, tornaram-se fortemente dependentes dos seus sistemas informáticos para gerir as suas atividades e suportar a tomada de decisão.

Gestores de topo, preocupam-se com as dramáticas consequências que apresenta para a sua competitividade, um acidente que afete o funcionamento dos seus sistemas informáticos e a informação que processam.

Sensibilizada com o tema, a ISS *Facility Services*, pretendeu desenvolver uma análise às suas atuais políticas de segurança da informação, que proporcionasse um contributo ativo para a otimização das boas práticas de Segurança dos seus Sistemas de Informação.

Iniciando-se a partir de uma análise contextual da organização, na caracterização do serviço de gestão de tecnologias de informação e dos sistemas de informação, que estão sob a sua responsabilidade, este projeto reflete a visão e as melhores práticas correntes no que diz respeito à segurança dos sistemas de informação.

Realizado com o apoio da Norma Internacional ISO/IEC 27002:2005, adotada e reconhecida pela maioria dos países que utilizam sistemas de informação organizacionais como plataformas essenciais de desenvolvimento, dirige o seu estudo para a otimização de práticas operacionais de segurança da informação em áreas relevantes como: As Políticas de segurança, a Organização da segurança da informação, a Gestão dos recursos, a Segurança física e ambiental, a Gestão das operações e comunicações, o Controlo de acessos, a Gestão de incidentes de segurança da informação e a Gestão da continuidade do negócio.

A transparência das preocupações debatidas neste trabalho é um contributo para que a segurança da informação e dos sistemas de informação na ISS, alcance o nível adequado face às responsabilidades de garantir a confidencialidade, a integridade, e a disponibilidade da informação organizacional.

Abstract

Today, most organizations regardless of industry where they operate have become highly dependent on their computer systems to manage their activities and support the decision.

Top managers, are concerned about the dramatic consequences for their competitiveness when presented with an accident that affects the operation of their systems and information processing.

Sensitive with the topic, the ISS Facility Services, sought to develop an analysis of their current policies for information security, providing it as an active contribution to the optimization of best practices for security of its Information Systems.

Booting up from a contextual analysis of the organization, the characterization of the service of information technologies management and information systems that are under its responsibility, the project reflects the vision and current best practices in regard to the security of information systems.

Conducted with the support of the International Standard ISO/IEC 27002:2005, adopted and recognized by most countries that use organizational information systems platforms as essential for development, the study aimed to optimize the operational practices of Information Security in areas relevant such as: Security policy, Organizing information security, Asset management, Physical and environmental security, Communications and operations management, Access control, Information security incident management and Business continuity management.

The transparency of the concerns discussed in this paper is a contribution for the Information Security and Information Systems in ISS, to achieve the appropriate level given the responsibility to ensure the confidentiality, integrity, and availability of organizational information.

Lista de Siglas

SI – Sistemas de Informação

TI – Tecnologias de Informação

ISS – Integrated Support Services

BS – British Standard

ISO – International Organization for standardization

IEC – International Electrotechnical Commission

DSI – Departamento de Sistemas de Informação

ERP – Enterprise Resource Planning

CRM – Customer Relationship Manager

VPN – Virtual Private Network

SQL – Structured Query Language

CPD – Centro de Processamento de Dados

STIC - Segurança de Tecnologias de Informação e Comunicação

Índice

Resumo	1
Abstract	2
Índice	4
1 Introdução	10
1.1 Motivação	10
1.2 Âmbito do projeto	10
1.3 Objetivos	10
1.4 Estrutura do relatório	11
2 Enquadramento teórico.....	13
2.1 IT Governance.....	13
2.2 O que é a segurança da informação?.....	13
2.3 A importância da segurança da informação	14
2.4 Norma ISO/IEC 27002:2005.....	14
2.4.1 O que é a ISO/IEC 27002?	14
2.4.2 Por que utilizar a ISO/IEC 27002?	15
2.4.3 Antecedentes.....	16
2.4.4 ISO 27002 versus ISO27001	17
2.4.5 Áreas de controlo.....	17
2.5 Análise de risco	18
3 Caracterização da ISS Facility Services	19
3.1 Identificação.....	19
3.2 Localização em Portugal	20
3.3 Missão, Objetivos, Valores e Visão	20
3.4 Política da Qualidade, Ambiente e Segurança	21
3.5 Estrutura organizacional.....	22
3.6 Caracterização da atividade da organização.....	22
4 Departamento de Sistemas de Informação	24
4.1 Missão, atividade e responsabilidades	24
4.2 Estrutura funcional.....	25
5 Caracterização da arquitetura do SI/TI.....	26
5.1 Arquitetura de rede de comunicações	27
5.2 Arquitetura de equipamentos	27
6 Caracterização do Centro de Processamento de Dados	29
6.1 Localização	29
6.2 Identificação dos ativos instalados.....	29
6.3 Sistemas de informação (matrizes de análise).....	29

6.4	Serviços vs condições face ao negócio	30
6.4.1	Interpretação	31
6.5	Serviços vs indisponibilidades aceitável	31
6.5.1	Interpretação	32
6.6	Incidentes vs nível de risco vs probabilidade de ocorrência	32
6.6.1	Interpretação	32
7	Aplicação da norma ISO/IEC 27002:2005	33
7.1	Áreas de controlo analisadas	33
7.2	Análise e otimização das atuais políticas	34
7.3	Gap analize.....	35
8	Conclusões e perspetivas de trabalho futuro	36
8.1	Conclusões	36
8.2	Perspetivas de trabalho futuro	37
9	Anexos.....	38
	Anexo A – Auditoria aos sistemas de informação.....	38
5	Políticas de segurança	38
5.1	Política de segurança da informação	38
5.1.1	Documento de políticas de segurança dos sistemas de informação	38
5.1.2	Revisão da política de segurança da informação	38
	Propostas de otimização (5.1 - Política de segurança da informação).....	39
6	Organização da segurança	40
6.1	Organização interna	40
6.1.1	Compromisso da Direção com a segurança da informação	40
6.1.2	Coordenação da segurança da informação.....	40
6.1.3	Atribuição de responsabilidades para a segurança da informação.....	41
6.1.4	Processo de autorização para as infraestruturas de processamento da informação.....	41
6.1.5	Acordos de confidencialidade.....	41
6.1.6	Contatos com autoridades.....	41
6.1.7	Contatos com grupos de interesse especial.....	41
6.1.8	Revisão independente da segurança da informação.....	42
	Propostas de otimização (6.1 – Organização interna)	42
6.2	Entidades externas.....	43
6.2.1	Identificação de riscos relacionados com entidades externas	43
6.2.2	Identificação da segurança na interação com clientes	43
6.2.3	Identificação da segurança nos acordos com entidades externas.....	43
7	Gestão dos recursos	45
7.1	Responsabilidade dos recursos.....	45
7.1.1	Inventário dos recursos	45
7.1.2	Propriedade dos recursos	45

7.1.3	Utilização aceitável dos recursos	45
	Propostas de otimização (7.1 – Responsabilidade dos recursos)	46
7.2	Classificação da informação	46
7.2.1	Recomendações para classificação	46
7.2.2	Identificação e tratamento da informação	46
	Propostas de otimização (7.2 – Classificação da informação).....	47
9	Segurança física e ambiental	48
9.1	Áreas seguras	48
9.1.1	Perímetro de segurança física	48
9.1.2	Controlos de entrada física	48
9.1.3	Segurança em escritórios, salas e instalações	48
9.1.4	Proteção contra ameaças externas e ambientais.....	49
9.1.5	Trabalhar em áreas seguras.....	49
9.1.6	Acesso público e áreas de cargas e descargas.....	49
	Propostas de otimização (9.1 – Áreas seguras)	50
9.2	Segurança de equipamentos	51
9.2.1	Localização e proteção de equipamentos.....	51
9.2.2	Utilitários de suporte	51
9.2.3	Segurança de cablagens	52
9.2.4	Manutenção dos equipamentos.....	52
9.2.5	Segurança de equipamentos fora do perímetro da organização	52
9.2.6	Reutilização e alienação segura de equipamentos	53
9.2.7	Remoção de propriedade	53
	Propostas de otimização (9.2 – Segurança de equipamentos)	53
10	Gestão das operações e comunicações	54
10.1	Procedimentos e responsabilidades operacionais.....	54
10.1.1	Documentação dos procedimentos de operação	54
10.1.2	Gestão de mudanças	54
10.1.3	Segregação de funções.....	54
10.1.4	Separação dos recursos de desenvolvimento, teste e de produção.....	55
	Propostas de otimização (10.1 – Procedimentos e responsabilidades operacionais).....	55
10.2	Gestão de serviços prestados por terceiros.....	56
10.2.1	Entrega de serviços.....	56
10.2.2	Revisão e monitorização de serviços prestados por terceiros	56
10.2.3	Gestão de mudanças para serviços prestados por terceiros.....	56
	Propostas de otimização (10.2 – Gestão de serviços prestados por terceiros).....	57
10.3	Planeamento e aceitação dos sistemas	57
10.3.1	Gestão de capacidade.....	57
10.3.2	Aceitação de Sistemas	58

Propostas de otimização (10.3 – Planeamento e aceitação dos sistemas).....	58
10.4 Proteção contra códigos maliciosos e códigos móveis.....	58
10.4.1 Controlos contra códigos maliciosos	59
10.4.2 Controlos contra código móvel.....	59
Propostas de otimização (10.4 – Proteção contra códigos maliciosos e códigos móveis).....	59
10.5 Cópias de segurança.....	59
10.5.1 Cópias de segurança das informações	60
Propostas de otimização (10.5 – Cópias de segurança).....	60
10.6 Gestão da segurança das redes	60
10.6.1 Controlos das redes.....	60
10.6.2 Segurança dos serviços de rede	61
Propostas de otimização (10.6 – Gestão da segurança das redes).....	61
10.7 Manuseio de suportes de dados.....	61
10.7.1 Gestão de suportes de dados amovíveis.....	61
10.7.2 Inutilização de suportes de dados	62
10.7.3 Procedimentos para tratamento da informação	62
10.7.4 Segurança da documentação dos sistemas.....	62
Propostas de otimização (10.7 – Manuseio de suportes de dados).....	62
10.8 Troca de informação	63
10.8.1 Políticas e procedimentos para troca de informação.....	63
10.8.2 Acordos para a troca de informação	63
10.8.3 Suportes de dados em trânsito	64
10.8.4 Mensagens eletrónicas.....	64
10.8.5 Sistemas de informação do negócio.....	64
Propostas de otimização (10.8 – Troca de informação).....	64
10.9 Serviços de comércio eletrónico	65
10.10 Monitorização	65
10.10.1 Registos de auditoria	65
10.10.2 Monitorização da utilização do sistema.....	66
10.10.3 Proteção da informação dos registos	66
10.10.4 Registos de administrador e utilizador.....	66
10.10.5 Registos de falhas	66
10.10.6 Sincronização dos relógios	67
Propostas de otimização (10.10 – Monitorização)	67
11 Controlo de Acessos.....	68
11.1 Requisitos de negócio para o controlo de acesso	68
11.1.1 Política de controlo de acessos	68
Propostas de otimização (11.1 – Requisitos de negócio para o controlo de acesso).....	68
11.2 Gestão de acessos do utilizador.....	69

11.2.1	Registo do utilizador.....	69
11.2.2	Gestão de privilégios	69
11.2.3	Gestão da palavra-passe de utilizador.....	69
11.2.4	Revisão dos direitos de acesso de utilizador.....	70
	Propostas de otimização (11.2 – Gestão de acessos do utilizador).....	70
11.3	Responsabilidades dos utilizadores.....	70
11.3.1	Utilização de palavras-passe.....	70
11.3.2	Equipamento sem monitorização.....	71
11.3.3	Política de mesa e ecrã limpo	71
	Propostas de otimização (11.3 – Responsabilidades dos utilizadores).....	71
11.4	Controlo de acesso à rede.....	72
11.4.1	Política de utilização dos serviços de rede.....	72
11.4.2	Autenticação para ligação externa do utilizador.....	72
11.4.3	Identificação de equipamentos em redes	72
11.4.4	Configuração de proteção de portas de diagnóstico remoto	73
11.4.5	Segregação de redes.....	73
11.4.6	Controlo de conexão de rede	73
11.4.7	Controlo de roteamento das redes.....	73
	Propostas de otimização (11.4 – Controlo de acesso à rede).....	73
11.5	Controlo de acesso ao sistema operativo.....	74
11.5.1	Procedimentos seguros de entrada no sistema (log-on).....	74
11.5.2	Identificação e autenticação de utilizador.....	75
11.5.3	Sistema de gestão de palavra-passe	75
11.5.4	Utilização de utilitários de sistema	75
11.5.5	Limite de tempo de sessão.....	75
11.5.6	Limitação de horário de conexão.....	75
	Propostas de otimização (11.5 – Controlo de acesso ao sistema operativo).....	76
11.6	Controlo de acesso à aplicação e à informação.....	76
11.6.1	Restrição de acesso à informação	76
11.6.2	Isolamento de sistemas sensíveis.....	77
	Propostas de otimização (11.6 – Controlo de acesso à aplicação e à informação).....	77
11.7	Computação móvel e teletrabalho.....	77
11.7.1	Computação e comunicação móvel	77
11.7.2	Teletrabalho.....	78
	Propostas de otimização (11.7 – Computação móvel e teletrabalho).....	78
13	Gestão de incidentes de segurança da informação	79
13.1	Notificação de vulnerabilidades e eventos de segurança da informação.....	79
13.1.1	Notificação de eventos de segurança da informação	79
13.1.2	Notificação de vulnerabilidades de segurança da informação	79

Propostas de otimização (13.1 – Notificação de vulnerabilidades e eventos de segurança da informação)	80
13.2 Gestão de incidentes de segurança da informação e melhorias	80
13.2.1 Responsabilidades e procedimentos	80
13.2.2 Aprendizagem com os incidentes de segurança da informação	80
13.2.3 Recolha de provas	81
Propostas de otimização (13.2 – Gestão de incidentes de segurança da informação e melhorias)	81
14 Gestão da continuidade do negócio	82
14.1 Aspetos da gestão da continuidade do negócio, relativos à segurança da informação	82
14.1.1 Inclusão da segurança da informação no processo de gestão da continuidade do negócio	82
14.1.2 Continuidade do negócio e análise/avaliação de riscos	83
14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	83
14.1.4 Estrutura do plano de continuidade do negócio	83
14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio	83
Propostas de otimização (14.1 – Aspetos da gestão da continuidade do negócio, relativos à segurança da informação)	84
Anexo B – ISS/DSI - Checklist de Auditoria	85
Anexo C – Listagem de severidades/prioridades	97
15 Referências bibliográficas	98

1 Introdução

1.1 Motivação

O projeto realizado surge na fase conclusiva da Licenciatura em Informática de Gestão, permitindo desta forma uma perspetiva efetivamente abrangente do papel dos Sistemas de Informação nas organizações.

A realização de um estudo desta ordem, numa área vital para as organizações, perspectivou-se aquando da escolha do projeto final de curso, como um desafio interessante para a formação e experiência enquanto elementos chave dos sistemas de informação nas organizações onde profissionalmente os autores estão inseridos.

Por fim, estamos cientes dos benefícios que podemos colher a curto prazo, pelo facto de realizar um trabalho efetivamente útil a uma realidade organizacional, a da ISS.

1.2 Âmbito do projeto

O Projeto procura responder ao interesse da organização ISS, em desenvolver uma análise de recolha de informação acerca do estado atual de segurança dos SI.

A ISS tem a noção de que os suportes tecnológicos no interior da organização crescem exponencialmente, deixando pouca margem para a necessária reorganização interna ao nível dos procedimentos de gestão.

Com essa consciência e aumentada a dimensão, a complexidade e a criticidade dos SI/TI que estão sob a sua responsabilidade, equacionam-se de forma mais premente questões relacionadas com a confidencialidade, a integridade e a disponibilidade da informação, às quais, a estrutura técnica deve dar resposta.

Pretende-se otimizar um conjunto de boas práticas para melhorar e atualizar a atual política de segurança da informação seguida pela ISS, assegurando-se desta forma, que o recurso à informação da organização se encontra devidamente protegido através dos melhores procedimentos e práticas.

1.3 Objetivos

Os objetivos deste projeto foram definidos de modo a ir ao encontro das necessidades de análise referente à Segurança da Informação da ISS, tendo-se delineado os seguintes objetivos:

- análise estratégica da organização;

- identificar todos os bens informáticos instalados no centro de processamento de dados (CPD) da organização com vista à realização de uma análise de risco;
- identificar ameaças e vulnerabilidades que poderão comprometer o correto funcionamento dos SI de modo a extinguir ou diminuir o grau de probabilidade de ocorrência;
- verificar os procedimentos atuais que asseguram a segurança da informação na organização comparando-os com o normativo exposto pela ISO/IEC 27002:2005 *Information technology – Security techniques - Code of practice for information security management* dando lugar a otimizações;
- extrair as informações necessárias para a verificação, controlo e apresentação de alteração das políticas de segurança.
- apresentar prioridades de implementação de modo que se atinjam diferentes níveis de segurança e que esses níveis sejam perceptíveis para a organização através de escalonamentos de risco tornando as decisões adaptáveis às necessidades.

1.4 Estrutura do relatório

A estrutura do relatório encontra-se dividida em oito secções. A **primeira secção** faz referência ao tema do trabalho através de uma introdução, onde é apresentada a motivação, o âmbito do projeto, os objetivos a atingir e a estrutura pela qual o relatório se encontra dividido.

Na **segunda secção** procede-se à contextualização do tema do trabalho através de explicações teóricas que têm como intuito, sensibilizar o leitor para o tema através de alguns dos assuntos de referência da atualidade. Nesta secção é explicada a definição de segurança de informação e a sua importância com enfoque na norma ISO/IEC 27002:2005.

Seguidamente, na **terceira secção**, é identificada a organização onde foi realizado o trabalho. Nesse sentido, procede-se à apresentação e caracterização da organização.

A **quarta secção** estreita o âmbito de caracterização geral da organização e detalha em particular o Departamento de Sistemas de Informação (DSI). Para tal, identifica-se a sua missão, responsabilidades, principais atividades e a estrutura organizacional do departamento.

Na **quinta secção**, encontra-se a caracterização da arquitetura dos SI e das TI. Relativamente à arquitetura dos SI, é apresentado os vários SI que suportam as várias áreas de negócio e a forma como estão interligados. A arquitetura das TI, apresenta uma estrutura lógica representativa do modo como a comunicação de dados se apresenta dimensionada e configurada. Por fim, é representado um diagrama de componentes que descreve a arquitetura de equipamentos a utilizar no suporte ao SI, e a distribuição dos diversos componentes aplicativos.

A **sexta secção** caracteriza o CPD. Esta caracterização, entre outras particularidades, localiza o CPD e identifica os ativos instalados no seu interior. Nesta secção é realizada uma análise aos SI de modo a identificar criticidades em relação às necessidades do negócio.

Na **sétima secção** são identificadas as áreas de controlo analisadas. É igualmente apresentado o modelo conceptual da realização do projeto. É nesta secção que são apresentados os resultados da aplicação da norma, ou seja, o GAP Analize, sendo este apresentado na forma de gráficos de radar.

Finalmente, na **oitava secção**, são apresentadas as principais conclusões e as propostas para trabalho futuro.

2 Enquadramento teórico

2.1 IT Governance

Para se atingir o sucesso na atual economia da informação, a gestão empresarial (“*enterprise governance*”) e a gestão da informação (“*IT governance*”) não podem mais ser disciplinas separadas. Uma Gestão empresarial efetiva potencia a focagem das competências e experiências individuais e de grupo nos pontos em que estas podem ser mais produtivas, mede e monitoriza o desempenho e toma decisões sobre situações críticas. A gestão da informação, desde sempre considerada como um facto que permite alavancar a estratégia empresarial, deve agora ser considerada como parte integrante dessa mesma estratégia.

A segurança da informação é uma componente chave do *IT governance*. À medida que as TI, e a informação por si própria, contribuem cada vez mais para a estratégia das atividades das organizações, do mesmo modo uma gestão efetiva quer das TI, quer da informação, torna-se numa preocupação estratégica para as direções e administrações.

2.2 O que é a segurança da informação?

“A informação é um ativo que, como qualquer outro ativo importante, é essencial para o negócio de uma organização e, conseqüentemente, necessita ser devidamente protegida. Este facto é especialmente importante no ambiente dos negócios, cada vez mais interligado. Como resultado deste assinalável aumento da interligação, a informação encontra-se exposta a uma grande variedade de ameaças e vulnerabilidades.

A informação existe em diversa formas: impressa, escrita em papel, em formato eletrónico, transmitida por correio ou eletronicamente, apresentada em filmes ou falada. Seja qual for a forma ou o meio através do qual é partilhada ou armazenada, é recomendado que seja sempre devidamente protegida.

Segurança da informação é a proteção da informação de vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controlos adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controlos necessitam ser estabelecidos, implementados, monitorizados, analisados e melhorados, onde necessário, de modo a garantir que os objetivos do negócio e de segurança da organização sejam alcançados. Isto deve ser feito em conjunto com outros processos de gestão do negócio.” [ISO/IEC 27002:2005: IX].

2.3 A importância da segurança da informação

“A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o *cash-flow*, o lucro, o cumprimento de requisitos legais bem como a imagem da organização junto do mercado.

As organizações, os seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrónicas, espionagem, sabotagem, vandalismo, incêndio, inundação bem como catástrofes naturais. Danos causados por código malicioso, *hackers*, e ataques de *denial of service* são cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação é importante para os negócios, tanto no sector público como no privado e para proteger infraestruturas críticas. Em ambos os sectores, a função da segurança da informação é viabilizar os negócios como o governo eletrónico (*e-gov*) ou o comércio eletrónico (*e-business*) e evitar ou reduzir os riscos relevantes. A interligação de redes públicas e privadas e a partilha de recursos de informação aumentam a dificuldade no controlo de acessos. A tendência da computação distribuída reduz a eficácia da implementação de um controlo de acesso centralizado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controlos a serem implementados requer um planeamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os colaboradores da organização. Pode ser necessária também a participação de acionistas, fornecedores, terceiros, clientes ou outras partes externas à organização. Uma consultora externa especializada pode também ser necessária.” [ISO/IEC 27002:2005: IX].

2.4 Norma ISO/IEC 27002:2005

2.4.1 O que é a ISO/IEC 27002?

ISO 27002 é uma norma internacionalmente reconhecida que propõe um "Código de práticas para a gestão da segurança da informação". Esta norma, publicada pela *International Organization for Standardization*, ou ISO¹, em dezembro de 2000, como ISO 17799, é agora parte da série ISO27XXX. A ISO 27002 é de alto nível, de âmbito alargado e de natureza

¹ ISO (<http://www.iso.ch>) é uma organização fundada em 1947, cuja missão é a elaboração, aprovação e publicação de referenciais internacionais em diferentes domínios.

conceptual. Esta abordagem permite que seja aplicada em vários tipos de empresas e aplicações. A ISO 27002 é a única norma de segurança da informação dedicada à orientação da gestão da segurança da informação, num campo geralmente regido por detalhes operacionais.

Enquanto norma predominantemente conceptual, a ISO 27002 não é uma norma técnica, nem está orientada ao produto ou à tecnologia nem é uma metodologia de avaliação de equipamentos.

A ISO 27002 é, no entanto, uma base de controlos de segurança da informação que todos os programas de segurança da informação DEVEM abordar, de alguma maneira, o que a torna internacionalmente reconhecida como um conjunto de melhores práticas.

2.4.2 Por que utilizar a ISO/IEC 27002?

O campo da segurança da informação tem sido tradicionalmente baseado em melhores práticas e em orientações. Embora esta sabedoria acumulada seja válida, também está sujeita a várias interpretações e aplicações, nem sempre coerentes e harmoniosas. A ISO 27002 é uma tentativa de codificar e padronizar essa orientação, com os seguintes benefícios:

- um catálogo de controlos internacionalmente reconhecido, que pode aumentar a interoperabilidade da segurança da informação e a confiança com os parceiros comerciais;
- um parâmetro para avaliar a abrangência do programa de segurança da informação;
- um veículo que permite documentar as diligências devidas;
- um chapéu sob o qual vários regulamentos de proteção de dados podem ser tratados.

As razões para seguir um Programa de Segurança da Informação baseado na ISO 27002 variam:

- para algumas indústrias um programa de segurança da informação baseado na ISO 27002 pode-se tornar numa exigência de facto;
- para organizações sujeitas à regulamentação governamental, a ISO 27002 pode aumentar a eficiência e eliminar a redundância no cumprimento de normas múltiplas de proteção da informação, através de um conjunto de controlos normalizados;
- para organizações centradas nos dados, a percepção do cliente de um programa de segurança da informação baseado na ISO 27002 pode oferecer uma vantagem de marketing;
- um programa de segurança da informação baseado na ISO 27002 proporciona um certo grau de capacidade de defesa.

2.4.3 Antecedentes

A ISO 27002 é descendente direta da norma ISO 17799, que por sua vez, é descendente direta da norma *Security Information Management BS 7799-1* do *British Standard Institute (BSI)*², instituto que há muito que adota uma postura pró-ativa no campo da evolução da segurança da informação.

Em resposta às exigências da indústria foi criado, no início dos anos de 1990, um grupo de trabalho dedicado à segurança da informação, culminando num código de boas práticas para gestão de segurança da informação em 1993. Este trabalho evoluiu para a primeira versão da norma BS 7799 lançado em 1995.

No final dos anos 1990, em resposta às exigências da indústria, o BSI criou um programa para acreditar empresas de auditoria, ou organismos de certificação, com competências para auditar a BS 7799. Simultaneamente, foi criado um *steering committee*, culminando com a atualização e publicação da BS 7799 em 1998, 1999, 2000 e, finalmente, em 2002. Por esta altura a segurança da informação tornou-se notícia de primeira página e uma preocupação a nível mundial para utilizadores de computadores.

Enquanto algumas organizações utilizavam a norma BS 7799, a procura crescia por uma norma de segurança da informação reconhecida internacionalmente, sob a égide de um órgão também reconhecido internacionalmente, como a ISO. Esta procura levou ao aceleração pelo BSI da BS 7799 Parte 1, culminando no seu primeiro lançamento pela ISO como ISO/IEC 17799:2000, em dezembro de 2000.

Para manter a coerência com a nova nomenclatura da série de normas ISO27xxx, a ISO17799 foi atualizada e relançada como ISO 27002 em junho de 2005.

² BSI (www.bsigroup.com) é o organismo nacional de normas do Reino Unido. Fundado em 1901, tem uma reputação reconhecida mundialmente pela integridade, independência e inovação na produção de normas que promovem as melhores práticas. A sua missão é desenvolver e comercializar soluções de normas e padronização, que atendam às necessidades das empresas e da sociedade.

2.4.4 ISO 27002 versus ISO27001

Ambas as normas servem propósitos distintos, pelo que é importante entender a diferença entre a ISO27002 e a ISO27001.

ISO27001	ISO27002
Uma norma de auditoria baseada em requisitos auditáveis	Um guia de implementação baseada em sugestões de melhores práticas
Uma lista de controlos de gestão que uma organização TEM DE considerar	Uma lista de controlos operacionais que uma organização DEVE considerar
Utilizada como um meio de auditar e certificar um sistema de gestão de segurança da informação das organizações	Utilizada como um meio para avaliar a abrangência de um programa de segurança da informação das organizações

2.4.5 Áreas de controlo

Tal qual como na definição de segurança da informação, a ISO 27002 define a informação como um importante ativo de negócio que pode existir em muitas formas e necessita ser adequadamente protegida. Do mesmo modo, a ISO 27002 define a segurança da informação como a sua proteção de uma ampla gama de ameaças para garantir a continuidade do negócio, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e oportunidades de negócio. Esta abrangência faz com que os controlos da ISO 27002 sejam transversais a múltiplas disciplinas de segurança, incluindo elementos de:

- segurança operacional;
- segurança aplicacional;
- segurança de plataformas computacionais;
- segurança de redes,
- segurança física.

De modo a atingir este objetivo, a ISO 27002 identifica 11 áreas de controlo, 39 objetos de controlo, e 133 controlos. Cada controlo é ao mesmo tempo definido e dotado com guias de implementação para esclarecer o espírito e a intenção do controlo. Note-se que a implementação de um controlo pode envolver qualquer combinação das disciplinas mencionadas anteriormente. As áreas de controlo, objetivos de controlo e atributos-chave de controlo foram os objetos principais de estudo deste projeto, os quais serão desenvolvidos mais à frente.

2.5 Análise de risco

A norma ISO/IEC 27002:2005, salienta para a importância de se realizar uma análise de risco, para se seleccionar devidamente os controlos da norma.

“A análise de risco deve identificar e priorizar riscos contra o negócio. Os resultados devem guiar e determinar para as melhores ações de gestão de segurança da informação a serem seguidas bem como os controlos adequados a serem implementados” [ISO/IEC 27002:2005: 5]. Como ponto de partida para a seleção de controlos, embora não seja realizado de forma exhaustiva, o que necessitaria de um tempo de preparação mais longo e um envolvimento diferente com a direção da ISS, que não se coaduna com os tempos estabelecidos para a realização deste projeto académico, é realizada uma análise de risco à atual situação de segurança dos SI, para que a organização possa retirar um conjunto de boas práticas para melhorar a sua política de segurança.

O modelo de análise de risco adota a conceptualização de Mamede e é esquematizado através da figura 1.

A sua conceptualização pretende responder às seguintes questões:

- qual o objeto ameaçado?
- qual o grau de risco do mesmo?
- qual o nível da ameaça?
- quais as limitações com as quais temos de trabalhar?

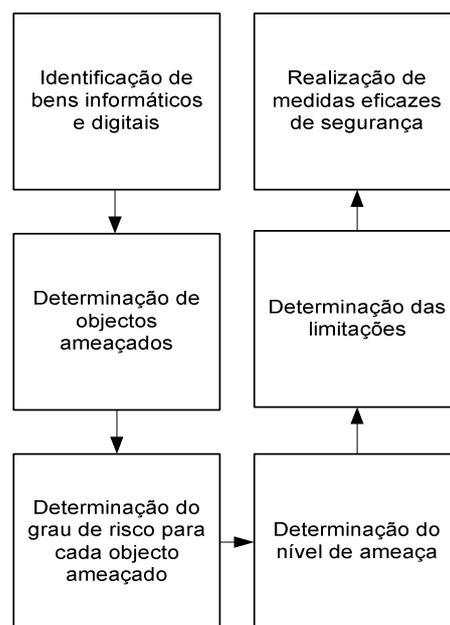


Figura 1 – Modelo de análise

Fonte: Mamede, 2006: 24

3 Caracterização da ISS Facility Services

Para se ter uma perceção do ambiente onde foi realizado o projeto, faz-se uma apresentação da organização. Nesse âmbito, este capítulo identifica a ISS, a sua localização, e procede ao enquadramento no seu meio económico através da explicitação da Missão, Visão, Objetivos e Valores.

3.1 Identificação

ISS é uma Multinacional Dinamarquesa fundada há mais de 100 anos, hoje em dia é um dos maiores líderes no mercado de Serviços/Outsourcing, e um dos maiores grupos mundiais, com mais de 520.000 empregados em 53 Países.

Em Portugal, a ISS estabeleceu-se a partir de 1 de Julho de 1992, sendo considerado o 10º maior empregador em Portugal no ano de 2010.

Com a evolução para o “*Full Facility Service*”, a prestação de vários serviços, nomeadamente, manutenção técnica de edifícios, certificação energética, jardinagem, receção e acolhimento, logística interna, *pest control/HACCP*, *merchandising*, trabalho temporário, serviços de hotelaria, hospedeiras, gestão de recursos humanos, higiene e limpeza permitem criar sinergias com evidentes benefícios financeiros aos clientes, facto importante para uma maior competitividade, já que a entrega da operação é efetuada pelos diversos quadros operacionais e pelas 4 empresas que compõem o Grupo ISS em Portugal.

A capacidade e experiência dos profissionais da ISS na entrega de todos estes serviços conduziram a uma distinção como a 2ª melhor empresa global do mundo de *outsourcing* pela *Internacional Association of Outsourcing Professionals* (IAOP).



3.2 Localização em Portugal

A ISS está presente em todo o país, com 9 delegações e sede em Carnaxide. Com esta abrangência geográfica disponibiliza serviços em diversos pontos do país, conseguindo ter uma cobertura total de norte a sul, incluindo ilhas.

Sede e Delegação de Lisboa

Rua Moinho da Barrunchada, nº 4 - 1º Dtº
2795-544 Carnaxide

Delegação do Porto

Rua Francisco Silva Duarte, nº 127
4475-269 Maia

Delegação de Coimbra

Estrada de Coselhas - Armazém Frente
3000-125 Coimbra

Delegação de Almeirim

Zona Industrial, Lote 42
2080-221 Almeirim

Delegação de Lisboa

Av. Almirante Reis, nº 84 - Piso Intermédio
1150-021 Lisboa

Delegação de Setúbal

Rua António José Baptista, 108
2910-398 Setúbal

Delegação de Albufeira

Sítio dos Cortesões, Cx A9
8200-559 Albufeira

Delegação Região Autónoma da Madeira

Caminho da Ladeira, nº 114
9020-089 Funchal

Delegação Região Autónoma dos Açores

Zona Comercial dos Valados, Via Q, nº 17
9500-652 Ponta Delgada



3.3 Missão, Objetivos, Valores e Visão

A ISS apresenta como **Missão** [ISS, “About Us”], a responsabilidade de executar e gerir um conjunto integrado de serviços, que criem sinergias e flexibilidade, de forma a proporcionar mais valias operacionais e financeiras aos seus clientes. Para cumprir a sua missão, orienta os

colaboradores dentro das áreas administrativas e de gestão congéneres da atuação humana definindo os seguintes **Objetivos** [ISS, “*About Us*”]:

- desenvolver e prestar serviços de elevada qualidade;
- contribuir para a otimização dos recursos económicos dos seus clientes criando sinergias entre os diversos serviços;
- consolidar e expandir a sua posição de liderança mundial como companhia internacional prestadora de serviços.

No cumprimento da sua Missão e Objetivos, assume como **Valores** [ISS, “*Communication Department*”] Honestidade, Empreendedorismo, Responsabilidade, Excelência, Respeitabilidade.

Gerindo com sabedoria a sua Missão e Valores, e com eficácia os seus Objetivos, traça como **Visão** [ISS, “*Communication Department*”] desenvolver e liderar globalmente a indústria de serviços de suporte a instalações.

3.4 Política da Qualidade, Ambiente e Segurança

A Política da ISS consiste em desenvolver e prestar serviços no mercado de *Facility Services*, centrados primordialmente em:

- elevados padrões de qualidade, que conduzam à satisfação dos seus clientes;
- exigentes níveis de segurança & saúde para os seus colaboradores, bem como para os que trabalham em seu nome, que previnam lesões, ferimentos e danos para a saúde;
- eficientes soluções para promover a prevenção da poluição;

com base numa estratégia de melhoria contínua dos seus processos, contribuindo para um desenvolvimento sustentável.

Assim, a ISS:

- orienta a sua conduta pelos valores corporativos da honestidade, responsabilidade, iniciativa e qualidade;
- garante que, no desenvolvimento do seu negócio, integra a gestão dos aspetos de Segurança & Saúde e Ambientais em todas as suas vertentes. Compromete-se a cumprir todos os requisitos legais e outros requisitos aplicáveis no âmbito da Qualidade, da Segurança & Saúde e do Ambiente;
- assegura a atribuição de funções e responsabilidades no âmbito da gestão da Qualidade, da Segurança & Saúde e do Ambiente, para uma implementação efetiva do Sistema de Gestão Integrado.

- cada colaborador é responsável pela sua própria Segurança e Saúde, bem como pela dos seus colegas;
- promove iniciativas de Formação, Informação e Sensibilização que desenvolvam práticas, atitudes e responsabilidades orientadas para a melhoria da Qualidade, Segurança & Saúde e do Ambiente;
- adota, sempre que possível, as melhores tecnologias disponíveis, minimizando os riscos e os impactos ambientais inerentes à sua atividade, nomeadamente na utilização criteriosa dos recursos, na gestão dos resíduos, na prevenção dos acidentes de trabalho e doenças profissionais;
- está empenhada em criar uma cultura que mobilize os seus colaboradores para o cumprimento da presente Política, nomeadamente na concretização dos objetivos da Qualidade, da Segurança & Saúde e do Ambiente.

Enquanto elemento da sociedade civil, a ISS assume como prioridade da sua política de recursos humanos a integração de pessoas com necessidades especiais nos seus quadros, num objetivo de inclusão social.

A direção da ISS compromete-se a divulgar, interna e externamente esta política, aos seus colaboradores e parceiros, revendo-a sempre que seja necessário.

3.5 Estrutura organizacional

A ISS é composta por cerca de 9.000 colaboradores, sendo que destes, cerca de 300 trabalham diretamente na sede e delegações da organização e os restantes estão, na sua grande maioria, a prestar serviço nas instalações dos clientes.

3.6 Caracterização da atividade da organização

A área de negócio da ISS, é a especialização de serviços que são *no core* para o cliente. Com esse intuito, reúne num único produto a integração de vários serviços.

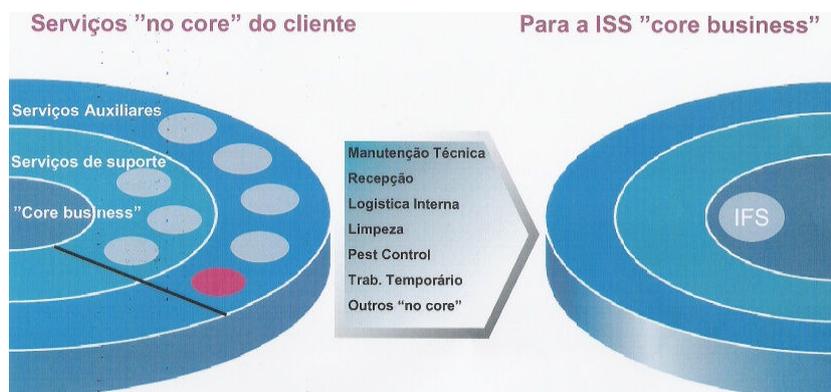


Figura 2 – Esquemática da estratégia de negócio da ISS

A ISS Portugal organizou-se em unidades especializadas por segmento de mercado, de forma a ir de encontro das necessidades específicas de cada cliente. Os segmentos pelos quais se especializou são:

- **Serviços técnicos e de gestão de edifícios** – renovação e otimização de instalações elétricas, construção civil, segurança, vigilância e redes de tecnologias de informação, construção de espaços verdes, controlo de acessos; auditorias de eficiência e performance;
- **Serviços de apoio a escritórios** – receção, central telefónica e gestão de correio (interno/externo), *call center*, logística interna, mudanças, serviço de estafeta, plantas de interior;
- **Serviços de trabalho temporário** – trabalho temporário, recrutamento, seleção, formação;
- **Serviços de higiene e limpeza** – limpeza diária de manutenção e limpeza especializada (*room maid*, transportes, hospitais, indústria, indústria alimentar), fornecimento de consumíveis e equipamentos de higiene;
- **Catering** – *catering* de eventos, assim como o apoio à organização de conferências ou seminários.

4 Departamento de Sistemas de Informação

Um trabalho que incide sobre a segurança dos SI, naturalmente remete para a necessidade de se apresentar e caracterizar o DSI, de forma a obter uma visão resumida acerca do departamento.

O DSI iniciou as suas atividades em 2006 e no decorrer do seu percurso sofre várias reestruturações, conseqüentes do aumento da atividade que a ISS atingiu e continua a atingir, devido aos seus objetivos ambiciosos. Como tal, os sistemas de informação foram obrigados a acompanhar o seu crescimento organizacional e a suportar os seus objetivos estratégicos. Esta realidade remete para a necessidade de existência de uma equipa cada vez mais competente que dê suporte aos SI.

4.1 Missão, atividade e responsabilidades

Segundo o responsável, o DSI apresenta como **Missão** a responsabilidade de garantir que as tecnologias de informação e por conseqüentes os próprios SI suportem adequadamente as necessidades de negócio da organização. Com esse intuito, o departamento assume as seguintes atividades:

- manutenção, reparação e instalação de equipamento informático;
- formação e apoio aos utilizadores na utilização de sistemas aplicacionais;
- gestão da rede do SI;
- apoio à gestão de bases de dados;
- análise e implementação de projetos.

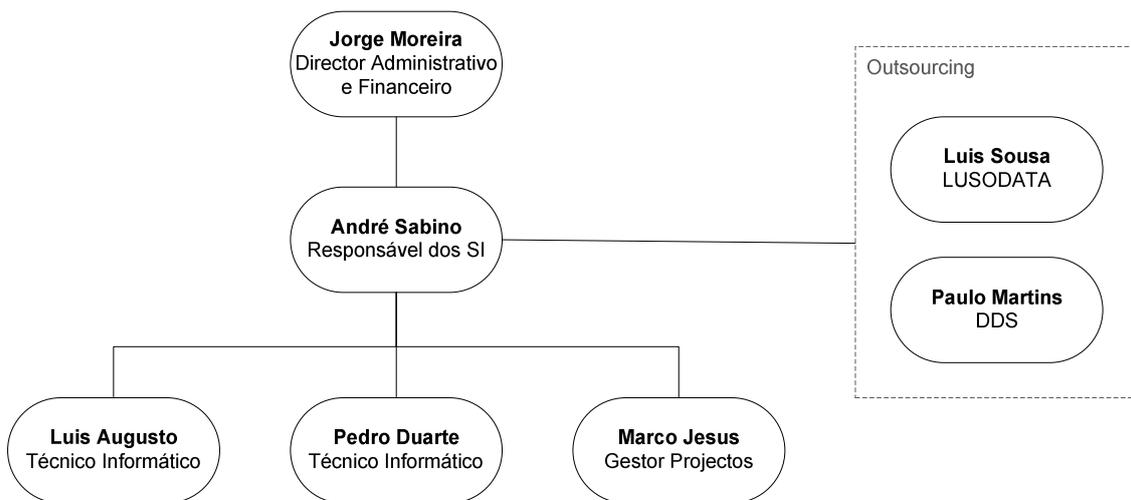
Identificou-se na data de realização deste projeto, que as responsabilidades do departamento, recaiam sobre um parque informático com as seguintes dimensões:

Descrição	Número
Desktops	122
Laptops	140
Servidores	14
Equipamentos de Impressão	32
Equipamentos Ativos de Rede (Routers & Switch)	32
Equipamentos Wireless	4

4.2 Estrutura funcional

O DSI é constituído por 4 pessoas que compõem uma estrutura simples (organigrama abaixo) e que se dividem pelas seguintes funções:

- 2 pessoas para gestão da rede, apoio dos utilizadores, manutenção das bases de dados e formação de utilizadores;
- 1 gestor de projetos;
- 1 responsável pela coordenação administrativa.



5 Caracterização da arquitetura do SI/TI

A arquitetura do SI é composta sobre uma primeira linha de serviços básicos (autenticação de utilizadores - “*Active Directory*”, Correio Eletrónico, *Internet*, *Intranet* e Portais Colaborativos) implementados numa Arquitetura *Microsoft – Windows Server 2003 R2* e *Windows Server 2008 R2* – e um conjunto de subsistemas verticais interligados a um subsistema central, cuja função é a de suportar os vários processos de cada unidade de negócio da organização.

Os sistemas de gestão de recursos humanos, gestão financeira, gestão de materiais, estão integrados e suportados tecnologicamente por um *Enterprise Resource Planner (ERP)*³ da IBM através do *Software AS400*. O sistema de gestão de clientes, é suportado por tecnologia denominada como *Customer Relationship Manager (CRM)*⁴.

Cada área de negócio da ISS possui um SI para suportar um conjunto de necessidades específicas e inerentes a cada uma das áreas.

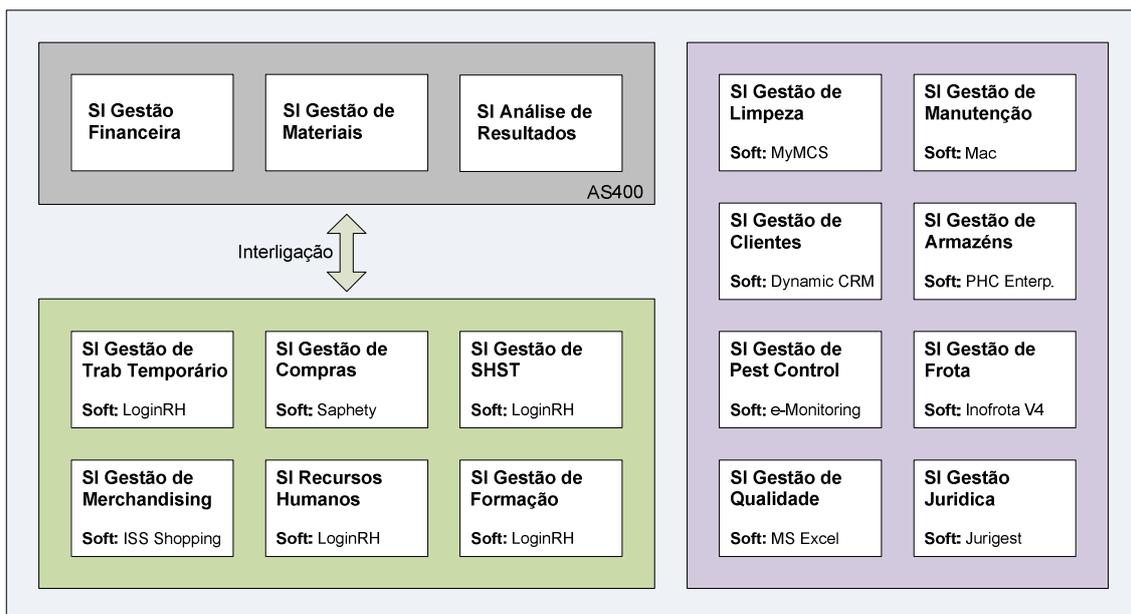


Figura 3 – representação esquemática do SI

³ ERP são sistemas de informação que integram todos os dados e processos de uma organização num único sistema. A integração pode ser vista sob a perspetiva funcional ou sistémica.

⁴ CRM são ferramentas que automatizam as funções de contacto com o cliente, ou seja, ajudam a manter um bom relacionamento com os clientes armazenando e inter-relacionando, de forma inteligente, informações sobre as suas atividades e interações com a empresa.

5.1 Arquitetura de rede de comunicações

As Comunicações são roteadas através de equipamentos *Cisco* e/ou *Huawei* em circuitos dedicados, que estabelecem *Virtual Private Networks* (VPN) entre o SI da sede da ISS em Carnaxide e os SI das várias delegações. Internamente a rede de comunicação da ISS utiliza tecnologia *Gigabit Ethernet* de variante 1000 Base-TX, especificada pela norma IEEE 802.3ab e possui uma velocidade de ligação à internet de 4Mbps. A arquitetura desenhada, contempla atribuição dinâmica de endereço de IP, controlo e replicação de domínios, controlo de correio eletrónico e equipamentos que garantem a segurança da rede através da implementação de *Firewalls*.

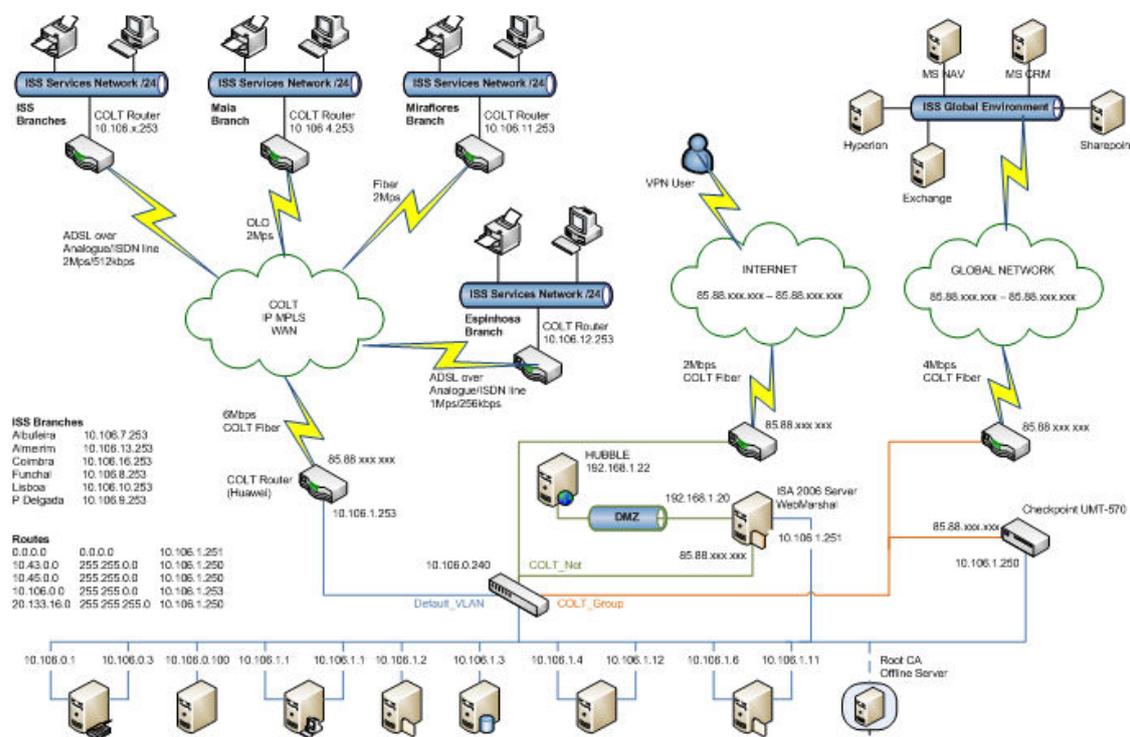


Figura 4 – estrutura da rede

5.2 Arquitetura de equipamentos

O Diagrama de Instalação apresentado na figura 5, enquadra-se nos Diagramas Físicos de *Unified Modeling Language* (UML), linguagem *standard* utilizada na modelação. O Diagrama descreve a Arquitetura dos equipamentos a utilizar no suporte ao SI e a distribuição dos diversos componentes aplicacionais pelos elementos referenciados na arquitetura.

Na ISS identificaram-se como elementos da arquitetura:

- o “Core” do Sistema (cor amarela) constituído por cinco servidores dedicados a gerir e controlar todo o SI da organização (*Domain Controller, File/Print Server, Structured query language (SQL) reporting, Internet Security Acceleration (ISA) Application Server*);
- dois servidores para operações de segurança, (cor verde) *Backup* e Consola de Antivírus.
- oito Servidores aplicativos (cor vermelha) onde residem os vários componentes de *software* instalados para suportar os processos de negócio.

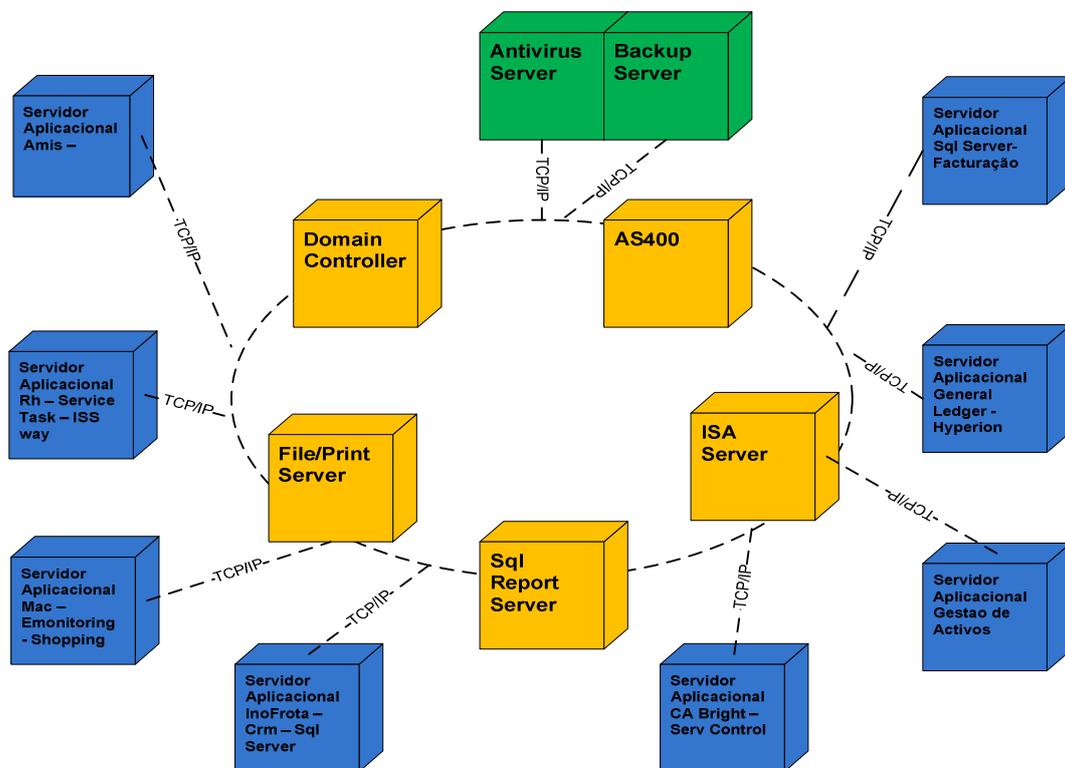


Figura 5 – Diagrama de Instalação do SI

A existência de vários subsistemas aplicativos heterogêneos e a necessidade de interligação entre os vários subsistemas e a camada *core*⁵ do sistema, remete para a necessidade de integração de sistemas, considerado como um processo crítico de implementação.

⁵ Entende-se por camada core do sistema de informação todos os servidores que disponibilizam os serviços considerados básicos para o funcionamento dos SI

6 Caracterização do Centro de Processamento de Dados

No enquadramento teórico, aquando da apresentação da norma ISO/IEC 27002:2005 refere a importância de se avaliar os riscos atuais, quer em toda a organização, partes da organização e/ou um sistema de informação específico. Neste caso em concreto, será efetuada uma avaliação ao CPD, com o objetivo de identificar ameaças e vulnerabilidades.

6.1 Localização

O CPD da ISS está situado numa das salas das instalações de Carnaxide. Trata-se de uma sala perfeitamente dimensionada para a sua finalidade, onde tem no seu interior uma câmara de segurança especialmente desenhada para acomodar todos os elementos de *hardware*. Os benefícios de os elementos ativos do SI se encontrarem dentro de uma câmara de segurança (*shelter*)⁶, traduz-se em segurança adicional contra, incêndio, água, pó, gases corrosivos, queda de escombros, explosão e acesso não autorizado.

6.2 Identificação dos ativos instalados

Verificou-se que todos os ativos do SI que estão no interior do CPD encontram-se devidamente identificados. A ISS utiliza um *software* específico denominado *ServiceDesk* para facilitar a gestão de ativos informáticos.

Para além de facilitar a identificação do equipamento, facilita também a verificação dos contratos de manutenção ou das assistências técnica e na própria gestão do equipamento no que concerne à segurança dos mesmos.

6.3 Sistemas de informação (matrizes de análise)

Conhecida a localização do CPD e tendo-se verificado que os ativos no seu interior estão corretamente identificados, importa medir os níveis de criticidade que cada serviço de informação representa face ao negócio e perceber algumas das condicionantes que o DSI enfrenta quando necessita de intervir nos mesmos de forma a solucionar problemas. Com base nesta informação, será possível medir o grau de complexidade de funcionamento e de operacionalidade do SI, sendo esta informação útil para se obter uma visão geral e atualizada sobre a situação atual.

⁶ Câmara de segurança é uma sala especificamente desenhada e construída para acolher equipamento crítico de um SI. Trata-se de salas com equipamento de refrigeração em que os materiais de construção são resistentes a catástrofes.

6.4 Serviços vs condições face ao negócio

A matriz de serviços vs condições face ao negócio apresentada na tabela 1 tem os seguintes objetivos de análise:

- identificar todos os serviços disponibilizados pelo SI que apresentem um elevado grau de criticidade face ao negócio.
- perante os serviços identificados com um elevado grau de criticidade face ao negócio, avaliar o grau de dependência externa relativamente a três dimensões: *software* do sistema, *software* aplicacional e *hardware*.

As informações necessárias para a construção da matriz foram obtidas através da análise dos ativos encontrados no CPD e avaliadas com base no conhecimento de operacionalidade do responsável pelo DSI.

Salienta-se que os resultados obtidos na avaliação podem variar consoante o conjunto de tarefas a realizar num dado período de tempo. Ao avaliar a criticidade de um serviço, esse pode apresentar um nível de criticidade baixo face ao negócio na maior parte do tempo, mas ser suscetível de passar a apresentar um nível de criticidade mais elevado, se durante um determinado período de tempo se tornar indispensável para o cumprimento do funcionamento do negócio (e.g. aplicação de processamento de salários).

Condições face ao negócio Serviços	Criticidade		Dependência Externa					
	Baixa	Alta	Hardware		Software de Sistema		Software Aplicacional	
			Baixa	Alta	Baixa	Alta	Baixa	Alta
AMIS		x		x		x		x
General Ledger		x		x		x		x
Hyperion	x		x		x		x	
Login RH		x	x		x			x
Service Task	x		x		x			x
ISS way	x		x		x			x
Mac	x		x		x			x
E - Monitoring	x		x		x		x	
Shopping	x		x		x			x
Ino Frota	x		x		x			x
Portal RH	x		x		x			x
Facturação		x		x		x		x
CA Bright Store		x	x		x		x	
Isa Server		x		x		x		x
Surf Control		x		x		x		x

Tabela 1 – Matriz de análise de criticidade face ao negócio

6.4.1 Interpretação

- perante todos os serviços, 47% são considerados muito críticos face ao negócio;
- 77% do *hardware* onde se encontram instalados os serviços considerados muito críticos face ao negócio estão dependentes de entidades externas para reparação em caso de avaria;
- 43% do *software* de sistema, responsável por manter o correto funcionamento do servidor onde se encontram os serviços críticos, está dependente de entidades externas em caso de avaria;
- 57% do *software* aplicacional, responsável por suportar especificamente cada serviço considerado crítico face ao negócio, está dependente de entidades externas.

6.5 Serviços vs indisponibilidades aceitável

A matriz representada na tabela 2 representa, para cada serviço, o tempo de indisponibilidade aceitável medido em dias. O grau de indisponibilidade aceitável para cada serviço foi avaliado através do conhecimento de operacionalidade do responsável pelo DSI, face à realidade e necessidades do negócio.

Serviços	Indisponibilidade aceitável		
	Grau 1 (≤3 dias)	Grau 2 (≤2 dias)	Grau 3 (≤1 dia)
AMIS		X	
General Ledger			X
Hyperion		X	
Login RH			X
ServiceDesk		X	
ISS way		X	
Mac		X	
E-monitoring		X	
Shopping		X	
InoFrota	X		
Portal RH	X		
Faturação		X	
CA Bright Store		X	
Isa Server			X
Surf Control			X
Estatísticas	13,33%	60,00%	26,67%

Tabela 2 – avaliação da indisponibilidade dos serviços

6.5.1 Interpretação

- 26,67% dos serviços são considerados críticos para o negócio, logo, só podem estar indisponíveis no máximo por um dia.

Tal como na avaliação da criticidade face ao negócio, a medição do grau de indisponibilidade aceite para cada serviço foi realizada perante a normalidade das necessidades da organização.

6.6 Incidentes vs nível de risco vs probabilidade de ocorrência

A tabela 3 representa ameaças e vulnerabilidades que podem colocar em causa o bom funcionamento do SI, e que podem ser originadas por causas internas ou externas à organização. Para cada uma é medida a probabilidade de ocorrência e o nível de ameaça que o risco representa para o negócio.

Nível do Risco	ALTO	<p>Inundações e incêndio</p> <p>Desabamento de terras</p> <p>Falhas no sistema de <i>backups</i></p> <p>Assalto às instalações</p> <p>Intrusão na cablagem</p> <p>Quebra de segurança do equipamento</p>	<p>Falhas nas comunicações</p> <p>Avaria de <i>software</i></p> <p>Falta de conhecimentos técnicos para resolver problemas</p> <p>Avarias de <i>hardware</i></p>	 <p>- Demasiada concentração de Tarefas</p>
	MÉDIO	<p>Falha no controlo de acesso</p> <p>Falhas na reparação</p>		
	BAIXO	<p>Quebra do perímetro de segurança</p>		
		BAIXO	MÉDIO	ALTO
Probabilidade de Ocorrência				

Tabela 3 – Matriz de Análise de Ameaças e Vulnerabilidades

6.6.1 Interpretação

- 81,3% dos incidentes são considerados de alto nível de risco para o negócio;
- dos 81,3% considerados de alto nível de risco para o negócio, apenas 8% apresentam uma probabilidade alta de ocorrência.

7 Aplicação da norma ISO/IEC 27002:2005

7.1 Áreas de controlo analisadas

O estudo incide sobre os dois domínios de segurança de tecnologias de informação e comunicação (STIC), isto é, segurança física e segurança lógica. As áreas de controlo e objetivos de controlos analisados neste projeto foram as abaixo identificadas, de acordo com a numeração da norma:

5 – Políticas de segurança

5.1 - Política de segurança da informação

6 – Organização da segurança

6.1 – Organização interna

6.2 – Entidades externas

7 – Gestão dos recursos

7.1 – Responsabilidade dos recursos

7.2 – Classificação da informação

9 – Segurança física e ambiental

9.1 – Áreas seguras

9.2 – Segurança de equipamentos

10 – Gestão das operações e comunicações

10.1 – Procedimentos e responsabilidades operacionais

10.2 – Gestão de serviços prestados por terceiros

10.3 – Planeamento e aceitação dos sistemas

10.4 – Proteção contra códigos maliciosos e códigos móveis

10.5 – Cópias de segurança

10.6 – Gestão da segurança das redes

10.7 – Manuseio de suportes de dados

10.8 – Troca de informação

10.9 – Serviços de comércio eletrónico

10.10 – Monitorização

11 – Controlo de Acessos

11.1 – Requisitos de negócio para o controlo de acesso

11.2 – Gestão de acessos do utilizador

11.3 – Responsabilidades dos utilizadores

11.4 – Controlo de acesso à rede

11.5 – Controlo de acesso ao sistema operativo

11.6 – Controlo de acesso à aplicação e à informação

11.7 – Computação móvel e teletrabalho

13 – Gestão de incidentes de segurança da informação

13.1 – Notificação de vulnerabilidades e eventos de segurança da informação

13.2 – Gestão de incidentes de segurança da informação e melhorias

14 – Gestão da continuidade do negócio

14.1 – Aspetos da gestão da continuidade do negócio, relativos à segurança da informação

Não foram incluídas na análise as seguintes áreas de controlo:

8 – Segurança em recursos humanos (seria necessário o envolvimento do Director de Recursos Humanos o que, devido ao tempo disponível, quer da pessoa quer do projecto em causa, optou-se por não incluir este ponto);

12 – Aquisição, desenvolvimento e manutenção de sistemas de informação (é uma área de controlo com grande enfoque no desenvolvimento de sistemas. Obrigava a um conhecimento aprofundado sobre o código das aplicações e envolvimento com entidades externas, não sendo compatível com o âmbito do projecto);

15 – Conformidade (seria necessário o envolvimento do responsável do Departamento Jurídico o que, devido ao tempo disponível, quer da pessoa quer do projecto em causa, optou-se por não incluir este ponto).

7.2 Análise e otimização das atuais políticas

Foi realizada uma análise controlo a controlo (*Anexo A – Auditoria aos sistemas de informação*), para todas as áreas de controlo acima identificadas, utilizando o seguinte padrão de registo de análise:

<i>Área de Controlo</i>	
Objeto de controlo	
Objetivo	
Controlos	
Prática organizacional	
Proposta de otimização	
Descrição	
Prioridade (com base no anexo C)	

7.3 Gap analize

O *GAP analize* foi realizado com base na *checklist* de auditoria (**Anexo B – ISS/DSI - Checklist de auditoria**), que por sua vez foi baseada no ponto 7.2 – **Análise e otimização das atuais políticas**. A figura 6 representa a análise do estado da organização no que respeita às 8 áreas de controlo analisadas e a figura 7 a análise dos 27 objetos de controlo que constituem as 8 áreas de controlo.

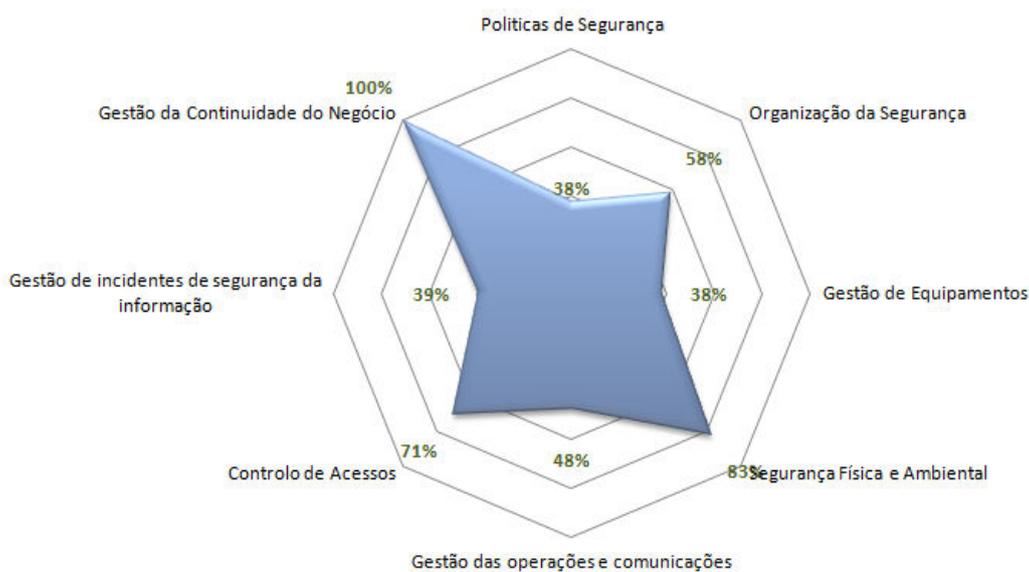


Figura 6 – *GAP analize* das 8 áreas de controlo analisadas

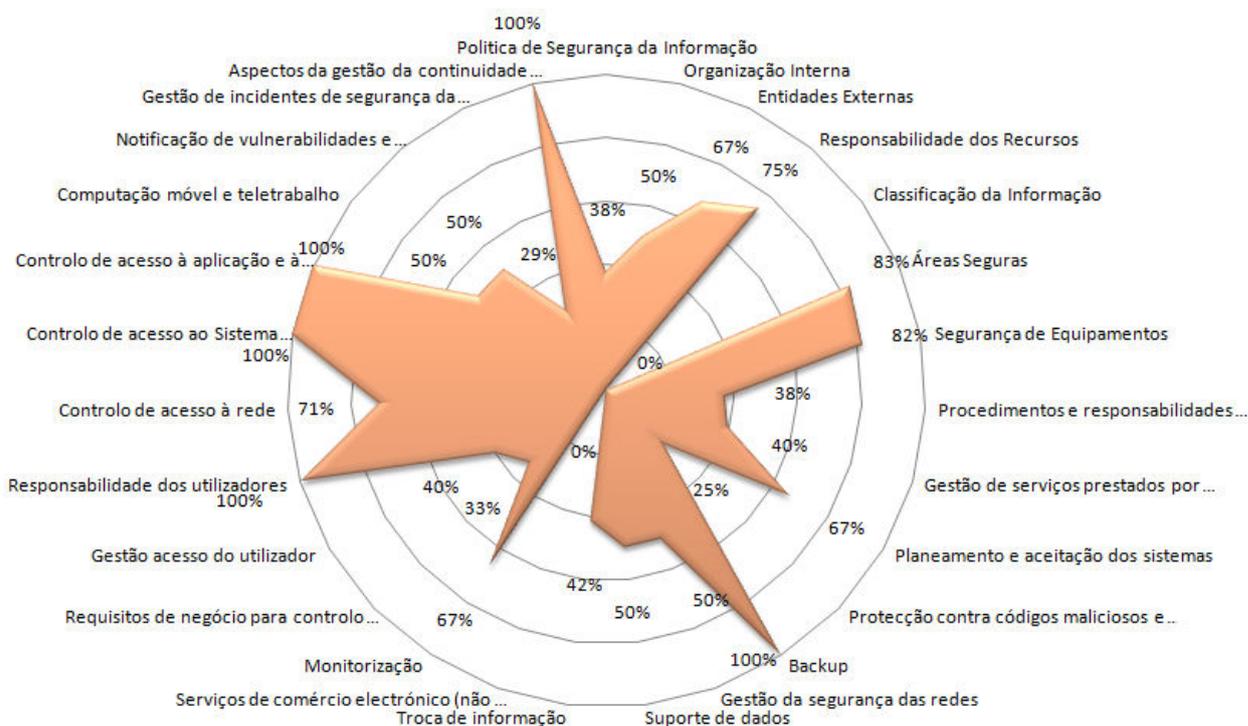


Figura 7 – *GAP analize* dos 27 objetos de controlo

8 Conclusões e perspectivas de trabalho futuro

Neste capítulo apresentam-se as conclusões retiradas do trabalho realizado e as perspectivas a considerar para trabalho futuro.

8.1 Conclusões

Após análise da organização de uma forma sistémica, e de se ter aplicado a norma ISO/IEC 27002:2005 às práticas da ISS, percebe-se que a organização integra nos seus procedimentos organizacionais um conjunto de medidas de segurança, que revelam uma preocupação acrescida para assegurar a informação do negócio.

Se por um lado é verdade que muitos são os riscos identificados como potenciais ameaças para o SI da ISS, é igualmente verdade que muitas são as medidas tomadas para atenuar essas ameaças.

A intenção deste projeto foi de verificar se a atual política de segurança de informação seguida pela ISS se encontrava atual e adaptada às suas necessidades.

Facilmente se comprova a consistência e atualidade da política da ISS relativamente à segurança do seu SI, pelo número de otimizações que foram aferidas através da norma ISO/IEC 27002:2005. No total, foram alvo de estudo 8 áreas de controlo da norma, o que representa aproximadamente 73% do total de controlos deste normativo

Apesar do estado de segurança dos SI da ISS ser bastante elevado, foi possível propor um conjunto de otimizações com vista a alcançar melhorias significativas na sua atual política.

Conclui-se desta forma, uma etapa de melhoria de um sistema, através do auxílio das tecnologias de informação e comunicação, sem esquecer que a informação vai muito além do sistema tecnológico de suporte e que os métodos de a gerir, manter e guardar se encontram em permanente mudança.

Como tal, a flexibilidade das políticas de segurança deve permitir reagir prontamente e de forma adequada a qualquer alteração do risco, da necessidade de proteção e das vulnerabilidades detestadas no sistema.

A contínua monitorização, controlo e *reporting* constitui uma tarefa decisiva para alcançar o objetivo proposto e manter elevados índices de segurança, com a correspondente abrangência necessária, numa estratégia global que se pretende eficaz.

8.2 Perspetivas de trabalho futuro

No âmbito do trabalho desenvolvido, considera-se que o DSI deveria dar continuidade à análise realizada à atual política de segurança dos sistemas de informação.

Nesse sentido, para completar a análise realizada, o DSI deverá ter a perspetiva de analisar as áreas de controlo da norma ISO/IEC 27002:2005 não abordadas neste projeto:

- 8 – Segurança em recursos humanos;
- 12 – Aquisição, desenvolvimento e manutenção de sistemas de informação;
- 15 – Conformidade.

9 Anexos

Anexo A – Auditoria aos sistemas de informação

5 Políticas de segurança

5.1 Política de segurança da informação

Objetivo: Fornecer à Direção orientações e suporte para a segurança dos sistemas de informação em concordância com os requisitos do negócio e regulamentações pertinentes.

A Direção deve estabelecer uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação por toda a organização.

5.1.1 Documento de políticas de segurança dos sistemas de informação

- **Controlo**

Um documento de segurança de sistemas de informação deve ser aprovado pela Administração, publicado e comunicado a todos os colaboradores e parceiros externos relevantes.

- **Prática organizacional**

Existe uma política de segurança baseada na norma ISO/IEC 17799:2005 e devidamente aprovada pela direção. Todavia, não está publicada nem foi divulgada da devida forma aos colaboradores da organização.

5.1.2 Revisão da política de segurança da informação

- **Controlo**

A política de segurança da informação deve ser revista em intervalos planeados ou na ocorrência de alterações significativas na organização, de modo a assegurar a sua pertinência, adequação e eficácia.

- **Prática organizacional**

Embora exista uma pessoa responsável pelo desenvolvimento, revisão e avaliação do documento de políticas de segurança, o mesmo não é revisto em intervalos planeados ou na ocorrência de alterações significativas.

Propostas de otimização (5.1 - Política de segurança da informação)

- ***Descrição***

Sugere-se que seja identificado um período para revisão do documento de políticas de segurança (e.g. semestral) bem como a sua divulgação em canais privilegiados de comunicação interna, tais como, correio eletrónico e intranet.

- ***Prioridade***

3 – Ligeira

6 Organização da segurança

6.1 Organização interna

Objetivo: Gerir a segurança da informação dentro da organização.

Deve ser estabelecida uma *framework* de gestão para iniciar e controlar a implementação da segurança da informação dentro da organização.

A Direção deve aprovar a política de segurança da informação, atribuir papéis de segurança, coordenar e rever a implementação da segurança por toda a organização.

Se necessário, deve ser estabelecida uma fonte de consultoria especializada em segurança da informação e disponibilizada dentro da organização. Devem ser desenvolvidos contactos com grupos ou entidades externas especialistas em segurança, incluindo autoridades relevantes, para acompanhar as tendências da indústria, monitorizar *standards* e métodos de avaliação e estabelecer os adequados pontos de ligação quando estiver a lidar com incidentes de segurança da informação. Deve ser encorajada uma aproximação multidisciplinar.

6.1.1 Compromisso da Direção com a segurança da informação

- **Controlo**

A Direção deve apoiar ativamente a segurança dentro da organização, através de orientações claras, demonstrando o seu compromisso, definindo responsabilidades de forma clara e reconhecendo as responsabilidades pela segurança da informação.

- **Prática organizacional**

Em conformidade com a norma.

6.1.2 Coordenação da segurança da informação

- **Controlo**

As atividades de segurança devem ser coordenadas por representantes de diversas partes da organização com papéis e funções relevantes.

- **Prática organizacional**

Não conforme, porque neste momento a coordenação está assente numa única pessoa.

6.1.3 Atribuição de responsabilidades para a segurança da informação

- **Controlo**

Todas as responsabilidades para a segurança da informação devem ser claramente definidas.

- **Prática organizacional**

Em conformidade com a norma.

6.1.4 Processo de autorização para as infraestruturas de processamento da informação

- **Controlo**

Deve ser definido e implementado um processo de gestão de autorização para novas infraestruturas de processamento da informação.

- **Prática organizacional**

Em conformidade com a norma.

6.1.5 Acordos de confidencialidade

- **Controlo**

Devem ser identificados e regularmente revistos requisitos para acordos de confidencialidade e/ou de não divulgação, que reflitam as necessidades organizacionais de proteção da informação.

- **Prática organizacional**

Não conforme.

6.1.6 Contatos com autoridades

- **Controlo**

Devem ser mantidos contatos apropriados com autoridades relevantes.

- **Prática organizacional**

Não conforme.

6.1.7 Contatos com grupos de interesse especial

- **Controlo**

Devem ser mantidos contatos apropriados com grupos de interesse especial, fóruns especialistas em segurança da informação e associações profissionais.

- ***Prática organizacional***

Em conformidade com a norma.

6.1.8 Revisão independente da segurança da informação

- ***Controlo***

A estratégia organizacional para a gestão da segurança da informação e a sua implementação (e.g. controlos, objetivos dos controlos, políticas, processos e procedimentos para a segurança da informação) deve ser analisada por entidades independentes, em intervalos planeados ou quando ocorram alterações significativas, relativas à implementação da segurança.

- ***Prática organizacional***

Não conforme.

Propostas de otimização (6.1 – Organização interna)

- ***Descrição***

Sugere-se o envolvimento dos representantes das diversas partes da organização, com papéis e funções relevantes, de modo a que estes participem na coordenação das atividades de segurança. Os acordos de confidencialidade devem abranger todos os utilizadores que usufruam das infraestruturas de processamento da informação.

Quanto à comunicação com as autoridades, deve ser realizado um documento com os contactos de todas as entidades de segurança pública relevantes (e.g. bombeiros, proteção civil, polícia de segurança pública, entre outros) que operem na mesma zona que a ISS. O documento deve especificar concretamente em que casos e por quem são contactadas as referidas autoridades.

Por fim, sugere-se que a estratégia organizacional para a gestão da segurança da informação e a sua implementação seja analisada por entidades independentes em intervalos planeados ou quando ocorram alterações significativas, relativas à implementação da segurança.

- ***Prioridade***

3 – Afeta ligeiramente

6.2 Entidades externas

Objetivo: Manter a segurança da informação e das infraestruturas de processamento que são acedidas, processadas ou geridas por entidades externas.

A segurança da informação e das infraestruturas de processamento não deve ser reduzida pela introdução de produtos ou serviços de entidades externas.

Deve ser controlado o acesso das entidades externas às infraestruturas de processamento e comunicação da informação.

Deve ser efetuada uma análise de risco para determinar as implicações de segurança e requisitos de controlo, aquando da necessidade de trabalhar com entidades externas, que necessitem de acesso à informação ou infraestruturas de processamento da informação, ou ainda, na obtenção ou entrega de um produto ou serviço de ou para entidades externas.

6.2.1 Identificação de riscos relacionados com entidades externas

- **Controlo**

Devem ser identificados os riscos, para a informação e infraestruturas de processamento da informação da organização, dos processos de negócio que envolvam entidades externas. Devem ainda ser implementados controlos apropriados antes de se conceder o acesso.

- **Prática organizacional**

Em conformidade com a norma.

6.2.2 Identificação da segurança na interação com clientes

- **Controlo**

Devem ser identificados e considerados todos os riscos de segurança antes de conceder aos clientes acesso aos ativos ou à informação da organização.

- **Prática organizacional**

Não aplicável, em virtude de não existir acesso de clientes à informação da organização.

6.2.3 Identificação da segurança nos acordos com entidades externas

- **Controlo**

Devem ser contemplados todos os requisitos relevantes de segurança da informação nos acordos com entidades externas que envolvam o acesso, processamento, comunicação ou gestão da informação ou das infraestruturas de processamento da informação, ou o acréscimo de produtos e/ou serviços às infraestruturas de processamento de informação.

- ***Prática organizacional***

Em conformidade com a norma.

- ***Descrição***

Nenhuma otimização a aplicar.

- ***Prioridade***

Não aplicável.

7 Gestão dos recursos

7.1 Responsabilidade dos recursos

Objetivo: Alcançar e manter a proteção adequada dos recursos da organização.

Todos os recursos devem ser inventariados e devem ter um proprietário responsável.

Todos os proprietários dos recursos devem ser identificados e atribuída a responsabilidade pela apropriada manutenção dos controlos. A implementação dos controlos específicos pode ser delegada pelo proprietário, conforme apropriado, mas o proprietário mantém-se responsável pela devida proteção dos recursos.

7.1.1 Inventário dos recursos

- **Controlo**

Todos os recursos devem ser inequivocamente identificados e deve ser mantido um inventário de todos os recursos importantes.

- **Prática organizacional**

Todos os recursos são identificados com uma etiqueta da ISS, com uma numeração única, e registados na aplicação *ServiceDesk*.

7.1.2 Propriedade dos recursos

- **Controlo**

Todas as informações e recursos associados a infraestruturas de processamento da informação devem ter um proprietário designado pela organização.

- **Prática organizacional**

Está identificado na aplicação *ServiceDesk* um proprietário para cada recurso associado a infraestruturas de processamento da informação, sendo que, não são realizadas análises periódicas às classificações e restrições de acesso, tendo em conta as políticas de controlo em vigor.

7.1.3 Utilização aceitável dos recursos

- **Controlo**

Devem ser documentadas, classificadas e implementadas as regras para a utilização aceitável da informação e dos recursos das infraestruturas de processamento da informação.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (7.1 – Responsabilidade dos recursos)

- **Descrição**

Sugere-se que sejam realizadas análises periódicas às classificações e restrições de acesso, tendo em conta as políticas de controlo em vigor.

- **Prioridade**

2 – Afeta moderadamente

7.2 Classificação da informação

Objetivo: Assegurar que a informação receba um nível adequado de proteção.

A informação deve ser classificada de modo a que indique a necessidade, prioridades e nível de proteção esperado quando do tratamento da informação.

A informação tem vários níveis de sensibilidade e criticidade. Alguns itens podem requerer um nível adicional de proteção ou tratamento especial. Deve ser utilizado um esquema de classificação da informação para definir níveis de proteção apropriados e determinar a necessidade de tratamento especial.

7.2.1 Recomendações para classificação

- **Controlo**

A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

- **Prática organizacional**

Não existe um esquema ou matriz que classifique a informação, mas esta está separada mediante as várias áreas funcionais da organização ou pelo valor da informação.

7.2.2 Identificação e tratamento da informação

- **Controlo**

Devem ser definidos um conjunto de procedimentos para identificação e tratamento da informação de acordo com o esquema adotado pela organização.

- ***Prática organizacional***

Não existe uma matriz que estabeleça a classificação da informação, logo, não estão definidos os procedimentos para identificação e tratamento da informação de acordo com a mesma.

Propostas de otimização (7.2 – Classificação da informação)

- ***Descrição***

Sugere-se a elaboração de uma matriz para a classificação da informação e do seu valor para a organização. Após a elaboração da matriz, deverão ser desenvolvidos e implementados os procedimentos para identificação e tratamento da mesma.

- ***Prioridade***

3 – Afeta gravemente

9 Segurança física e ambiental

9.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

As infraestruturas críticas de processamento da informação devem estar alojadas em áreas seguras, protegidas por perímetros de segurança definidos com barreiras de segurança e controlos de acesso apropriados. Devem ser fisicamente protegidos de acessos não autorizados, danos e interferências.

A proteção oferecida deve ser compatível com os riscos identificados.

9.1.1 *Perímetro de segurança física*

- **Controlo**

Deve ser implementada uma barreira de segurança (e.g. paredes, verificação de controlo de acessos, entre outros) para proteger as áreas que contenham as informações ou infraestruturas de processamento da informação.

- **Prática organizacional**

Em conformidade com a norma, porque todo e qualquer acesso à organização é controlado por uma segurança que previne o acesso de estranhos. Não existe qualquer equipamento de processamento de informação que esteja acessível a pessoas estranhas à organização. Existem diversos perímetros de segurança no interior da mesma.

9.1.2 *Controlos de entrada física*

- **Controlo**

As áreas seguras devem ser protegidas por controlos de acesso apropriados que garantam que apenas é permitido o acesso a colaboradores autorizados.

- **Prática organizacional**

Em conformidade com a norma, através da utilização de terminais biométricos instalados nos diversos perímetros de segurança permitindo, unicamente, acesso a colaboradores autorizados.

9.1.3 *Segurança em escritórios, salas e instalações*

- **Controlo**

Deve ser definida e implementada segurança física em escritórios, salas e instalações.

- ***Prática organizacional***

Em conformidade com a norma, dado que o Centro de Processamento de Dados (CPD) da ISS está instalado numa câmara de segurança (*shelter*), localizada nas instalações de Carnaxide, devidamente projetada para alojar todo o equipamento informático. A câmara de segurança é composta por um material específico que garante proteção no caso de incêndio, desabamento de terras, inundações, gases corrosivos e poeiras, reforçando desta forma, a segurança de todo o equipamento do CPD. O acesso físico ao CPD é realizado por pessoal autorizado, com recurso à leitura de dados biométricos.

9.1.4 Proteção contra ameaças externas e ambientais

- ***Controlo***

Deve ser definida e implementada segurança física contra fogo, inundações, terremotos, explosões, desordem pública e outras formas de desastres.

- ***Prática organizacional***

Em conformidade com a norma, já que a utilização da câmara de segurança garante, na sua totalidade, a proteção física de todo o equipamento conforme mencionado no Controlo 9.1.3.

9.1.5 Trabalhar em áreas seguras

- ***Controlo***

Devem ser definidas e implementadas proteção física e recomendações para trabalhar em áreas seguras.

- ***Prática organizacional***

Existem áreas seguras, mas não estão documentados os procedimentos a ter quando são realizadas tarefas dentro das mesmas.

9.1.6 Acesso público e áreas de cargas e descargas

- ***Controlo***

Pontos de acesso, tais como, áreas de cargas e descargas e outros pontos por onde pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados das infraestruturas de processamento da informação de modo a evitar acessos não autorizados.

- ***Prática organizacional***

Em conformidade com a norma, visto que a área destinada à receção de pessoas estranhas ao serviço está inserida num perímetro de segurança que possui um responsável por controlar as

zonas de entrada do edifício. Os materiais recebidos nas instalações são sempre conferidos pelo responsável.

Propostas de otimização (9.1 – Áreas seguras)

- ***Descrição***

Sugere-se a elaboração de documentos que especifiquem os procedimentos a adotar quando são realizadas tarefas dentro das áreas seguras, nomeadamente, regras de segurança (e.g. situações de incêndio, falhas de segurança, desastres naturais, entre outros).

- ***Prioridade***

3 – Afeta ligeiramente

9.2 Segurança de equipamentos

Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de recursos e interrupção da atividade da organização.

Os equipamentos devem ser protegidos contra ameaças físicas e do meio ambiente.

A proteção dos equipamentos, incluindo os que são usados fora do local, é necessária para reduzir o risco de acesso não autorizado às informações e proteger contra perdas e danos. Podem ser necessários controlos adicionais para a proteção contra ameaças físicas e para a proteção de instalações de suporte, como a infraestrutura de fornecimento energético e de cablagem.

9.2.1 Localização e proteção de equipamentos

▪ *Controlo*

Os equipamentos devem estar localizados ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como, as oportunidades de acesso não autorizado.

▪ *Prática organizacional*

Em conformidade com a norma, na medida em que todos os equipamentos estão localizados em áreas seguras e com as devidas condições ambientais, tais como, temperatura, humidade, poeiras, entre outros.

9.2.2 Utilitários de suporte

▪ *Controlo*

Os equipamentos devem estar protegidos contra a falha energética e outras interrupções causadas por utilitários de suporte.

▪ *Prática organizacional*

Em conformidade com a norma, dado que existem múltiplas alimentações no CPD, evitando um único ponto de falha no fornecimento de energia. Os equipamentos cruciais para o correto funcionamento da atividade estão protegidos através de *Uninterruptable Power Systems* (UPS) e geradores a gasóleo. As instalações estão equipadas com luzes de emergência e os interruptores de energia de emergência estão devidamente localizados.

9.2.3 Segurança de cablagens

- **Controlo**

As cablagens de energia e telecomunicações que transportam dados ou que dão suporte aos serviços de informação devem ser protegidas contra interceção ou danos.

- **Prática organizacional**

As cablagens de telecomunicações e corrente elétrica estão instaladas com recurso a calhas técnicas e separadas de modo a prevenir interferências na comunicação. É utilizada cablagem de rede *Unshielded Twisted Pair* (UTP) categoria 6. A Cablagem está identificada através de numeração de modo a facilitar a sua identificação, contudo não existe um documento de correspondência entre os pontos de rede e os equipamentos.

9.2.4 Manutenção dos equipamentos

- **Controlo**

Os equipamentos devem ser alvo de uma correta manutenção de modo a assegurar a sua integridade e disponibilidade permanente.

- **Prática organizacional**

Os equipamentos são mantidos por pessoas autorizadas a realizar as operações de manutenção, de acordo com as recomendações do fabricante. O DSI é responsável por planear as ações de manutenção e manter os registos de reparação, embora nem sempre sejam realizados registos de todas as falhas e manutenções preventivas.

9.2.5 Segurança de equipamentos fora do perímetro da organização

- **Controlo**

Devem ter tomadas medidas de segurança para equipamentos que operem fora do local, tendo em consideração os diversos riscos decorrentes do facto de trabalhar fora da organização.

- **Prática organizacional**

Em conformidade com a norma, visto serem realizadas avaliações de risco à utilização de equipamentos de processamento da informação fora da organização. A instalação destes equipamentos só é realizada após aprovação da gestão.

9.2.6 Reutilização e alienação segura de equipamentos

- **Controlo**

Os suportes de dados de equipamentos devem ser analisados antes de serem descartados de modo a garantir que todos os dados sensíveis e *softwares* licenciados tenham sido removidos com segurança.

- **Prática organizacional**

Em conformidade com a norma. Todos os equipamentos da ISS estão ao abrigo de acordos de *leasing* e, aquando da sua devolução, são objeto de uma limpeza de todos os dados e/ou *softwares* licenciados.

9.2.7 Remoção de propriedade

- **Controlo**

Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.

- **Prática organizacional**

Em conformidade com a norma, uma vez que, existem controlos de segurança que não permitem a remoção de equipamento sem a devida aprovação. Todos os *softwares* originais são guardados e apenas o DSI tem acesso a este material. A utilização de câmaras de vigilância dentro dos escritórios garante a prossecução deste controlo.

Propostas de otimização (9.2 – Segurança de equipamentos)

- **Descrição**

Sugere-se a elaboração de um documento que faça corresponder os pontos de rede aos equipamentos (incluir identificação das placas de rede utilizadas, no caso de equipamentos que utilizem mais do que uma). No que respeita ao registo de falhas, sugere-se um maior rigor no seu registo na aplicação *ServiceDesk*. Um dos pontos mais críticos a evitar é a aceitação de pedidos de assistência por outro meio que não o *ServiceDesk*.

- **Prioridade**

3 – Afeta ligeiramente

10 Gestão das operações e comunicações

10.1 Procedimentos e responsabilidades operacionais

Objetivo: Garantir a operação correta e segura dos recursos de processamento da informação.

Devem ser estabelecidas responsabilidades e procedimentos para a gestão e operação de todos os recursos de processamento da informação. Isto inclui o desenvolvimento de procedimentos operacionais apropriados.

Deve ser utilizada a segregação de funções, quando possível, para reduzir o risco de má utilização ou uso negligente dos sistemas.

10.1.1 Documentação dos procedimentos de operação

- **Controlo**

Os procedimentos operacionais devem ser documentados, mantidos, atualizados e disponibilizados a todos os utilizadores que deles necessitem.

- **Prática organizacional**

Existem procedimentos operacionais documentados, mantidos e atualizados, embora não abranjam a totalidade dos processos inerentes aos Sistemas de Informação.

10.1.2 Gestão de mudanças

- **Controlo**

As modificações nos recursos de processamento da informação e sistemas devem ser controladas.

- **Prática organizacional**

Em conformidade com a norma, visto ser regra a presença de pelo menos um elemento do DSI quando é necessário realizar qualquer modificação nos recursos de processamento de informação.

10.1.3 Segregação de funções

- **Controlo**

As funções e áreas de responsabilidade devem ser segregadas de modo a reduzir as oportunidades de acesso não autorizado ou modificação não intencional dos recursos da organização.

- ***Prática organizacional***

Face à pequena dimensão do DSI, existe algo semelhante a uma política de segregação de funções, mas a mesma está na base de uma relação de confiança e não através de mecanismos de controlo.

10.1.4 Separação dos recursos de desenvolvimento, teste e de produção

- ***Controlo***

Os recursos de desenvolvimento, teste e de produção devem ser separados de modo a reduzir o risco de acessos ou modificações não autorizados aos sistemas operacionais.

- ***Prática organizacional***

Não existem ambientes distintos de desenvolvimento, de testes e de produção para todos os sistemas operacionais.

Propostas de otimização (10.1 – Procedimentos e responsabilidades operacionais)

- ***Descrição***

Sugere-se o alargamento da documentação de todos os procedimentos operacionais inerentes ao DSI e revisão periódica (e.g. anual) e/ou quando os procedimentos forem alvo de alterações significativas.

Quanto à segregação de funções, devido à pequena dimensão do DSI, compreende-se a dificuldade de implementação deste controlo, pelo que, se sugere que sejam implementados outros controlos adicionais, tais como, monitorização de atividades, auditoria, maior supervisão por parte da gestão, entre outros.

Em relação à separação dos recursos, o objetivo passa por implementar a separação em todos os sistemas operacionais, embora conscientes da dificuldade do cumprimento deste controlo, principalmente pela componente financeira.

- ***Prioridade***

2 – Afeta moderadamente

10.2 Gestão de serviços prestados por terceiros

Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos definidos com terceiros.

A organização deve verificar a implementação dos acordos, monitorizar a sua conformidade e gerir as mudanças de modo a garantir que os serviços entregues estão de acordo com os requisitos acordados com os terceiros.

10.2.1 Entrega de serviços

- **Controlo**

Deve ser assegurado que os controlos de segurança, as definições de serviço e os níveis de entrega incluídos nos acordos de prestação de serviços com terceiros, são implementados executados e mantidos.

- **Prática organizacional**

Em conformidade com a norma. As definições de serviço e os níveis de entrega são sempre definidos a nível contratual ou, quando este não existe, por ser um terceiro pouco recorrente, a nível da proposta/adjudicação de serviço.

10.2.2 Revisão e monitorização de serviços prestados por terceiros

- **Controlo**

Os serviços, relatórios e registos fornecidos por terceiros devem ser monitorizados e revistos regularmente. Quando possível, devem ser realizadas auditorias regulares.

- **Prática organizacional**

Embora exista um controlo por parte dos elementos do DSI sobre os trabalhos realizados por terceiros, não são realizadas auditorias regulares.

10.2.3 Gestão de mudanças para serviços prestados por terceiros

- **Controlo**

A mudança de provisão de serviços prestados por terceiros, incluindo a manutenção e melhoramento de políticas de segurança da informação, procedimentos e controlos existentes, devem ser geridos tendo em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.

- **Prática organizacional**

Não implementado.

Propostas de otimização (10.2 – Gestão de serviços prestados por terceiros)

▪ *Descrição*

Sugere-se a realização de auditorias regulares para a revisão e monitorização de serviços prestados por terceiros, através da utilização de formulários e/ou de *software* apropriado.

Não existindo qualquer processo de controlo da Gestão de mudanças para serviços prestados por terceiros, sugere-se que o DSI participe ativamente nas reuniões de gestão estratégica da organização, para que, sempre que necessário, solicite aos terceiros um ajuste dos serviços prestados com o objetivo dos mesmos se adequarem à nova estratégia/necessidades.

Também deve ser comunicado pelos terceiros, por via formal, todas e quaisquer alterações aos serviços prestados e, sempre que possível, validado pelo DSI.

▪ *Prioridade*

1 – Afeta gravemente

10.3 Planeamento e aceitação dos sistemas

Objetivo: Minimizar o risco de falhas nos sistemas.

O planeamento e a preparação prévios são requeridos para garantir a disponibilidade adequada de capacidade e recursos para entrega do desempenho desejado do sistema.

Devem ser efetuadas projeções de requisitos de capacidade futura, com o objetivo de reduzir o risco de sobrecarga dos sistemas.

Devem ser definidos, documentados e testados os requisitos operacionais para novos sistemas antes da sua aceitação e implementação.

10.3.1 *Gestão de capacidade*

▪ *Controlo*

A utilização dos recursos deve ser monitorizada e ajustada, e devem ser efetuadas projeções para requisitos futuros de capacidade, de forma a garantir o desempenho desejado do sistema.

▪ *Prática organizacional*

Em conformidade com a norma, uma vez que, são executados e analisados semanalmente indicadores de *performance* com vista a avaliar a capacidade dos recursos de processamento da informação e eventual necessidade de ajuste.

10.3.2 Aceitação de Sistemas

- **Controlo**

Devem ser definidos critérios formais de aceitação para novos sistemas, atualizações e novas versões, devendo também, serem realizados testes apropriados do(s) sistema(s) durante o seu desenvolvimento e antes da sua aceitação.

- **Prática organizacional**

Para sistemas Microsoft (e.g. sistemas operativo e aplicações de produtividade) e *software* partilhado pelo Grupo IT – ISS A/S (e.g. *Dynamic CRM, e-monitoring, hyperion*, entre outros) existe um procedimento formal de aceitação de novos sistemas, atualizações e novas versões. Para os restantes não existe qualquer procedimento formal.

Propostas de otimização (10.3 – Planeamento e aceitação dos sistemas)

- **Descrição**

Para os sistemas atualmente não abrangidos por procedimentos formais para Aceitação de Sistemas, sugere-se a implementação de uma aplicação (e.g. Microsoft Systems Management Server), que permite, de forma simplificada, a gestão de atualizações e novas versões.

- **Prioridade**

2 – Afeta moderadamente

10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

São necessárias proteções para prevenir e detetar a introdução de códigos maliciosos e códigos móveis não autorizados.

As infraestruturas de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como, vírus de computador, *worms* de rede, cavalos de Troia e bombas lógicas. Os utilizadores devem estar conscientes dos perigos do código malicioso. Quando apropriado, os gestores das infraestruturas de processamento da informação devem implementar controlos para prevenir, detetar e remover código malicioso e controlar códigos móveis.

10.4.1 Controlos contra códigos maliciosos

- **Controlo**

Devem ser implementados controlos de deteção, prevenção e recuperação para proteção contra códigos maliciosos, assim como procedimentos para a devida consciencialização dos utilizadores.

- **Prática organizacional**

Em conformidade com a norma.

10.4.2 Controlos contra código móvel

- **Controlo**

Onde o uso de código móvel seja autorizado, a configuração deve garantir que o código móvel opere de acordo com uma política de segurança da informação claramente definida e que códigos móveis não autorizados tenham a sua execução impedida.

- **Prática organizacional**

Não implementado.

Propostas de otimização (10.4 – Proteção contra códigos maliciosos e códigos móveis)

- **Descrição**

Sugere-se a implementação e divulgação pelos utilizadores de políticas de segurança que regulamentem a utilização de códigos móveis e implementem medidas que impeçam que a execução de código móvel não autorizado.

- **Prioridade**

2 – Afeta moderadamente

10.5 Cópias de segurança

Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

Devem ser estabelecidos procedimentos de rotina para implementar as políticas e estratégias definidas para a criação de cópias de segurança (ver 14.1) e possibilitar a criação de cópias de segurança dos dados e a sua recuperação em tempo útil.

10.5.1 Cópias de segurança das informações

- **Controlo**

As cópias de segurança das informações e dos *softwares*, devem ser regularmente efetuadas e testadas conforme a política definida.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (10.5 – Cópias de segurança)

- **Descrição**

Nenhuma otimização a aplicar.

- **Prioridade**

Não aplicável.

10.6 Gestão da segurança das redes

Objetivo: Garantir a proteção das informações na rede e a proteção da infraestrutura de suporte.

A gestão segura das redes, que pode ir para além da organização, requer cuidadosas considerações relacionadas com o fluxo de dados, implicações legais, monitorização e proteção.

Podem ser necessários controlos adicionais para proteger informações sensíveis a passar sobre as redes públicas.

10.6.1 Controlos das redes

- **Controlo**

As redes devem ser adequadamente geridas e controladas, de forma a protegê-las contra ameaças e a manter a segurança de sistemas e aplicações que as utilizam, incluindo a informação em trânsito.

- **Prática organizacional**

Existem alguns controlos contra ameaças na rede (desenvolvidos em 11.4 – Controlo de acesso à rede), mas insuficientes face aos riscos existentes, nomeadamente, ausência de sistemas de deteção de intrusão.

10.6.2 Segurança dos serviços de rede

- **Controlo**

As características de segurança, níveis de serviço e requisitos de gestão dos serviços de rede devem estar identificados e incluídos em qualquer acordo de serviços de rede, quer para serviços fornecidos internamente quer para serviços prestados por terceiros.

- **Prática organizacional**

Em conformidade com a norma, na medida em que foram estabelecidos, ao nível contratual, os níveis de serviço e gestão de requisitos de toda a rede, bem como a capacidade do prestador de serviços para uma gestão segura.

Propostas de otimização (10.6 – Gestão da segurança das redes)

- **Descrição**

Sugere-se a instalação de um sistema de deteção de intrusão, com o propósito de tornar mais proactivo o DSI, isto é, minimizar o risco de exposição da informação a eventuais ataques externos.

- **Prioridade**

1 - Severa

10.7 Manuseio de suportes de dados

Objetivo: Prevenir acesso não autorizado, modificação, remoção ou destruição de bens e a interrupção das atividades do negócio.

Os suportes de dados devem ser controlados e protegidos fisicamente.

Devem ser estabelecidos procedimentos operacionais adequados para proteger documentos, suportes de dados (e.g. tapes, discos), dados de entrada e saída e documentação dos sistemas contra divulgação não autorizada, modificação, remoção e destruição.

10.7.1 Gestão de suportes de dados amovíveis

- **Controlo**

Devem existir procedimentos implementados para a gestão de suportes de dados amovíveis.

- **Prática organizacional**

Existem procedimentos para as tapes, nomeadamente, no que respeita ao seu armazenamento, utilização, transporte e descontinuação.

10.7.2 Inutilização de suportes de dados

- **Controlo**

Os suportes de dados devem ser inutilizados de forma segura e protegida quando já não forem necessários, com recurso a procedimentos formais.

- **Prática organizacional**

Os suportes são inutilizados de forma segura quando atingem o fim de vida útil, todavia, não existe nenhum procedimento formal para esta operação.

10.7.3 Procedimentos para tratamento da informação

- **Controlo**

Devem ser estabelecidos procedimentos para o tratamento e armazenamento de informações, para as proteger contra a divulgação não autorizada ou uso indevido.

- **Prática organizacional**

Em conformidade com a norma, uma vez que, todos os suportes amovíveis de dados são armazenados em cofres preparados para esse efeito e cujo acesso é realizado, unicamente, por pessoal autorizado.

10.7.4 Segurança da documentação dos sistemas

- **Controlo**

A documentação dos sistemas deve ser protegida contra acessos não autorizados.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (10.7 – Manuseio de suportes de dados)

- **Descrição**

Sugere-se a implementação de procedimentos para gestão de suportes de dados amovíveis, excluindo as tapes, bem como o desenvolvimento de um controlo rigoroso e eficaz para a Inutilização de suportes de dados.

- **Prioridade**

2 - Moderada

10.8 Troca de informação

Objetivo: Manter o nível de segurança na troca de informação e *software* dentro e fora da organização.

A troca de informação e *software* entre organizações deve estar baseada numa política formal específica, através de um acordo entre as partes, devendo este estar em conformidade com toda a legislação pertinente.

Devem ser estabelecidos procedimentos e normas para proteger a informação e os suportes de dados físicos que contenham informação em trânsito.

10.8.1 Políticas e procedimentos para troca de informação

- **Controlo**

As políticas, procedimentos e controlos devem ser estabelecidos e formalizados de modo a proteger a troca de informação em todos os tipos de recursos de comunicação.

- **Prática organizacional**

Existe alguma atenção no que respeita à troca de informação, contudo, o nível de sensibilidade dos dados da organização nunca obrigou à implementação de procedimentos formais que previnam a interceção, cópia e modificação da informação. Pelos mesmos motivos (sensibilidade da informação), também não são utilizadas quaisquer técnicas de encriptação de dados. Não obstante, os colaboradores assinam termos de confidencialidade e são sensibilizados no sentido de evitarem deixar informação crítica em locais comuns (e.g. impressoras, centros de cópias).

10.8.2 Acordos para a troca de informação

- **Controlo**

Devem ser estabelecidos acordos para troca de informação e *software* entre a organização e entidades externas.

- **Prática organizacional**

A ISS tem uma *shortlist* de fornecedores de IT, com alguns dos quais já trabalha há largos anos, pelo que a confidencialidade da troca de informação está assente, maioritariamente, em relações de confiança ao invés de procedimentos formais, embora existam alguns.

10.8.3 Suportes de dados em trânsito

- **Controlo**

Os suportes de dados que contenham informação devem ser protegidos contra acessos não autorizados, uso impróprio ou alteração inadvertida durante o transporte externo aos limites físicos da organização.

- **Prática organizacional**

Em conformidade com a norma.

10.8.4 Mensagens eletrónicas

- **Controlo**

As informações que transitam em mensagens eletrónicas devem ser devidamente protegidas.

- **Prática organizacional**

Implementado parcialmente porque o serviço de correio eletrónico da ISS é gerido a nível mundial, por uma entidade certificada, garantindo desta forma o correto endereçamento e transporte das mensagens, disponibilidade e viabilidade do serviço, proteção contra acesso não autorizado e *Denial of Service*. Por outro lado, por opção da ISS em Portugal, não são utilizadas assinaturas digitais, logo, não é possível garantir que as mensagens se mantenham inalteradas.

10.8.5 Sistemas de informação do negócio

- **Controlo**

Devem ser desenvolvidos e implementados políticas e procedimentos para proteger as informações associadas com a interligação de sistemas de informação do negócio.

- **Prática organizacional**

Em conformidade com a norma. Sempre que é necessário estabelecer comunicações com entidades externas, são avaliados os riscos inerentes às operações e implementados os devidos procedimentos, de acordo com as boas práticas.

Propostas de otimização (10.8 – Troca de informação)

- **Descrição**

Podemos concluir que existe uma sensibilidade para este controlo, mas existe uma forte lacuna na formalização dos procedimentos, nomeadamente, criação de termos de confidencialidade e manuseamento da informação para todas as pessoas e entidades internas e externas.

No que respeita à troca eletrónica de mensagens, sugerimos a aquisição de assinaturas digitais, pelo menos, para os utilizadores mais críticos.

- **Prioridade**

2 - Moderada

10.9 Serviços de comércio eletrónico

Não aplicável ao negócio da ISS em Portugal

10.10 Monitorização

Objetivo: Detetar atividades não autorizadas de processamento de informação.

Os sistemas de informação devem ser monitorizados e devem ser registados eventos de segurança da informação.

Os registos (*logs*) de utilizador e registos de falhas devem ser utilizados para assegurar que os problemas de sistemas de informação são identificados.

As organizações devem estar de acordo com todos os requisitos legais relevantes aplicáveis à atividade de registo e monitorização.

A monitorização do sistema deve ser utilizada para verificar a eficácia dos controlos adotados e para verificar a conformidade com os modelos de política de acesso.

10.10.1 Registos de auditoria

- **Controlo**

Os registos de auditoria que contenham atividades dos utilizadores e outros eventos de segurança, devem ser produzidos e mantidos por um período de tempo acordado, para auxiliar em futuras investigações e monitorização de controlo de acesso.

- **Prática organizacional**

São mantidos alguns registos de auditoria referentes a algumas das ações realizadas pelos utilizadores, nomeadamente, acessos a sistemas operativos e aplicações, mas não ao nível de detalhe enunciado no controlo.

10.10.2 Monitorização da utilização do sistema

- **Controlo**

Devem ser estabelecidos procedimentos para a monitorização da utilização dos recursos de processamento da informação e os resultados das atividades de monitorização devem ser analisados com regularidade.

- **Prática organizacional**

São efetuados alguns registos de monitorização dos recursos de processamento de informação através do *Event Viewer*, mas não ao nível de detalhe enunciado no controlo.

10.10.3 Proteção da informação dos registos

- **Controlo**

Os recursos e informações dos registos devem ser protegidos contra falsificação e acesso não autorizado.

- **Prática organizacional**

Em conformidade com a norma.

10.10.4 Registos de administrador e utilizador

- **Controlo**

As atividades dos administradores e utilizadores do sistema devem ser registadas.

- **Prática organizacional**

São efetuados alguns registos das atividades dos administradores e utilizadores, mas não ao nível de detalhe enunciado no controlo.

10.10.5 Registos de falhas

- **Controlo**

As falhas ocorridas devem ser registadas e analisadas, e devem adotadas ações apropriadas para a correção das mesmas.

- **Prática organizacional**

Em conformidade com a norma, para os procedimentos em vigor.

10.10.6 Sincronização dos relógios

- **Controlo**

Os relógios de todos os sistemas de processamento de informação relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa, previamente acordada.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (10.10 – Monitorização)

- **Descrição**

Sugere-se um aumento do detalhe do nível de auditoria, isto é, que o mesmo tenha em conta o acesso a todos os objetos e/ou aplicações, conforme indicado no controlo.

- **Prioridade**

1 - Severa

11 Controlo de Acessos

11.1 Requisitos de negócio para o controlo de acesso

Objetivo: Controlar o acesso à informação.

O acesso à informação, infraestruturas de processamento da informação e processos de negócio devem ser controlados, com base nos requisitos de negócio e segurança da informação.

As regras de controlo de acesso devem ter em consideração as políticas para autorização e disseminação da informação.

11.1.1 Política de controlo de acessos

- **Controlo**

A política de controlo de acessos deve ser estabelecida, documentada e revista com base nos requisitos de negócio e de segurança da informação.

- **Prática organizacional**

Embora os acessos físicos e lógicos sejam atribuídos em consonância com a política da organização, os mesmos não são revistos periodicamente e não são entregues, quer a colaboradores quer a entidades externas, quaisquer declarações dos requisitos de negócio que devem ser cumpridos.

Propostas de otimização (11.1 – Requisitos de negócio para o controlo de acesso)

- **Descrição**

Sugere-se a criação de uma declaração que indique os requisitos de negócio que devem ser cumpridos pelos controlos de acesso, e estes devem ser entregues aos colaboradores e às entidades externas. É ainda sugerido que os controlos de acesso sejam definidos pelo DSI, com uma periodicidade previamente definida (e.g. semestral), juntamente com os responsáveis de cada departamento.

- **Prioridade**

3 - Severa

11.2 Gestão de acessos do utilizador

Objetivo: Assegurar o acesso do utilizador autorizado e prevenir acesso não autorizado a sistemas de informação.

Devem ser implementados procedimentos formais para controlar a distribuição de direitos de acesso a serviços e sistemas de informação.

Os procedimentos devem cobrir todas as fases do ciclo de vida de acesso do utilizador desde o seu registo inicial, como novos utilizadores, até ao cancelamento final do registo. Deve ser dada atenção especial, quando apropriado, para a necessidade de controlar a distribuição de direitos de acesso privilegiado que permitam aos utilizadores mudar o controlo de sistemas.

11.2.1 Registo do utilizador

- **Controlo**

Deve existir um procedimento formal para o registo e cancelamento de utilizador para garantir e revogar os acessos em todos os serviços e sistemas de informação.

- **Prática organizacional**

Em conformidade com norma, visto que todos os pedidos de registo e cancelamento de utilizador são registados na aplicação *ServiceDesk*.

11.2.2 Gestão de privilégios

- **Controlo**

A concessão e utilização de privilégios devem ser restritas e controladas.

- **Prática organizacional**

Em conformidade com a norma.

11.2.3 Gestão da palavra-passe de utilizador

- **Controlo**

A concessão de palavras-passe deve ser controlada através de um processo de gestão formal.

- **Prática organizacional**

Não conforme.

11.2.4 Revisão dos direitos de acesso de utilizador

- **Controlo**

O gestor deve realizar, em intervalos regulares, e com recurso a um processo formal, a revisão dos direitos de acesso dos utilizadores.

- **Prática organizacional**

Não conforme.

Propostas de otimização (11.2 – Gestão de acessos do utilizador)

- **Descrição**

Sugere-se a implementação de um procedimento formal de atribuição de palavras-passe, com recurso a um documento que vise não só formalizar este procedimento, mas também responsabilizar o utilizador pela indevida utilização da mesma.

Sugere-se adicionalmente a implementação de um processo formal de revisão dos direitos dos utilizadores, com um intervalo regular definido (e.g. semestral).

- **Prioridade**

1 - Severa

11.3 Responsabilidades dos utilizadores

Objetivo: Prevenir o acesso não autorizado dos utilizadores e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

A cooperação de utilizadores autorizados é essencial para uma segurança efetiva.

Os utilizadores devem estar conscientes das suas responsabilidades para manter um efetivo controlo de acesso, particularmente em relação à utilização de palavras passe e à segurança dos seus equipamentos.

Deve ser implementada uma política de mesa e ecrã limpo de forma a reduzir o risco de acessos não autorizados ou danos a documentos/papéis, suportes de dados e recursos de processamento da informação

11.3.1 Utilização de palavras-passe

- **Controlo**

Os utilizadores devem ser solicitados a seguir as boas práticas de segurança da informação na seleção e utilização de palavras-passe.

- ***Prática organizacional***

Em conformidade com a norma.

11.3.2 Equipamento sem monitorização

- ***Controlo***

Os utilizadores devem assegurar que os equipamentos sem monitorização tenham a proteção adequada.

- ***Prática organizacional***

Em conformidade com a norma.

11.3.3 Política de mesa e ecrã limpo

- ***Controlo***

Deve ser adotada uma política de mesa limpa de papéis e de suportes de dados removíveis e política de ecrã limpo para os recursos de processamento da informação.

- ***Prática organizacional***

Em conformidade com a norma.

Propostas de otimização (11.3 – Responsabilidades dos utilizadores)

- ***Descrição***

Nenhuma otimização a aplicar.

- ***Prioridade***

Não aplicável.

11.4 Controlo de acesso à rede

Objetivo: Prevenir acessos não autorizados aos serviços de rede.

O acesso aos serviços de rede internos e externos deve ser controlado.

Os utilizadores com acessos às redes e aos serviços de rede não devem comprometer a segurança desses serviços e devem assegurar:

a) utilização de interfaces apropriadas entre a rede da organização e as redes de outras organizações e/ou redes públicas;

b) utilização de mecanismos de autenticação apropriados para os utilizadores e equipamentos;

c) execução do controlo de acesso de utilizadores aos serviços de informação.

11.4.1 Política de utilização dos serviços de rede

- **Controlo**

Os utilizadores devem receber acesso apenas para os serviços que tenham sido especificamente autorizados a utilizar.

- **Prática organizacional**

Em conformidade com a norma.

11.4.2 Autenticação para ligação externa do utilizador

- **Controlo**

Devem ser utilizados métodos apropriados de autenticação para controlar acessos de utilizadores remotos.

- **Prática organizacional**

Em conformidade com a norma.

11.4.3 Identificação de equipamentos em redes

- **Controlo**

Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar ligações originadas de localizações e equipamentos específicos.

- **Prática organizacional**

Não conforme.

11.4.4 Configuração de proteção de portas de diagnóstico remoto

- **Controlo**

Devem ser controlados os acessos físicos e lógicos a portas de diagnóstico remoto.

- **Prática organizacional**

Não conforme.

11.4.5 Segregação de redes

- **Controlo**

Grupos de serviço de informação, utilizadores e sistemas de informação devem ser segregados em redes.

- **Prática organizacional**

Em conformidade com a norma.

11.4.6 Controlo de conexão de rede

- **Controlo**

Para redes partilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de ligação dos utilizadores deve ser restrita, alinhada com a política de controlo de acesso e os requisitos de aplicações do negócio.

- **Prática organizacional**

Em conformidade com a norma.

11.4.7 Controlo de roteamento das redes

- **Controlo**

Deve ser implementado controlo de roteamento na rede, de modo a assegurar que as ligações de computadores e fluxos de informação não violem a política de controlo de acesso das aplicações do negócio.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (11.4 – Controlo de acesso à rede)

- **Descrição**

Sugere-se a implementação de um sistema de identificação de equipamentos em rede (e.g. identificação de *Mac Address*, aquisição de soluções tipo NAC – *Network Admission Control* ,

bloqueio de portas de *switch*, etc...) de modo a evitar a ligação de equipamentos não autorizados.

Sugere-se adicionalmente, a realização de um estudo aprofundado sobre a necessidade de utilização de todas as portas de diagnóstico ativas, visto não existir qualquer documentação sobre o seu atual estado.

- ***Prioridade***

1 - Severa

11.5 Controlo de acesso ao sistema operativo

Objetivo: Prevenir acesso não autorizado aos sistemas operativos.

Os recursos de segurança da informação devem ser usados para restringir o acesso aos sistemas operativos a utilizadores autorizados. Estes recursos devem permitir:

- a) autenticação de utilizadores autorizados, de acordo com a política de controlo de acesso definida;
- b) registo das tentativas de autenticação nos sistemas com sucesso ou falha;
- c) registo de utilização de privilégios especiais no sistema;
- d) disparo de alarme quando as políticas de segurança dos sistema são violadas;
- e) fornecer meios apropriados para autenticação;
- f) restrição do tempo de ligação dos utilizadores, quando aplicável.

11.5.1 Procedimentos seguros de entrada no sistema (log-on)

- ***Controlo***

O acesso aos sistemas operativos deve ser controlado por um procedimento seguro de entrada no sistema (*log-on*).

- ***Prática organizacional***

Em conformidade com a norma.

11.5.2 Identificação e autenticação de utilizador

- **Controlo**

Todos os utilizadores devem possuir um identificador único (ID de utilizador) para uso pessoal e exclusivo, e deve existir uma técnica adequada de autenticação para validar a identidade do utilizador.

- **Prática organizacional**

Em conformidade com a norma.

11.5.3 Sistema de gestão de palavra-passe

- **Controlo**

Os sistemas de gestão de palavras-passe devem ser interativos e devem assegurar palavras-passe de qualidade.

- **Prática organizacional**

Em conformidade com a norma.

11.5.4 Utilização de utilitários de sistema

- **Controlo**

A utilização de programas utilitários capazes de se sobreporem aos controlos dos sistemas e aplicações devem ser restritos e estritamente controlados.

- **Prática organizacional**

Não aplicável, visto a organização não possuir esse tipo de *software*.

11.5.5 Limite de tempo de sessão

- **Controlo**

As sessões inativas devem ser encerradas após um período definido de inatividade.

- **Prática organizacional**

Em conformidade com a norma.

11.5.6 Limitação de horário de conexão

- **Controlo**

Devem ser utilizadas restrições nos horários de conexão de modo a proporcionar segurança adicional para aplicações de alto risco.

- **Prática organizacional**

Não aplicável, visto ser pratica e necessidade da empresa, que os sistemas estejam disponíveis 24/7, exceto na realização dos *backups* e/ou intervenções técnicas previamente agendadas.

Propostas de otimização (11.5 – Controlo de acesso ao sistema operativo)

- **Descrição**

Nenhuma otimização a aplicar.

- **Prioridade**

Não aplicável.

11.6 Controlo de acesso à aplicação e à informação

Objetivo: Prevenir o acesso não autorizado à informação contida nos sistemas de aplicação.

Os recursos de segurança da informação devem ser utilizados para restringir o acesso aos sistemas de aplicação.

O acesso lógico à aplicação e informação deve ser restrito a utilizadores autorizados. Os sistemas de aplicação devem:

a) controlar o acesso dos utilizadores à informação e às funções dos sistemas de aplicação, de acordo com uma política de controlo de acesso definida;

b) proporcionar proteção contra acesso não autorizado para qualquer *software* utilitário, sistema operativo e *software* malicioso, que seja capaz de se sobrepor ou contornar os controlos da aplicação ou dos sistemas operativos;

c) não comprometer outros sistemas com os quais os recursos de informação são compartilhados.

11.6.1 Restrição de acesso à informação

- **Controlo**

O acesso à informação e às funções dos sistemas de aplicações por utilizadores e pessoal de suporte deve ser restrito e de acordo com o definido na política de controlo de acesso.

- **Prática organizacional**

Em conformidade com a norma.

11.6.2 Isolamento de sistemas sensíveis

- **Controlo**

Os sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (11.6 – Controlo de acesso à aplicação e à informação)

- **Descrição**

Nenhuma otimização a aplicar.

- **Prioridade**

Não aplicável.

11.7 Computação móvel e teletrabalho

Objetivo: Garantir a segurança da informação quando se utiliza a computação móvel e recurso a teletrabalho.

A proteção requerida deve ser proporcional ao risco inerente a esta forma de trabalho. Quando se utiliza a computação móvel, os riscos de trabalhar num ambiente desprotegido devem ser considerados e deve ser aplicada a proteção adequada. No caso do teletrabalho a organização deve aplicar proteção ao local do teletrabalho e assegurar que os requisitos de segurança adequados estão implementados.

11.7.1 Computação e comunicação móvel

- **Controlo**

Deve ser estabelecida uma política formal e devem ser tomadas medidas apropriadas para a proteção contra os riscos da utilização de recursos de computação e comunicação móvel.

- **Prática organizacional**

Existe uma política formal embora não divulgada de forma eficaz. Mais, as medidas de segurança adotadas contra o risco de utilização de computação e comunicação, não são as mais eficazes, visto não terem em conta os principais riscos.

11.7.2 Teletrabalho

- ***Controlo***

Devem ser desenvolvidas políticas, planos operacionais e procedimentos, e garantida a sua implementação, para as atividades de teletrabalho.

- ***Prática organizacional***

Em conformidade com a norma.

Propostas de otimização (11.7 – Computação móvel e teletrabalho)

- ***Descrição***

Sugere-se a realização de um estudo sobre a necessidade de utilização de computação móvel na organização e os riscos inerentes. Caso exista, devem ser identificados os utilizadores com essa necessidade, e estes devem ser formalmente informados sobre as regras de utilização.

- ***Prioridade***

2 - Moderada

13 Gestão de incidentes de segurança da informação

13.1 Notificação de vulnerabilidades e eventos de segurança da informação

Objetivo: Assegurar que vulnerabilidades e eventos de segurança da informação associados a sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo útil.

Devem ser estabelecidos procedimentos formais de registo e escalonamento. Todos os colaboradores e entidades externas devem estar conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e vulnerabilidades que possam ter impacto na segurança dos ativos da organização. Deve ser requerido que os eventos de segurança da informação e de vulnerabilidades sejam notificados, tão breve quanto possível, ao ponto de contacto designado para o efeito.

13.1.1 Notificação de eventos de segurança da informação

- **Controlo**

Os eventos de segurança da informação devem ser relatados através dos canais apropriados da direção, com a maior brevidade possível.

- **Prática organizacional**

Os eventos de segurança são comunicados, embora não exista um procedimento formal que os obrigue a serem relatados através dos canais apropriados da direção.

13.1.2 Notificação de vulnerabilidades de segurança da informação

- **Controlo**

Os colaboradores e entidades externas ligados aos sistemas e serviços de informação devem ser instruídos a registar e notificar qualquer observação ou suspeita de fragilidade.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (13.1 – Notificação de vulnerabilidades e eventos de segurança da informação)

▪ *Descrição*

Deve ser implementado um procedimento formal para a notificação de eventos de segurança da informação, junto com um procedimento de resposta a incidente e escalonamento, identificando a ação a ser adotada ao receber um evento de segurança da informação.

▪ *Prioridade*

2 - Moderada

13.2 Gestão de incidentes de segurança da informação e melhorias

Objetivo: Assegurar que seja dado um enfoque consistente e efetivo à gestão de incidentes de segurança da informação.

Devem ser definidos responsabilidades e procedimentos para o manuseio efetivo de eventos de segurança da informação e vulnerabilidades, assim que estes tenham sido comunicados. Deve existir um processo de melhoria contínua aplicado às respostas, monitorização, avaliação e gestão total de incidentes de segurança da informação.

A recolha de provas, sempre que exigida, deve assegurar a conformidade com as exigências legais.

13.2.1 Responsabilidades e procedimentos

▪ *Controlo*

As responsabilidades e procedimentos de gestão devem ser estabelecidos de modo a assegurar respostas rápidas, efetivas e ordenadas de incidentes de segurança da informação.

▪ *Prática organizacional*

Existem procedimentos que asseguram respostas rápidas para os recursos de processamento da informação, onde são realizados registos de monitorização (ver 10.10.2), embora não de um modo formal.

13.2.2 Aprendizagem com os incidentes de segurança da informação

▪ *Controlo*

Devem ser estabelecidos mecanismos com o objetivo de permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorizados.

- ***Prática organizacional***

A organização não possui qualquer mecanismo que permita quantificar o custo dos incidentes. No que respeita à análise dos incidentes de segurança é feito algum registo através da aplicação *ServiceDesk*, embora de uma forma pouco regular, mas ainda assim permitindo alguma aprendizagem.

13.2.3 Recolha de provas

- ***Controlo***

Nos casos em que uma ação de acompanhamento contra uma organização ou pessoa, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), as provas devem ser recolhidas, armazenadas e apresentadas em conformidade com as normas de armazenamento de provas da(s) jurisdição(ões) pertinente(s).

- ***Prática organizacional***

Não conforme. A organização nunca se deparou com a necessidade de envolver uma ação legal (civil ou criminal), e como tal, não possui qualquer procedimento.

Propostas de otimização (13.2 – Gestão de incidentes de segurança da informação e melhorias)

- ***Descrição***

Devem ser estabelecidas responsabilidades e procedimentos de gestão de modo a assegurar respostas rápidas, efetivas e ordenadas de incidentes de segurança da informação. No que respeita à aprendizagem com os incidentes, sugere-se um registo mais rigoroso dos mesmos no *ServiceDesk* ou qualquer outra aplicação, e ainda, se possível, a implementação de um mecanismo de avaliação e quantificação dos custos resultante.

Finalmente, deve ser realizado um estudo para obtenção da admissibilidade de provas, isto é, a organização deve assegurar que os seus sistemas de informação estão de acordo com qualquer norma ou boas práticas publicadas para produção de provas admissíveis.

- ***Prioridade***

1 - Severa

14 Gestão da continuidade do negócio

14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retoma em tempo útil, se for o caso.

O processo de gestão da continuidade do negócio deve ser implementado para minimizar o impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação. Esta tarefa deve identificar os processos críticos e integrar a gestão da segurança da informação com as exigências da continuidade do negócio e com outros requisitos de continuidade relativos a aspetos, tais como, operações, colaboradores, materiais, transportes e instalações.

As consequências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços devem estar sujeitas a uma análise de impacto no negócio. Os planos de continuidade do negócio devem ser desenvolvidos e implementados de modo a assegurar que as operações essenciais sejam recuperadas em tempo útil. A segurança da informação deve ser uma parte integrante do processo global de continuidade do negócio e da gestão de outros processos dentro da organização.

14.1.1 Inclusão da segurança da informação no processo de gestão da continuidade do negócio

- ***Controlo***

Deve ser desenvolvido e mantido um processo de gestão para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio.

- ***Prática organizacional***

Em conformidade com a norma.

14.1.2 Continuidade do negócio e análise/avaliação de riscos

- **Controlo**

Devem ser identificados os eventos que possam causar interrupções aos processos de negócio, bem como a probabilidade e impacto de tais interrupções e as consequências para a segurança da informação.

- **Prática organizacional**

Em conformidade com a norma.

14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

- **Controlo**

Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível e escala de tempo requeridos, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

- **Prática organizacional**

Em conformidade com a norma.

14.1.4 Estrutura do plano de continuidade do negócio

- **Controlo**

Deve ser mantida uma estrutura básica dos planos de continuidade do negócio. Esta deve assegurar que os planos são consistentes para cumprir os requisitos de segurança da informação e capazes de identificar prioridades para testes e manutenção.

- **Prática organizacional**

Em conformidade com a norma.

14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio

- **Controlo**

Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de modo a assegurar a sua permanente atualização e efetividade.

- **Prática organizacional**

Em conformidade com a norma.

Propostas de otimização (14.1 – Aspetos da gestão da continuidade do negócio, relativos à segurança da informação)

- ***Descrição***

Nenhuma otimização a aplicar.

- ***Prioridade***

Não aplicável.

Anexo B – ISS/DSI - Checklist de Auditoria

IT Service Management ISO/IEC 27002:2005 ISS/DSI Checklist de Auditoria Information technology - Security techniques - Code of practice for information security management						
Políticas de Segurança						
Objetos de Controlo						
5.1	Política de Segurança da Informação	Secção	Questão de Auditoria	Resultados		
5.1.1	Documento de Políticas de Segurança dos Sistemas de Informação		Existe uma Política de Segurança de Sistemas de Informação aprovada pela Direção, publicada e comunicada aos utilizadores de forma apropriada?	Sim	Parcial	N/A
5.1.2	Revisão da Políticas de Segurança de Informação		A Política estabelece um compromisso e define a abordagem organizacional para a gestão da segurança da informação?	Sim	Parcial	N/A
			A Política de Segurança é revista em intervalos de tempo devidamente planeados e em caso de ocorrência de alterações significativas na organização?	Sim	Parcial	N/A
			Está nomeado pela organização um responsável pelo desenvolvimento, revisão e avaliação do documento de Políticas de Segurança de Sistemas de Informação?	Sim	Parcial	N/A
Organização da Segurança						
Objetos de Controlo						
6.1	Organização Interna	Secção	Questão de Auditoria	Resultados		
6.1.1	Compromisso da administração com a segurança da informação		Se a administração demonstra apoio ativo das medidas de segurança. Isto pode ser feito através de uma direção clara, o empenho demonstrado, atribuição explícita e/ou reconhecimento das responsabilidades de segurança da informação.	Sim	Parcial	N/A

Controlo	Secção	Questão de Auditoria	Resultados		
			Sim	Não	Parcial
6.1.2	Coordenação da segurança da informação	Se as atividades de segurança da informação são coordenadas por representantes de diversas partes da organização, com papéis e responsabilidades pertinentes.	Sim	Parcial	N/A
6.1.3	Atribuição de responsabilidade para a segurança da informação	Se as responsabilidades para a proteção de ativos individuais e para a realização de processos de segurança específicos, foram claramente identificados e definidos.	Sim	Parcial	N/A
6.1.4	Processo de autorização para as infraestruturas de processamento da informação	Se o processo de autorização de gestão é definido e implementado para qualquer nova instalação de processamento de informação dentro da organização.	Sim	Parcial	N/A
6.1.5	Acordo de confidencialidade	Se a necessidade de organização para confidencialidade ou Acordo de Confidencialidade para a proteção de informação é claramente definida e periodicamente revista.	Sim	Parcial	N/A
6.1.6	Contactos com autoridades	Se existe um procedimento que descreve quando e por quem devem ser contactadas as autoridades relevantes (ex: bombeiros, proteção civil, etc...) e como o incidente deve ser relatado.	Sim	Parcial	N/A
6.1.7	Contactos com grupos de interesse especial	Se os devidos contactos com grupos de interesses especiais, fóruns de segurança, outros especialistas ou associações profissionais são mantidos.	Sim	Parcial	N/A
6.1.8	Revisão independente da segurança da informação	A segurança da informação e sua implementação é analisada de forma independente em intervalos planeados ou quando ocorrem alterações significativas relativas à implementação da segurança.	Sim	Parcial	N/A
Objetos de Controlo					
6.2 Entidades Externas					
Controlo	Secção	Questão de Auditoria	Resultados		
6.2.1	Identificação de riscos relacionados com entidades externas	Se os riscos inerentes ao acesso por entidades externas às infraestruturas de processamento de informação são identificados, e implementados os controlos apropriados antes de conceder acesso.	Sim	Parcial	N/A
6.2.2	Identificação da segurança na interação com clientes	Se todos os requisitos de segurança identificados são cumpridos antes de conceder acesso do cliente às informações da organização ou ativos.	Sim	Parcial	N/A
6.2.3	Identificação da segurança nos acordos com entidades externas	Se o acordo com terceiros envolvendo acesso, processamento, comunicação ou gestão de informação da organização cumpre todos os requisitos adequados de segurança.	Sim	Parcial	N/A

Gestão de Equipamentos						
Objetos de Controlo						
7.1 Responsabilidade dos Recursos						
Controlo	Secção	Questão de Auditoria	Resultados			
7.1.1	Inventário dos recursos	Todos os recursos estão devidamente identificados ou existe um inventário de todos os recursos importantes (características, software, licenças, valor)?	Sim	Não	Parcial	N/A
7.1.2	Propriedade dos recursos	Se para cada recurso está identificado um proprietário?	Sim	Não	Parcial	N/A
7.1.3	Utilização aceitável dos recursos	São realizadas análises periódicas às classificações e restrições de acesso tendo em conta as políticas de controlo em vigor? Se os regulamentos para o uso aceitável de informações e recursos foram identificados, documentados e implementados?	Sim	Não	Parcial	N/A
Objetos de Controlo						
7.2 Classificação da Informação						
Controlo	Secção	Questão de Auditoria	Resultados			
7.2.1	Recomendações para classificação	Se a informação é classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização?	Sim	Não	Parcial	N/A
7.2.2	Identificação e tratamento da informação	Estão definidos um conjunto de procedimentos para identificação e tratamento da informação de acordo com o esquema adotado pela organização?	Sim	Não	Parcial	N/A

Segurança Física e Ambiental						
Objetos de Controlo						
9.1 Áreas Seguras						
Controlo	Secção	Questão de Auditoria	Resultados			
9.1.1	Perímetro de segurança física	Se existe uma barreira de segurança para proteção das instalações e informações da organização?	Sim	Não	Parcial	N/A

Controlo	Secção	Questão de Auditoria	Resultados			
			Sim	Não	Parcial	
9.1.2	Controlos de entrada física	Se existem controlos de acesso a permitir unicamente a entrada a colaboradores autorizados em diversas áreas da organização?	Sim	Não	Parcial	N/A
9.1.3	Segurança em escritórios, salas e instalações	Se está vedado ao público o acesso às áreas onde estão localizados instalações e informações da organização?	Sim	Não	Parcial	N/A
9.1.4	Proteção contra ameaças externas e ambientais	As instalações e informações da organização estão protegidas contra danos provocados por fogo, inundações, terremotos, explosões, desordem pública e outras formas de desastres?	Sim	Não	Parcial	N/A
9.1.5	Trabalhar em áreas seguras	Se existe proteção física e documentos com recomendações para trabalhar em áreas seguras?	Sim	Não	Parcial	N/A
9.1.6	Acesso público e áreas de cargas e descargas	Se as áreas públicas e de cargas e descargas são controladas de forma a prevenir a entrada de pessoas não autorizadas?	Sim	Não	Parcial	N/A
Objetos de Controlo						
9.2	Segurança de Equipamentos					
Controlo	Secção	Questão de Auditoria	Resultados			
9.2.1	Localização e proteção de equipamentos	Se o equipamento é protegido para reduzir os riscos de ameaças ambientais e as oportunidades de acesso não autorizado?	Sim	Não	Parcial	N/A
9.2.2	Utilitários de Suporte	Se os equipamentos são protegidos contra falhas de energia e outras interrupções causadas por falhas serviços de apoio?	Sim	Não	Parcial	N/A
9.2.3	Segurança de cablagens	Se existem equipamentos de alimentação ininterrupta (UPS) para suporte dos recursos em caso de falha energética? Se as cablagens das infraestruturas de processamento de informação (energia e telecomunicações) são subterrâneas ou ficam abaixo do piso? Se a cablagem está claramente identificada de forma a minimizar erros de manuseamento e patching?	Sim	Não	Parcial	N/A
9.2.4	Manutenção de equipamentos	Se a manutenção dos equipamentos é realizada de acordo com as indicações dos representantes? Se são mantidos registos de todas as falhas e manutenções preventivas?	Sim	Não	Parcial	N/A
9.2.5	Segurança de equipamentos fora do perímetro da organização	Se foram avaliados os riscos de utilização de equipamentos fora das instalações da organização? Se a utilização de equipamentos de processamento de informação fora da organização é devidamente autorizado?	Sim	Não	Parcial	N/A

Controlo	Secção	Questão de Auditoria	Resultados			
9.2.6	Reutilização e alienação segura de equipamentos	Se os suportes de dados de equipamentos são analisados antes de serem descartados, de modo a garantir que todos os dados sensíveis e/ou softwares licenciados tenham sido removidos?	Sim	Não	Parcial	N/A
9.2.7	Remoção de propriedade	Se existem controlos de forma a garantir que equipamentos, informações e software não são removidos do local sem autorização prévia?	Sim	Não	Parcial	N/A

Gestão das operações e comunicações

Objetos de Controlo

10.1 Procedimentos e responsabilidades operacionais

Controlo	Secção	Questão de Auditoria	Resultados			
10.1.1	Documentação de procedimentos operacionais	Se os procedimentos operacionais, tais como, processamento e manuseamento da informação, backup, contactos de suporte, recuperação de sistemas e outros estão devidamente documentados?	Sim	Não	Parcial	N/A
10.1.2	Gestão de mudanças	Se as modificações nos recursos de processamento de informação e sistemas são devidamente controladas?	Sim	Não	Parcial	N/A
10.1.3	Segregação de funções	Se os direitos e as áreas de responsabilidade são separados, a fim de reduzir as oportunidades de modificação não autorizada ou utilização indevida de informações ou serviços?	Sim	Não	Parcial	N/A
10.1.4	Separação dos recursos de desenvolvimento, teste e de produção	Se os desenvolvimentos, testes e produção são realizados em separado de forma a minimizar o acesso não autorizado ou alterações aos sistemas operativos?	Sim	Não	Parcial	N/A

10.2 Gestão de serviços prestados por terceiros

10.2.1	Entrega serviço	Se os controlos de segurança, definições de serviços e níveis de entrega incluídos no acordo de prestação de serviços com os terceiros, são implementados, executados e mantidos pelo terceiro?	Sim	Não	Parcial	N/A
10.2.2	Revisão e monitorização de serviços prestados por terceiros	Se os serviços, relatórios e registos fornecidos por terceiros são regularmente revistos e monitorizados?	Sim	Não	Parcial	N/A
10.2.3	Gestão de mudanças para serviços prestados por terceiros	Se são regularizadas auditorias com regularidade aos serviços prestados por terceiros?	Sim	Não	Parcial	N/A
		As mudanças realizadas pela organização são consideradas nos serviços a serem prestados por terceiros?	Sim	Não	Parcial	N/A
		As mudanças realizadas por terceiros são consideradas nos serviços por estes prestados?	Sim	Não	Parcial	N/A

10.3 Planeamento e aceitação dos sistemas						
10.3.1	Gestão capacidade	Se as necessidades atuais são monitorizadas e se são realizadas projeções de necessidades futuras, de forma a garantir que o poder de processamento e armazenamento adequado esteja disponível?	Sim	Não	Parcial	N/A
10.3.2	Aceitação de Sistemas	Se existem processos formais de alterações (instalação e/ou upgrades) aos sistemas?	Sim	Não	Parcial	N/A
		Se são realizados testes durante o desenvolvimento e antes da sua implementação?	Sim	Não	Parcial	N/A
10.4 Proteção contra códigos maliciosos e códigos móveis						
10.4.1	Proteção contra código malicioso	Se os controles de prevenção, deteção e recuperação para proteção contra códigos maliciosos e procedimentos adequados de sensibilização dos utilizadores foram desenvolvidos e implementados?	Sim	Não	Parcial	N/A
		Se apenas é utilizado código móvel autorizado?	Sim	Não	Parcial	N/A
10.4.2	Proteção contra código móvel	Se a configuração garante que o código móvel autorizado opera de acordo com a política de segurança?	Sim	Não	Parcial	N/A
		Se a execução de códigos móveis não autorizados é impedida?	Sim	Não	Parcial	N/A
10.5 Backup						
10.5.1	Informação backup	Se o backup de dados e software é realizado e testado regularmente, de acordo com as políticas de backup implementadas?	Sim	Não	Parcial	N/A
		Se todas as informações essenciais e software podem ser recuperados após um desastre ou falha de suporte de dados?	Sim	Não	Parcial	N/A
10.6 Gestão da segurança das redes						
10.6.1	Controlos das redes	Se a rede é adequadamente mantida e controlada contra ameaças, de forma a manter a segurança dos sistemas e aplicações que utilizam a mesma (inclui informações em trânsito)?	Sim	Não	Parcial	N/A
		Se foram implementados controlos para garantir a segurança da informação em rede e proteção contra ameaças dos serviços ligados, tais como, acesso não autorizado?	Sim	Não	Parcial	N/A
10.6.2	Segurança dos serviços de rede	Se os recursos de segurança, níveis de serviço e gestão de requisitos, de todos os serviços de rede, são identificados e incluídos em qualquer contrato de serviços de rede?	Sim	Não	Parcial	N/A
		Se a capacidade do prestador de serviços, para uma gestão segura dos serviços acordados, é determinada e monitorizada regularmente?	Sim	Não	Parcial	N/A

10.7 Suporte de dados		Sim	Não	Parcial	N/A	
10.7.1	Gestão de suporte de dados amovíveis	Se existem procedimentos de segurança definidos para a gestão de suporte de dados amovíveis?	Sim	Não	Parcial	N/A
10.7.2	Inutilização de suporte de dados	Se os suportes de dados amovíveis são guardados de forma segura em ambientes protegidos?	Sim	Não	Parcial	N/A
10.7.3	Procedimentos para tratamento da informação	Os suportes de dados com informação sensível são guardados e/ou inutilizados de forma segura?	Sim	Não	Parcial	N/A
10.7.4	Segurança da documentação dos sistemas	Se existe um procedimento para lidar com o armazenamento da informação?	Sim	Não	Parcial	N/A
		Existe um registo formal dos destinatários dos suporte de dados?	Sim	Não	Parcial	N/A
		A documentação dos sistemas está restrita unicamente a pessoal autorizado?	Sim	Não	Parcial	N/A
10.8 Troca de informação						
10.8.1	Políticas e procedimentos de troca de informação	Se existem procedimentos formais que previnam a troca de informação, interceção, cópia, modificação, etc...?	Sim	Não	Parcial	N/A
10.8.2	Acordos para troca de informação	Se existem acordos referentes à troca de informação e software entre a organização e terceiros?	Sim	Não	Parcial	N/A
10.8.3	Suportes de dados em trânsito	Se o âmbito de segurança do acordo reflete a sensibilidade das informações de negócio envolvidas?	Sim	Não	Parcial	N/A
10.8.4	Mensagens eletrónicas	Se os suportes de dados contendo informações são protegidos contra o acesso não autorizado e/ou uso indevido durante o transporte para além fronteiras físicas da organização?	Sim	Não	Parcial	N/A
10.8.5	Sistemas de informação do negócio	As mensagens eletrónicas estão protegidas contra acesso não autorizado, modificação ou <i>denial of service</i> ?	Sim	Não	Parcial	N/A
		Se as políticas e procedimentos são desenvolvidos e aplicados para proteger a informação associada com a interligação dos sistemas de informação empresariais?	Sim	Não	Parcial	N/A
10.9 Serviços de comércio eletrónico (não aplicável ao negócio da ISS)						
10.9.1	Comércio eletrónico	Se as informações envolvidas no comércio eletrónico, que passam pela rede pública, estão protegidas contra atividades fraudulentas, disputas contratuais ou qualquer acesso não autorizado?	Sim	Não	Parcial	N/A
10.9.2	Transações On-line	Se as informações envolvidas em transações on-line são protegidas para prevenir transmissão incompletas, divulgação não autorizada, duplicação de mensagens não autorizadas ou replay?	Sim	Não	Parcial	N/A
10.9.3	Informação disponível ao público	Se a integridade da informação disponível ao público é protegida contra qualquer modificação não autorizada?	Sim	Não	Parcial	N/A

10.10 Monitorização					
10.10.1	Registo de auditoria	São criados e mantidos por tempo previamente definido os registos de auditoria das atividades dos utilizadores?	Sim	Não	Parcial
10.10.2	Monitorização da utilização do sistema	Se existem procedimentos de monitorização da utilização da informação?	Sim	Não	Parcial
10.10.3	Proteção da informação dos registos (logs)	Se os procedimentos de monitorização da utilização da informação são revistos periodicamente?	Sim	Não	Parcial
10.10.4	Registo (logs) de administradores e utilizadores	Se a informação dos registos está protegida contra pessoal não autorizado?	Sim	Não	Parcial
10.10.5	Registos de Falhas	Se são registadas as atividades dos administrador e utilizadores dos sistemas?	Sim	Não	Parcial
10.10.6	Sincronização dos Relógios	Se os procedimentos de monitorização da utilização da informação são revistos periodicamente?	Sim	Não	Parcial
		Se as falhas são registadas, analisadas e as devidas ações realizadas?	Sim	Não	Parcial
		Se os procedimentos de monitorização da utilização da informação são revistos periodicamente?	Sim	Não	Parcial
		Se os níveis de log necessários para os sistemas individuais são determinadas por uma avaliação de risco, tendo em conta a degradação do desempenho?	Sim	Não	Parcial
		Se os relógios de todos os sistemas de processamento de informação dentro da organização estão sincronizados com uma fonte de tempo precisa devidamente acordada?	Sim	Não	Parcial

Controlo de Acessos

Objetos de Controlo

11.1 Requisitos de negócio para controlo de acessos					
Controlo	Secção	Questão de Auditoria	Resultados		
11.1.1	Políticas de Controlo de Acesso	As políticas de controlo de acessos são desenvolvidas e revistas periodicamente de acordo com os requisitos do negócio?	Sim	Não	Parcial
		Os acessos físicos e lógicos são tido em consideração na política?	Sim	Não	Parcial
		São entregues aos utilizadores e prestadores de serviços um declaração dos requisitos de negócios que devem ser cumpridos pelos controlos de acesso?	Sim	Não	Parcial

11.2 Gestão acesso do utilizador		Questão de Auditoria		Resultados			
Controlo	Secção			Sim	Não	Parcial	N/A
11.2.1	Registo de utilizadores	Existe um procedimento formal de registo e eliminação de acesso por parte dos utilizadores aos sistemas de informação?		Sim	Não	Parcial	N/A
11.2.2	Gestão de privilégios	Se a atribuição de quaisquer privilégios no ambiente de sistema de informação é restrito e controlado, ou seja, privilégios são atribuídos de acordo com as necessidades e após autorização formal?		Sim	Não	Parcial	N/A
11.2.3	Gestão da palavra-passe de utilizador	Se a atribuição de palavras-passe é controlada através de um processo formal de gestão?		Sim	Não	Parcial	N/A
11.2.4	Revisão dos direitos de acesso de utilizador	Se os utilizadores assinam uma declaração onde se comprometem a manter a palavra-passe confidencial?		Sim	Não	Parcial	N/A
11.2.4	Revisão dos direitos de acesso de utilizador	Se existe um processo de revisão periódica, com intervalos regulares definidos, dos direitos de acesso dos utilizadores?		Sim	Não	Parcial	N/A
11.3 Responsabilidade dos utilizadores		Questão de Auditoria		Resultados			
Controlo	Secção			Sim	Não	Parcial	N/A
11.3.1	Utilização de palavra-passe	Se existe uma prática de segurança para orientar os utilizadores na escolha e manutenção das palavra-passe?		Sim	Não	Parcial	N/A
11.3.2	Equipamento sem monitorização	Se os utilizadores e fornecedores estão cientes das exigências de segurança e procedimentos para proteger o equipamento sem monitorização?		Sim	Não	Parcial	N/A
11.3.3	Política de mesa e ecrã limpo	Se existe na organização uma política de mesa limpa em relação aos papéis e suporte de dados amovíveis?		Sim	Não	Parcial	N/A
11.3.3	Política de mesa e ecrã limpo	Se a existe na organização uma política de ecrã limpo em relação aos recursos de processamento de informação?		Sim	Não	Parcial	N/A
11.4 Controlo de acesso à rede		Questão de Auditoria		Resultados			
Controlo	Secção			Sim	Não	Parcial	N/A
11.4.1	Política de utilização dos serviços de rede	Se os utilizadores têm somente acesso aos serviços que tenham sido especificamente autorizados a utilizar?		Sim	Não	Parcial	N/A
11.4.2	Autenticação para ligação externa do utilizador	Se são utilizados mecanismos de autenticação apropriados para controlar o acesso de utilizadores remotos?		Sim	Não	Parcial	N/A
11.4.3	Identificação de equipamentos em redes	Se a identificação automática do equipamento é considerado como um meio para autenticar conexões de locais e equipamentos específicos?		Sim	Não	Parcial	N/A
11.4.4.	Configuração de proteção de portas e diagnóstico remoto	Se o acesso físico e lógico para portas de diagnóstico estão bem controlados, ou seja, protegidos por um mecanismo de segurança?		Sim	Não	Parcial	N/A

Controlo	Secção	Questão de Auditoria	Resultados		
			Sim	Não	Parcial
11.4.5	Segregação de redes	Se os grupos de serviços de informação, utilizadores e sistemas de informação são segregados em redes?	Sim	Não	Parcial
					N/A
11.4.6	Controlo de conexão de rede	Se a rede (onde o negócio do parceiro e/ou de terceiros que necessitam de ter acesso ao sistema de informação) é segregada através da utilização de um perímetro de segurança, tais como, firewalls?	Sim	Não	Parcial
					N/A
11.4.7	Controlo de roteamento das redes	Se existe uma política de controlo de acessos que controle as conexões a redes partilhadas, especialmente aquelas que se estendem pelos limites da organização?	Sim	Não	Parcial
					N/A
11.5	Controlo de acesso ao Sistema Operativo				
Controlo	Secção	Questão de Auditoria	Resultados		
11.5.1	Procedimentos seguros de entrada no sistema (log-on)	Se o acesso ao sistema operativo é controlado por um processo de log-on seguro?	Sim	Não	Parcial
					N/A
11.5.2	Identificação e autenticação de utilizador	Se é atribuído um identificador exclusivo (ID de utilizador) para cada utilizador, tais como, operadores, administradores de sistema e todos os outros funcionários, incluindo técnicos?	Sim	Não	Parcial
					N/A
11.5.3		Se é utilizada uma técnica adequada de autenticação que permita a identificação do utilizador?	Sim	Não	Parcial
					N/A
11.5.4	Sistema de gestão de palavra-passe	Se as contas de utilizadores genéricos são fornecidas apenas sob circunstâncias excecionais em que há um benefício claro de negócios?	Sim	Não	Parcial
					N/A
11.5.5	Utilização de utilizadores de sistema	Se existe um sistema de gestão de palavras-passe que impõe vários controlos, tais como, palavra-passe individuais, alterações de palavra-passe, armazenar palavras-passe criptografada, etc...?	Sim	Não	Parcial
					N/A
11.5.6	Limite de tempo de sessão	Se os programas capazes de se sobreporem aos controlos dos sistemas e aplicações são restritos e estritamente controlados?	Sim	Não	Parcial
					N/A
11.6	Controlo de acesso à aplicação e à informação				
Controlo	Secção	Questão de Auditoria	Resultados		
11.6.1	Restrição do acesso à informação	Se o acesso à informação e às funções dos sistemas de aplicações por utilizadores e pessoal de suporte é restrito e está de acordo com a política definida no controlo de acesso?	Sim	Não	Parcial
					N/A
11.6.2	Isolamento de sistema sensíveis	Se os sistemas sensíveis são fornecidos com o ambiente computacional dedicado (isolado)?	Sim	Não	Parcial
					N/A

11.7 Computação móvel e teletrabalho		Questão de Auditoria		Resultados	
Controlo	Secção	Sim	Não	Parcial	N/A
11.7.1	Computação e comunicação móvel	Se existe uma política formal em vigor e medidas de segurança apropriadas para proteger contra o risco da utilização de computação e comunicação móvel?	Sim	Parcial	N/A
		Se os riscos, tais como trabalhar em ambiente desprotegido, é tido em consideração pela política de computação móvel?	Sim	Parcial	N/A
11.7.2	Teletrabalho	Se a política, plano operacional e procedimentos são desenvolvidos e implementados para atividades de teletrabalho?	Sim	Parcial	N/A
		Se a atividade de teletrabalho é autorizada e controlada pela gestão?	Sim	Parcial	N/A

Gestão de incidentes de segurança da informação

Objetos de Controlo

13.1 Notificação de vulnerabilidades e eventos de segurança da informação		Questão de Auditoria		Resultados	
Controlo	Secção	Sim	Não	Parcial	N/A
13.1.1	Notificação de eventos de segurança da informação	Se os eventos de segurança da informação são relatados através de canais de gestão apropriadas o mais rapidamente possível.	Sim	Parcial	N/A
13.1.2	Notificação de vulnerabilidades de segurança da informação	Se existe um procedimento que garante que todos os funcionários dos sistemas de informação e serviços são obrigados a observar e relatar qualquer falha de segurança no sistema ou serviços.	Sim	Parcial	N/A
13.2 Gestão de incidentes de segurança da informação e melhorias		Questão de Auditoria		Resultados	
Controlo	Secção	Sim	Não	Parcial	N/A
13.2.1	Responsabilidade e procedimentos	Se responsabilidades de gestão e procedimentos foram estabelecidos para assegurar uma resposta rápida, eficaz e ordenada aos incidentes de segurança da informação.	Sim	Parcial	N/A
		Se a monitorização dos sistemas, alertas e vulnerabilidades são usados para detetar incidentes de segurança da informação.	Sim	Parcial	N/A
13.2.2	Aprendizagem com os incidentes de segurança da informação	Se existe um mecanismo para identificar e quantificar o tipo, volume e custos dos incidentes de segurança da informação.	Sim	Parcial	N/A
		Se as informações obtidas a partir da avaliação dos incidentes de segurança ocorridos no passado são utilizadas para identificar incidentes recorrentes ou de alto impacto.	Sim	Parcial	N/A

13.2.3	Recolha de Provas	Se as ações de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação envolve uma ação legal (civil ou criminal).	Sim	Não	Parcial	N/A
		Se as provas relacionadas com o incidente são recolhidas, mantidas e apresentadas em conformidade com as regras para provas definidas na respetiva jurisdição.	Sim	Não	Parcial	N/A
		Se os procedimentos internos desenvolvidos são seguidos na recolha e apresentação de provas com a finalidade de instauração de um processo disciplinar dentro da organização?	Sim	Não	Parcial	N/A

Gestão da Continuidade do Negócio

Objetos de Controlo

14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Controlo	Seção	Questão de Auditoria	Resultados			
14.1.1	Inclusão da segurança da informação no processo de gestão da continuidade do negócio	Se existe um processo de gestão em vigor que trata dos requisitos de segurança da informação para desenvolver, manter e dar continuidade do negócio em toda a organização?	Sim	Não	Parcial	N/A
14.1.2	Continuidade do negócio e análise/avaliação de riscos	Se os eventos que causam interrupção do processo de negócio são identificados, juntamente com a probabilidade e impacto de tais interrupções e suas consequências para a segurança da informação?	Sim	Não	Parcial	N/A
14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	Se os planos foram desenvolvidos para manter e restaurar as operações de negócio, dentro do nível e prazo exigido, após uma interrupção ou falha?	Sim	Não	Parcial	N/A
		Se o plano considera a identificação e concordância de responsabilidades, perda aceitável, processo de recuperação e restauro, documentação do processo e os testes regulares?	Sim	Não	Parcial	N/A
		Se existe um quadro único de plano de continuidade de negócios?	Sim	Não	Parcial	N/A
14.1.4	Estrutura do plano de continuidade do negócio	Se esta estrutura é mantida para assegurar que todos os planos são consistentes e identificam as prioridades para testes e manutenção?	Sim	Não	Parcial	N/A
		Se o plano de continuidade de negócios satisfaz os requisitos de segurança da informação identificada?	Sim	Não	Parcial	N/A
14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	Se os planos de continuidade de negócios são testados regularmente para garantir que estão atualizados e são eficazes?	Sim	Não	Parcial	N/A
		Se os testes ao plano de continuidade garantem que todos os membros da equipe de recuperação e outras equipas relevantes estão cientes dos planos e suas responsabilidades?	Sim	Não	Parcial	N/A

Anexo C – Listagem de severidades/prioridades

Ameaça	Descrição
1 severa	processo de negócio significativamente afetado; não há procedimento de recuperação ou contorno do problema; uma solução ou contorno do problema é necessária imediatamente
2 moderada	processo de negócio está afetado; exposição à perda de dados; operação normal do negócio não foi afetada
3 ligeira	perda de alguma funcionalidade; não há exposição imediata à perda de dados ou processo de negócio

15 Referências bibliográficas

Calder, A., Watkins, S., (2008), “*IT governance: a manager's guide to data security and ISO 27001/ISO 27002*”, Kogan Page, 4ª Edição.

Carlson, Tom (2008), “Understanding ISO 27002”. Acedido em Julho 2011, no Web site da Orange Parachute: <http://www.orangeparachute.com>

ISO/IEC 27002 (2005). *International Standard: Information technology — Security techniques — Code of practice for information security management*

Mamede, H., (2006), “*Segurança Informática nas Organizações*”, FCA – Editora de Informática, Lisboa

Nunes, M., O’Neill, H. (2009), “*Fundamental de UML*”; FCA – Editora de Informática, 2º Edição, Lisboa

Acedido em Julho 2011 ao Web site British Standards Institution, <http://bsigroup.com>