UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

MESTRADO EM: Gestão de Sistemas de Informação

Comparação da "COBIT Security Baseline e do ISO 17799: 2000 para a produção da lista de requisitos de um plano director para a Segurança dos Sistemas de Informação numa Organização

Domingos Manuel da Silva Pereira

Orientação: Mestre José Maria Pedro

Júri:

Presidente: Doutor António Maria Palma dos Reis

Vogal: Doutor Manuel João Correia do Nascimento Pereira

Vogal: Doutora Maria Fernanda Abreu Sampaio

Vogal: Mestre João Maria Pedro

Junho de 2006

GLOSSÁRIO DE TERMOS E ABREVIATURAS

AICPA - American Institute of Certified Public Accountants

ASIS - American Society for Industrial Security

BIPM - Bureau International des Poids et Mesures

BS - British Standard

CBK - Common Body of Knowledge'

CEO - Chief Executive Officer

CIA - Central Inteligence Agency

CIO - Chief Information Officer

CNDP - Comissão Nacional de Dados Pessoais.

COBIT - Control Objectives for Information and related Technology

COSO - Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework

CRM - Costumer Relationship Manager

CSOTC – Committee of Sponsoring Organizations of the Treadway Commission

CTCPEC - Canadian Trusted Computer Product Evaluation Criteria

ERP - Enterprise Resource Planning

FTP - File Transport Protocol

IEC - International Electrotechnical Commission

IIA - Institute of Internals Auditors

IPAC - Instituto Português de Acreditação

IPQ - Instituto Português de Qualidade

ISACA - Information Systems Audit and Control Association

ISC^2 - International Information Systems Security Certification Consortium

ISMA - Information Systems Management Architecture

ISMS -Information Security Management System

ISO - International Organization for Standardization

IT - Information Technology

ITGI - Information Technology Governance Institute

ITIL - IT Infrastructure Library.

ITPM - IT Process Model

ITSEC - Information Technology Security Evaluation Criteria

NIST - National Information Systems Security (INFOSEC)

NSTISSC - National Security Telecommunications and Information Systems Security Committee

OECD - Organisation for Economic Co-operation and Development

OGC - Office of Government Commerce

OVM - Organismos de Verificação Metrológica

PDSSI - Plano Director para a Segurança dos Sistemas de Informação

SAC – Systems Auditability and Control

SAS 44 – Audit risk and materiality in conducting an Audit

SAS 55 – Consideration of the Internal Control Structure in a financial statement audit

SAS 78 - Consideration of the Internal Control Structure in a financial statement audit: An amendement to SAS nº 55

SE-CMM - Software Engineering Capability Maturity Model

SI/TI – Sistemas Informação / Tecnologias de Informação

SPQ - Sistema Português da Qualidade

SSE-CMM - Systems Security Engineering Capability Maturity Model

TCSEC - Trusted Security Evaluation Criteria

TI - Tecnologias de Informação

TOE - Target of Evaluation

RESUMO E PALAVRAS-CHAVE

Construir uma lista de requisitos para um Plano Director para a Segurança dos Sistemas de Informação.

Domingos Manuel da Silva Pereira

***Mestrando em*: Gestão dos Sistemas de Informação**

Provas concluídas em: Junho de 2006

A Segurança e o Controlo Interno dos sistemas de informação nas organizações, são disciplinas que se intersectam no seu âmbito de acção.

O COBIT é, na óptica do ISACA, o modelo adequado para o Governo da função IT nas organizações, e como tal propõe um conjunto de instrumentos que facilitam o seu desenvolvimento pela Gestão da função SI da organização. Recentemente propôs ao mercado uma proposta mínima a respeitar para a segurança dos sistemas da informação das organizações a que chamou de "Cobit Security Baseline".

O BS7799-2 pretende alargar o âmbito do anterior standard BS7799, adoptado pela ISO como ISO17799, e situa-lo também como referencial chave para a criação de um sistema de gestão para a Segurança dos sistemas de informação nas organizações. Mantêm no entanto no seu anexo A, todas as boas praticas que o seu anterior "Code of Pratice" propunha na ISO 17799, o qual constitui uma proposta a adequar a cada organização para o estabelecimento dos requisitos de um programa (plano director) para a segurança dos sistemas de informação nas organizações

Esta investigação pretende tirar conclusões sobre a utilidade de ambas as normas, "Cobit Security Baseline ISBN: 1-893209-79-2 " e da "ISO 17799:2000 ", para o estabelecimento da lista de requisitos de um programa (plano director) para a segurança dos sistemas de informação numa organização e em paralelo contribuir para a sistematização de conceitos ligados à Gestão da Segurança dos Sistemas de Informação.

Palavras-chave: Segurança dos Sistemas de Informação; Cobit Security Baseline; BS 7799-2; ISO 17799: 2000; Conceitos de Segurança dos Sistemas de informação; Planeamento da Segurança dos Sistemas de Informação;

ABSTRACT AND KEY WORDS

Building a list of requirements for a System Information Security Program

Domingos Manuel da Silva Pereira

***Master in*: Information System Management**

Exam concluded in: June 2006

Organizations Information Systems Security and Internal Control are disciplines that intercept frequently their scope.

COBIT is according to ISACA the right model to IT Governance. Recently ITGI-ISACA deliver a document that states the minimum security control any organization should apply at is information system architecture. This document is named 'Cobit Security Baseline'.

BS7799-2 enlarge the scope of the former standard, also known as ISO 17799, in order to establish a standard in what concerns a Information Security Management System. While it does this maintains the previous 'code of practice, ISO 17799' as the annex A, and enforce it during the process of analyse to fully justify any control the organization decided not implement. In fact this statement of applicability turns to be the list of requirements of a Security Program.

This investigation work intend to conclude about the effectiveness and efficiency of using Cobit Security Baseline or ISO 17799, to draw the list of requirements of a Security Program and in parallel to contribute to clarify some of the concepts that belong to the scientific domain of Information Security Management.

Key words: Information Systems; Informatio Systems Security; BS7799-2; ISO 17799:2000; Concepts of Information Systems Security Management; Informatio Systems Security Program.

Índice

LISTA DE FIGURAS, TABELAS OU OUTRAS ILUSTRAÇÕES **10**

Figuras *10*
Tabelas *11*

AGRADECIMENTOS **12**

1. INTRODUÇÃO **13**

2. A ABORDAGEM DE INVESTIGAÇÃO UTILIZADA. **14**

2.1 A perspectiva filosófica do Realismo Critico, adoptada neste trabalho. *17*
2.2 Estratégia de investigação ou abordagem metodológica adoptada neste trabalho. *20*
2.3 Desenho da investigação realizada *24*

3. CONCEITOS ASSOCIADOS À GESTÃO DA SEGURANÇA E CONTROLO INTERNO DA INFORMAÇÃO MANIPULADA PELAS TECNOLOGIAS DE INFORMAÇÃO **27**

3.1 O que é um sistema de gestão ? *27*
3.2 O que é um Sistema de Informação ? *34*
3.2.1 Classificação dos sistemas de informação na óptica da sua participação na decisão. 37
3.3 O que é o Controlo Interno dos Sistemas de Informação baseados nas TI ? *40*
3.4 O que é Segurança dos Sistemas de Informação baseados nas TI ? *44*
3.5 Quais os termos e papeis para a classificação da informação nas empresas *49*
3.6 O que é a identificação, a autenticação, a autorização e a privacidade no contexto da segurança da informação ? *55*
3.7 O que é um Risco ? *64*
3.8 Ameaças inerentes à função IT e o seu reflexo no negocio *65*
3.9 O que é a gestão dos riscos ? *73*
3.10 O que é garantir ou credibilizar a segurança dos sistemas IT ? *78*
3.11 Qual é objectivo de um controlo de segurança do sistema de informação ? *83*
3.12 O que são politicas, normas, guias e procedimentos de segurança (Policies, Standards, Guidelines and Procedures) ? *91*
3.13 O que é definir os requisitos de um sistema ? *97*
3.14 O que é um Plano Director (ou Programa) para a Segurança dos Sistemas de Informação ? *104*

4. O CASO DE ESTUDO REALIZADO **112**

4.1 INTRODUÇÃO AO CASO DE ESTUDO 112
4.2 O ESTUDO DO CASO NO IPQ 115
4.2.1 A missão e principais áreas de negocio: *116*
4.2.2 O Organigrama simplificado do IPQ *116*
4.2.3 Inventário breve do seu sistema de informação baseado nas tecnologias de informação e avaliação qualitativa do seu impacto no negócio *117*
4.3 O MÉTODO DE REALIZAÇÃO DO ESTUDO DO CASO 118

5. CONCLUSÕES DO TRABALHO DE INVESTIGAÇÃO **122**

6. BIBLIOGRAFIA **127**

ANEXO – O QUE É O SISTEMA PORTUGUÊS DA QUALIDADE (SPQ) ? **131**

O que é a normalização, a metrologia e qualificação ? *132*
O Processo NP 132
Subsistema de Qualificação 133
As actividades de Metrologia 133

ANEXO – CHECKLIST A PARTIR DA SECURITY BASELINE DO COBIT **136**

ANEXO - CHECKLIST A PARTIR DA ISO 17799 ..... **144**

Lista de figuras, tabelas ou outras ilustrações

Figuras

Figura 1 - Da realidade à estratégia de investigação 15

Figura 2 – da estratégia de investigação ao desenho explicito da mesma 16

Figura 3 – As ontologias do realismo critico, do interpretivismo e do positivismo. 18

Figura 4 – Desenho da investigação realizada neste trabalho 24

Figura 5– O ciclo PDCA da Qualidade 32

Figura 6 – Componentes de um sistema de gestão 32

Figura 7 – Modelo genérico de processo de negocio 33

Figura 8 – Relação entre a pirâmide de Anthony e os sistemas de informação da empresa 38

Figura 9 – Politicas, Garantia e Mecanismos de Segurança 49

Figura 10 – Serviços e mecanismos de segurança para os níveis OSI na norma ISO-7498-2 .. 58

Figura 11 – Serviços de Segurança necessários ao objectivo disponibilidade 61

Figura 12 – Elementos relevantes para a Garantia do Sistema incluindo a Segurança 62

Figura 13 – Uma metodologia faseada para a Analise do Risco 75

Figura 14 - Risk Management: Organização e Responsabilidades 77

Figura 15 - Risk Management, Planeamento Estratégico e Contabilidade de Gestão 78

Figura 16 – O que se espera de um controlo de segurança 83

Figura 17 - Hierarquia das politicas de Segurança de Informação 92

Figura 18 – Relações entre Politicas 96

Figura 19 – Níveis de requisitos num projecto de desenvolvimento de software 101

Figura 20 – Processo para o planeamento e gestão da Segurança IT na empresa 104

Figura 21 – Organigrama simplificado do IPQ 117

Tabelas

Tabela 1 – Ontologia, Epistemologia, Metodologia e Método 16

Tabela 2 – Ontologias e Epistemologias nas ciências naturais e sociais 18

Tabela 3 – tabela de decisão para a escolha da estratégia de investigação 21

Tabela 4 – Comparação dos sistemas de controlo (SCI) vigentes em 1996 40

Tabela 5 – comparação das protecções gerais da TR 13335-4 com outros referenciais normativos 86

Tabela 6 – Comparação das protecções específicas dos SI/TI propostas em diversos documentos normativos 88

Tabela 7 – Comparação do nível de detalhe proposto nos referenciais em estudo 125

Agradecimentos

Gostaria de agradecer ao meu orientador, professor José Maria Pedro, por todo o apoio, orientação e encorajamento prestado durante o processo de realização deste trabalho de investigação.

Ao IPQ e em particular ao seu responsável pelos sistemas de informação, O Dr Jacinto Ramos, pela sua disponibilidade para viver e reflectir sobre o processo de investigação em curso.

Aos meus colegas da Pós-Graduação na Gestão dos Sistemas de Informação pela alegria, entusiasmo e entreajuda que me proporcionaram. Uma palavra especial para o meu grupo de trabalho, e ao Fernando Almeida pela amizade e disponibilidade que teve e tem para comigo.

Aos meus pais e aos meus irmãos pela estima e preocupação constante que manifestam comigo. A família poderá não ser sempre um espaço de encontro, no sentido de Alberoni, mas é sempre para mim um espaço de entreajuda, compreensão e afectos.

À minha mulher, Dina e às minhas filhas, Ana e Joana, dedico este trabalho.

1. Introdução

O controlo interno e a segurança dos sistemas de informação são disciplinas que dominam cada vez mais a preocupação dos CIO e CEO das organizações que se vêem cada vez mais dependentes dos seus sistemas de informação para operarem no dia a dia.

A visão externa desta informação é cada vez mais insuficiente para que a realidade do mundo que a gera, seja conhecido e controlado/gerido

A União Europeia tem vindo a legislar sobre esta matéria, à semelhança dos USA e é previsível que a breve trecho maiores exigências legais sejam impostas às organizações no domínio do controlo interno e segurança dos sistemas de informação.

Um estudo sobre o grau de cobertura e o modo como duas propostas normativas tão relevantes como o Cobit Security Baseline e da ISO 17799:2000 contribuem para o estabelecimento da lista de requisitos de um programa (plano director) para a segurança dos sistemas de informação numa organização, apoiado pela síntese de um conjunto significativo de conceitos ligados ao domínio da gestão da segurança dos sistemas de informação, constituirá certamente um instrumento útil a qualquer CIO ou gestor de sistemas de informação.

2. A abordagem de investigação utilizada.

Caldeira (2004) citando Frankfort-Nachmias (1992) esclarece que o objectivo principal das ciências sociais é produzir um corpo de conhecimento confiável, que nos permita explicar, prever e perceber o mundo social.

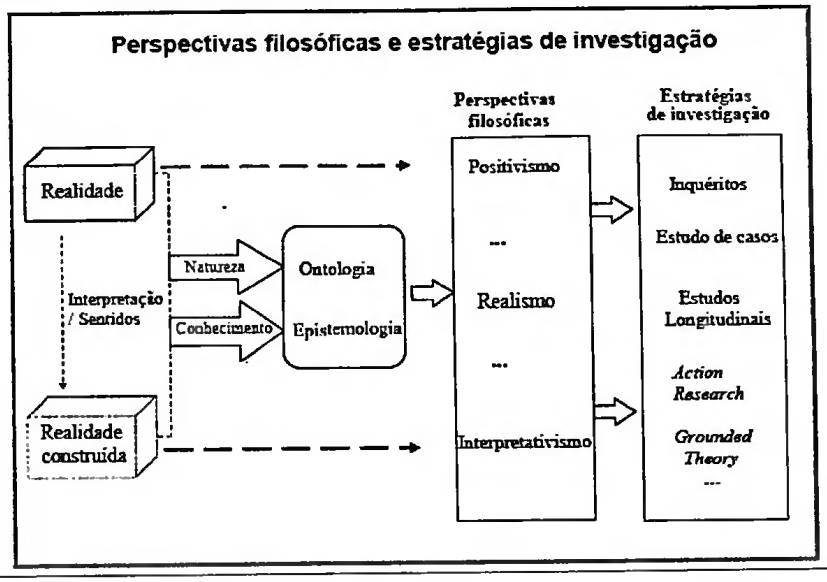
Por outro lado os sistemas de informação são uma ciência social (Rivas, 1989). E útil ver as organizações e os sistemas de informação como 'constructs' sociais (Gazendam, 2004)

A estratégia de investigação adoptada deve ter subjacente uma perspectiva filosófica que permita perceber as crenças e assumpções que o investigador tem sobre a natureza do fenómeno que pretende investigar (a sua ontologia) e o seu ponto de vista relativamente ao modo como pode adquirir conhecimento relativamente ao mesmo fenómeno (a sua epistemologia). Caldeira sustenta que existe habitualmente uma relação forte entre a estratégia de investigação adoptada e a perspectiva filosófica do investigador relativamente à ontologia da realidade a investigar e à epistemologia que acredita adequada para a conhecer. Os métodos de investigação não são validos por si mesmo. Necessitam de uma contextualização filosófica coerente com as suas práticas.

Finalmente a estratégia de investigação deve instanciar-se num desenho concreto da aplicação da estratégia genérica ao objecto de investigação

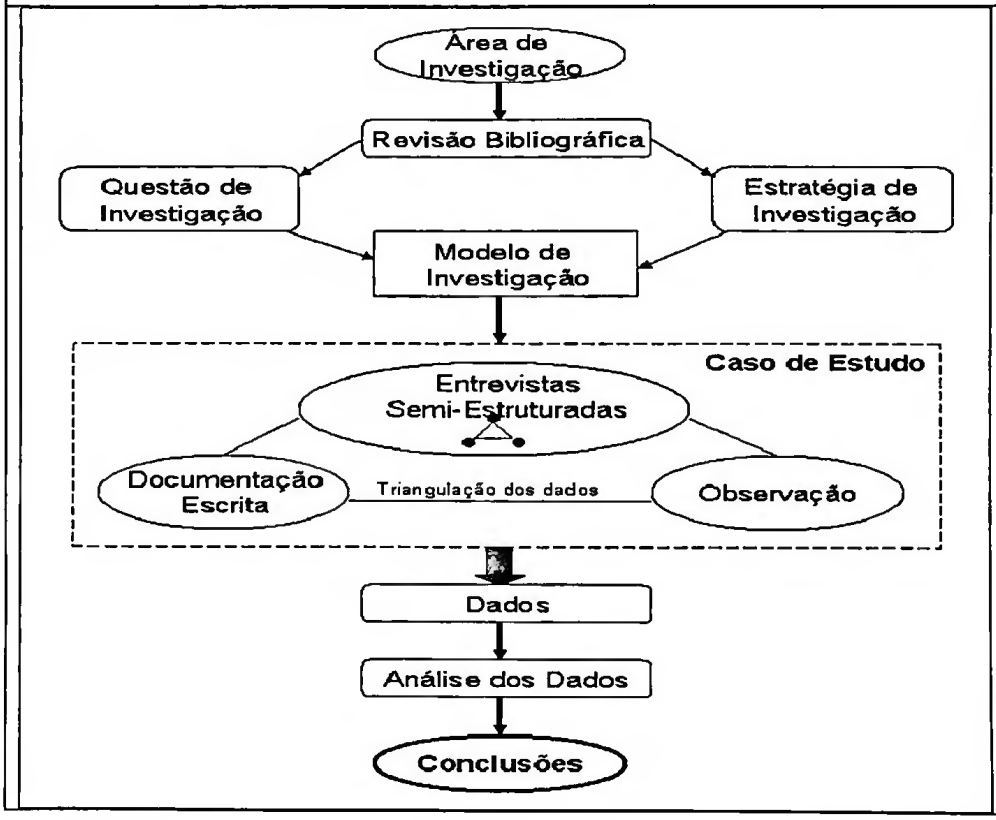
Caldeira apresenta a lógica inerente a esta sequência num conjunto de slides que se apresentam de seguida:

Figura 1 - Da realidade à estratégia de investigação



O desenho instanciado da investigação :

Figura 2 – da estratégia de investigação ao desenho explicito da mesma



Mark Easterby-Smith et al (2002) tentam de igual modo organizar o debate à volta das investigação em gestão, domínio das ciências sociais, propondo a seguinte tabela:

Tabela 1 – Ontologia, Epistemologia, Metodologia e Método	
Ontologia	**Assumpções que fazemos acerca da natureza da realidade**
Epistemologia	**Conjunto genérico de assumpções que fazemos de modo a conhecer (inquire into) a natureza do mundo**

Metodologias	**Combinação de técnicas que utilizamos para conhecer uma determinada situação** (que sugere ser entendido como o desenho da investigação que Caldeira propoe)
Métodos	**Técnicas individuais para recolha de dados, analise, etc**

2.1 A perspectiva filosófica do Realismo Critico, adoptada neste trabalho.

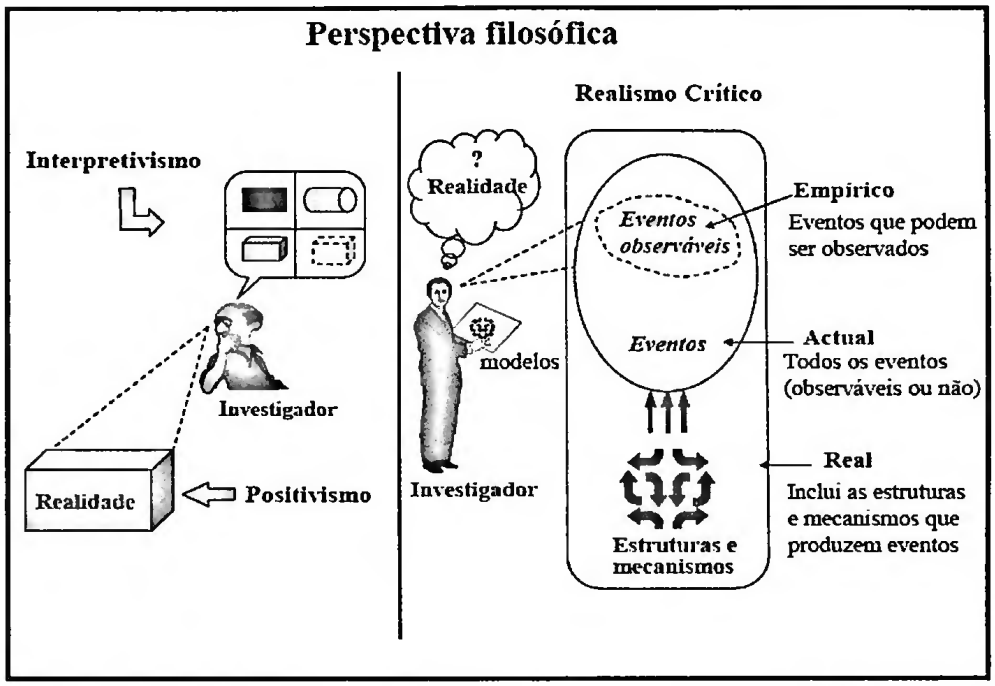
Caldeira (2000) refere que o Realismo é uma perspectiva filosófica emergente, com a sua própria ontologia e epistemologia. Citando Blaikie, " Embora partilhe o desejo do positivismo para produzir explicações causais, e a perspectiva interpretativista na natureza da realidade social, o realismo argumenta uma visão da ciência distinta de ambas".

Clarifica a ontologia do realismo citando Bhaskar : " as coisas existem e actuam independentemente das nossas descrições, mas apenas as podemos conhecer em condições particulares", ou seja a ciência é vista como uma tentativa sistemática de expressar em pensamento as estruturas e formas de actuar das coisas que existem independentemente do pensamento.

Continuando a citar Bhaskar, Caldeira apresenta os três três domínios da realidade, o empírico, o actual e o real, os quais servem para classificar experiências, eventos, mecanismos e estruturas. O empírico é feito das experiências, dos eventos que podem ser observados; O actual é composto dos eventos quer possam ou não ser observados; O domínio do real consiste nas estruturas e mecanismos que produzem os eventos. O realismo é assim baseado na assumpção que as abstracções que fazemos das estruturas e mecanismos (conceptualizações) e os eventos que observamos (o domínio empírico) não representam completamente o real, seja as estruturas e mecanismos seja o actual.

Caldeira (2004) apresenta esta ideia num slide alegre:

Figura 3 – As ontologias do realismo critico, do interpretivismo e do positivismo.



Mark Easterby-Smith et al (2002) sintetizam na tabela seguinte as ontologias e epistemologias nas ciências naturais e sociais:

Tabela 2 – Ontologias e Epistemologias nas ciências naturais e sociais

Ontologia das ciências naturais	Realismo Tradicional	Realismo Interno	Relativismo	
Ontologia das ciências sociais		Representação	Relativismo	Nominalização

Verdade	É estabelecida pela correspondência entre observações e fenómenos	E determinada através da verificação das previsões	Requer consenso entre diferentes pontos de vista	
Factos	São concretos	São concretos mas não podem ser acedidos directamente	Depende do ponto de vista do observador	São todos criações dos seres humanos
Epistemologia das ciências naturais	**Positivismo**		**Relativismo**	
Epistemologia das ciências sociais		**Positivismo**	**Relativismo**	**Construção Social**

Do ponto de vista epistemológico, Caldeira (2000) cita Blaikie, para justificar que o realismo crítico é metodologicamente aberto, ou seja não define uma metodologia específica. " O realismo está relacionado com métodos de desenvolvimento apropriados à situação particular que pretende investigar". De novo o princípio, que embora aceite que o mundo social é real e existe, aceita também a perspectiva interpretativista que a sociedade é produzida e reproduzida pelos seus membros, os quais podem ter percepções e interpretações diferentes da mesma realidade.

Dobson (2001) propõe que para o investigador realista, as suas crenças ontológicas, são mais determinantes do que a epistemológica, na escolha da metodologia de investigação em cada situação concreta.

O realismo crítico afirma que as condições para o conhecimento não surgem nas nossas mentes mas na estrutura da realidade, e que esse conhecimento não é universal nem intemporal (Mingers, 2004).

Mingers (2004) questiona o que são leis causais, ou antes o que é que causa ou gera os eventos, dadas as regularidades que podem ser estabelecidas nos experiências e a

habitual falta de regularidade fora do âmbito fechado das experiências. De igual modo pergunta como podemos assegurar-nos que as regularidades são baseadas em conexões reais em vez de simples coincidências. A resposta que propõe é que devem existir entidades duradouras, físicas (i.e. átomos ou organismos), sociais (pex o mercado ou a família) ou conceptuais (i.e. categorias ou ideias), observáveis ou não, que tem poder ou tendência para actuar de determinada maneira. A operação continua destes entidades e a sua interacção gera (i.e. causa), mas é independente de, o fluxo dos eventos. As entidades podem ter poder que no entanto não exercem num dado momento (pode ser necessário uma experiência para o desplotar), ou o poder pode ser exercido mas não se manifestar em eventos por causa de actuação contrária de quaisquer outros mecanismos generativos.

Almeida (2005) citando Bryman e Bell (2003) afirma que o Realismo Crítico implica duas coisas. Primeiro, implica que ao contrário do positivismo que pressupõem que a conceptualização do cientista sobre a realidade reflecte directamente a realidade, o realismo crítico afirma que a conceptualização do cientista é simplesmente uma forma de conhecer essa realidade. Segundo, e por consequência, o realismo crítico contrariamente ao positivismo admite nas suas explicações, termos teóricos que cuja responsabilidade não resulta da observação.

2.2 Estratégia de investigação ou abordagem metodológica adoptada neste trabalho.

Caldeira (2000) e Mingers (2004) citando Orlikowski e Baroudi (1991) e Farhoomand, (1992) esclarecem que a investigação nos sistemas de informação tem vindo a ser dominadas por três estratégias dominantes; a experimentação laboratorial, os inquéritos e os estudo de casos. A evolução desta área relativamente recente do conhecimento

SI/TI, dum foco inicial na tecnologia para uma cada vez maior ênfase nas questões sociais, levou a uma mudança numa perspectiva mais positivista inicial para uma perspectiva mais interpretativista. Citando Galliers (1992) "os investigadores dos sistemas de informação estão-se a dar conta das limitações das aproximações cientificas do seu trabalho, dada a natureza técnico-sociológica do seu campo de investigação".

Yin (1994) propõe a seguinte tabela de decisão para a escolha da estratégia de investigação adequada:

Tabela 3 – tabela de decisão para a escolha da estratégia de investigação

Estratégia	**Forma das questões de investigação ?**	**Requer controlo sobre os eventos comportamentais ?**	**Foca-se em eventos comportamentais ?**
Experimentação	Como ? Porquê ?	Sim	Sim
Inquéritos (survey)	Quem ? O quê ? Onde? Quantos ? Que volume ?	No	Sim
Análise de arquivo	Quem ? O quê ? Onde? Quantos ? Que volume ?	Não	Sim/Não
Historia	Como ? Porquê ?	Não	Não
Estudo de Caso	Como ? Porquê ?	Não	Sim

Escreve Yin (1994), que o estudo de caso é preferível na examinação de eventos contemporâneos, quando os comportamentos relevantes não podem ser manipulados. O estudo de caso sustenta-se em muitas das mesmas técnicas da Historia, mas adiciona duas fontes de evidência que a estratégia histórica habitualmente não contempla, a observação directa e a entrevista sistemática.

Yin distingue ainda a estratégia de estudo de caso que metodologicamente cobre todo o ciclo de vida da investigação, de métodos específicos utilizados para a recolha de dados como a etnografia ou observador-participante.

Gummesson (2000) esclarece que o método de participante-observador constitui o núcleo da antropologia/etnografia, e participante com intervenção activa é chamado 'action reseach'. Embora os métodos de participante-observador e action-research dependam largamente de métodos qualitativos, os métodos quantitativos podem jogar um papel relevante na recolha e analise dos dados.

Bryman e Bell (2003) apresentam os papeis do investigador participante observador distribuídos por um domínio extremado entre envolvimento na situação em estudo e completo isolamento do que lá se passa, gerando assim um gradiente de completa participação a completo observador. Neste gradiente, no papel de observador-participante, o investigador entrevista sobretudo os actores e pouco observa.

Gummesson (2000) estabelece em dez pontos o que considera ser o seu conceito de action research dirigida à gestão, e nos dois primeiros afirma:

- Os investigadores de "action research" lideram a acção. Ou seja estão comprometidos na mudança dos processos ou situações que estudam
- O método "action research" tem dois objectivos, por um lado contribuir para o Cliente e por outro contribuir para a ciência.

Almeida (2005) cita Benbasat *et al* (1987) para identificar três pontos fortes da pesquisa em SI/TI baseada em casos de estudo:

- O investigador pode estudar o sistema de informação num ambiente natural, aprender mais sobre o estado da arte e gerar teorias a partir da prática;

- O investigador pode compreender a natureza e complexidade do processo em curso;
- Podem ser adquiridos conhecimentos valiosos sobre novos tópicos que emergem no campo de mudança acelerada dos SI/TI.

A selecção de um referencial normativo para estabelecer os requisitos do plano director para a segurança dos sistemas de informação Portugal, e no mundo, é um fenómeno contemporâneo, a Security Baseline do COBIT surgiu em 2004, e as questões organizacionais a par com o conteúdo de cada uma das propostas normativas assumem um papel relevante no êxito de qualquer das escolhas para o propósito referido, a produção dos requisitos do plano director.

Este trabalho procura perceber o porquê da escolha de um referencial versus o outro propondo um "como" para tal, dado que há altura do trabalho não foi possível encontrar organizações que tivessem passado pela experiência de comparar qualquer um dos referenciais.

O autor teve de construir inquéritos partindo dos referenciais normativos propostos e fazer passar a empresa que se disponibilizou para este trabalho, pelo conjunto de entrevistas necessários à obtenção das respostas inerentes a cada um dos questionários.

O detalhe desta odisseia está descrito mais à frente, e a sua reflexão levou o autor a adoptar a estratégia de estudo de caso, com a utilização preponderante do método de participação-observador, no gradiente de observador-participante acima referido, embora com algum espírito do método do action research, dado que houve ao longo da investigação a preocupação do investigador que as respostas que o entrevistado foi

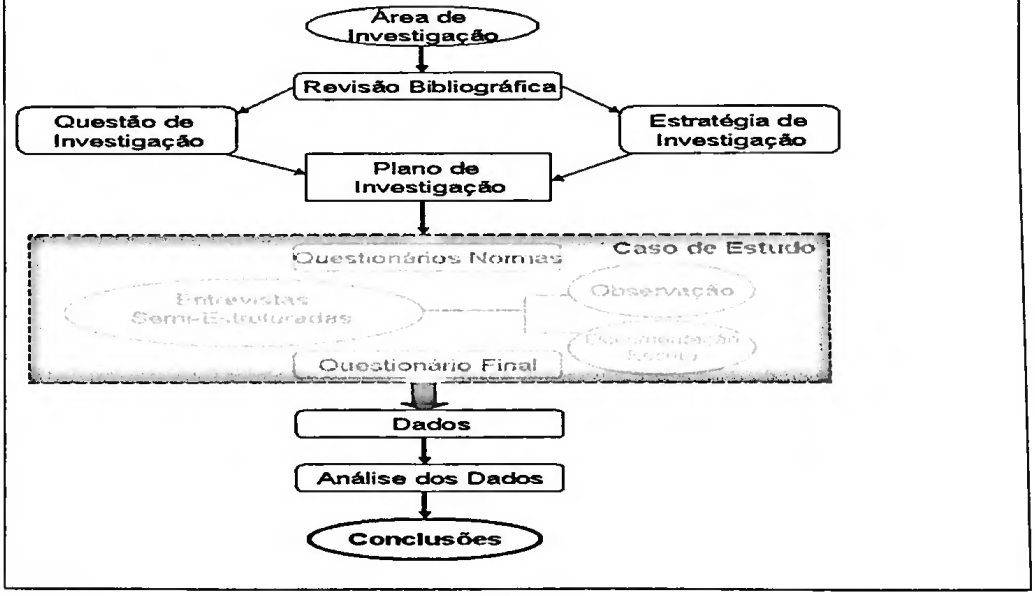
dando ao longo de qualquer um dos questionários pudessem constituir um resultado útil para a própria organização.

2.3 Desenho da investigação realizada

O desenho da investigação é a lógica que liga os dados a recolher (e as conclusões a produzir) à questão de investigação inicial. Cada estudo empírico tem um desenho de investigação implícito, senão mesmo explícito, Yin (1994).

Coloquialmente um desenho de investigação é um plano de acção, mas é muito mais do que um plano. O objectivo principal do desenho é ajudar a evitar a situação na qual a evidencia não endereça as questões da investigação inicial, Yin (2004).

Figura 4 – Desenho da investigação realizada neste trabalho



A área de investigação deste trabalho é a da Segurança dos sistemas de informação baseados nas tecnologias da Informação. Como já foi referido, trata-se de uma área hoje

em dia muito relevante para as organizações que depositam nos seus sistemas de informação e em particular nas soluções tecnológicas e processuais que os materializam a forma habitual de executar as operações do negocio que lhes garantem a sua sobrevivência e desenvolvimento.

A revisão bibliográfica teve como objectivo actualizar o autor no conhecimento actual que envolve o tema da investigação, permitir-lhe identificar a questão de investigação particular que deveria tratar, e finalmente permitir a clarificação dos conceitos e temas desta área de um modo pedagógico, ou seja pretende-se deste modo contrariar, no domínio desta tese, a constatação de Schrader, (citado por Capurro, 2004), 'A literatura da ciência da informação é caracterizada por caos conceptual'.

A questão de investigação já foi apresentada no capítulo do tema do trabalho. Pretende-se tirar conclusões sobre a utilidade das normas, "Cobit Security Baseline ISBN: 1-893209-79-2 " e da "ISO 17799:2000" para o estabelecimento da lista de requisitos de um plano director para a segurança dos sistemas de informação numa organização.

A aproximação filosófica e a estratégia de investigação escolhidas no trabalho já foram apresentadas acima.

Dada a dificuldade de encontrar empresas que estivessem disponíveis para autorizar um estudo de caso nesta área, e ainda que tivessem tido a experiência de construir uma lista de requisitos do seu plano director para a segurança dos sistemas de informação a partir dos dois referenciais normativos, o autor viu-se confrontado com a necessidade de fazer passar o Cliente pela experiência de analisar questionários construídos directamente a partir de cada uma das normas-documentos referidos, de modo a permitir ao Cliente a experiência psicológica que o habilitasse a poder pronunciar-se sobre o interesse, integralidade e eficácia de cada uma para a construção do referido plano.

A autor teve ao longo das varias entrevistas uma atitude mais de observador do que de participante, tentando, sempre que necessário, ajudar o entrevistado a perceber melhor o domínio das questões colocadas, o modo como se mapeiam à sua realidade em termos de arquitectura de sistemas de informação, procurando que o resultado directo das respostas ao questionário pudessem constituir um resultado útil à empresa que se disponibilizou para o trabalho, mas evitou forçar qualquer resultado nas respostas ás questões concretas, tanto mais que o interlocutor é um gestor da função SI/TI com uma larga experiência na função e nas tecnologias que sustentam a sua arquitectura.

Ao longo dos dois meses em que as entrevistas decorreram foi possível ler alguns documentos e observar alguns sistemas da empresa, bem como conhecer a equipa que gere o sistema de informação assente nas TI, na empresa. De qualquer modo o instrumento principal para a reflexão final do entrevistado, e do autor, foram as entrevistas semi-estruturadas à volta dos questionários construídos para cada um dos referenciais.

Após as reuniões entrevistas foi submetido ao entrevistado um questionário que o ajudasse a pronunciar-se sobre a escolha que proponha entre ambos os referenciais para a criação da lista de requisitos do plano director.

É o resultado deste ultimo questionário e a vivência do processo do próprio autor que sustentam as conclusões deste trabalho, que serão apresentadas num capítulo próprio.

3. Conceitos associados à gestão da segurança e controlo interno da informação manipulada pelas Tecnologias de Informação

3.1 O que é um sistema de gestão ?

E útil pesquisar no google (www.google.com) conteúdos subordinados à questão "what is a management system". Pelo menos a 22 de novembro de 2004, os resultados da pesquisa foram francamente positivos.

De acordo com Charlton e Andras, a teoria de sistemas pode ajudar na resposta. Os sistemas convivem com a complexidade do ambiente que os rodeia, criando modelos simplificados do mesmo. Por outro lado os sistemas são definidos em termos dos processos que aí decorrem. Alguns sistemas são ainda capazes de se modelarem a si próprios, constituindo este auto-modelo na linguagem da teoria de sistemas uma sistema cibernético de segunda ordem. Propõem assim os autores que a gestão seja vista como uma forma de auto-modelização da organização, e como tal, um sistema de gestão é um processo através do qual uma organização gera uma representação dos seus próprios processos.

Ou seja a gestão depende da capacidade de modelar a organização a gerir. É esta modelização que permite à gestão realizar as suas actividades distintivas de processamento de informação, tais como a monitorização, avaliação, previsão e controlo. A finalidade para a qual estas actividades distintivas são dirigidas, definem a função da gestão. A função da gestão é o produto da interacção do ambiente e do sistema de gestão. Para um sistema de gestão tudo alem de si mesmo, é ambiente, mas a organização que é gerida é o seu ambiente mais imediato. Como definição de sistema de gestão os autores afirmam que é o caminho e o processamento da informação amostrada

ao longo dos processos modelados. Os sistemas de gestão são assim sistemas de processamento de informação abstractos.

De acordo com a empresa Quality Management Internacional, INC (2004) um sistema de gestão é uma colecção e inter-relação de partes que convertem interessados necessitados, em interessados satisfeitos. Por outro lado um sistema de gestão é composto por quatro partes essenciais:

- Políticas e objectivos que guiam a organização
- Responsabilidades definidas de modo a que cada pessoa saiba o que é esperado de si
- Processos definidos que liguem as pessoas aos objectivos do negocio
- Dados partilhados e analisados para melhorar o desempenho da organização

As Políticas são directivas da gestão de topo destinadas a inspirar o funcionamento do sistema de gestão. Os objectivos conduzem pessoas e processos tornando perceptível o que deles se espera no concreto.

- Objectivos de negócio são requisitos para o 'aqui e agora'
- Objectivos estratégicos são requisitos para o estado futuro que se deseja
- Objectivos de processos são requisitos que devem ser atingidos de modo a permitir concretizar os objectivos de negócio e os estratégicos

A definição de responsabilidades vai habitualmente para além do organograma da empresa e da descrição das funções exercidas por cada posto de trabalho. Deve

clarificar os valores e cultura que a empresa persegue, e dar resposta às seguintes questões:

- Quem é responsável por perceber as necessidades e estabelecer objectivos?
- Quem tem autoridade para desenhar e planear a execução dos processos?
- Como são alocados recursos e controlados os processos ?
- Como é que os lideres inspiram as equipas para controlar e melhorar os processos de modo a que estes satisfaçam as necessidades e objectivos da organização ?

Os Processos constituem a parte maior do sistema de gestão e recebem habitualmente a maior atenção. Os processos aplicam recursos e controlo para converter entradas em entregas que satisfaçam os interessados internos e externos à organização. Existem em vários níveis de abstracção dentro de uma organização com relações distintas em cada nível:

- Nivel 0: Necessidades de tesouraria
- Nivel 1: Obter Trabalho > Executar Trabalho > Receber Pagamento
- Nivel 2: Marketing > Vendas > Desenho de Produtos e Serviços > Produção > Entrega > Apoio Pós Venda.
- Nivel 3 : Cadeia de Valor para Produtos ou Clientes
- Nivel 4 : Outros níveis mais agregados

Um processo bem definido deve identificar entradas críticas, recursos e controlos necessários a satisfazer os objectivos e deve ser suficientemente documentado de modo a assegurar o seu controlo.

Os dados (na óptica do sistema de gestão) são registos utilizados para demonstrar ate que ponto o sistema satisfaz os requisitos e objectivos a que se destina, e evoluem habitualmente ao longo do seguinte ciclo:

- Os dados analisados tornam-se informação
- A informação percebida pelas pessoas e equipas torna-se conhecimento
- O Conhecimento conduz à sabedoria através de um processo de decisão consciente e informado.

Devem ser apenas recolhidos os dados necessários á tomada de decisão e à avaliação do atingimento ou não dos objectivos. No entanto a medida certa é difícil de obter em particular se o sistema de gestão não é ainda maduro. Ou seja o desenvolvimento de um sistema de gestão obriga à análise dos processos do sistema para determinar os locais correctos para medição e recolha de dados de modo a permitir decisões que tornem o sistema eficaz e eficiente.

Uma visão complementar da Quality Management Internacional e em linha com a perspectiva que a teoria de sistemas tem de um sistema de gestão, é proposta no volume I dos quatro volumes que compõem a proposta da IBM, 'A Management system for the Information Business' do inicio dos anos 80. Esta proposta da IBM é uma síntese evolutiva de outras propostas anteriores, das quais se destaca a ISMA, Information Systems Management Architecture, de 1979, a qual deu também origem ao ITPM, IT

Process Model, que como reconheceu a OGC, está na base do ITIL, IT Infrastructure Library.

Propõe a IBM nesta monografia que os elementos constituintes de um sistema de gestão são os seguintes:

- Processos de negócio – Um conjunto lógico relacionado de actividades e decisões necessários á gestão dos recursos do negocio
- Classes de dados – Categorias de informações logicamente relacionadas necessárias para a concretização dos processos do negocio
- Organização – Agrupamento lógico de pessoas e responsabilidades destinado a concretizar os processos do negócio
- Sistemas e ferramentas – Conjunto lógico de hardware e software destinado a suportar os processos do negócio

Os processos do negócio são assim vistos como a modelização das actividades e decisões que ocorrem na organização, a qual constitui como vimos o ambiente mais próximo do sistema de gestão.

Estes processos do negocio, são de seguida agrupados em actividades de planeamento, execução, medição e controlo, e é nos processos destinados ao planeamento que surge o estabelecimento dos objectivos e políticas referidas na abordagem da Quality Management Internacional. A imagem seguinte ilustra a composição proposta de um sistema de gestão :

Figura 5– O ciclo PDCA da Qualidade

O ciclo PDCA – Plan Do Control Act, tão próprio dos sistemas de qualidade, pode ser representado por seu lado da seguinte forma:

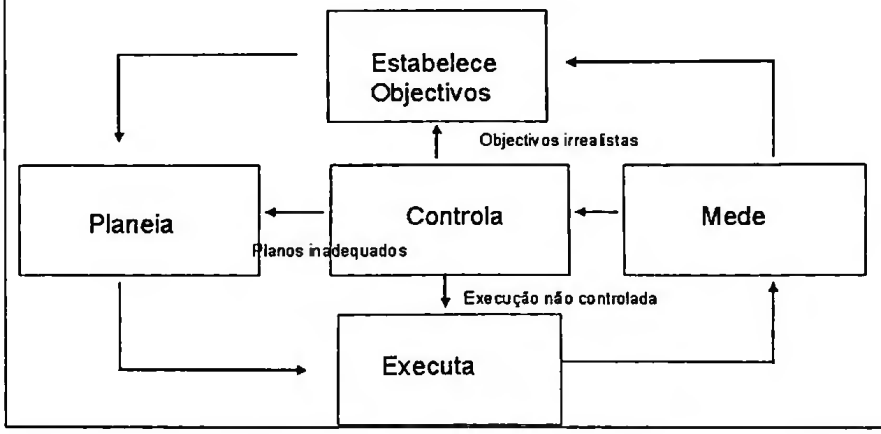
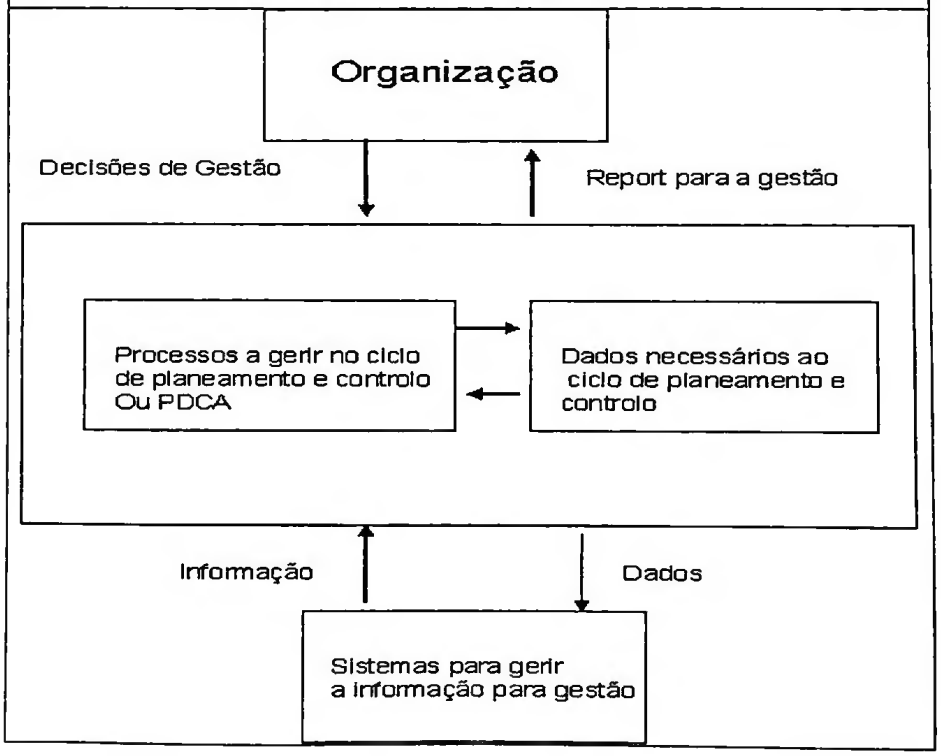


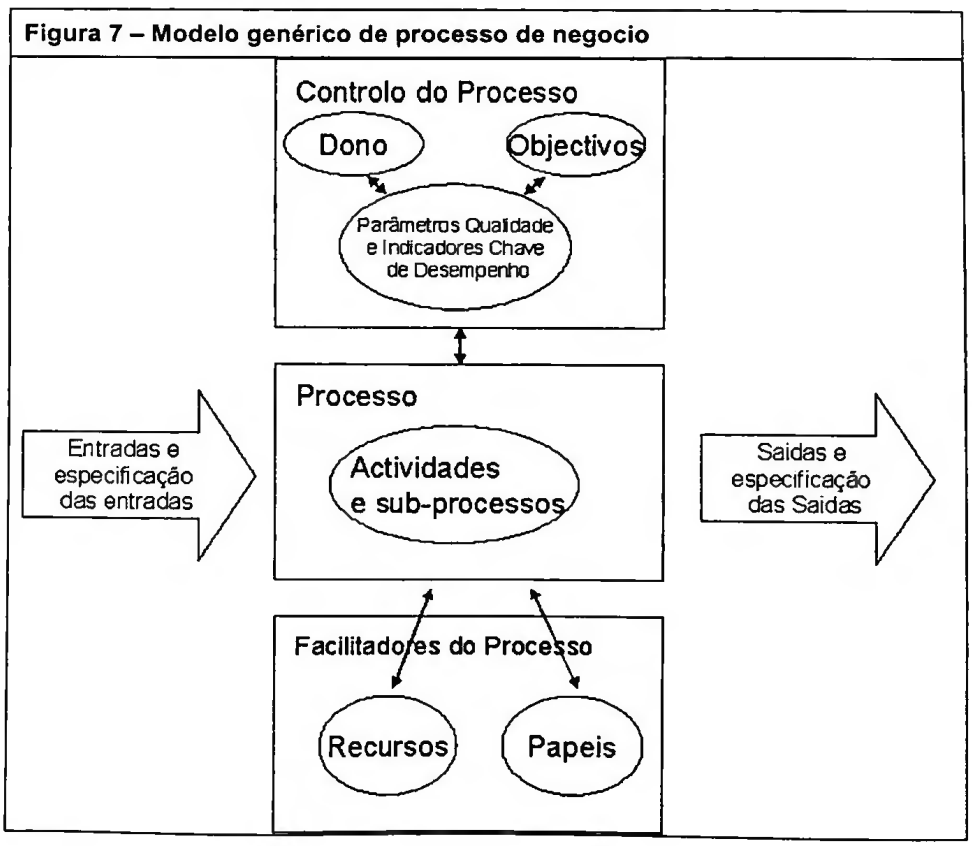
Figura 6 – Componentes de um sistema de gestão



Curioso ainda é reparar na recursividade destes conceitos de gestão, em linha afinal com a teoria de sistemas. Tomando a definição e composição de um processo de negócio proposta pelo ITIL, temos que:

- Um processo é um conjunto inter-relacionado de actividades realizadas por agentes com a intenção de satisfazer um propósito ou atingir um objectivo.
- Os elementos que devem compor a completa descrição de um processo de negocio:

Figura 7 – Modelo genérico de processo de negocio



Os parâmetros de qualidade são as normas estabelecidas pelo responsável máximo pelo processo (o Dono) as quais devem guiar as actividades que compõem o processo. Os Indicadores Chave de Desempenho são as informações construídas a partir dos dados recolhidos para controlo do processo que dão a conhecer do correcto desempenho do mesmo. Os papéis do processo são os agentes que nele intervém organizados debaixo de uma hierarquia que tem como responsável maior o dono do processo, que mais não é do que um papel a realizar por um elemento da organização.

3.2 O que é um Sistema de Informação ?

Ward (1995) define sistema de informação como um sistema que liga entrada de dados, processamento, e informação de saída de um modo coerente e estruturado.

Esta definição, que apresenta numa monografia centrada sobre gestão dos sistemas de informação, foca o conceito agregado de sistemas de informação em sistemas formais, isto é, estruturados, embora reconheça que hoje em dia a tecnologia de informação é também utilizada para facilitar a execução de processos de tratamento de informação informal, como correio electrónico, processamento de dados, fax, entre outros.

Ward acrescenta que todos os sistemas de informação formais de uma organização podem um dia beneficiar da tecnologia de informação já disponível. Qualquer processo em que os dados são recolhidos, arquivados, acedidos, analisados, sintetizados e formatados para uma pessoa ou para outro processo usar, é um potencial alvo da tecnologia.

No mesmo contexto entende Ward ser necessário definir Tecnologia de Informação, de modo a diferencia-la do conceito de sistemas de informação. Este conceito diz respeito ao 'hardware' que compõe os computadores e as redes de comunicações e ao 'software' que corre nesse 'hardware'.

Recursos IT são os especialistas e as competências necessárias para utilizar a tecnologia de informação eficaz e eficiente nas organizações.

Ward clarifica também a distinção que deve ser estabelecida entre dados e informação. Em seu entender 'Dados' é a matéria prima ('raw material', números, palavras, imagens) que é processada no sistema, o qual produz informação. Informação é aquilo que as pessoas necessitam, para através da sua experiência e competências (skills), gerarem conhecimento.

De facto, lembra Ward, pode ser um processo baseado em computadores a produzir conhecimento, como se pretende nos sistemas de inteligência artificial, dos quais os expert systems são um caso particular. Ou seja a informação produzida num processo, pode tornar-se os dados, manteria prima, de outro processo.

Capurro (2003) afirma que no discurso científico, os conceitos não são elementos verdadeiros ou falsos de alguma parte da realidade. São sobretudo construções (constructs) concebidos para realizar um trabalho o melhor possível. Assim concepções distintas de termos fundamentais são mais ou menos frutuosas dependendo das teorias (e no final das acções praticas) que se destinam a suportar.

Tomemos por exemplo as definições dos mesmos conceitos de dados, informação e conhecimento no contexto da perspectiva de um sistema cognitivo

Amaral e Pedro (2004) no contexto das teorias do conhecimento e em particular da perspectiva cognitivista, sustentam que um sistema cognitivo, seja humano ou computador, cria representações da realidade e aprende gradualmente através da manipulação dessas representações. A realidade pode ser constituída por objectos, acontecimentos ou factos, e pode ser distinta da verdade, que é aquilo que o objecto realmente é.

O ser humano capta a realidade através dos sentidos que lhe permitem ver, tactear, saborear, cheirar e ouvir. Os sentidos geram pequenos sinais elementares neste processo de captação, que são objecto de um primeiro processo de abstracção, gerando dados. Os dados são assim conjuntos de factos discretos e objectivos sobre eventos recebidos via os sentidos.

Para se transformarem em informação os dados deverão conter um significado capaz de cativar o destinatário. Citando Bateson, ' a informação é a diferença que faz a diferença' porque provoca alteração no estado de conhecimento do indivíduo. A informação provem portanto dos dados mas deverá ter significado para o destinatário para ser considerada como tal, isto é, deve (Davenport & Prusak, 1998, citados pelos autores) :

- Possuir contexto, atribuindo objectivo aos dados
- Ser categorizada, a partir de uma abstracção da realidade constituída por categorias
- Ser valorizada no contexto das categorias
- Permitir o controlo de erro induzido pela categorização
- Ter coerência percebida com outros dados relativos à mesma realidade,

Conhecimento como informação refere-se a significado é contextualizado e relacional. Contrariamente a informação, refere-se a crenças e compromisso (envolvimento). Conhecimento é assim uma perspectiva dirigida à acção (Nonaka e Takeuchi, citados pelos autores). O conhecimento localiza-se nos agentes (pessoas ou máquinas) enquanto os dados fazem parte do ambiente exterior e é a informação que os relaciona. (Max Boisot, citado pelos autores). É a mente que transforma informação em conhecimento, através dos seguintes mecanismos (Davenport & Prusak, citados pelos autores):

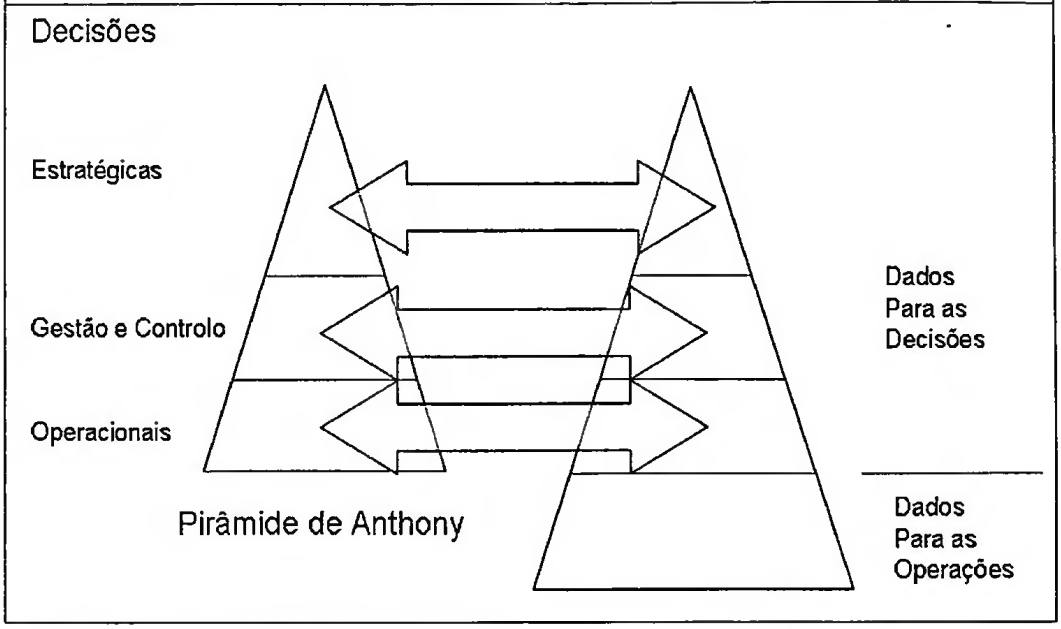
- Comparação – como é que esta informação sobre esta situação se compara com outras situações?
- Consequências – que implicações tem esta informação para as decisões e acções?
- Conexão – como é que este novo conhecimento se relaciona com outros?
- Conversação – o que é que os outros pensam sobre esta informação?

Dado que só é possível adquirir conhecimento, se soubermos aprender, estes mecanismos são ferramentas de aprendizagem.

3.2.1 Classificação dos sistemas de informação na óptica da sua participação na decisão.

Edward et al (1991) reconhecendo dificuldades em definir sistemas de informação, propõe como alternativa vários critérios para classificar os sistemas de informação num contexto de gestão. Destes critérios debruça-se com algum cuidado na classificação dos sistemas de informação na óptica da sua participação no processo de decisão na organização. Tomando por referencia a figura seguinte:

Figura 8 – Relação entre a pirâmide de Anthony e os sistemas de informação da empresa



Estes autores lembram que para além de todos os dados necessários à tomada de decisão, existe a necessidade de gerar e gerir os dados operativos da empresa, como por exemplo os dados dos salários, da contabilidade, do sistema de encomendas e facturação. Estes dados não são necessários para a tomada de decisão mas tem de existir para a empresa continuar a laborar. Tipicamente são pré-definidos e tendem a não variar muito no tempo. Embora não sejam produzidos para as necessidades de informação de gestão da empresa, é a partir deles que esta informação é produzida. Ou seja a gestão deverá apenas preocupar-se com estes dados se não forem produzidos ou se forem produzidos com deficiências, à luz dos critérios adequados ao seu controlo e segurança.

Uma outra abordagem que ajuda a definir e classificar os sistemas de informação é proposta por Gazendam (1993). Estes autores propõem metáforas para alguns tipos de sistemas de informação. As metáforas são de acordo com Collins (1987), citado pelos

autores, uma forma imaginativa de descrever algo referindo-se a uma outra coisa que tem as qualidades que pretendemos exprimir. É um modo condensado de exprimir significado por analogia.

Começam os autores por situar os sistemas de informação nas organizações virtuais. Uma organização virtual é uma organização que consiste em actores humanos e virtuais. Uma organização que consiste apenas em actores humanos é uma organização real. Uma organização que consiste apenas em actores virtuais é um sistema de informação. Numa organização virtual os actores humanos e virtuais têm responsabilidades e competências distintas. Os sistemas de informação geralmente representam coisas e conceitos do mundo, mas também criam coisas, conceitos, eventos no mundo fazendo pré-representações dessas mesmas entidades.

Um sistema de informação parece ter duas partes:

- A parte do actor virtual que cria (determina) novas entidades
- A parte que representa ou pré-apresenta entidades do mundo

Antes de se referirem às metáforas associadas aos sistemas de informação os autores, referem que as metáfora da arquitectura é aplicada frequentemente para explicar o modo como entidades sociais são construídas, pelo que pode ser aplicada a organizações, a sistemas de informação e a organizações virtuais.

Uma arquitectura é o modo como o sistema é composto por sub-sistemas, cada um com as suas funcionalidades e responsabilidades (o desenho do sub-sistema) e as regras que regulam a cooperação entre os sub-sistemas. A arquitectura de um sistema é também habitualmente especificada a vários níveis de granularidade e funcionalidade (constituindo uma escala de progressiva abstracção), de um modo consistente.

As metáforas que apresentam para os sistemas de informação são a fabrica (mill) caracterizada pelo processamento eficiente de grandes quantidades de dados. Os sistemas de informação como células, caracterizados pela sua interacção fluente e adequada com outras células. Neste caso o sistema de informação consiste em objectos que preservam a sua integridade e reagem a eventos. Os sistemas de Informação como mente (mind), caracterizados pela sua capacidade de utilização de conhecimento, autonomia e aprendizagem. Estas três metáforas podem ser combinadas, e habitualmente aparecem combinadas nas organizações.

3.3 O que é o Controlo Interno dos Sistemas de Informação baseados nas TI ?

Vale a pena referir Colbert e Bowen (1996), que comparam sistemas de controlo vigentes à data do artigo, propostos por organizações de renome no mercado:

Tabela 4 – Comparação dos sistemas de controlo (SCI) vigentes em 1996

	Cobit	SAC	COSO	SAS 55/78
Audiência Principal	Gestores, Utilizadores; Auditores de Sistemas de Informação	Auditores Internos	Gestores	Auditores Externos
Como é visto o Sistema de Controlo Interno	Conjunto de processos incluindo politicas, procedimentos, praticas e estruturas organizacionais	Conjunto de processos, sub-sistemas e pessoas	Processos	Processos
Objectivos Organizacionais do SCI	Eficiência e Eficácia das Operações; Confidencialidade, Integridade e disponibilidade da Informação;	Eficiência e Eficácia das Operações; Apresentação confiavel dos dados financeiros; Respeito por	Eficiência e Eficácia das Operações; Apresentação confiavel dos dados financeiros; Respeito por	Apresentação confiavel dos dados financeiros; Respeito por regras e leis; Eficiência e Eficácia das

	Apresentação confiavel dos dados financeiros; Respeito por regras e leis;	regras e leis;	regras e leis;	Operações;
Componentes ou Domínios	Domínios: Planeamento e Organização; Aquisição e Implementação; Entrega e Suporte; Monitorização	Componentes: Ambiente de Controlo; Controlo dos sistemas manuais e automáticos; Procedimentos;	Componentes: Ambiente de Controlo; Controlo via a Gestão do Risco; Monitorização da informação sobre as actividades e da apresentação da informação	Componentes Ambiente de Controlo; Controlo via a Gestão do Risco; Monitorizaçã o da informação sobre as actividades e da apresentação da informação
Foco	Tecnologia da Informação	Tecnologia da Informação	Organização no seu todo	Declarações Financeiras
Avaliação da Eficácia do SCI	Para um período de tempo	Para um período de tempo	Num dado momento	Para um período de tempo
Responsabilidade pelo SCI	Gestão	Gestão	Gestão	Gestão
Tamanho da documentação que descreve o SCI	187 paginas em quatro documentos (versão 1)	1193 paginas em 12 módulos	353 paginas em quatro volumes	63 paginas em dois volumes
Organização que propõe o SCI	ISACA	IIA	CSOTC	AICPA

Este artigo publicado em 1996, identificava já o COBIT e o SAC como sistemas de controlo internos focados nas tecnologias de informação, dado o seu suporte fundamental às operações de negócio das organizações. No entanto em 1996, o SAC não identificava com clareza a segurança das TI, como um dos seus objectivos organizacionais enquanto sistema de controlo interno (SCI). Os relatórios posteriores do

SAC, em particular a sua versão de 2002, centra a segurança das TI, como um dos objectivos principais do sistema de controlo que propõe.

Os autores referem ainda que qualquer um destes sistemas de controlo cresceu sobre o trabalho dos outros. Por exemplo o sistema COBIT, hoje na sua versão 3, recolheu do Relatório COSO, a definição de Controlo :

'Politicas, procedimentos, práticas e estruturas organizacionais desenhadas para fornecer uma garantia razoável de que os objectivos de negocio serão atingidos e os acontecimentos indesejáveis serão prevenidos, ou detectados e corrigidos.'

E do relatório SAC de 1994, a definição de Objectivo do Controlo IT:

'Uma declaração do resultado desejado ou do propósito a ser conseguido pela implementação dos procedimentos de controlo, numa actividade IT.'

Qualquer um dos dois sistemas de controlo focados nas TI, o COBIT e o SAC, propõem processos para a gestão da função IT. O COBIT em particular partiu da analise do ITIL, para organizar os processos que entende necessários à gestão da função IT de uma organização em 4 domínios, o Planeamento e Organização, Aquisição e Implementação, Entrega e Suporte de Serviços IT, e Monitorização. Segundo esta proposta, estes quatro domínios e os 34 processos associados, são os necessários para a gestão adequada dos recursos da função IT, dados, aplicações informáticas, tecnologia, infra-estruturas para hospedar a tecnologia (facilities) e pessoas. Os actuais 34 processos da versão 3 do COBIT, executados adequadamente, permitem a gestão dos recursos referidos, e produzem como resultado disso informação que respeita os requisitos de negocio essenciais (e com alguma sobreposição) que esta informação deve possuir: eficácia, eficiência, confidencialidade, integridade, disponibilidade, cumprimento das leis e normas da empresa e fiabilidade da realidade que representa.

A proposta COBIT, propõe de seguida 34 objectivos de controlo de alto-nível associados a cada um dos 34 processos para a gestão da função IT, e detalha esta proposta de objectivação do controlo em 318 objectivos de controlo, os quais se distribuem para cada um dos 34 processos, entre 3 a 30. Ver a este propósito o documento 'Control Objectives' disponíveis no 'site' da ISACA, www.isaca.org .

Como explica a introdução de quase todos os documentos COBIT, o propósito deste detalhe na objectivação dos controlos necessários ao IT, é o de facilitar aos responsáveis pelos processos de negocio suportados pelas TI, a enumeração dos requisitos de negocio a respeitar na prestação da função IT, nos processos de negocio à sua responsabilidade, evitando que mais tarde possam ser considerados como primeiros responsáveis de algum mau desempenho do seu processo, devido a uma prestação de serviço inadequada da função IT ao mesmo.

De facto o COBIT é um sistema dirigido aos sistemas de informação centrados nas tecnologias de informação que continua a oferecer uma visão própria aos auditores dos sistemas de informação, mas que tem vindo progressivamente a afirmar-se como um modelo de governo da função IT nas organizações, ou seja um sistema de gestão.

O COBIT e o SAC partilham o facto de proporem sistemas de controlo para toda a função IT, desde os sistemas e sub-sistemas operativos às aplicações. Tanto o COBIT como o SAC, propõem também controlos para a segurança dos sistemas de informação suportados em TI, repartidos pelos domínios e componentes de acordo com a organização de cada documento, ou seja misturados com os restantes controlos propostos por cada um dos referenciais, os quais tem uma abrangência que está para alem do âmbito da segurança dos sistemas de informação.

3.4 O que é Segurança dos Sistemas de Informação baseados nas TI?

As definições embora próximas e com elementos sempre comuns não convergem inteiramente.

Assim na sua proposta recente, o ITGI (2004) propõe a seguinte definição que considera consensual para a maioria dos utilizadores das TI, no intróito do documento 'Cobit Security Baseline':

Um sistema de segurança para as TI considera-se bem sucedido quando:

- Os sistemas de informação (informação, sistemas e comunicações) estão disponíveis e utilizáveis quando necessário, resistem adequadamente a ataques e conseguem recuperar de falhas. (propriedade disponibilidade)
- A informação é disponibilizada e apresentada apenas a quem tem direito de a ver (propriedade confidencialidade)
- A informação é protegida contra modificações não autorizadas ou erros de modo a que o rigor, integralidade e validade são mantidos (propriedade integridade)
- As transacções de negócio ou a troca de informações entre empresas, clientes, fornecedores ou parceiros são confiáveis. (propriedades autenticação e não-repudiação)

Para tal é necessário que os activos (informação e sistemas) sejam prioritizados e as protecções (safeguards) implementadas de acordo com o risco e valor envolvidos.

Krutz e Vines (2001), tentando sintetizar a visão do International Information Systems Security Certification Consortium (ISC)^2 do seu 'Common Body of Knowledge' (CBK) para os profissionais da segurança dos sistemas de informação, propõem a seguinte definição de segurança dos sistemas de informação:

Todos os controlos e salvaguardas de segurança dos sistemas de informação, todas as ameaças, vulnerabilidades e processos de segurança, estão sujeitos ao crivo dos três mandamentos (tenets) da segurança dos sistemas da Informação, cuja abreviatura em inglês coincide com uma conhecida instituição Americana, a C.I.A., a saber:

- Confidencialidade (C) é a propriedade que determina que a informação não fica disponível de modo acidental ou intencional, a quem não tem autorização para a conhecer, em qualquer dos ambientes em que é tratada (no sistema central ou local, na rede, nos mapas impressos)
- Integridade (I) é a propriedade que determina que a informação,
  - não é alterada por pessoas ou processos não autorizados
  - Que pessoas autorizadas não efectuam modificações não-autorizadas
  - Que os dados que constituem a informação são interna (entidades do modelo de dados) e externamente (relação dos dados com os objectos que abstraem) consistentes, e completos.
- Disponibilidade (A) é a propriedade que determina que a informação está acessível para as pessoas ou processos autorizados, quando é necessária para as operações do negocio. Ou seja esta propriedade implica também a disponibilidade dos serviços de segurança de modo a garantir as duas outras propriedades.

Sintetizando poderiamos avançar que na óptica destes autores segurança dos sistemas de informação 'é o sistema desenvolvido de modo a preservar três propriedades no sistema de informação que protege: A sua confidencialidade, a sua integridade e a sua disponibilidade.'

Stoneburner (2001), propõe na publicação 800-33 do National Institute of Standards and Technology dos Estados Unidos da América (NIST), a seguinte definição composta:

'A finalidade da Segurança das TI é permitir que a organização cumpra a sua missão e atinja os seus objectivos de negocio implementando sistemas que tenham a devida atenção (due care) aos riscos próprios das TI, dirigidos à organização, aos seus parceiros e clientes.'

'Esta finalidade é obtida através dos seguintes objectivos de segurança:

- Disponibilidade (dos sistemas e dados apenas para a utilização prevista)

  Disponibilidade é o requisito tendente a garantir (assure) que os sistemas trabalham adequadamente e o serviço não é negado aos utilizadores autorizados. Este objectivo protege contra:

  - Tentativas intencionais ou acidentais que realizem apagamentos não autorizados de dados e/ou provoquem situações de negação de utilização dos serviços disponíveis.
  - Tentativas para utilizar o sistema ou os seus dados para propósitos não autorizados.
- Integridade (do sistema e dos dados)

  A integridade tem duas faces:

  - A Integridade dos dados. A propriedade que determina que os dados não são alterados de um modo não autorizado enquanto estão na memoria, durante processamento ou em trânsito
  - A Integridade do sistema. A propriedade que um sistema possui, quando executa uma função pretendida de um modo adequado, livre de manipulações não autorizadas

- Confidencialidade (dos dados e da informação de sistema)

  Confidencialidade é o requisito que pretende que a informação confidencial ou privada não seja dada a conhecer a indivíduos não autorizados. A protecção da confidencialidade aplica-se aos dados em memória, durante o processamento e enquanto em trânsito.

- Responsabilização (Accountability; ao nível do individuo)

  A responsabilização é o requisito que determina que as acções de uma entidade podem ser rastreadas (traced) de modo unívoco para essa entidade.

  - Esta propriedade traduz-se habitualmente num requisito da política organizacional e suporta directamente a não-repudiação, a dissuasão, o isolamento de falhas, a detecção e prevenção de intrusão e acção posteriores de recuperação e actuação legal.

- Garantia (Assurance – que os quatro objectivos foram adequadamente atingidos)

  A garantia é a propriedade em que se baseia a confiança adquirida que as medidas de segurança, técnicas e organizacionais, funcionam como se pretende na protecção do sistema e da informação que processa. Os outros quatro objectivos de segurança (integridade, disponibilidade, confidencialidade e responsabilidade) são atingidos de modo adequado via uma determinada implementação quando:

  - A funcionalidade pretendida está presente e correctamente implementada,
  - Existe protecção suficiente contra erros não-intencionais (devidos a utilizadores e software) e,
  - Existe suficiente resistência para tentativas de penetração ou rodeio (bypass) aos mecanismos de segurança implementados.

A garantia torna visível que para um sistema ser considerado seguro, não basta responder bem aos seus requisitos funcionais, mas também estar preparado para impedir que determinadas acções possam acontecer. O desenho de um sistema é concebido ainda que de modo implícito para um determinado nível de garantia.

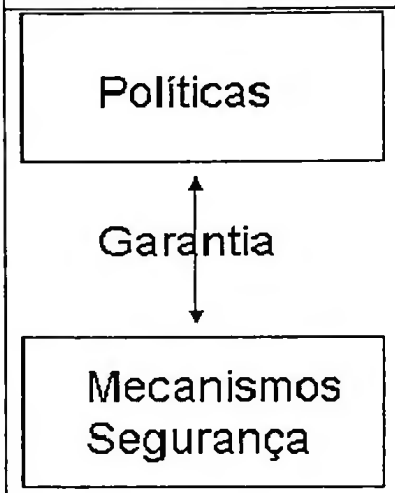
Esta propriedade surge ligada à definição de Garantia da Informação (information assurance), tal como foi definida Agosto de 1997, pelo NSTISSC:

São as operações de informações (IO) que protegem e defendem a informação e os sistemas de informação, assegurando a sua confidencialidade, autenticidade, integridade, disponibilidade e não-repudiação. Inclui ainda as operações necessárias para repor os sistemas de informação, pela incorporação de capacidades de protecção, de detecção e de reacção.

Outra ajuda para entender o conceito de 'assurance' é prestada por Clifton e Bishop (2004) que apresentam as seguintes definições relacionadas:

- *Entidade Confiável* (em que se pode confiar – trustworthy entity) tem evidência credível suficiente que nos leve a acreditar que o sistema corresponderá aos seus requisitos
- *Confiança (Trust)* é uma medida baseada na evidencia credível disponível
- *Garantia (Assurance)* é a confiança que uma entidade atinge os seus requisitos de segurança, baseada na evidência fornecida pela aplicação de técnicas de garantização, como métodos formais, desenho, testes, etc.

Figura 9 – Politicas, Garantia e Mecanismos de Segurança



	Declaração dos requisitos de segurança que explicita as expectativas relativas aos mecanismos de segurança
	Prova que os mecanismos cumprem os requisitos, apresentando evidência garantizadora, e aprovações suportadas nessa evidência
	Entidades executáveis desenhadas e implementadas, para cumprir os requisitos de segurança estabelecidos nas politicas.

3.5 Quais os termos e papeis para a classificação da informação nas empresas

De acordo com Krutz e Vines (2001), a informação produzida ou processada pela empresa deve ser classificada de acordo com a sua sensibilidade à perda ou conhecimento público da mesma. A sua classificação deve ser realizada pelos 'donos' da informação. É habitual encontrar as seguintes classificações no sector privado:

- Pública

  Informação dita não-classificada, que se chegar ao público em geral não traz impacto negativo significativo
- Sensível

Protecção que deve ser protegida quer na óptica da sua confidencialidade, quer na óptica da sua integridade

- Privada

  Informação considerada de carácter particular, e é apenas destinada a ser utilizada pela empresa. A sua publicação pode causar dado à empresa ou aos seus empregados.

- Confidencial

  Informação considerada muito sensível e que é destinada unicamente a utilização interna na empresa. Exemplo disto é por exemplo informação sobre planos de aquisição ou fusão com outras empresas, desenvolvimento de novos produtos.

Já no sector governamental, as classificações habituais são as seguintes:

- Não-classificado

  A disponibilidade desta informação ao público em geral não coloca problemas à administração pública

- Sensível, mas não classificada (SBU)

  Informação que tem algum grau de reserva, mas que se vier a aparecer no público, não cria problemas sérios, à administração pública

- Confidencial

  Informação que se aparecer no público, pode trazer alguns problemas à segurança nacional

- Secreta

  Informação que se aparecer no público, pode trazer sérios problemas à segurança nacional.

- Ultra-secreta

O nível mais elevado. Se esta informação surge no público, pode acarretar problemas muito graves à segurança nacional.

Os mesmos autores explicam os benefícios que decorrem desta classificação da informação:

- Demonstram o comprometimento da organização para com as protecções de segurança
- Ajudam a identificar os activos de informação mais críticos para as organizações
- Suportam os requisitos associados à segurança IT, no que respeita aos activos de informação
- Ajudam a identificar que protecções devem ser aplicadas a estes activos
- Podem ser necessários para responder à regulamentação em vigor na organização, a leis ou a estar em conformidade com os requisitos impostos por códigos de outra natureza a que a organização pretenda respeitar

Os papéis e responsabilidades dos diferentes actores no processo de classificação da informação deve ser claramente definido. São habituais os seguintes papéis:

- Dono (Owner)

  Esta pessoa é a responsável pelo recurso informação que deve ser protegido. Este 'dono' tem aos olhos da empresa, a responsabilidade final, pela protecção dos dados e de acordo com o princípio de 'ter preocupação por' (due care) pode ser responsabilizado por danos que possam suceder a este recurso.

  Tipicamente tem as seguintes responsabilidades:

  - Classificar a informação na óptica da segurança, tendo presente nas necessidades do negócio relativamente à protecção desta informação
  - Rever esta classificação periodicamente.

- Delegar a sua responsabilidade na protecção da informação no guardião

- Guardião da Informação (Costudian)

  Este papel tem delegado em si a responsabilidade de proteger a informação do 'dono' e está habitualmente atribuído à equipa de IT.

  Tipicamente este papel tem os seguintes deveres:

  - Realizar salvaguarda (backups) dos dados e teste das mesmas salvaguardas regularmente.
  - Realizar a recuperação da informação a partir das salvaguarda quando for necessário
  - Manter a informação salvaguardada de acordo com a política de salvaguardas, prevista para cada classificação.
  - Alem destes o guardião pode ainda ser o administrador do esquema de classificação em vigor.

- Utilizador (end-user)

  Qualquer entidade (pessoa ou processo) que utiliza de modo habitual a informação para o exercício das suas tarefas na empresa. Pode ser visto como um consumidor da informação

  Deveres que estas entidades devem observar:

  - Devem respeitar os procedimentos estabelecidos na política de segurança da empresa e aderir aos guias recomendados para a utilização dos procedimentos
  - Devem 'ter preocupação por' (due care) preservar a informação que utilizam no seu trabalho (tal como deve estar previsto na política de segurança)
  - Devem utilizar os recursos de computação da empresa apenas para finalidades relacionadas com a empresa, e não para uso pessoal.

As normas portuguesas SEGNAC, referem-se também à classificação de activos na óptica da segurança nacional, e em particular da classificação da informação.

Assim a SEGNAC 1, no capitulo 3, começa por afirmar que 'as entidades com competência para atribuir uma classificação de segurança, devem perante vários casos concretos, verificar se se justifica a sua atribuição e, em caso afirmativo, escolher criteriosamente o grau adequado, em harmonia com as definições apresentadas neste capitulo.

Explica de seguida que a classificação é usada tendo em vista duas finalidades:

- Assinalar as matérias que carecem de protecção de segurança, consequentemente, determinar o conjunto de medidas de segurança de que as mesmas devem beneficiar, quando em arquivo ou em deposito, em curso de manuseamento, em transporte ou em transmissão através de meios ou processos de comunicação
- Designar o grau de credenciação dos indivíduos que, pelas suas funções, tenham necessidade de manusear ou tomar conhecimento de tais matérias.

No ponto 3.2 a SEGNAC 1, detalha os graus de classificação dos activos de informação na óptica da segurança nacional, 'muito secreto', 'secreto', 'confidencial' e 'reservado'. Esclarece ainda que não se tratando de um grau de classificação, os documentos podem ainda levar a indicação de 'não-classificado', para evidenciar que o documento foi objecto de análise na óptica da segurança e não lhe foi atribuído nenhuma classificação que justifique cuidados adicionais.

Regulamenta no ponto 3.3.1 que as entidades que podem classificar um documento como 'muito secreto' são o Primeiro-Ministro, Ministros, Secretários de Estado, Presidentes dos Governos Regionais, Governadores Civis e a Autoridade Nacional de

Segurança. E embora esta responsabilidade possa ser delegada, só o pode ser feito para entidades com as competências necessárias para efectuar esta classificação.

A SEGNAC 4 cujo objecto é a segurança informática, no capítulo 6 regulamenta a classificação, preparação e segurança de dados e programas classificados.

No artigo 68, 'marcação de programas classificados' diz que todos os programas devem ter, em comentário, as seguintes indicações:

- Classificação – a qual indica o grau de classificação de programa: muito secreto, secreto, confidencial ou reservado;
- Numero de referencia – o qual identifica o programa para a segurança
- Datas de Revisão – as quais indicam as datas de eventuais revisões globais ulteriores, numero do exemplar e indicação de ser o original ou qual o numero da copia
- Nome do programa – o qual indica o nome do programa ou sub-programa
- Descrição sobre a funcionalidade do programa ou sub-programa, tratando-se de um sub-programa, deve ser indicado o nome do programa do qual ele é sub-programa
- Autor – nome do responsável pelo desenvolvimento do programa
- Notas – as quais configuram indicações relevantes para a utilização de programas por terceiros, como, por exemplo, opções de compilação ou 'linkagens' necessárias.
- Historial – esta secção documenta as modificações feitas ao código original. Por cada alteração significativa deve existir uma entrada nesta zona que descreva sucintamente as modificações introduzidas.

No artigo 69, 'classificação da documentação de programas',

- A documentação de programas classificados deve ter uma classificação igual `a dos respectivos programas.

- As regras sobre documentação classificada, enunciadas nos SEGNAC 1 e SEGNAC 2, aplicam-se a toda a documentação de programas classificados

Na óptica dos controlos operacionais e técnicos, de acordo com a norma NIST SP800-12, ou serviços de segurança operacionais e técnicos, NIST SP800-35, a SEGNAC 4 continua a ser uma boa referencia na segurança informática.

3.6 O que é a identificação, a autenticação, a autorização e a privacidade no contexto da segurança da informação?

Estes conceitos apresentados por Krutz e Vines (2001), e por uma lista considerável dos documentos guias para a segurança dos sistemas de informação suportados nas TI, como a SEGNAC4, a ISO/IEC TR 13335-1, a ISO/IEC 17799, a ISO 7498-2 surgem associados a muitas das tecnologias, mecanismos e objectivos ou propriedades dos sistemas de segurança, daí a importância da sua definição.

- Identificação (Identification)

  O sistema através do qual o utilizador diz quem é ao sistema a que pretende aceder

- Autenticação (Authentication)

  O sistema através do qual o sistema valida a identidade que o utilizador apresenta

- Autorização (Authorization)

  O sistema que atribui direitos e permissões a um utilizador ou a um processo, de modo a aceder a um conjunto de recursos. Após a identificação e autenticação acontecerem com sucesso o sistema atribui ao utilizador um conjunto de direitos e permissões. (Quem não se lembra dos filmes do 007 e das frases celebres 'permission to come aboard ? ... granted')

- Privacidade

Sistema que atribui a um utilizador autenticado um nível de privacidade que lhe permite aceder a recursos com um nível de privacidade igual ou inferior ao utilizador.

Hoje em dia a reflexão sobre o condicionamento da privacidade tendo presente as novas tecnologias emergentes, está muito alem da definição anterior de Krutz e Vines, a qual descreve outro mecanismo de controlo de acessos a recursos, dito mandatário. (eu tenho um nível de privacidade e por via disso acedo a todos os activos de informação classificados expressamente com um nível igual ou inferior ao meu).

Crompton (2001), reflecte sobre o conceito da privacidade e relaciona-o com a autonomia e dignidade do individuo, na sociedade. Cita a primeira definição de privacidade, 'como o direito de ser deixado em paz' (the right to be let alone).

Novas tecnologias que alimentam o debate à volta da privacidade incluem:

- A internet
- O crescimento exponencial das capacidades de memorização e analise dos dados
- A vigilância por vídeo da população em geral (Câmaras para desincentivar o terrorismo, nos táxis, nos ATMs)
- Informação de localização como um sub-produtos dos telefones moveis
- A nossa capacidade crescente de identificar pessoas via a retina, voz, DNA e outras biometrias
- Testes genéticos e o nosso conhecimento crescente do DNA

O quadro legislativo português, consagra um conjunto de leis sobre esta matéria, disponíveis no url:www.cnpd.pt. A Lei n.º 67/98 de 26 de Outubro 'LEI DA

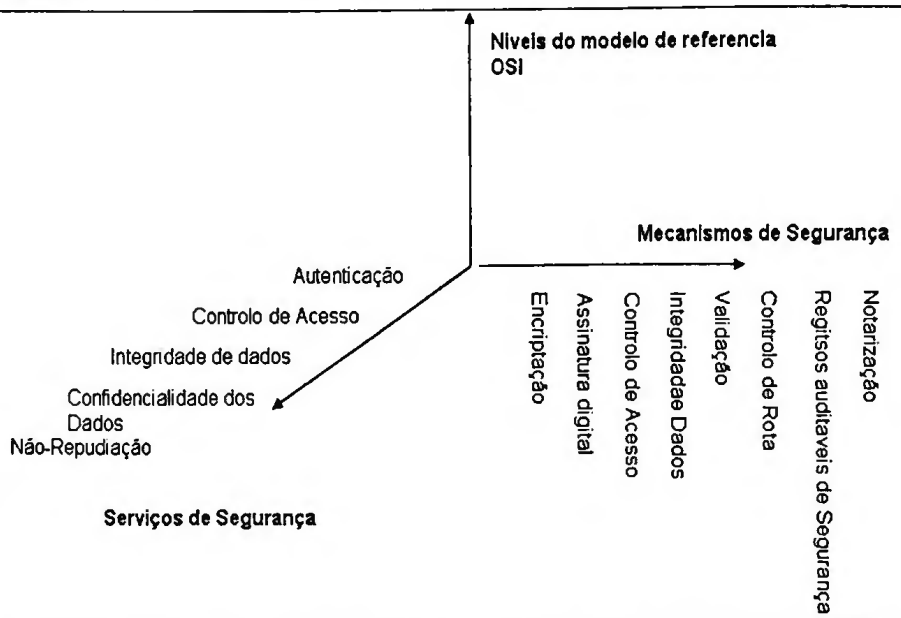
PROTECÇÃO DE DADOS PESSOAIS', apresenta no seu artigo 3º definições as seguintes definições para 'dados pessoais' e ' tratamento de dados':

«Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

«Tratamento de dados pessoais»: qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

Estes conceitos aparecem em modelos e contexto distintos como propriedades, requisitos e serviços de segurança. A norma ISO 7498-2 que trata de serviços e mecanismos de segurança básicos em cada um dos sete níveis do modelo OSI, Open System Interconnection, refere alguns deles do seguinte modo:

Figura 10 – Serviços e mecanismos de segurança para os níveis OSI na norma ISO-7498-2



A norma avisa que está apenas preocupada com os serviços e mecanismos de segurança necessários para que o trânsito dos dados entre os níveis 'peer' se faça de modo adequado.
Esta lógica de serviços decorre do próprio modelo no qual um actor do nível n+1 invoca serviços do nível N para fazer circular a mensagem a entregar ao seu interlocutor situado no mesmo nível n+1.

Ou seja a norma ISO 7498-2 alerta que não está preocupada com os serviços de segurança necessários nos sistemas finais, nas instalações onde se encontram e na organização que os gere.

Assim e de acordo com Bauknecht (2000), os serviços de segurança são implementados por mecanismos, e como exemplo o serviço de identificação e autenticação , é conseguido à custa dos seguintes mecanismos:

- Identificação dos utilizadores e respectivas palavras chave (user-id e passwords)
- Cartões de acesso (Tokens; smart-cards)
- Biométricas

A norma NIST SP800-33 propõe também um modelo de serviços de segurança que a figura seguinte exemplifica, onde os serviços aparecem arrumados por três categorias, de prevenção, de suporte e detecção e recuperação, e pela sua interacção conseguem satisfazer os objectivos da segurança de IT, tal como esta norma os identifica; disponibilidade, integridade, confidencialidade, responsabilização e garantia de segurança (ver secção anterior).

Serviços de Suporte:

- Identificação (e atribuição de nome)
- Gestão de chaves criptográficas
- Administração de segurança
- Protecções de sistema onde as funcionalidades de segurança estão implementadas

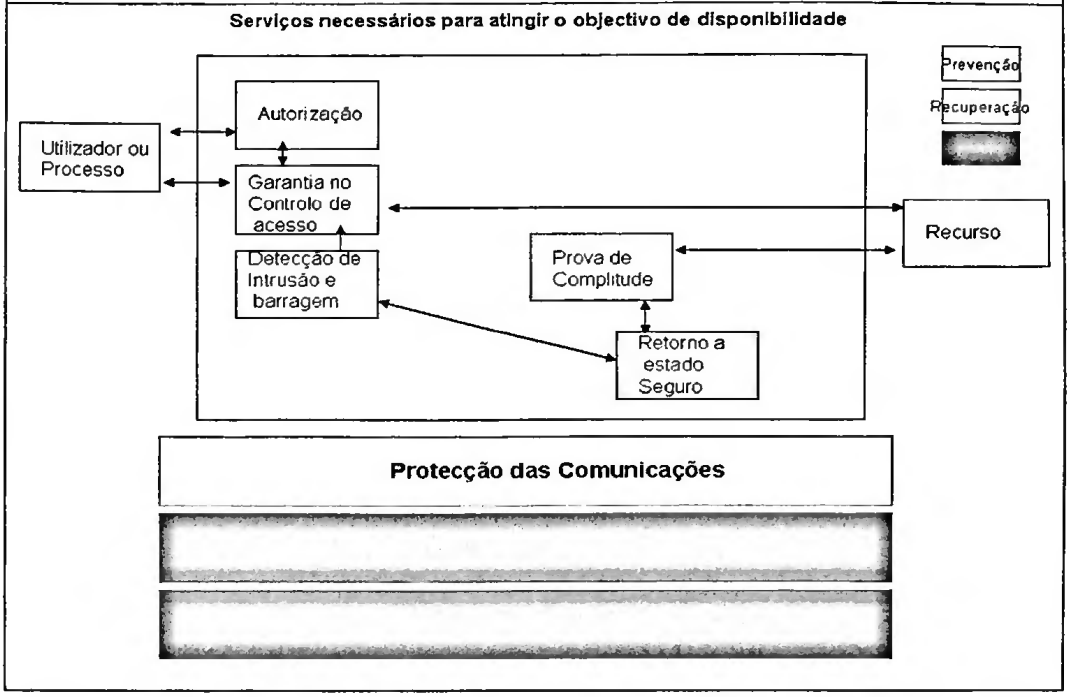
Serviços de Prevenção:

- Comunicações protegidas, o qual assegura a integridade, disponibilidade e confidencialidade dos dados em transito
- Autenticação
- Autorização
- Garantia do controlo de acesso de acordo com as politicas adoptadas na organização (Access control enforcement)
- Não-repudiação. Serviço que assegura a propriedade de responsabilização referida atrás.
- Transmissão privada.

Serviços de detecção e recuperação

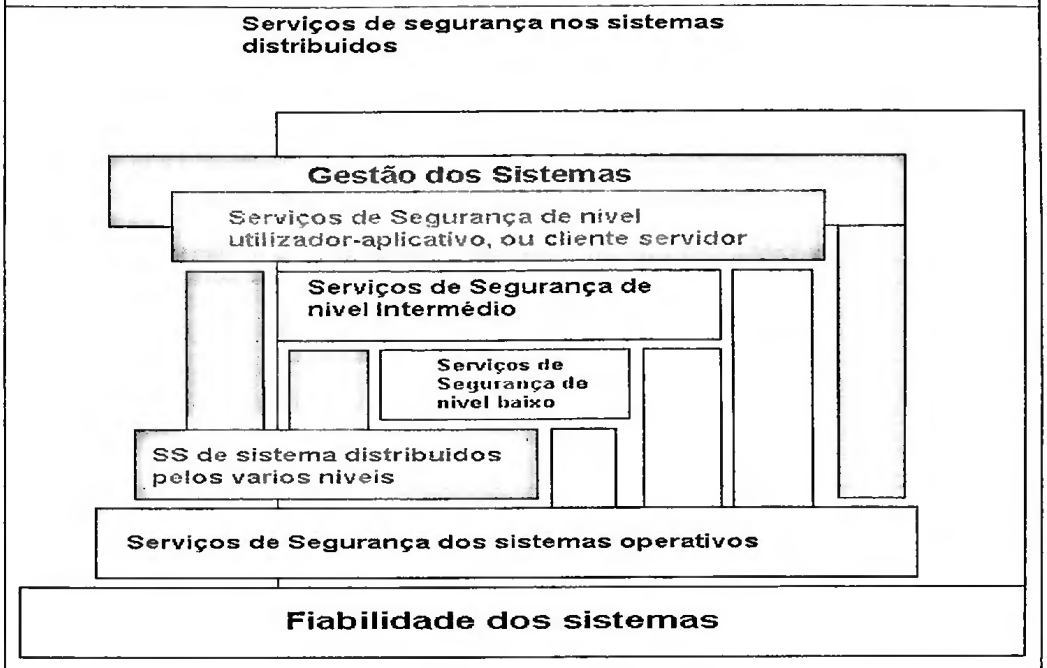
- Auditoria. Relevante para detectar incidentes que já aconteceram e para permitir detectar e corrigir vulnerabilidades do sistema a proteger
- Detecção de intrusão e barragem (intrusion detection and containment)
- Prova de integralidade (Prove of wholeness)
- Repor estado seguro. Quando uma brecha na segurança acontece o sistema deve ser capaz de retornar a um estado que é conhecido como seguro.

Figura 11 – Serviços de Segurança necessários ao objectivo disponibilidade



A proposta deste modelo engloba já os sistemas finais e a transferência de mensagens, embora a importância da robustez dos sistemas operativos onde correm os mecanismos de segurança, distribuídos ao longo dos diferentes elementos da rede, seja devidamente evidenciada na figura seguinte:

Figura 12 – Elementos relevantes para a Garantia do Sistema incluindo a Segurança



Esta figura releva alguns aspectos essenciais para a construção da confiança na robustez de um sistema distribuído, na óptica dos seus objectivos de segurança, qualquer que seja a definição adoptada:

1. Na base da arquitectura do sistema distribuído deve residir um conjunto de opções que sejam trave mestra na construção de um sistema confiável (reliability), a saber:
    a. Implementação de soluções técnicas o menos complexas possível
    b. Utilização de componentes confiáveis

c. Desenhar o sistema de modo a limitar penetrações, seja pela diminuição das vulnerabilidades, seja pela implementaçao de capacidade de detecção e recuperação

d. Integrar a tecnologia de modo adequado ao ambiente operativo onde se vai integrar

e. Adicionar medidas de protecção não técnicas (procedimentais e organizacionais)

2. Serviços de Segurança dos Sistemas Operativos

   Mesmo existindo ao nível do sistema operativo serviços de segurança, estes invocam os serviços e executam mecanismos do próprio sistema operativo. Se estes serviços e mecanismos não forem robustos, a segurança do sistema pode ser circundada e subvertida. Dai que a segurança do sistema dificilmente será maior do que a robustez do próprio sistema operativo.

3. O gráfico ilustra outra realidade que é o facto de embora alguns serviços de segurança residam num determinado nível lógico da hierarquia do modelo OSI, os mecanismos que o implementam estão de facto dispersos lógica e fisicamente, em objectos distintos. A imagem mostra como cada nível (layer) depende das capacidades dos níveis mais baixos, e mesmo dos mecanismos dos sistemas operativos.

4. Finalmente alguns serviços de segurança não existem num único nível, mas são conseguidos pela cooperação de diversos mecanismos de vários níveis distintos. Um exemplo comum é o serviço de identificação e autenticação: O interface do utilizador, tipicamente parte do nível aplicativo (cliente telnet p.e.) interage com

o utilizador para obter a informação necessária; A informação é então passada a um processo que verifica se está correcta; este processo provavelmente corre a nível do sistema operativo, ou ao nível da apresentação, sessão ou mesmo dos níveis de rede do modelo OSI; Pode ainda acontecer que a informação seja transmitida através da rede para outro servidor (um autenticador de rede p.e.).

3.7 O que é um Risco ?

De acordo com Turban at al, citado por Finne (1998), um risco é a 'probabilidade de uma ameaça se concretizar'. Esta probabilidade e o impacto no negocio uma vez materializada a ameaça é algo que depende da pessoa que os estima. Segerstahl, citado for Finne(1998), afirma que, 'o modo como as pessoas percepcionam e reagem aos riscos é habitualmente um mistério tanto para os cientistas especialistas em ciências naturais como para os decisores envolvidos profissionalmente no controlo e gestão de uma crise'.

De acordo com Smith citado por Finne(1998), 'risco em qualquer contexto é sempre a soma de ameaças, (eventos que podem ter impacto negativo no negocio da empresa), vulnerabilidades (fraquezas da empresa face a estas ameaças), e valor dos activos ameaçados. Ou seja

Risco = Ameaças + Vulnerabilidades + Valor dos activos ameaçados.

Poder-se-à discutir se em vez da soma o produto não seria a operação mais adequada, dado que se algum dos factores for zero, o total deveria ser zero, mas o que a equação ilustra é a relação directa entre o risco e qualquer um dos operadores.

3.8 Ameaças inerentes à função IT e o seu reflexo no negocio

A preocupação com a gestão de segurança nos sistemas IT só se justifica pela existência de ameaças mais ou menos prováveis que a verificarem-se podem produzir impactos negativos de gravidade distinta no negócio da empresa.

A norma NIST SP800-12 descreve as ameaças comuns no seu capítulo 4;

- Erros e Omissões
    - A norma refere uma estatística que sugere que 65% das perdas das organizações devidas aos sistemas de informação são devidas a erros e omissões. Erros na introdução dos dados, que aproveitam vulnerabilidades dos programas que os recolhem. Erros no desenvolvimento e programação, habitualmente designados de 'bugs' (piolhos) podem variar o seu impacto desde insignificante até catastróficos.
- Fraude e Roubo
    - Os sistemas de computadores podem ser manipulados de modo a 'automatizarem' os métodos clássicos de fraude e o roubo, e mesmo a inovarem no mesmo sentido. Um exemplo clássico é a passagem de pequenas importâncias para uma determinada conta, que pode ser proveitoso se operar sobre um número largo de contas.
    - Esta ameaça é sobretudo aproveitada por pessoas da casa.
    - A norma refere um estudo da Safeware Insurance segundo o qual em 1992 foram roubados 882 milhões de dólares de computadores pessoais.
- Sabotagem de empregados

- Movimentos de 'downsizing' nas empresas provocam o desagrado e desejo de vingança nos empregados que podem aproveitar antigas autorizações de acesso para sabotar os activos dos sistemas de informação.
- Embora o número destes incidentes sejam estimados como menores dos incidentes devidos aos roubos e fraudes, o seu impacto pode no entanto ser muito elevado.

- Perda de suporte físico e de infra-estrutura ambiental
  - Perda de energia eléctrica, inundações, fogo, motins civis, greves são alguns exemplos de ameaças que se podem traduzir em perdas substanciais para as empresas.
- Crackers (malicious Hackers)
  - Estas pessoas acedem aos sistemas de computadores, sem serem autorizados para tal e podem produzir todo o tipo de impactos negativos nos sistemas de informação com impactos que podem ser desastrosos.
  - Uma dificuldade associada a esta ameaça é que não são claros os objectivos destas pessoas. Tanto podem apenas ver informação como podem alterar os dados com ou sem proveito próprio.
- Espionagem industrial
  - A espionagem industrial é o acto de subtrair dados proprietários de empresas privadas ou governamentais. Um estudo patrocinado pela American Society for Industrial Security (ASIS) apuraram que o roubo de informação de negócio aumentou 260% desde 1985. Tipicamente os

dados traficados são preços, informação sobre processos, desenvolvimento de produtos e especificações.

- Código malicioso
  - Código malicioso, diz respeito a vermes (worms), viroses, cavalos de tróia, bombas lógicas e outros tipos de código 'não convidado'. Embora muito associado a ameaças nos computadores pessoais, pode atacar noutras plataformas.
  - Estudos em 1993 concluíram que embora o número de viroses tenha aumentado exponencialmente o número de incidentes não.
- Espionagem de governos estrangeiros
  - A maioria dos governos dispõe de serviços de informação que pesquisam todo o tipo de informação. A CIA (Central Inteligence Agency) será o mais conhecido destes serviços.
- Ameaças à privacidade pessoal
  - A acumulação de grandes quantidades de dados sobre cada um de nós, desde a actividade que desenvolvemos com os nossos cartões de credito ou de debito, às actividades administrativas que desenvolvemos com reflexo nos sistemas de informação suportados em TI, coloca uma ameaça seria sobre a privacidade de cada um de nós. Neste sentido os governos tem produzido legislação tendente a reduzir esta ameaça.
  - Em Portugal a CNDP (Comissão Nacional de Dados Pessoais), é o órgão responsável pela vigilância da legislação em vigor sobre esta matéria

A norma ISO/IEC TR 13335-4 no capítulo 10, aborda este tema de um modo distinto. Começa por reflectir sobre o reflexo para o negócio da perda dos objectivos de segurança de acordo com a sua própria definição.

Assim a perda de confidencialidade pode trazer consigo os seguintes impactos negativos ao negócio:

- Perda de confiança dos seus clientes e deterioração da sua imagem publica
- Responsabilidade legais que resultam do desrespeito pela legislação em vigor no que respeita à confidencialidade
- Colocar em risco a privacidade e segurança dos Colaboradores
- Perdas financeiras

A perda de integridade;

- Permitir fraudes
- Levar à tomada de decisões incorrectas
- Interrupção das operações de negocio
- Perda de confiança dos seus clientes e deterioração da imagem publica
- Perdas financeiras
- Responsabilidades legais devidas ao incumprimento da legislação em vigor

A perda de disponibilidade que pode manifestar em cenários pouco graves, até situações de extrema gravidade como a destruição de centros informáticos, pode acarretar;

- A tomada de decisões incorrectas
- Incapacidade de executar tarefas critica
- Perda de confiança dos seus clientes e deterioração da imagem publica
- Perdas financeiras

- Responsabilidades legais ou contratuais que resultem da legislação em vigor ou do cumprimento de metas estabelecidas nos contratos com terceiros (p.e. os contratos SWIFT na Banca)
- Custos significativos para recuperar da situação

Perda de responsabilização, permite e potencia;

- Manipulação do sistema pelos seus utilizadores
- Fraudes
- Espionagem industrial
- Acções não rastreáveis
- Falsas acusações
- Responsabilidades legais.

A perda de autenticidade, permite;

- Fraudes,
- A utilização de um processo valido, que utiliza no entanto dados falsos o que produz resultados indevidos
- Manipulação da organização dos terceiros
- Espionagem industrial
- Falsas acusações
- Ser accionado por desrespeito à lei em vigor

A perda de fiabilidade, permite;

- Fraude,
- Perca de cota de mercado
- Desmotivação da equipa

Sugere a norma que a resposta às questões levantadas para cada um dos seis objectivos de segurança, deve permitir classifica-los como sério, menor ou não necessário.

De seguida a norma aborda as ameaças tipo conhecidas para cada um dos objectivos de segurança de modo a permitir a selecção das defesas mais adequadas para as ameaças que façam sentido no contexto do sistema.

Assim as ameaças tipo para o objectivo confidencialidade são no entender da norma as seguintes:

- Escutar (eavesdropping)
    - Ouvir indevidamente uma conversa telefónica, aceder fisicamente a uma linha de comunicação de dados (line tapping)
- Radiação electromagnética
    - Pode ser utilizada para obter conhecimento sobre a informação de um sistema informático
- Código malicioso
    - Por exemplo capturando as senhas (passwords) do utilizador, que digita no seu posto de trabalho
- Falsificação da identidade do utilizador (Masquerading user identity)
    - Fazendo-se passar por quem não é desse modo aceder a informações não autorizadas
- Reencaminhamento de mensagens, ou desvio de mensagens
- Falhas de software
    - Estes erros se acontecerem no objecto destinado a proteger a confidencialidade, pode constituir uma entrada indevida
- Roubo

- Acessos não autorizados a computadores, dados e serviços aplicativos
- Acessos não autorizados a 'media' de memoria

As ameaças tipo para o objectivo integridade identificadas na norma são em muitos casos as mesmas do objectivo confidencialidade.

- Deterioração dos 'media' que guardam os dados
- Erros na manutenção dos processos em vigor
- Código malicioso
- Falsificação da identidade do utilizador, conseguindo deste modo acesso a dados a que não tem direito
- Reencaminhamento de mensagens, ou desvio de mensagens
- Repudiação da autoria da mensagem ou evento
- Falhas de software ('bugs')
- Falha da alimentação eléctrica e sistemas de apoio que suportam o funcionamento dos equipamentos TI
- Falhas técnicas das infra-estruturas que compõem a arquitectura TI, como a rede de comunicação de dados
- Erros na transmissão das mensagens
- Acesso não autorizado aos computadores, dados, serviços e aplicações
- Execução de programas e dados não autorizados
- Acesso não autorizado a 'media' com dados guardados
- Erros do utilizador

Ameaças face ao objectivo disponibilidade,

- Ataques destrutivos

- Deterioração dos 'media' que guardam os dados
- Falha nos equipamentos e serviços de comunicação
- Fogo e inundações
- Erros na manutenção dos processos IT
- Código malicioso
- Falsificação da identidade do utilizador
- Reencaminhamento de mensagens, ou desvio de mensagens
- Má utilização intencional dos recursos seja por colaboradores ou por terceiros
- Desastres naturais
- Falhas de software
- Falha da alimentação eléctrica e sistemas de apoio que suportam o funcionamento dos equipamentos TI
- Falhas técnicas das infra-estruturas que compõem a arquitectura TI, como a rede de comunicação de dados
- Roubo
- Sobrecarga de tráfego. Tipo de ameaça que quando intencional é conhecida por 'denial of service'
- Erros de transmissão
- Acesso não autorizado aos computadores, dados, serviços e aplicações
- Execução de programas e dados não autorizados
- Acesso não autorizado a 'media' com dados guardados
- Erros dos utilizadores

- Deterioração dos 'media' que guardam os dados
- Falha nos equipamentos e serviços de comunicação
- Fogo e inundações
- Erros na manutenção dos processos IT
- Código malicioso
- Falsificação da identidade do utilizador
- Reencaminhamento de mensagens, ou desvio de mensagens
- Má utilização intencional dos recursos seja por colaboradores ou por terceiros
- Desastres naturais
- Falhas de software
- Falha da alimentação eléctrica e sistemas de apoio que suportam o funcionamento dos equipamentos TI
- Falhas técnicas das infra-estruturas que compõem a arquitectura TI, como a rede de comunicação de dados
- Roubo
- Sobrecarga de tráfego. Tipo de ameaça que quando intencional é conhecida por 'denial of service'
- Erros de transmissão
- Acesso não autorizado aos computadores, dados, serviços e aplicações
- Execução de programas e dados não autorizados
- Acesso não autorizado a 'media' com dados guardados
- Erros dos utilizadores

No que respeita ao objectivo de responsabilização qualquer ameaça que possa impedir a atribuição de uma acção a alguém deve ser considerada. Como exemplo,

- Partilha de contas de utilizador
- Não rastreabilidade das acções executadas
- Falsificação da identidade do utilizador
- Falhas de software
- Acesso não autorizado aos computadores, programas e dados

No que respeita aos objectivos de autenticidade e fiabilidade a norma não avança com outros tipos de ameaças alem dos anteriores, relembra no entanto que um sistema que apresente um comportamento inconsistente seja ao nível do sistema seja das aplicações que ai correm tem como consequência a perda de confiança dos seus utilizadores.
Cohen (1997b) apresenta um sistema de classificação para ataques (que constituem ameaças) à segurança dos sistemas de informação que contempla 94 métodos, de novo sem preocupação de hierarquia ou estruturação entre si. Por exemplo o ataque 6 resulta dos terramotos, o 7 da radiação solar, o 14 resulta da fragilidade dos planos de teste aos sistemas, o 31 da ameaça que representa recrutar um atacante para a empresa e o 45 das vulnerabilidades dos 'daemons' de UNIX que podem ser utilizados pelo atacante para obter privilégios indevidos. Trata-se na prática de nível de descrição mais detalhado do que o apresentado nas normas já referidas, embora como o próprio autor afirma seguramente não completo para todos os sistemas.

3.9 O que é a gestão dos riscos?

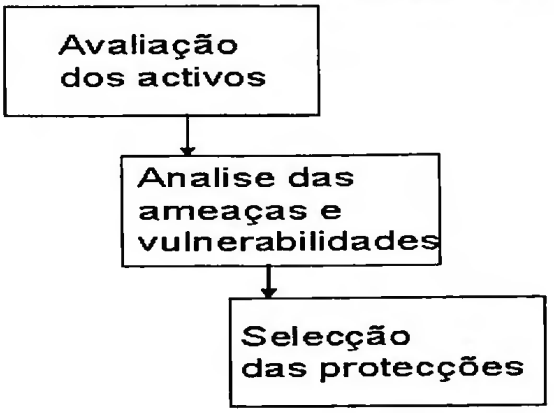
Caelli et al citado por Finne (1998), escreve que a gestão do risco tem como finalidade identificar, medir e controlar eventos incertos de modo a minimizar as perdas e optimizar o retorno do dinheiro investido com o propósito da segurança.

Esta definição sugere desde logo de acordo com Finne(1998), que não é possível eliminar totalmente os riscos associados á segurança da informação, dada a natureza do objecto a segurar e porque alguns dos riscos estão fora do controlo da empresa.

Caelli et al citado por Finne(1998), define análise de risco, como a etapa da gestão dos riscos, onde se minimizam os mesmos, pela aplicação de medidas de segurança adequadas às ameaças, vulnerabilidades e activos a proteger. De seguida definem avaliação do risco como a etapa da gestão dos riscos onde é realizada a análise dos activos e vulnerabilidades de modo a estabelecer a perda expectável que pode resultar se certos eventos ocorrerem, tendo presente a probabilidade de ocorrerem. A finalidade desta ultima etapa é na opinião dos autores o de avaliar se as salvaguardas existentes são adequadas para reduzir a probabilidade da perda, ou o impacto da perda a um nível aceitável.

Para outros autores citados por Finne(1998), como Anderson et al, a análise do risco compreende as etapas de análise e avaliação dos riscos

Figura 13 – Uma metodologia faseada para a Analise do Risco



De acordo com Finne (1998), a justificação do custo associado ás protecções seleccionadas, é um problema serio que os gestores dos riscos enfrentam, porque não é fácil calcular o retorno do investimento necessário. Finne (1998) recorda Anderson et al, que escreve que seria simpático se a análise do risco permitisse chegar a algo quantificável do género: ' temos uma probabilidade de 89,5% de sofrer uma perda de 100 000 FIM este ano'. A indústria Seguradora acumulou já dados actuariais para chegar a esta quantificação, mas no domínio da segurança da informação ainda não existe histórico suficiente para este efeito. Esta falta de dados históricos está também relacionada com a resistência que as empresas tem em declarar às seguradoras que foram alvo de fraudes relacionadas com a segurança de informação (ou outras), dado que a cultura vigente sugere que perdem a face perante o mercado, em particular no mercado financeiro onde a informação é matéria prima, produto semi-acabado e produto final.

E ainda interessante tentar enquadrar a gestão de risco ao nível da função IT, com a disciplina global de 'risk management' na óptica global dos riscos do negócio. Beja propõe um modelo agregador que as figuras que se seguem ilustram. De acordo com

este autor o risco associado aos sistemas de informação, deve ser enquadrado nos riscos operacionais os quais define como o risco de que deficiências nos sistemas de informação ou nos controlos internos resultem em percas inesperadas. Continua afirmando que 'pela sua natureza ligada a falhas humanas ou de sistemas, a procedimentos ou controlos inadequados, a desastres naturais e a situações similares, a maior parte destes riscos são difíceis de quantificar, embora sejam passíveis de escrutínio, controlo, graduação e monitorização. As alterações ocorridas no contexto e na forma de exercício dos negócios tornou estes riscos de tal modo relevantes que o relatório do Comité de Supervisão Bancária de Basileia, conhecido por Basileia II, contempla a introdução do seu tratamento explícito. O Comité de Supervisão Bancária de Basileia considera mesmo que o risco operacional é um risco importante que os bancos enfrentam, pelo que os mesmos devem possuir capital suficiente para protecção deste tipo de riscos. Esta imposição das entidades reguladoras veio incentivar a criação de modelos específicos para a quantificação dos riscos operacionais'

Figura 14 - Risk Management: Organização e Responsabilidades

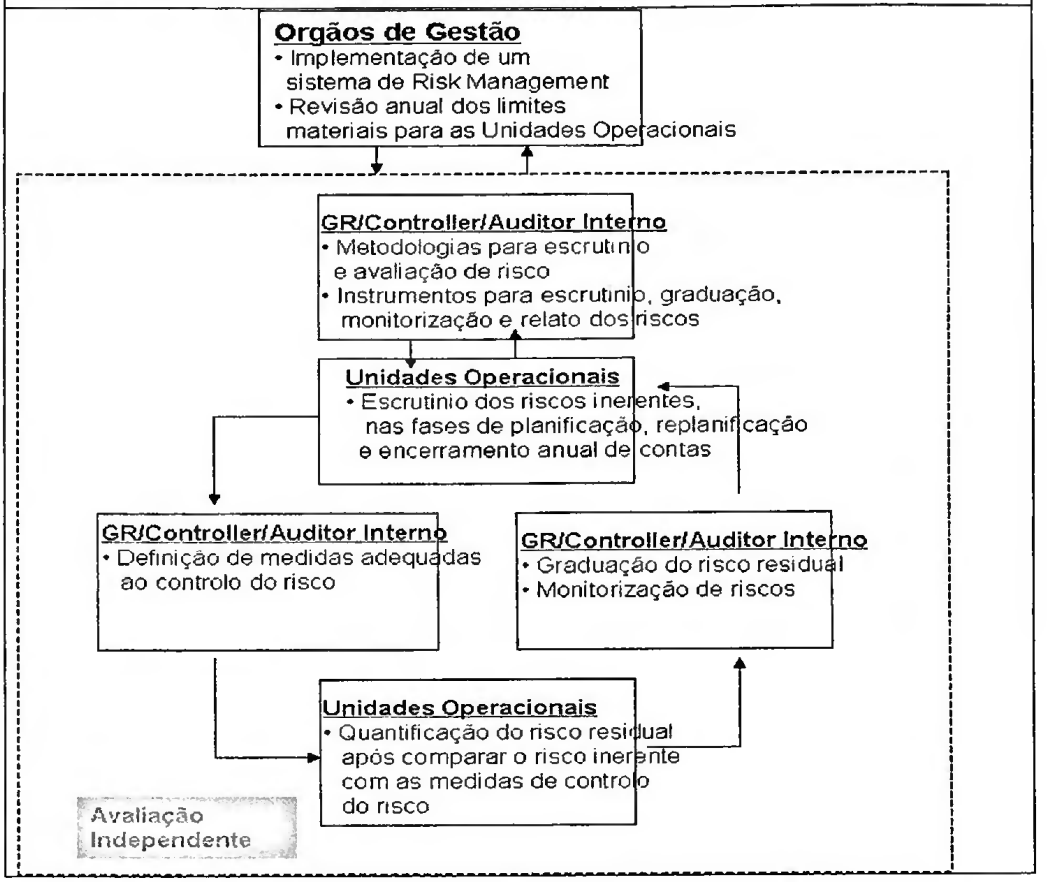
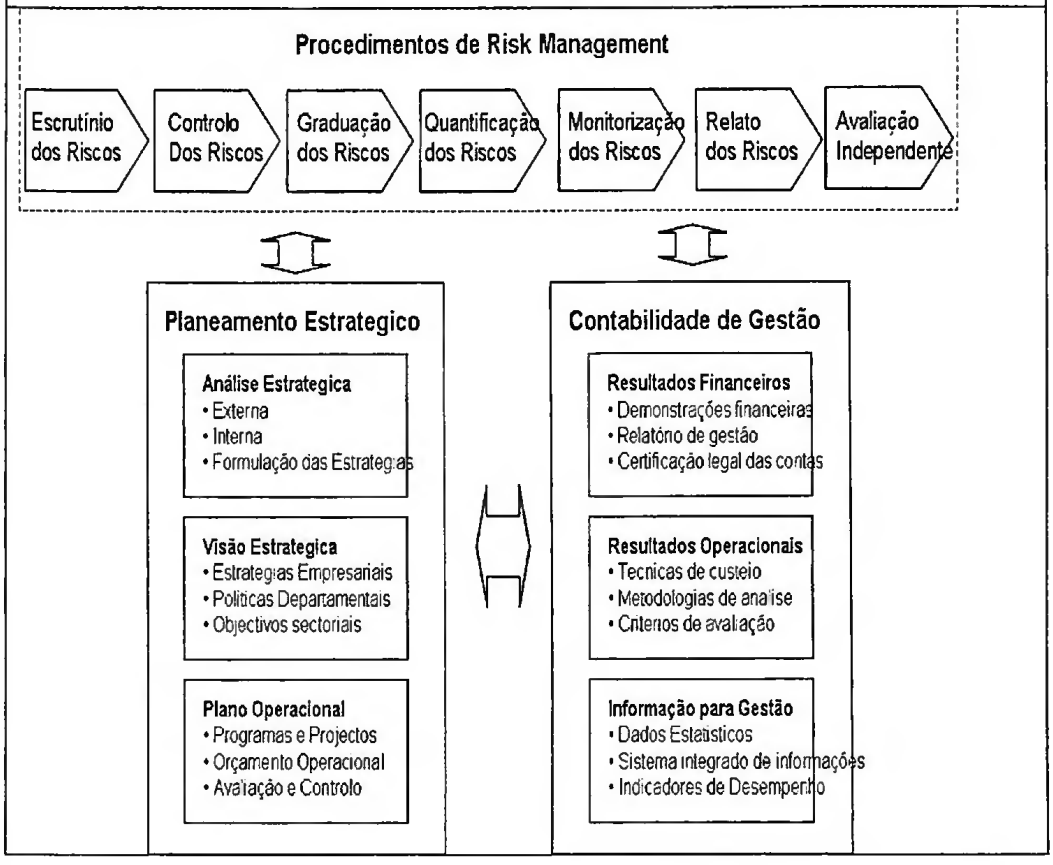


Figura 15 - Risk Management, Planeamento Estratégico e Contabilidade de Gestão



3.10 O que é garantir ou credibilizar a segurança dos sistemas IT ?

De acordo com Solms (1996), o objectivo final dos esforços da gestão da segurança de informação foram e continuam a ser, fornecer confiança na segurança dos serviços de informação de uma organização. Hoje em dia esta confiança é exigida internamente e externamente por parceiros e clientes. Este autor propõe cinco critérios a respeitar pelas

organizações de modo a credibilizar o seu sistema de segurança, seja ao nível dos produtos e sistemas, seja ao nível da função IT que os envolve.

1° Critério: Produtos e Sistemas IT confiáveis, de acordo com as certificações TCSEC, ITSEC e 'Common Criteria' não asseguram a confiança na segurança da função IT, mas contribuirão para a mesma como um dos blocos da construção.

2° Critério: Uma avaliação centrada na auditoria é necessária para garantir que as politicas, procedimentos, funções e temas relacionados, da segurança, na função IT, existem e estão a ser praticadas como prescrevem.

3° Critério: O esquema de avaliação deve tomar como âmbito toda a função IT e não deve ser restringido a qualquer produto ou sistema

4° Critério: O esquema de avaliação, deve prever níveis distintos de confiança na segurança IT implementada.

5° Critério: As normas e critérios definidos devem ser suficientemente precisos para permitir auto-avaliações para fins internos.

O mesmo autor refere o TCSEC, Trusted Security Evaluation Criteria, inicialmente publicado em 1985, como o primeiro esquema de avaliação de segurança de produtos e sistemas a ter aceitação alargada na indústria IT. Como resposta a este esquema surgiram o ITSEC, Information Technology Security Evaluation Criteria em 1990 na Europa e o CTCPEC, Canadian Trusted Computer Product Evaluation Criteria em 1993

no Canadá. Harmonização posterior destes critérios de avaliação de segurança, deu origem ao CC, 'Common Criteria' disponível no URL www.commoncriteria.org .

O projecto CC, 'critérios comuns' para a avaliação da segurança de produtos e sistemas das tecnologias de informação, define um conjunto de conceitos e princípios e propõe um modelo genérico de avaliação. Propõe ainda 'constructs', novos objectos, para expressar objectivos de Segurança IT, seleccionar e definir requisitos de segurança e escrever especificações de alto nível para produtos e serviços. Um produto ou sistema objecto de avaliação de segurança de acordo com os CC, é designado de TOE, Target of Evaluation, ou traduzindo livremente o 'alvo de uma avaliação' (Casmir, 2003).

No que respeita as esquemas de avaliação da segurança da função IT Solms (1996) refere o BS7799-1 como um 'código de boas praticas' que deve orientar os gestores e os técnicos responsáveis pela referida segurança, na implementação de um conjunto de controlos de segurança reconhecidos pela industria como conjunto mínimo adequado de modo a reduzir substancialmente os riscos inerentes à função IT na perspectiva da segurança. Estes controlos organizados em dez tipos distintos são propostos como uma base (baseline) de partida, que a industria reconhece como boas praticas e como tal asseguram o respeito e inspiram confiança entre os actores da industria, o que justifica também que uma analise de risco e de custo-beneficio habitualmente longos tenham de acontecer para justificar a sua implementação.

Esta abordagem ao estabelecimento de controlos de segurança pode já ser encontrada na Datapro (1985), que afirma que embora tenham já sido desenvolvidos métodos para conduzir revisões de segurança baseados em analise de risco de modo a detectar

vulnerabilidades e identificar controlos apropriados, muitas organizações adoptam as soluções desenvolvidas por outros para as vulnerabilidades mais comuns. Aplicar as praticas de segurança geralmente utilizadas, é atractivo quando os problemas e necessidades são similares entre as organizações.

Este referencial torna-se ainda um instrumento importante para os auditores responsáveis por se pronunciarem sobre a segurança da função IT, dado que pode substituir a falta de politicas e normas da organização e o próprio juízo subjectivo do auditor sobre os controlos mais adequados a implementar.

E interessante referir que `a data do artigo de Solms (1996), esta norma BS7799-1 não tinha ainda subjacente um esquema de certificação e acreditação, o qual estava a ser estudado, e veio a ser mais tarde constituído após a publicação da norma BS7799-2.

Casmir (2003) explica que o BS7799-1 acabou por evoluir para uma norma ISO, a ISO/IEC 17799:2000 a qual pode de facto ser vista como um conjunto de 'coisas' boas a implementar, e que aprofundamentos posteriores, que já borbulhavam em 1996, derem origem à norma BS 7799-2, cuja versão actual é a BS7799-2:2002, a qual é uma especificação norma de um sistema de gestão de segurança da informação (ISMS). A versão actual desta norma instrui a gestão da função IT, a aplicar a norma ISO/IEC 17799:2000 (Parte-1) e a construir, operar, manter e melhorar um ISMS, sistema de gestão para a segurança da informação, tomando como referencia o ciclo 'Plan-Do-Control-Act' tão do agrado das normas de sistemas de gestão da qualidade.

O SSE-CMM, Systems Security Engineering Capability Maturity Model, www.sse-cmm.org, que na sua versão II foi publicado como o documento ISO/IEC 21827, tem como objectivo tornar a engenharia de segurança uma disciplina definida, madura e quantificada (Casmir, 2003).

À semelhança do SE-CMM, Software Engineering Capability Maturity Model, também o SSE-CMM estabelece patamares de competência no domínio da segurança dos sistemas de informação suportados nas TI:

0. Não existe
1. Desempenhado informalmente
2. Planeado e controlado.
3. Bem definido
4. Controlado quantitativamente,
5. Continuamente melhorado

Num documento em que mapeia o SSE-CMM com outros documentos guia para a segurança IT, Hopkinson (1999) esclarece que contrariamente a estes guias/normas a missão do modelo SSE-CMM não é ajudar o gestor a estabelecer um programa de segurança IT na sua organização ou ajuda-lo a verificar se todos os aspectos relevantes estão considerados. A missão do SSE-CMM, é a de avaliar o nível de maturidade dos processos estabelecidos na organização para que esta atinja o nível de segurança que deseja. O principio do SSE-CMM é o de que quanto mais maduro o processo estiver, e tomando as restantes variáveis como iguais, melhor e mais consistentemente serão os resultados do mesmo, independentemente da aproximação e método que utilizar para atingir tais resultados.

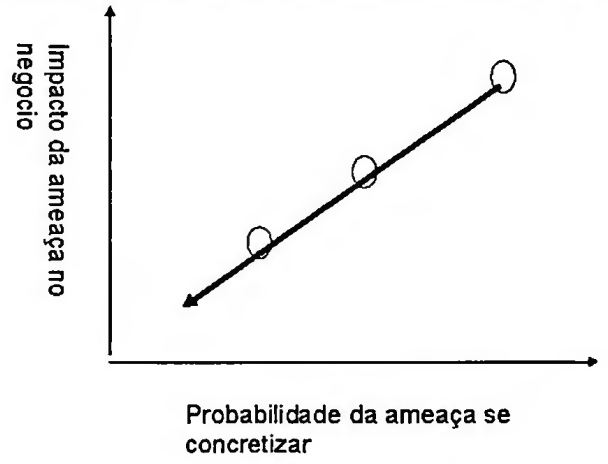
Embora a finalidade do SSE-CMM seja o descrito, o mesmo autor adianta que este pode ser olhado como uma 'base de trabalho' (framework) genérico para a segurança IT da organização dado que cobre com as suas áreas de processo (Process Areas) subdivididas cada uma delas nas praticas básicas (basic pratices), os domínios da engenharia,

projecto e organização, o que torna possível o mapeamento com os outros guias, como o BS7799, ou o ISO/IEC 13335-parte 2 ou o NIST Handbook.

3.11 Qual é objectivo de um controlo de segurança do sistema de informação ?

De acordo com Krutz e Vines (2001), o objectivo principal de um controlo de segurança é o de reduzir o efeito conjugado das ameaças e vulnerabilidades à segurança do sistema de informação a um nível tolerado pela empresa. A figura seguinte ajuda a perceber o que se espera do controlo de segurança.

Figura 16 – O que se espera de um controlo de segurança



Pretende-se que o controlo seja capaz de reduzir simultaneamente a probabilidade de ocorrência da ameaça e o seu impacto no negócio. (note-se que o impacto deverá ser analisado à luz das três propriedades, disponibilidade, integridade e confidencialidade) Um controlo devidamente implementado fará a curva aproximar-se do ponto (0,0), sem no entanto lá chegar dado que a partir de certa altura diminuir a probabilidade ou o impacto obrigará a um investimento sem retorno expectável (Finne, 1998).

As palavras protecção (safeguard) e controlo (control) são utilizadas de modo indistinto na literatura. Assim o NIST SP-800 12, refere-se a três tipos de controlos de segurança, os de gestão, os operacionais e os técnicos, embora esclareça que alguns controlos ou protecções cruzam as fronteiras de cada uma das tipologias que define do seguinte modo:

- Controlos de Gestão dizem respeito a controlos que focam habitualmente a gestão do programa de segurança e a gestão do risco na organização. Trata-se habitualmente de técnicas e preocupações típicos da gestão do programa da segurança nos sistemas da informação. São propostos os seguintes controlos (ou protecções) de gestão:
    - Politicas para a Segurança dos Sistemas de Informação
    - Gestão do programa para a Segurança dos sistemas de informação
    - Gestão do risco na segurança dos sistemas de informação
    - Segurança e planeamento no ciclo dos sistemas de informação baseados em computadores
    - Garantização (Assurance).

- Controlos Operacionais referem-se de um modo geral a controlos ou protecções que são implementados e executados por pessoas, em alternativa a sistemas automáticos. Para que possam ser implementados requerem habitualmente conhecimentos técnicos adequados, e o seu êxito total depende habitualmente de actividades de gestão e controlos técnicos. São propostos os seguintes controlos (ou protecções) operacionais:

- Questões ligadas aos utilizadores/pessoas que utilizam os sistemas de computadores
- Preparar-se para desastres e contingências
- Lidar com incidentes de segurança dos sistemas de informação
- Consciencialização, treino e formação
- Segurança nas actividades de suporte e operação dos sistemas baseados em computadores
- Segurança física e no ambiente onde os sistemas estão hospedados

- Controlos Técnicos focam-se nos controlos de segurança executados pelo sistema. Ou seja o seu funcionamento correcto depende muito do bom funcionamento do sistema. Habitualmente para que possam ser totalmente bem sucedidos estes controlos envolvem significativas considerações procedimentais e devem estar em linha com os controlos de gestão estabelecidos. São propostos os seguintes controlos (ou protecções) técnicos:
  - Identificação e Autenticação
  - Controlo de Acessos lógico
  - Registos para auditoria
  - Criptografia

A norma ISO/IEC TR 13335-4 propõe um guia para selecção de protecções de segurança nos sistemas de informação, centrado em duas estratégias, a chamada base mínima, ou como resultado de uma análise detalhada de risco a um sistema considerado de elevado risco. A aproximação à base mínima divide-se ainda em dois níveis, a aproximação simples que selecciona as protecções gerais e especificas dos sistemas de

informação de acordo com o tipo de sistema a que se destina, ou a avançada que selecciona as protecções de acordo com as preocupações e ameaças que rodeiam o sistema em termos dos seus objectivos de segurança, confidencialidade, integridade, disponibilidade, responsabilidade, autenticidade e fiabilidade.

Esta norma 'arruma' as protecções dos sistemas de informação em dois grandes grupos, os oriundos da segurança física e da gestão que podem ser aplicados à segurança dos sistemas de informação e as protecções próprias dos sistemas IT. Esta norma compara a instanciação em categorias e sub-categorias dos seus dois tipos de protecções com a proposta de outros normativos que identificam e propõem controlos para a segurança dos sistemas de informação:

Tabela 5 – comparação das protecções gerais da TR 13335-4 com outros referenciais normativos

ISO/IEC TR 13335-4	**Código para a pratica da gestão dos sistemas de informação – BS7799-1**	**Manual para a protecção base dos sistemas IT**	**NIST SP-800 12**
A	***Protecções Físicas e Organizacionais***		
A.1	***Politicas e Gestão da Segurança IT***		
1. Politica de Segurança IT na Empresa	3.1	1.1 e 1.2	5.1
2. Politica para a Segurança dos Sistemas IT		1.1 e 1.2	5.2 e 5.3
3. Gestão da Segurança IT	4.1.1 e 4.1.2	1.1 e 1.2	6
4. Alocação de Responsabilidades	4.1.3	1.3	2.4, 2.5 e 3
5. Organização da Segurança IT	4.1	1.2	3.5
6. Identificação e avaliação dos activos	5	2.2	7.1
7. Aprovação dos sistemas IT	4.1.4	-	8

A.2	*Verificação da Conformidade da Segurança*		
1. Conformidade com Politicas e Protecções da Segurança IT	12.2	1.2	10.2.3
2. Conformidade com requisitos legais e regulamentares	12.1	3.1 e 3.2	6.3 e 10.2.3
A.3	*Tratar Incidentes*		
1. Reporte de Incidentes de Segurança	6.3.1	M2	12
2. Report de Fraquezas de Segurança	6.3.2	M2	12
3. Report de erros no Software	6.3.3	M2	12
4. Gestão de Incidentes	8.1.3	M2	12
A.4	*Pessoal*		
1. Protecções para pessoal permanente e temporário	6.1	3.2 e M3	10.1
2. Protecções para pessoal contratado	6.1	-	10.3
3. Treino e Consciencialização de Segurança	6.2	1.2 e M3	13 e 10.1.4
4. Processo disciplinar	6.3.5	3.2 e M3	-
A.5	*Temas Organizacionais*		
1. Gestão da Configuração e da Mudança	8.2 e 10.5	-	14.3 e 8.4.1
2. Gestão das Capacidades	8.2.1	-	-
3. Documentação	8.1.1 e 8.6.3	M2	14.6
4. Manutenção	7.2.4	M2	14.7
5. Monitorização de mudanças relevantes de segurança	-	1.2	7.3.3
6. Traços (evidencias) para auditoria e registo (Audit Trails and Logging)	8.4	M2	18
7. Teste de Segurança	-	M2	8.4.3
8. Controlo dos 'Media'	8.6	8 e M2	14.5
9. Garantir Apagamento das Memorias	-	M4	-
10. Segregação de deveres	8.1.4	M2	-
11. Utilização correcta do software	12.1.2	M2	-
12. Controlo das alterações do software	10.5.1 e 10.5.3	M2	-

A.6	*Planeamento da Continuidade do Negocio*		
1. Estratégia para a continuidade do negocio	11.1.1 e 11.1.2	3.3 e M6	11.2, 11.3 e 11.4
2. Plano para a continuidade do negocio	11.1.3 e 11.1.4	3.3 e M6	11.5
3. Teste e actualização do plano	11.1.5	3.3 e M6	11.6
4. Salvaguardas (backups)	8.4.1	3.4	14.4
A.7	*Segurança Física*		
1. Protecção do Material	7.1	4.1, 4.3 e M1	15.1
2. Protecção ao Fogo	7.2.1	-	15.2
3. Protecção aos Líquidos e Aguas	7.2.1	M2	15.5
4. Protecção contra desastres naturais	7.2.1	M2	15.4
5. Protecção contra Roubos	7.1	1.2	15.1
6. Ar condicionado e energia eléctrica	7.2.2	M2	15.6
7. Cabelagem	7.2.3	4.2 e M1	-

Comparando as protecções próprias dos sistemas das TI,

Tabela 6 – Comparação das protecções específicas dos SI/TI propostas em diversos documentos normativos

ISO/IEC TR 13335-4	**Código para a pratica da gestão dos sistemas de informação – BS7799-1**	**Manual para a protecção base dos sistemas IT**	**NIST SP-800 12**
B	*Protecções especificas dos sistemas TI*		
B.1	*Identificação e Autenticação*		
1. I&A baseado em algo que o utilizador conhece	9.2.3, 9.3.1, 9.4 e 9.5.1	M4	16.1
2. I&A baseado em algo que o utilizador possui.	9.2.3, 9.3.1, 9.4 e 9.5.1	-	16.2

3. I&A baseado em algo que o utilizador é.	9.2.3, 9.3.1, 9.4 e 9.5.1	-	16.3
B2	***Controlo lógico dos Acessos e Auditoria***		
1. Politica de Controlo de Acesso	9.1	M2	17.1, 17.2 e 17.3
2. Acesso dos Utilizadores aos Computadores	9.2, 9.3 e 9.5	M4	17.1, 17.2 e 17.3
3. Acesso dos Utilizadores aos Dados, aos Serviços e às Aplicações	9.4 e 9.6	M4	17.1, 17.2 e 17.3
4. Rever e actualizar os direitos de acesso	9.1 e 9.2.4	M2	17.4
5. Traços e evidencias (Trails) para registo da actividade (Log)	9.7	M4	18
B.3	***Protecção contra código malicioso***		
1. Visualizadores (Scanners)	8.3	M4	-
2. Validadores de Integridade (Checkers)	8.3	M4	-
3. Controlo para a circulação dos 'media' transportáveis	7.3.2	-	-
4. Procedimentos de salvaguarda	8.3	M4	-
B.4	***Gestão da Rede***		
1. Procedimentos Operativos	8.5.1	M2	-
2. Planeamento do Sistema	8.2	M2 e M4	8.4
3. Configuração da rede	-	M4	-
4. Segregação da Rede	9.4.6	M2	-
5. Monitorização da Rede	9.7	M2	18.1.3
6. Detecção de Intrusão	-	-	18.1.3
B.5	***Criptografia***		
1. Protecção da Confidencialidade dos dados	10.3.2	M4	19.5.1
2. Protecção da Integridade dos Dados	10.3.3	M4	19.5.2
3. Não-repudiação	10.3.4	-	19.2.3
4. Autenticidade dos Dados	10.3.2	M4	19.5.2
5. Gestão das Chaves	10.3.5	-	19.3

Cohen (1997a) descreve 140 classes de métodos destinados a defender os sistemas baseados em computadores. Estas 140 classes de protecções aparecem no entanto sem preocupações de hierarquia ou profundidade. Por exemplo os 'general accepted systems security principles' da norma NIST SP800-14 aparecem nesta lista nas classes 126 à 133, e de acordo com este normativo estes princípios são respeitados em todas as quinze praticas de protecção dos sistemas de informação propostas no mesmo. Permitiram no entanto ao autor concluir um conjunto de propriedades emergentes nestas 140 classes que à data constituíam o catálogo publicado mais completo, a saber:

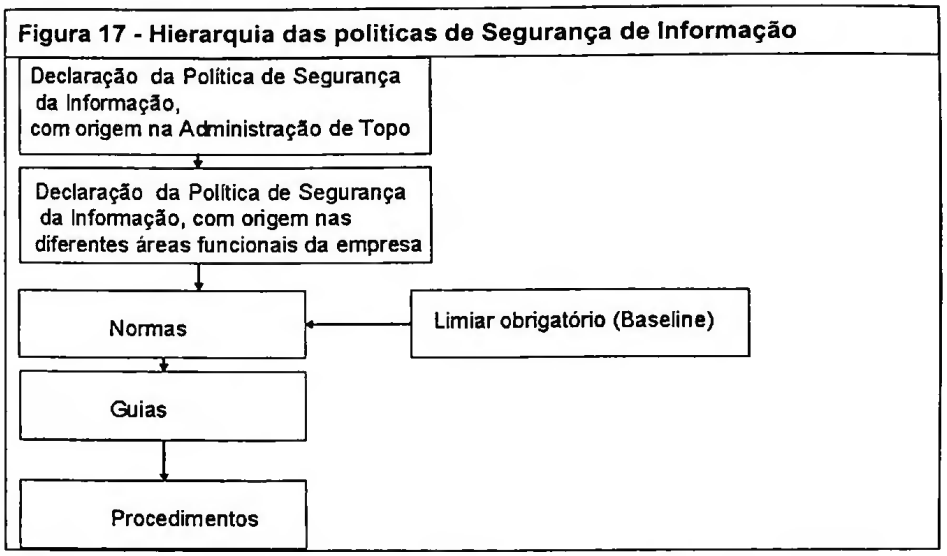
- Não-ortogonalidade
    - As classes apresentadas não são ortogonais, isto é, existem sobreposições significativas entre elas
- Sinergia
    - As sinergias que existem entre as classes de defesas não podem ser estatisticamente manipuladas. Assim duas defesas com uma eficácia de 90% pode não resultar numa eficácia combinada de 99%, mas sim em 0% de eficácia. Concluiu o autor que os efeitos sinérgicos entre as diversas classes não estão ainda suficientemente compreendidos.
- Não-Específicos
    - A maioria das classes de defesa propostas não são dirigidas a uma arquitectura ou a uma situação. Lembra no entanto o autor que as defesas reais são sempre muito específicas e o diabo, dizem, está nos detalhes.
- Descritivos apenas
    - As classes apresentadas são apenas descritas. Ou seja não foram completamente analisadas e definidas no sentido matemático do termo

- Aplicabilidade limitada
    - A aplicabilidade de cada classe deve ser ponderada para cada situação particular, dado que pode ou não ser adequada á mesma
- Incompleta
    - As classes apresentadas são ainda muito provavelmente incompletas para constituir uma defesa inexpugnável dos sistemas baseados em computadores

3.12 O que são políticas, normas, guias e procedimentos de segurança (Policies, Standards, Guidelines and Procedures) ?

De acordo com Krutz e Vines (2001), o termo política no seu sentido mais amplo, engloba todos os quatro tipos referidos no título, que no seu conjunto constituem a Politica de Segurança de Informação da organização. De acordo com os mesmos autores uma Política de Segurança da Informação bem escrita é essencial para uma pratica de segurança sólida.

A divisão entre os quatro conceitos consegue ser melhor percebida, a partir da sua hierarquia habitual na empresa, que a figura seguinte retrata:



A norma NIST SP 800-14, esclarece que o termo 'politica de segurança para computadores' (computer security policy) tem mais do que um significado. Este documento afirma que Politica (policy) é o conjunto de directivas da gestão de topo, destinadas a criar um programa de segurança das TI, estabelecer os seus objectivos gerais (goals) e atribuir responsabilidades. Alem desta definição a mesma palavra é usada para referir regras especificas de segurança para sistemas particulares, como a politica de privacidade do email, ou da segurança na utilização do fax.

Propõe assim este documento orientador, que as organizações possuam três tipos de politicas:

- Programas
- Especificas de um tema (issue specific)
- Especificas de um sistema

Detalhando o conteúdo de uma politica de programa, diz a norma que esta deve:

- Criar e definir um programa para a segurança nas TI
    - Esta politica deve deixar claro a que recursos se aplica

- Estabelece as direcções estratégicas da Organização na segurança das TI
    - Alem das grandes preocupações da organização, podem aqui surgir os objectivos gerais que a organização pretende atingir
- Atribuir responsabilidades
- Focar as questões que se podem levantar relativas ao respeito pelos enquadramentos legais e internos a respeitar (compliance)
    - Estas regras a fazer respeitar focam duas vertentes:
        - As responsabilidades a assacar às unidades que tem a seu cargo o cumprimento dos requisitos do programa de segurança
        - O uso de penalidades e acções disciplinares que decorrem do não cumprimento das regras instituídas

As políticas específicas de um tema (issue specific), devem:

- Focar um tema especifico que num dado momento se coloque, como por exemplo estabelecer uma politica de privacidade para o email, na organização
- Ser actualizada frequentemente, dado que tratando-se de temas recentes pode acontecer que o modo apropriado de garantir a segurança nessa tecnologia ou solução não esteja ainda suficientemente madura à data da publicação da primeira politica
- Conter uma declaração que esclarece a posição da organização relativamente ao tema, na óptica da segurança, responsabilidades, normas a respeitar e ponto de contacto para questões que possam surgir.

As políticas específicas de um sistema, devem:

- Focar-se nas decisões tomadas pela gestão e destinadas a proteger um sistema particular, devem ser tornadas publicas. Exemplo de uma decisão destas, é o

modo como a gestão responsabiliza cada pessoa pelas acções que executa no sistema.

- As decisões da gestão devem ser suportadas numa análise técnica que as justifique
- Variar de sistema para sistema, dados os objectivos específicos e ambientes específicos de cada sistema.
- Ser expressas em regras. Por exemplo 'quem' faz o 'quê' e a 'quem' sob que 'circunstancias '.

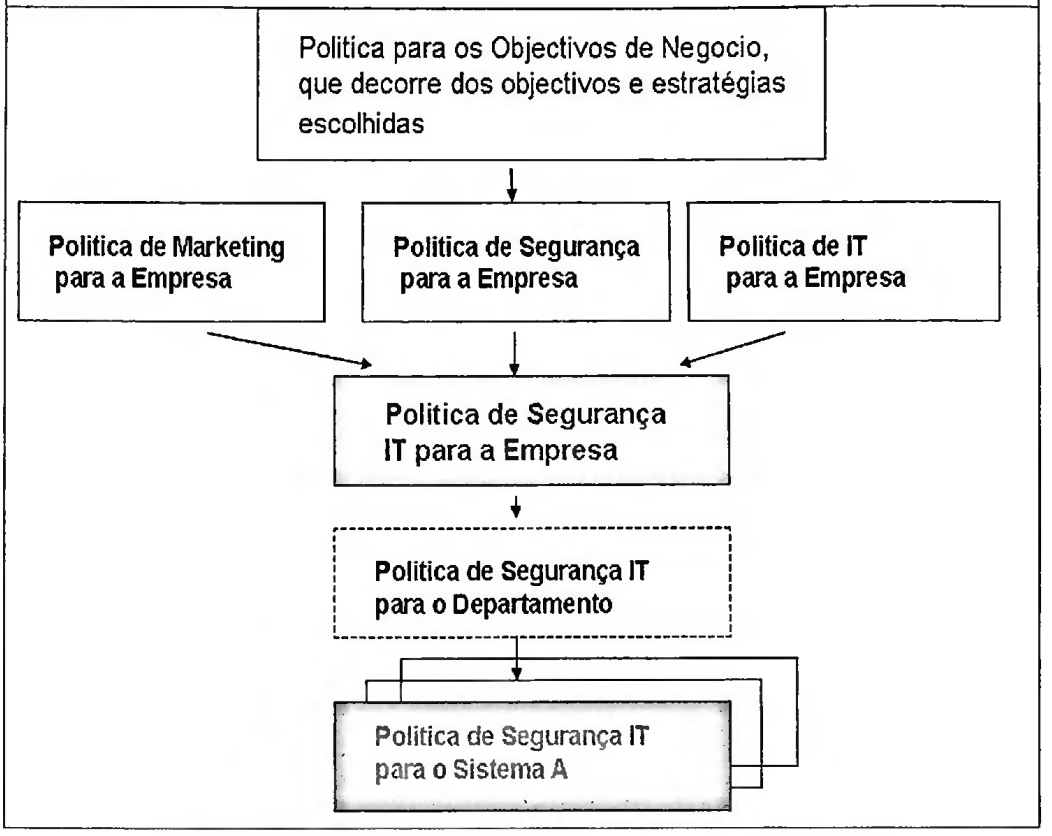
Os três tipos de politicas devem:

- Ser complementadas.
    - Dado que cada politica pode ser escrita a um nível elevado de abstracção, as organizações devem desenvolver, normas (standards), guias de utilização (guidelines) e procedimentos (procedures) que permitam aos utilizadores, gestores e outros interessados um caminho seguro para a implementação da politica definida pela gestão. Estas normas, guias de utilização e procedimentos devem ser disseminados na organização via manuais e regulamentos.
- Visíveis
    - A visibilidade das políticas, facilita muito a sua implementação em toda a organização.
- Suportadas pela Gestão
    - Sem o suporte e pressão da gestão, qualquer politica tende a ser esquecida e negligenciada.
- Consistente

- As novas politicas, devem ser coerentes, com outras directivas, leis, cultura organizacional, procedimentos e missão da organização.

A norma ISO/IEC TR 13335-2 (1997), propõe uma definição e um conjunto de considerações próximas das propostas pelas referências e autores anteriores, como desde logo a próxima figura ajuda a entender:

Figura 18 – Relações entre Politicas



Objectivos (o que tem de ser alcançado), Estratégias (Como se vai conseguir alcançar) e Politicas (As regras a respeitar para atingir os objectivos) podem ser definidos aos vários níveis da organização e dentro de cada departamento. Assim, explica a norma, que para se conseguir uma segurança nas TI eficaz, é necessário alinhar objectivos, estratégias e politicas para cada nível da empresa e para cada unidade de negócio. Consistência é relevante.

Por outro lado o comprometimento da gestão deve ser visível numa politica para a segurança TI negociada, formalmente aprovada e documentada.

No entender da mesma norma os elementos mínimos que devem estar presentes numa politica para as TI, na empresa, são os seguintes:

- Os requisitos de segurança nas TI, por exemplo, em termos de confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade e fiabilidade, aos olhos dos donos dos activos a proteger.
- Organização da função e atribuição de responsabilidades.
- Integração da segurança no sistema de desenvolvimento e aquisição de sistemas TI
- Directivas e procedimentos
- Definição de classes para classificação da informação
- Estratégias para a gestão do risco
- Planeamento de contingência
- Questões relacionadas com os colaboradores, com particular preocupação pelas pessoas que ocupam posições sensíveis na óptica da segurança das TI
- Consciencialização e treino
- Obrigações legais e regulamentares
- Gestão dos contratos de 'outsourcing' no quadro da segurança TI
- Tratamento de incidentes de Segurança

3.13 O que é definir os requisitos de um sistema ?

Uma pesquisa no Google permite encontrar documentos úteis para responder a esta questão.

Assim John Mylopoulos (2004), cita Ross para definir requisitos como :

' Definir os requisitos de um sistema é uma avaliação cuidadosa das necessidades que o sistema tem de satisfazer, ... deve dizer porque razão o sistema é necessário, tendo

presente as condições actuais e previsíveis no futuro, ... deve dizer que características (feactures) do sistema servirão e satisfarão o contexto a que se destina, ... e deve dizer como é que o sistema deverá ser construído'.

Esta definição pode confundir a presunção habitual que os requisitos se destinam a estabelecer o que é que (what) o sistema deve ser capaz de fazer, e não como (how) vai fazer isso, mas o próximo slide da apresentação esclarece o contexto do 'como' da definição anterior.

'Os requisitos descrevem o sistema relativamente ao seu ambiente e não ao seu funcionamento interno'.

Os requisitos constituem assim a especificação do novo sistema. Servem como contracto entre Cliente e Desenvolvedor.

Existem tipicamente dois tipos de requisitos, os funcionais e os não-funcionais. Os funcionais:

- Descrevem o processamento (i.e. as funções a serem suportadas) do novo sistema
- Descreve as entradas (inputs) que irão chegar ao novo sistema
- Descreve as saídas (outputs) que o novo sistema irá produzir
- Finalmente, descrevem os dados que o novo sistema terá de gerir.

Os não-funcionais descrevem o modo (how well) o sistema irá suportar os requisitos funcionais, e daí que sejam também designados de requisitos de qualidade. Esta descrição pode incluir:

- Critérios de desempenho
- Requisitos de fiabilidade (Reliability)
- Considerações de segurança

- Requisitos de usabilidade
- ... outros

O que recolhemos junto dos nossos diferentes interlocutores para chegar aos requisitos?

- Cenários (use cases) a partir dos quais poderemos inferir requisitos funcionais e não-funcionais
- Os cenários descrevem sequências de eventos desejadas que o novo sistema deve suportar
- Os cenários descrevem também sequencias não desejadas, que o sistema deve impedir

Como especificamos os requisitos ?

- Através de modelização (visual)
- Sem nunca esquecer que o modelo é apenas uma aproximação do mundo

Wiegers (1999), explica que um problema da indústria de software é a falta de definições comuns para os termos que são usados para descrever aspectos do trabalho que ai se faz.

Isto deve-se na opinião do autor, no que respeita ao termo 'requisitos', ao facto de existirem múltiplos níveis nos requisitos de software, todos eles legítimos, e que representam cada um perspectivas diferentes e graus distintos de detalhe e precisão.

Wiegers, cita exemplos de varias definições de requisitos, como a definição do IEEE (1997), que define requisito como;

- Uma condição ou capacidade necessária pelo utilizador para resolver um problema ou atingir um objectivo

- Uma condição ou capacidade que tem de ser satisfeita, ou possuída pelo sistema, ou componente, para satisfazer um contracto, uma norma, uma especificação ou outra qualquer formalidade imposta.

a definição de Jones (1994);

- A afirmação de necessidades dos utilizadores, que dispara o desenvolvimento de um sistema

a definição de Alan Davis (1993), que alarga a definição anterior para;

- Uma necessidade de utilizador ou uma característica particular, uma função ou atributo do sistema que pode ser sentida a partir de uma posição externa a esse sistema

diz Wiegers, que ambas as definições anteriores reforçam a componente 'o que/what' vai ser o sistema, em vez do 'como/how' vai ser desenhado ou construído.

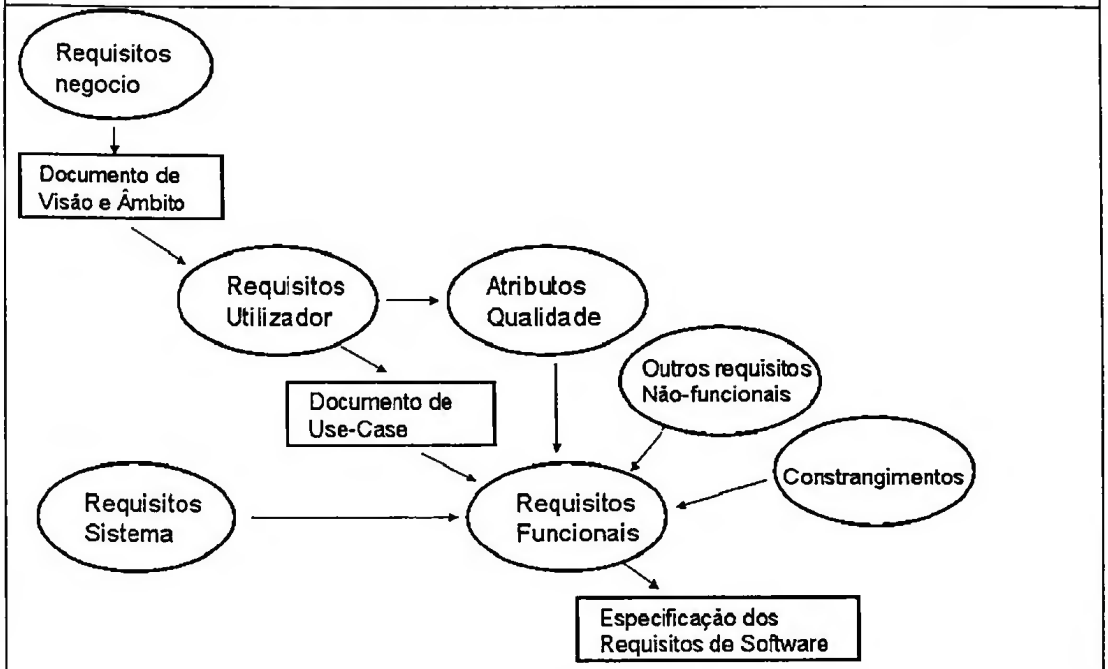
No entanto cita a definição de Sommerville e Sawyer (1997) como exemplo de uma definição que avança também para as características que o sistema deve respeitar;

- Os requisitos são ... uma especificação do que deve ser implementado. São descrições do modo como o sistema de deve comportar, ou de uma característica ou propriedade do sistema. Podem ser um constrangimento ao processo de desenvolvimento do sistema.

Lembra ainda Wiegers que qualquer forma documentada de requisitos, é simplesmente um modelo ou representação, daquilo que são os verdadeiros requisitos, que residem na cabeça das pessoas.

Wiegers, apresenta um diagrama com a sua visão dos diferentes níveis de requisitos associados a um projecto de desenvolvimento de software;

Figura 19 – Níveis de requisitos num projecto de desenvolvimento de software



Firesmith (2005), afirma que contrariamente aos requisitos funcionais, os requisitos de segurança dos sistema de informação, que se enquadram nos chamados requisitos de qualidade ou não-funcionais, tendem a não variar muito, dai que a reutilização de 'templates' de requisitos de segurança faça sentido.

A um nível de abstracção elevado todas as aplicações tendem a ter os mesmos tipos de activos vulneráveis; as suas pessoas, os seus dados, o seu hardware, as suas comunicações. Do mesmo modo os seus activos vulneráveis, tendem a ser objecto do mesmo tipo de ameaças; roubo, vandalismo, acessos não autorizados, destruição, fraude, com origem no mesmo tipo de atacantes; hackers, crackers, ladrões, empregados

descontentes, espiões industriais, os quais podem ser classificados (profiled) de acordo com as suas motivações e competências.

Embora o tipo especifico de ataque (roubo da password, leitura dos dados na rede, virus) dependa de acordo com a arquitectura de segurança objecto do ataque, a similitude de activos, ameaças, e atacantes tende a que a arquitectura dos mecanismos de segurança destinados a proteger os activos sejam semelhantes (user-id; passwords; firewall; sistemas de detecção de intrusão; anti-vírus), e os requisitos a estabelecer previamente aos mecanismos ainda mais semelhantes entre as varias aplicações.

Propõe Firesmith que as equipas de projecto estabeleçam requisitos de segurança que não imponham desde logo mecanismos de segurança específicos, ou seja que se centrem sobre o que necessitam e em que grau.

Firesmith lembra que os requisitos de segurança sendo requisitos de qualidade, devem ser expressos como um factor de qualidade, decomposto num conjunto de sub-factores:

- Identificação, é o grau como uma coisa (sistema) identifica as suas externalidades antes de interagir com elas.
- Autenticação, é o grau como algo (sistema) confirma a identificação afirmada pelas suas externalidades, antes de interagir com elas
- Autorização, é o grau como o acesso e uso de privilégios das externalidades autenticadas existe e é feito cumprir
- Imunidade, é o grau como uma coisa (sistema) se protege a si mesma, de infecções, provocadas por programas não autorizados.
- Integridade, é o grau como as comunicações ou os componentes de hardware, dados e programas, são protegidos de corrupções intencionais.

- Detecção de intrusão, é o grau como intrusões tentadas ou bem sucedidas, de pessoas ou programas, são detectadas, gravadas e notificadas
- Não-repudiação, é o grau como uma terceira parte envolvida num interacção com o sistema (mensagem, transacção), é impedida de poder mais tarde negar com sucesso ter estado envolvido nessa interacção
- Privacidade (ou confidencialidade) é o grau como dados sensíveis que passam na rede, se mantêm resguardados de acessos não autorizados de pessoas ou programas.
- Auditoria de segurança, é o grau como pessoal de segurança, tem condições para auditar o estado e uso, dos mecanismos de segurança, analisando os eventos de segurança gerados.
- Sobrevivência, é o grau como algo (sistema) continua a cumprir a sua missão prestando os seus serviços essenciais, mesmo debaixo de um ataque.
- Protecção física, é o grau como uma coisa (sistema) se protege a si mesma de assaltos físicos.

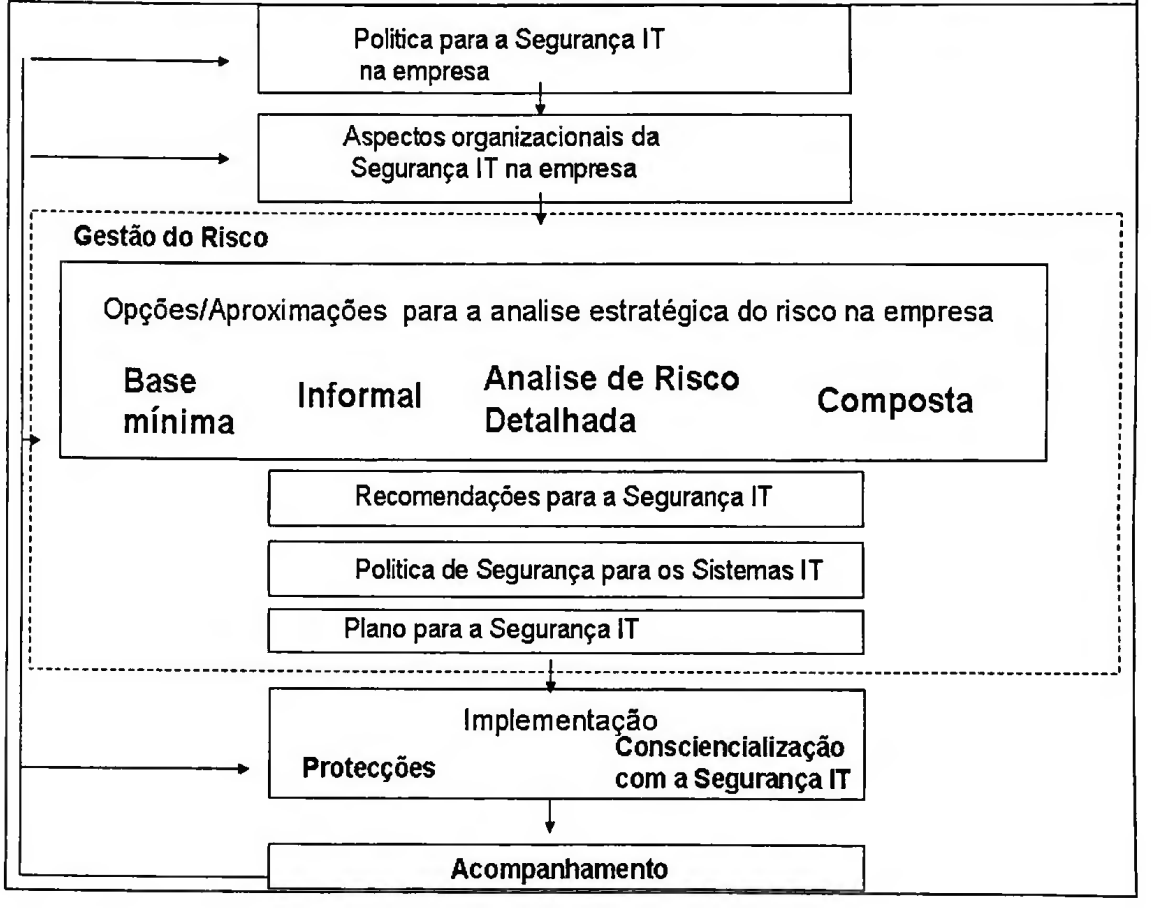
Para cada subfactor de segurança podem existir várias instanciações (designadas de 'criteria') que são descrições distintas da aplicação do mesmo sub-factor no sistema, e medidas ('measure') que medem o grau de existência do sub-factor no sistema.

Um requisito de segurança segundo Firesmith, pode assim ser definido como uma especificação da quantidade mínima do subfactor de segurança, estabelecido em termos das suas diversas descrições ('criteria') e das suas medidas.

3.14 O que é um Plano Director (ou Programa) para a Segurança dos Sistemas de Informação ?

A norma ISO/IEC TR13335-2 explica que o planeamento e gestão da segurança TI é o processo global para estabelecer e manter um programa da segurança TI na organização. Programa e Plano Director na pratica da gestão são considerados sinónimos.

Figura 20 – Processo para o planeamento e gestão da Segurança IT na empresa



O ponto de partida para este processo, é a definição dos objectivos de segurança para as TI da organização, os quais são já o resultado dos objectivos estabelecidos do negócio. De seguida deverá ser definida a estratégia e a politica da organização para a segurança das TI, organização. Parte desta politica como vimos atrás, refere-se à criação de uma estrutura organizacional que deverá assegurar os objectivos estabelecidos. A figura

inicia-se na etapa do estabelecimento da política para a segurança dos sistemas de informação.

O segundo bloco da figura respeita à gestão do risco e está dividido em quatro blocos:

- Definição da estratégia adequada face ao risco de segurança TI da organização, e tendo presente o quadro da politica acima estabelecida
- Selecção de controlos (protecções) para cada um dos sistemas TI, como resultado da análise de risco efectuada ou dos controlos mínimos que decidir aplicar
- Formulação de politicas de segurança para cada sistema TI, a partir das recomendações de controlos anteriormente produzidas, e se necessário actualização da politica corporativa.
- Construção dos planos de segurança TI necessários para a implementação dos controlos, baseados nas politicas aprovadas para cada sistema.

O terceiro bloco da figura respeita compreende a execução dos planos para implementar as protecções (controlos) seleccionados, e em paralelo sensibilizar a comunidade utilizadora, nas suas diversas categorias, para os riscos inerentes, as responsabilidades e boas praticas a respeitar.

O quarto bloco da figura respeita ao acompanhamento, ou gestão corrente do programa colocado no terreno, e inclui:

- Manutenção das protecções, de modo a assegurar a sua operação eficaz
- Verificação que assegure que as protecções estão em linha, conformidade com as politicas estabelecidas (compliance)
- Monitorizar os activos, ameaças, vulnerabilidades e protecções para detectar diferenças que possam afectar os riscos
- Tratar de incidentes que possam ocorrer assegurando uma resposta apropriada.

Lembra a norma que todas as actividades de segurança TI, são mais eficazes se ocorrerem uniformemente em toda a organização e preferencialmente no início de criação de cada sistema TI. Esta recomendação tem recentemente dado lugar a trabalho de pesquisa no sentido de uma aproximação por padrões, que permita integrar a IA, garantização da informação (Information Assurance), em todos os níveis da engenharia da empresa no que respeita aos seus SI/TI, ver Heaney et al (2002).

Esta abordagem é muito semelhante à proposta da norma BS7799-2:2002 que adiciona à sua anterior parte 1, a dimensão de um sistema de gestão da segurança SI/TI. A introdução esclarece que a norma foi preparada para oferecer aos gestores do negócio e ao seu 'staff' um modelo para iniciar e gerir um sistema de gestão para a Segurança da Informação (ISMS no acrónimo inglês) eficaz. Ou seja um propósito muito próximo do da norma anterior.

A norma refere que promove a aproximação pelos processos para estabelecer, implementar, operar, monitorar, manter e melhorar a eficácia do ISMS da empresa. Uma empresa deve identificar e gerir muitas actividades de modo a operar com eficácia. Qualquer actividade que utilize recursos e seja gerida de modo a permitir a transformação de entradas em saídas pode ser considerada um processo. A aproximação por processos numa empresa é a constatação do sistema de processos que compõem a actividade da empresa, a sua interacção e consequente gestão orientada para a finalidade da empresa.

Continua a norma afirmando que o modelo Plan-Do-Check-Act (PDCA) pode ser aplicado para todos os processos que compõem o ISMS. Assim o ISMS recebe como

entradas os requisitos e expectativas das partes interessadas na segurança dos sistemas de informação e através da execução dos processos necessários entrega às mesmas partes interessadas informação que respeita tais requisitos e expectativas.

A norma informa que sendo um sistema de gestão é compatível e está alinhada com outros sistemas de gestão, nomeadamente com os standards para a gestão da qualidade, BS EN ISO 9001:2000.

Detalhando o processo como a norma propõe o planeamento e gestão da segurança IT na empresa, ou seja o estabelecimento e gestão do ISMS:

- Estabelecer o ISMS (Planear)
    - Definir o âmbito do ISMS em termos da característica do negocio, da organização, a sua localização, activos e tecnologia
    - Definir uma politica associada ao ISMS tendo presente os mesmos termos anteriores, e que seja capaz de:
        - Incluir uma base de trabalho que estabeleça os objectivos do ISMS, um conjunto de princípios e um sentido da acção a tomar no que respeita à segurança IT.
        - Tome em consideração os requisitos do negocio e os legais e as obrigações contratuais estabelecidas no domínio da segurança
        - Estabeleça a organização estratégica e o contexto de gestão de risco nos quais o ISMS vai tomar lugar
        - Estabeleça critérios contra os quais o risco será avaliado
        - Tenha sido aprovada pela gestão da empresa
    - Definir uma aproximação sistemática à avaliação do risco
    - Identificar os riscos

- Avaliar os riscos
- Identificar e avaliar opções para o tratamento dos riscos
- Seleccionar objectivos de controlo e controlos para o tratamento dos riscos
    - Os objectivos de controlo e os controlos devem ser selecionados do anexo A da norma, o qual está alinhado inteiramente com a parte 1 da mesma norma designada de código de pratica. (Code of Pratice)
- Preparar uma declaração de aplicabilidade (Statement of Applicability)
    - Os objectivos de controlo, os controlos seleccionados e as razoes para a sua selecção devem ser documentadas na declaração de aplicabilidade. A exclusão de qualquer objectivo de controlo e controlo da lista do anexo A deve ser justificada.
- Obter aprovação da gestão para os riscos residuais e autorização para a implementação e operação do ISMS

- Executar (Do)
    - Formalizar um plano de tratamento de riscos que identifique a acção apropriada de gestão, responsabilidades e prioridades para a gestão dos riscos inerentes à segurança IT
    - Implementar o plano de tratamento dos riscos de modo a atingir os objectivos de controlo identificados
    - Implementar os controlos seleccionados de modo a atingir os objectivos de controlo
    - Implementar programas de treino e consciencialização em segurança IT
    - Gerir as operações
    - Gerir os recursos

- Implementar os procedimentos e outros controlos capazes de detectar e responder em termo oportuno a incidentes de segurança

- Monitorar e rever o ISMS (Check)
  - Executar procedimentos de monitorização e outros controlos para:
    - Detectar em tempo oportuno erros nos resultados dos processamentos
    - Identificar em tempo oportuno tentativas de intrusão e incidentes de segurança que tenham falhado ou tenham sido bem sucedidos
    - Permitir à gestão determinar se as actividades de segurança delegadas a colaboradores ou implementadas via sistemas IT estão a ser bem executadas.
    - Determinar as acções tomadas para resolver as quebras de segurança no quadro das prioridades do negocio
  - Executar revisões regulares da eficácia do ISMS (incluindo a politica, objectivos de controlo e controlos em vigor) tomando em linha de conta resultados de auditorias, incidentes, sugestões e retorno das partes interessadas
  - Rever o nível de risco residual e aceitável, tomando em conta as alterações que se vão verificando (na organização, na tecnologia, nos objectivos do negocio, nas ameaças conhecidas, no ambiente que envolve a organização, como o quadro legislativo)
  - Conduzir auditorias internas ao ISMS com periodicidades programadas
  - Executar uma revisão de gestão ao ISMS de modo regular, pelo menos uma vez por ano de modo a assegurar-se que o âmbito se mantêm valido e são identificados melhoramentos ao ISMS

- Registar acções, eventos que possam ter impacto na eficácia ou desempenho do ISMS

- Manter e melhorar o ISMS (Act)
  - Implementar os melhoramentos identificados para o ISMS
  - Tomar acções preventivas e correctivas. Aplicar as lições aprendidas nas experiências de segurança vividas noutras organizações e na própria
  - Comunicar os resultados e acções desenvolvidas às partes interessadas
  - Assegurar-se que os melhoramentos atingiram os seus propósitos

A norma detalha de seguida:

- Os requisitos documentais a respeitar, em linha com o sistema de gestão da qualidade definido na norma BS EN ISO 9001:2000 (ponto 4.3)
- a responsabilidade da gestão no ISMS, (ponto 5)
- a revisão de gestão do ISMS (ponto 6)
- Os três modos para o melhorar, de modo continuo, por acção correctiva sobre não-conformidades detectadas ou por acção preventiva que previna eventuais não-conformidades (ponto 7)
- O anexo A da norma, designado de Objectivos de Controlo e Controlos, que são obtidos directamente das clausulas 3 a 12 da norma BS ISO/IEC 17799:2000.

O ITGI-ISACA lançou muito recentemente (final de 2004) uma proposta de referencial mínimo de boas praticas, centrada na segurança dos sistemas de informação suportados em TI, partindo dos objectivos de controlo e controlos da actual versão do COBIT, a

que chamou, 'Cobit Security Baseline', e apresenta-a do mesmo modo distribuída pelos domínios do Cobit, ou seja percorrendo o ciclo tradicional de gestão já referido:

- Estabelecer Objectivos para os controlos de Segurança
  - Identificados aos longo dos domínios que a Cobit Security Baseline percorre
- Planear,
  - Domínio COBIT do planear e organizar,
- Fazer,
  - Domínio COBIT de adquirir e implementar,
  - Domínio COBIT da entrega aos utilizadores do serviço IT, e respectivo suporte.
- Comparar e corrigir
  - Domínio COBIT de monitorar e avaliar

4. O Caso de Estudo realizado

4.1 Introdução ao Caso de Estudo

Não foi fácil conseguir a autorização de uma empresa para efectuar um estudo de caso subordinado ao tema da Gestão da Segurança dos Sistemas de Informação. As empresas contactadas, reagiram de modo distinto ao pedido, o qual foi naturalmente canalizado através de pessoa conhecida. A preocupação de desvendar a um desconhecido as suas eventuais vulnerabilidades de segurança, somada do facto de recear que pudessem aparecer numa dissertação de mestrado, levaram a maioria das empresas contactadas a recusar o pedido, ainda que em momentos e etapas distintas do processo.

Houve quem nem respondesse ao pedido, quem tivesse a delicadeza de responder a recusa-lo, quem o tenha levado a Conselho de Administração e posteriormente feito chegar a recusa. Foi escrito um texto que tentou minimizar os temores de divulgação do estado da segurança da empresa que embarcasse no estudo de caso e que de seguida se apresenta:

'Exmos Srs,

Na sequência de contactos com os responsáveis pela Direcção de Informática da XPTO, venho deste modo descrever e caracterizar o estudo de caso que me proponho desenvolver, de modo a permitir à Instituição avaliar da viabilidade e interesse deste propósito.

Independentemente da vossa decisão desde já agradeço o tempo de gestão que lhes tomei e aos Srs MM e ZZ agradeço o interesse e ajuda prestadas.

Propósito do meu estudo de caso:

Comparar a norma BS7799-2 e a proposta COBIT para a elaboração de um programa para a gestão dos sistemas de informação suportados nas TI numa instituição, em termos da facilidade de dialogo com as diferentes populações da Instituição, técnica e de negocio, áreas cobertas no programa e adequação dos resultados à Instituição.

O que me proponho fazer:

Partindo de duas listas de verificação construídas a partir da proposta da norma e do referencial COBIT irei em períodos distintos entrevistar responsáveis pelo negocio da XPTO, pela Direcção Informática e outros elementos que a XPTO entenda relevantes, de modo a identificar o estado actual da segurança das TI na XPTO, o estado desejado e o programa (conjunto de projectos coordenados) necessário para o atingir.

Existirão assim dois períodos distintos, Março a Abril, Maio a Junho, nos quais deverei entrevistar as mesmas pessoas, um dedicado à norma BS7799 e outro ao referencial COBIT, de modo a permitir que as questões do inquérito anterior não estejam frescas no momento das entrevistas suportadas no segundo referencial.

Ou seja, embora em ambos os casos tenha de passar pela identificação do estado actual da XPTO no que respeita à segurança nas TI, essa constatação não terá de ser descrita no trabalho que incorpora a tese propriamente dita, uma vez que aquilo que pretendo é concluir se foi mais fácil chegar aí por um ou outro referencial.

Obviamente que no decorrer das entrevistas, das notas que aí recolher e na observação directa dos sistemas e procedimentos ficarei a conhecer tal estado o que me leva ao próximo ponto.

Privacidade da informação recolhida na XPTO, eventual reserva do nome da Instituição na tese a publicar e utilização do resultado do meu estudo.

Desde já afirmo por minha honra que manterei confidencialidade sobre o que me for dado a conhecer na XPTO no que respeita aos seus sistemas de segurança para as TI.

O Prof Palma dos Reis, responsável pelo mestrado em gestão dos sistemas de informação, questionado pelo meu orientador sobre a eventualidade do anonimato da Instituição na tese, propõe a seguinte solução de compromisso:

> *Caro Mestre José Maria Pedro,*
>
> *É compreensível a preocupação da XPTO, e o anonimato do caso não será lesivo*
> *ao candidato. Contudo, o texto da tese deverá incluir uma descrição da situação da XPTO que, não a identificando, deverá especificar de que tipo de*
> *organização se trata, o tipo de actividade, e indicadores de dimensão.*
>
> *Esta especificação genérica da XPTO (não a identificando mas descrevendo-a)*
> *deve ser validada no início do projecto com a XPTO.*
>
> *O desejo de direito de analisar e poder solicitar alterações ao documento é*
> *também normal numa organização que se disponibiliza para o desenvolvimento*
> *de um caso de estudo. Claro que envolve algum risco, pois a tese passa a*
> *depender da decisão da XPTO, mas, de uma forma geral, não têm surgido*
> *problemas com acordos dessa natureza. Deve contudo ficar especificado que a*
> *XPTO, dispondo de 15 a 30 dias para solicitar alterações à tese, assume a*
> *aprovação tácita da tese se não comentar o seu conteúdo no prazo acordado.*
>
> *Com os melhores cumprimentos,*
> *António Palma dos Reis*

Autorizo ainda a XPTO a utilizar do modo que lhe for mais conveniente os resultados do meu trabalho que contará com o meu melhor empenho no tempo disponível para o executar, sendo certo que não poderei em circunstancia alguma ser responsabilizado por qualquer inconveniente ou prejuízo que dai possa resultar para a XPTO, incluindo o facto de não poder concluir o estudo de caso, o que naturalmente desejo que não aconteça e ao contrario possa contribuir de modo positivo para a Instituição.
Fico assim a aguardar a vossa decisão que a ser positiva agradeço que seja acompanhada pela indicação do interlocutor que a XPTO designar para acompanhar o meu trabalho, facilitar internamente os contactos necessários, validar e aprovar os meus escritos e os termos em que autoriza a realização do trabalho.
Muito cordialmente,'.

A mesma argumentação foi usada para o IPQ, a quem por mão amiga fiz chegar o mesmo pedido, o qual após a compreensiva reflexão, deu o acordo à realização doa estudo do caso.

Moral da historia, duas:

- No momento actual é provável que as empresas não estejam disponíveis para participarem na investigação da segurança dos sistemas de informação.
- Quem tem amigos nos locais certos, tem habitualmente a vida mais facilitada.

4.2 O estudo do caso no IPQ

As primeiras conversas com o meu interlocutor serviram para compreender melhor a missão do IPQ, as suas principais áreas de negocio, o modo como está organizado para responder às solicitações dos seus parceiros, fornecedores, clientes e colaboradores, e

naturalmente o modo como a função SI/TI da empresa suporta e participa nos processos ao longo da famosa pirâmide de Anthony.

4.2.1 A missão e principais áreas de negocio:

'O Instituto Português da Qualidade (IPQ) é a entidade nacional responsável pela gestão, coordenação geral e desenvolvimento do Sistema Português da Qualidade (SPQ) - enquadramento legal para os assuntos da Qualidade, a nível nacional, no domínio voluntário - bem como de outros sistemas de qualificação no domínio regulamentar, que lhe sejam conferidos por lei.

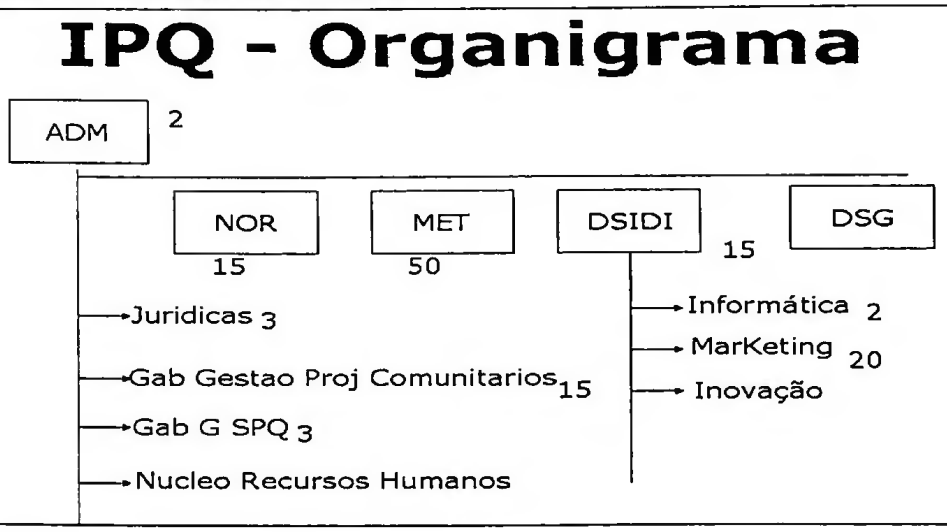
O IPQ, criado em 12 de Julho de 1986, cumpre a missão de contribuir para o desenvolvimento económico, por via do aumento da produtividade e da competitividade, através da gestão do Sistema Português da Qualidade (SPQ) nos seus três sub-sistemas: Normalização, Metrologia e Qualificação.

A Acreditação foi, entretanto, separada por imperativos comunitários, tendo sido criado o IPAC- Instituto Português de Acreditação, pelo DL nº 125/2004, de 31 de Maio, continuando no entanto o IPQ, enquanto gestor e coordenador do SPQ, a definir as políticas e estratégias do sub-sistema da Qualificação onde a Acreditação se inclui.'

A somar às suas atribuições legais, o IPQ desenvolve uma área de negócio que consiste na venda dos documentos normativos. Esta actividade está hoje em dia suportada informaticamente numa Loja Virtual de Comercio Electrónico, acessível através do site do IPQ.

4.2.2 O Organigrama simplificado do IPQ

Figura 21 – Organigrama simplificado do IPQ



Um total de cerca de 120 colaboradores

4.2.3 Inventário breve do seu sistema de informação baseado nas tecnologias de informação e avaliação qualitativa do seu impacto no negócio.

Serviços informáticos/aplicações disponíveis aos utilizadores finais

- Email
- File System para partilha de ficheiros-documentos em particular as próprias normas
- Impressão de qualidade
- Fax Server
- Acesso ao Exterior – aplicações Internet Web; FTP;
- Aplicação Patrimonial/Tesouraria/Administrativa/Pessoal
- Base Dados – Acervo Normativo
- Site do IPQ que aloja Loja Electrónica

As três últimas aplicações representam 50% dos serviços de produção informática prestados

Perdas de Produtividade por indisponibilidade dos Serviços Informáticos:

- **Comunicação com o exterior em baixo:**
  - ✓ 30-50% devidos à Normalização
  - ✓ 10% devidos à Metrologia
- **Minimal Gest (gestão Patrimonial)**
  - ✓ 80-90% da produtividade das pessoas da Gestão Financeira
- **Base Dados Acervo Normativo**
  - ✓ Loja Electrónica indisponível,
  - ✓ Baixa Produtividade na Normalização
- **Site IPQ**
  - ✓ Perda de Vendas
  - ✓ Imagem
- De facto 15mn de indisponibilidade de rede interna nota-se logo de modo 'vivo'.

4.3 O método de realização do estudo do caso

O tema de trabalho que como já foi referido pretendeu ter uma apreciação qualitativa da cobertura e eficácia do Cobit Security Baseline e da ISO 17799:2000 para o estabelecimento da lista de requisitos de um plano director para a segurança dos sistemas de informação numa organização, foi realizado ao longo de três mais três entrevistas que ocorrem no mês de Abril e Maio e Julho e Agosto.

As primeiras três entrevistas analisaram a lista de questões (checklist) proposta pela ITGI-ISACA como as questões essenciais para determinar os requisitos mínimos que a

organização tem de satisfazer para assegurar a segurança do seu sistema de informação de acordo. Este documento é designado por Cobit Security Baseline, foi traduzido para português e enviado ao meu entrevistado antes das reuniões se iniciarem. O documento traduzido que constituiu um inquérito de suporte às entrevistas, é apresentado em anexo. Após as reuniões as respostas às questões foram compiladas e entregues ao entrevistado que também tomava notas numa cópia da 'checklist'.

Passado cerca de um mês após a conclusão da lista de questões associadas à 'Cobit Security Baseline', de modo a que as questões e respostas deixassem de estar presentes na memória do entrevistado, iniciamos a nova ronda de reuniões debruçando-nos agora sobre o anexo A da norma BS7799-2, que consiste no essencial na proposta de boas praticas da norma ISO 17799. Foi construída uma lista de questões associadas aos diferentes itens que compõem os dez domínios do referido anexo/norma, a partir de uma tradução brasileira da norma ISO/IEC 17799:2000. Do mesmo modo as listas de questões foram enviadas previamente ao entrevistado, que utilizou uma copia para ir tomando notas ao longo das três reuniões. Posteriormente as respostas foram de novo coligidas e entregues ao entrevistado.

O entrevistado, responsável pelo núcleo de informática do IPQ, teve assim, como o entrevistador, oportunidade de sentir plenamente a profundidade e âmbito de cada proposta normativa para a produzir da lista de requisitos que poderiam constituir um caderno de encargos a satisfazer por uma entidade consultora, para o desenvolvimento e implementação das eventuais condições e sistemas de segurança que se verificassem necessárias e não satisfeitas pela arquitectura de segurança actual do IPQ.

No início de Setembro foi pedido ao entrevistado que respondesse ao seguinte questionário:

Passado que foi a experiência de diagnosticar o estado actual de segurança dos SI à luz dos referenciais propostos pela 'Cobit Security Baseline' e pelo ISO 17799:2000, pf responda às seguintes questões:

Qual dos referenciais entende ser mais útil para o estabelecimento dos requisitos que devem ser satisfeitos por um plano director para a segurança dos sistemas de informação na sua empresa.

- A 'baseline' de segurança proposta pelo COBIT ?
- A norma ISO 17799 ?

Pf justifique dentro do possível a sua escolha e se pretender tome como guia na sua justificação os seguintes critérios/questões.

- Áreas/domínios cobertos por cada um dos referenciais

- Detalhe escrito nos controlos que podem/devem estar presentes para que o risco residual seja considerado aceitável

- Antevisão proposta em cada um dos referenciais para os documentos politicas ou procedimentos que terão de existir na organização de modo a tornar evidente o quadro normativo pelo qual a organização gere a segurança dos seus sistemas de informação e mais tarde os audita.

- Afectação de tempo necessário para obter requisitos a incorporar no plano director para a segurança dos sistemas de informação.

- Diminuição da ambiguidade na definição dos requisitos que terão de ser satisfeitos no plano director (PDSSI).

O resultado que obteve ao confrontar o estado actual da sua organização face aos controlos aplicáveis à sua realidade, propostos por cada um dos dois referenciais, é em

seu entender suficiente para o estabelecimento da lista de requisitos que devem ser satisfeitas pelo plano director (PDSSI):

- Baseline segurança COBIT?

- ISO 17799 ?

Qual foi a percentagem de controlos que considerou não aplicáveis à sua empresa ?

- Baseline COBIT ?

- ISO 17799?

Grato pela sua colaboração.

5. Conclusões do trabalho de investigação

Dada a lógica do desenho da investigação, pretendeu-se que a vivência do processo de identificação do estado actual da função SI/TI e do 'gap' face ao proposto por qualquer um dos dois referenciais, constituísse a fonte para que o entrevistado e o próprio investigador, pudessem pronunciar-se qualitativamente sobre a melhor opção para a produção de um plano director para a segurança dos sistemas de informação, numa organização.

A reflexão do entrevistado está explicita nas respostas ao questionário que lhe foi proposto:

(Q1)
Qual dos referenciais entende ser mais útil para o estabelecimento dos requisitos que devem ser satisfeitos por um plano director para a segurança dos sistemas de informação na sua empresa.

A baseline de segurança proposta pelo COBIT ?
A norma ISO 17799: 2000 ?

(R1)
Para um plano director para a segurança considero que o referencial da Norma ISO 17799 é o mais aconselhável porque:

a) a cobertura de domínios da função SI/TI é maior, i.e, inclui um leque mais alargado de temas e assuntos (exemplos: Outsourcing e Critografia);

b) propõe uma biblioteca documental de registo de procedimentos e políticas mais dirigida a cada temática ou domínio;

c) reduz a ambiguidade (porque é mais detalhado) dos requisitos necessários à construção do plano director para a segurança.

Apesar destas vantagens, considero, no entanto, que a ISO 17799 é muito mais exigente do que o Cobit no que respeita ao tempo e recursos necessários para a recolha e manutenção da informação exigida pelos requisitos do plano director para a segurança.

(Q2)
O resultado que obteve ao confrontar o estado actual da sua organização face aos controlos aplicáveis à sua realidade, propostos por cada um dos dois referenciais, é em seu entender suficiente para o estabelecimento da lista de requisitos que devem ser satisfeitas pelo plano director (PDSSI) :

- Baseline segurança cobit ?
- ISO 17799 ?

(R2)
Qualquer dos referenciais (Cobit Security Baseline e ISO 17799) serviria para a construção
dum bom plano director para a segurança na minha organização. Contudo, se tivermos em vista a certificação da qualidade do sistema, a ISO 17799 é claramente o referencial que é obrigatório adoptar. Não tendo isto em mente, pessoalmente considero o 'Cobit Security Baseline' mais operacionalizável em qualquer organização.

(Q3)
Qual foi a percentagem de controlos que considerou não aplicáveis à sua empresa ?
- Baseline Cobit ?
- ISO 17799 ?

(R3)

Cobit Security Baseline - 0(zero)%

ISO 17799 - 8 em 62, aprox. 12%

Jacinto Ramos

A minha própria reflexão sugere algo próximo do entrevistado. De facto a norma ISO17799:2000, que é idêntica ao anexo A da norma BS7799-2, dá lugar na sua tradução directa a um questionário mais extenso, que cobre os mesmos requisitos de segurança, a diversos níveis da arquitectura dos sistemas de informação, suportados nas TIs. Assim algumas vezes temos a sensação de estar a repetir questões, porque por exemplo analisamos os mesmos requisitos para a rede de comunicação de dados, para os sistemas operativos e para as aplicações que correm nesses sistemas.

No entanto entendo esta repetição como pedagógica, dado que é possível que pela repetição, se conclua mais à frente que algo ficou por responder atrás.

Por outro lado do ponto de vista do estabelecimento das políticas, a norma ISO, sugere desde logo textos adequados à mesma, o que não acontece, pelo menos directamente na 'Cobit Security Baseline', que no entanto sugere os domínios COBIT, a partir dos quais as questões foram identificadas, dos quais é possível obter propostas de textos para as politicas relacionadas com os controlos da Baseline.

Outro aspecto relevante tem a ver com a credibilização da arquitectura de segurança a instalar, a qual pode ser reforçada pela certificação, proporcionada pela norma BS7799-2, que como foi dito inclui as boas praticas propostas pela ISO 17799. Num mundo cada vez mais virtual e global, certificados emitidos por entidades credíveis, geram credibilidade nos potenciais parceiros, por vezes mais do que a mudança interna que de facto acontece nas organizações.

E importante reter que a Cobit Security Baseline, é algo que surge recentemente a partir dum referencial voltado para o controlo e governo da função SI/TI nas organizações, enquanto a norma ISO17799 nasceu com o objectivo de propor boas praticas de segurança para os sistemas, sub-sistemas e aplicações críticas da arquitectura SI/TI das organizações, alias muito em linha com a proposta do NIST Special Publication 800-18 de Dezembro de 1998 que identifica para cada um dos três componentes referidos os controlos de gestão, técnicos e operacionais os quais são amplamente detalhados na NIST Special Publication 800-12, e evoluiu para uma proposta de sistema de gestão para a segurança dos sistemas de informação, suportados ou não nas TI.

Ou seja um nasce da síntese para o detalhe, o Cobit Security Baseline, e o outro do detalhe para a síntese, o BS7799-2, evolução da ISO 17799. E pois provável que o gestor ache mais eficaz a proposta COBOT, e um auditor a proposta ISO, esquecendo o factor certificação, apenas possível na BS7799-2.

A tabela seguinte ilustra o argumento anterior:

Tabela 7 – Comparação do nível de detalhe proposto nos referenciais em estudo

	Cobit Security Baseline	**ISO 17799**
Domínios	4 e orientados para o ciclo de gestão do sistema de segurança	10 e orientados para os tipos de controlos de gestão, técnicos e operacionais.
Objectivos chave identificados para atingir a Segurança pretendida	22	36
Controlos identificados para atingir o objectivo	39	157
Textos de apoio á verificação da implementação do controlo	Remete para o detalhe do controlo ou controlos no COBIT, ou seja não há apoio directo.	Muito extensos, e nalguns casos completos no que respeita á proposta de redacção das politicas a estabelecer

E assim provável que este primeiro referencial para a segurança dos sistemas de informação proposto pelo COBIT, seja sucessivamente enriquecido, ao longo de duas dimensões

- Cobertura mais detalhada dos diferentes domínios dos SI/TI, incorporando o texto dos controlos para os quais remete, na versão 2004, e as 'Management Guidelines', traduzidas em KGI –'Key Goals Indicators', KPI –'Key Performance Indicators', 'Critical Sucess Factors' e Maturity Models, que já hoje o COBIT apresenta
- Um mecanismo de certificação que credibilize as organizações relativamente à sua arquitectura de segurança dos sistemas de informação.

6. Bibliografia

Almeida F., (2005), Factores de sucesso no processo de adopção de CRM. Tese de Mestrado, Universidade de Lisboa - ISEG.

Amaral, Pedro (2004), O Capital Conhecimento - modelos de avaliação de activos intangíveis, Universidade Católica Editora

Bauknecht K.(2000), Lectures 2, 5 information security services ISO 7498-2, Solms & Eloff, 2000 (online) url - http://www.ifi.unizh.ch/ikm/Vorlesungen/sec/02.pdf

Beja Rui(2004), Risk Management Gestão, Relato e Auditoria dos Riscos do Negocio, Colecção Gestão, Áreas Editora, Outubro 2004

Bryman A., Bell, E. (2004), Business Research Methods, Nova York.: Oxford

BS7799-2:2002, Information security managements systems - Specification with guidance for use, British Standards

Caldeira M. (1998), Understanding the adoption and use of information systems/information technology in small and medium manufacturing enterprises: A study in Portuguese Industry, PhD Thesis, Cranfield University.

Caldeira M. (2000), Critical Realism: A philosophical perspective for case study research in social sciences, *EPISTEM*, 5-6, pp. 73-88.

Caldeira M. (2004), Slides de suporte às aulas da disciplina de 'Estratégia em contexto digital', parte académica do Mestrado em Gestão dos Sistemas de Informação no ISEG, ano lectivo de 2004-2005.

Capurro Rafael (2003), The Concept of Information, Annual Review of Information Science and Technology Ed. B. Cronin, Vol. 37 (2003) Chapter 8, pp. 343-411

Casmir Respickius(2003), 'An Approach to IT Security Education for Developing Countries', Licenciate Thesis, University of Stockholm, Junho 2003

Charlton BG, Andras P(2003). What is management and what do managers do? A system theory account, Philosophy of Management. 2003; 3: 1-15, (online) url - www.hedweb.com/bgcharlton/rip-management.html

Clifton, Bishop (2004), Assurance & Evaluation, (online) url - www.sis.pitt.edu/~jjoshi/IS2935/Fall04/Lecture10.pdf

Cobit Management Guidelines(2000), IT Governance Institute, July 2000,url - www.isaca.org

Cobit Mapping(2004), IT Governance Institute, 2004, url - www.isaca.org

Cobit Security Baseline(2004), IT Governance Institute, url - www.isaca.org

Cohen Fred (1997a), Information System Defences: A Preliminary Classification Scheme, Computers Security, 16, pags 94-114, Elsevier Science Ltd

Cohen Fred (1997b), Information System Attacks: A Preliminary Classification Scheme, Computers Security, 16, pags 29-46, Elsevier Science Ltd

Colbert Bowen (1996),A Comparison of Internal Controls: COBIT®, SAC, COSO and SAS 55/78, (online) url - http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=8174&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Crompton Malcolm (2002), Biometrics and Privacy - The End Of The World as We Know It Or The White Knight Of Privacy?, (online) url - http://biometricsinstitute.itdcorporation.net/cromptonspeech1.htm

Datapro Research Corporation(1985), Delran, NJ 08875 USA, IS15-400 Planning, Junho 1985

Dobson P. J. (2001), The Philosophy of Critical Realism – An Opportunity for Information Systems Research, Information Systems Frontiers, 3, 2, pp. 199-210.

DEPARTMENT OF DEFENSE (2003), Defense Federal Acquisition Regulation Supplement; Information Assurance, 48 CFR Parts 239 and 252

Edward et al (1995), The Essence of Information Systems, 2ª Ed, Prentice Hall

Finne Thomas(1998), Computers & Security, 17 pag 303-307, Elsevier Science Ltd, 1998

Firesmith Donald (2002), analysing and specifying reusable security requirements, (online) url - www.sei.cmu.edu/programs/acquisition-support/publications/firesmith-analyzing.pdf

Gazendam Henk, Information System Metaphors, (online), url - www.econ.uba.ar/servicios/publicaciones/journal3/contents/HGazendam/methaphors.htm

Gummesson Evert (2000), Qualitative Methods in Management Research, 2ª ed, Sage Publications

Heaney et al (2002), Information Assurance for Enterprise Engineering, The MITRE Corporation, McLean, VA (online) url - jerry.cs.uiuc.edu/~plop/plop2002/final/PLoP-2002-Heaney-7-22.pdf

Hickman James, R.(2001), Pratical IT Auditing, Warren Gorham & Lamont, 2001 Edition

Hopkinson John P.(1999), 'The relationship between the SSE-CMM and IT Security Guidance Document', EWA Canada Lda,1999,(online) url - www.sse-cmm.org

IBM(1981), A management system for the information business, Volume I – Management Overview, Julho 1981, 2ª Edição

ISO/IEC 17799:2000, information technology - code of pratice for information security management,

ISO/IEC TR-13335-1, Information Technology – Guidelines for the management of IT Security – Part 1: Concepts and Models for IT Security, 1996 Edition

ISO/IECTR-13335-2, Information Technology – Guidelines for the management of IT Security – Part 2: Managing and Planning IT Security, 1996 Edition

ISO/IECTR-13335-3, Information Technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security, 1996 Edition

ISO/IECTR-13335-4, Information Technology – Guidelines for the management of IT Security – Part 4: Selection of Safeguards, 2000 Edition

ITSM Portal(2005), (online), url - http://en.itsmportal.net/modules.php?op=modload&name=Sections&file=index&req=viewarticle&artid=64&page=1, 9-2-2005

Kruz and Vines(2001), The CISSP Prep Guide, Wiley

Mingers, J. (2004), Real-izing information systems: critical realism as an underpinning philosophy for information systems, Information and Organization, 14, pp. 87-103.

Mylopoulos (2004), Requirements analysis, (online) url - www.cs.toronto.edu/~jm/340S/Slides6/ReqA.pdf

NIST-Special Publication 800-18(1998), Guide for Developing Security Plans for Information Technology Systems, Special Publication 800-18, National Institute of Standards and Technology, Dezembro 1998, url - http://csrc.nist.gov/publications/nistpubs/index.html

NIST-Special Publication 800-33(2001), Underlying Technical Models for Information Technology Security, Special Publication 800-33, National Institute of Standards and Technology, Dezembro 2001, url - http://csrc.nist.gov/publications/nistpubs/index.html

NIST-Special Publication 800-35(2003), Guide to Information Technology Security Services, Special Publication 800-35, National Institute of Standards and Technology, Outubro 2003,url - http://csrc.nist.gov/publications/nistpubs/index.html

NIST-Special Publication 800-35 (1996), Generally Accepted Principles and Pratices for Securing Information Technology Systems, National Institute of Standards and Technology, Setembro 1996,url - http://csrc.nist.gov/publications/nistpubs/index.html

Quality Management International(2004), INC, (online), url - www.aworldofquality.com

Rivas Gomez (1989), Estruturas organizativas e informação na empresa, Editora Domingos Barreira

SEGNAC 1 (1988), Instruções para a defesa nacional, salvaguarda e defesa das matérias classificadas, Diário da Republica, série I, nº 279 de 3-12-1988

SEGNAC 2 (1988), Instruções para a defesa nacional, salvaguarda e defesa das materias classificadas, segurança industrial, tecnológica e investigação, Diário da Republica, série I, nº 245 de 24-10-1989

SEGNAC 3 (1988), Instruções para a Segurança Nacional-Segurança das Telecomunicações , Diario da Republica, I Série B, nº 68 de 23-3-1994

SEGNAC 4 (1988), Instruções para a defesa nacional, salvaguarda e defesa das materias classificadas, Diário da Republica, série I, nº 279 de 3-12-1988

Smith Mark et al (2002), Management Research - an Introduction, 2ª Ed, Sage Publications

SOLMS R, (1996), Information security management: the second generation, Computers and Security 15(4), Pag 281-288

Stoneburner Gary (2001) , Underlying Technical Models for Information Technology Security, Special Publication 800-33, National Institute of Standards and Technology,

Ward John (1995), Principles of Information Systems Management, Routledge

Wiegers Karl (1999), Software Requirements, Microsoft Press

Yin R., (1994), Case Study Research – Design and Methods, 2ª ed, Newbury Park: SAGE Publications Editions.

Anexo – O que é o Sistema Português da Qualidade (SPQ) ?

A pesquisa no site do IPQ, www.ipq.pt, ajuda muito a sintetizar os primeiros aspectos referidos.

O «Sistema Português da Qualidade (SPQ)» é a estrutura que engloba, de forma integrada, as entidades que congregam esforços para a dinamização da qualidade em Portugal e que assegura a coordenação dos três subsistemas - da normalização, da qualificação e da metrologia -, com vista ao desenvolvimento sustentado do País e ao aumento da qualidade de vida da sociedade em geral.

O IPQ é o «Órgão gestor do SPQ» - o órgão que garante o planeamento, a dinamização e a avaliação das actividades a desenvolver no âmbito do SPQ. (Decreto-Lei 140/2004 de 8 de Junho)

Em que consiste a Qualidade ?

«Qualidade» é o conjunto de atributos e características de uma entidade ou produto que determinam a sua aptidão para satisfazer necessidades e expectativas da sociedade. (Decreto-Lei nº 140/2004 de 8 de Junho)

O que é a normalização, a metrologia e qualificação ?

O Processo NP

O IPQ, como Organismo Nacional de Normalização (ONN), coordena, directamente ou com a colaboração de Organismos de Normalização Sectorial (ONS) por ele reconhecidos, a actividade normativa nacional, é da sua responsabilidade a disponibilização do Programa Anual de Normalização (PAN) o qual é preparado pelos ONS e coordenado pela Associação Portuguesa dos ONS (APONS) e a aprovação e homologação das Normas Portuguesas (NP).

De realçar que são consideradas Normas Portuguesas as **NP, NPEN, NPENISO, NPHD, NPENV, EN, ENISO, ENISO/IEC** e **ETS.**

As NP são, regra geral, elaboradas por Comissões Técnicas Portuguesas de Normalização, nas quais é assegurada a possibilidade de participação de todas as partes interessadas. Numa política de sistemática descentralização de actividades a entidades vocacionadas para o exercício respectivo, o IPQ reconhece entidades públicas, privadas ou mistas, como Organismos com funções de Normalização Sectorial em diversos domínios

O que é uma norma ?

Uma norma é um documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece regras, linhas directrizes ou características, para actividades ou seus resultados, garantindo um nível de ordem óptimo num dado contexto.

Subsistema de Qualificação

"o subsistema do SPQ que enquadra as actividades da acreditação, da certificação e outras de reconhecimento de competências e de avaliação da conformidade, no âmbito do SPQ".

Qual o organismo responsável pela Acreditação em Portugal?

Com a criação do Instituto Português de Acreditação, IP (IPAC) pelo Decreto-Lei 125/2004 de 31 de Maio, foram atribuídas a este organismo as atribuições no âmbito da acreditação ou reconhecimento da competência técnica dos agentes de avaliação da conformidade actuantes no mercado, que antes eram competência do IPQ. Assim, quaisquer informações sobre estas actividades devem ser obtidas junto do IPAC, nomeadamente através do seu sítio web: www.ipac.pt.

As actividades de Metrologia

Missão

Assegurar o rigor e a rastreabilidade das medições no território nacional, concretizando o objectivo Constitucional de soberania no domínio dos padrões de medida e do controlo dos instrumentos de medição necessários à indústria e à sociedade portuguesa em geral.

Visão

Ser um suporte da competitividade nacional e do bem estar dos cidadãos, por via de uma infra-estrutura metrológica tecnologicamente evoluída;
Ser a entidade nacional de referência na rede metrológica europeia em construção, contribuindo, assim, para a liderança da Europa no quadro da economia mundial, em linha com a Estratégia de Lisboa.

A METROLOGIA é um serviço de natureza laboratorial e regulamentar, cujas atribuições principais são:

- **Metrologia Científica**, envolvendo:
  - a realização e manutenção dos padrões nacionais;
  - participação nas comparações-chave do BIPM;
  - rastreabilidade dos padrões de referência.

- **Metrologia Legal**, abrangendo:
  - Elaboração de legislação;
  - Acompanhamento das directivas UE;
  - Coordenação do controlo metrológico;
  - Reconhecimento da qualificação de OVM;
  - Ensaios de aprovação e verificações metrológicas;
  - Formação de metrologistas;

- **Metrologia Aplicada, cujo objectivo principal é:**
  - Calibração de padrões e instrumentos de medição;
  - Organização de comparações interlaboratoriais

- Participação no sistema de acreditação nacional

Anexo – Checklist a partir da Security Baseline do Cobit

Domínio : Planear e Organizar		
Objectivo chave do controlo	**Passos mínimos necessários para implementar o controlo**	**Referencia cruzada com processos e dos seus controlos chave no COBIT**
Identificar a informação e os serviços críticos para a organização e ponderar sobre os seus requisitos de segurança	1. Partindo do impacto no negocio (refletido nos processos críticos do mesmo) identificar: o Dados que não podem ser mal usados ou perdidos o Serviços que tenham de estar disponíveis o Transações que necessitem ser confiáveis Ter em conta os seguintes requisitos de segurança: o Quem pode aceder e modificar os dados o Que retenção e backups são necessários o Que disponibilidade é necessária o Que autorização e verificação é necessária para transações electrónicas ?	P01 (Definir Plano Estratégico para o IT): 1.1 (IT como parte dos planos de longo e curto prazo da Organizaçao 1.8 (Avaliação dos actuais sistemas) P02 (Definir a arquitectura de informação): 2.2 (Corporate Data Dictionary and Data Syntax Rules) 2.3 (Esquema para a Classificação dos Dados) 2.4 (Níveis de Segurança)
Definir e comunicar as responsabilidades da Segurança no IT	2. Definir responsabilidades especificas para a gestão da segurança IT o Assegurar-se que estas estão atribuídas, comunicadas e devidamente percebidas o Ter em atenção o facto de não concentrar demasiadas atribuições numa mesma pessoa. o Fornecer os recursos necessários para o exercício dessas responsabilidades.	P04 (Definir as organização IT e as suas relações): 4.5 (Responsabilidade pela garantia da qualidade) 4.6 (Responsabilidade pela Segurança Lógica e Física) 4.9 (Supervisão) 4.10 (Segregação de Funções) 4.13 (Key IT Personnel)
Definir de modo apropriado e fazer circular os objectivos da gestão e os principais vectores de actuação no que respeita à segurança IT	3. Comunicar de modo consistente e discutir com regularidade as regras básicas para implementar os requisitos de segurança e responder a incidentes de segurança. Estabelecer os 'DO' e 'NotDo' mínimos e regularmente recordar às pessoas os riscos de segurança e as suas responsabilidades pessoais neste domínio.	P06 (Comunicar as finalidades e vectores de acção propostos pela Gestão): 6.2 (Responsabilidades da Gestão para a formulação de Politicas) 6.3 (Comunicação das Politicas) 6.6 (Respeito (compliance) com Politicas Procedimentos e Normas) 6.8 (Politica pilar (framework) para a Segurança e o de Controlo Interno) 6.9 (Direitos da Propriedade Intelectual) 6.11 (Comunicar a necessidade de consciencializar o risco da segurança.
Assegurar que as funções são executadas por técnicos conhecedores capazes de responder	4. No momento da contratação verificar referencias 5. Obter através de recrutamento ou contratação as competências necessárias para dar resposta aos requisitos de segurança da organização.	P07 (Gerir os recursos humanos): 7.1 (Recrutamento e promoção do pessoal) 7.2 (Qualificações do Pessoal)

inteiramente às exigências das funções de segurança	Avaliar anualmente o eventual gap que possa existir entre perfis e requisitos 6. Assegurar-se que nenhuma tarefa critica de segurança depende de uma única entidade.	7.7 (Avaliação do Desempenho das Funções do Pessoal)
Assegurar-se que as funções da Segurança IT respeitam as leis, regulamentos e outros requisitos externos aplicaveis	7. Identificar o que, se alguma coisa exista, que necessite ser feito com respeito a obrigações de segurança que respeitem a privacidade, direitos de propriedade intelectual, e outros requisitos de natureza legal, regulatoria, contratual ou de seguro. Motivar a equipa a compreender e ser pró-activa na resposta a estas obrigações de segurança	P08 (Garantir o respeito com os requisitos externos): 8.2 (Praticas e procedimentos para respeitar requisitos externos) 8.3 (Respeito pela segurança e ergonimia) 8.4 (Privacidade, Proriedade Intelectual e Fluxo de Dados) 8.5 (Comercio Electrónico) 8.6 (Respeito com Contratos de Seguradoras) DS12 (Gerir as Facilities): 12.4 (Segurança e Saúde do Pessoal)
Descobrir, prioritizar e conter ou aceitar os riscos de IT mais relevantes	8. Em momentos apropriados, discutir com os pessoas chaves da organização o que pode acontecer de errado com a Segurança IT que possa por em risco os objectivos do negócio. Ponderar como será melhor para proteger os serviços, dados e transacções que são críticos para o sucesso do negocio. Preparar um plano de acção para a gestão dos riscos que se foque nos riscos mais relevantes. 9. Sintetizar o entendimento da equipa para a necessidade de resposta e considerar meios que respeitar o equilíbrio de custo-eficácia para gerir os riscos de segurança identificados através de praticas de segurança (ex-Backups eficazes; controlo de acessos; protecção a vírus; firewalls) e coberturas de seguro.	P09 (avaliar Riscos): 9.1 (Avaliação do risco para os objectivos do negocio) 9.3 (Identificação do Risco) DS5 (Assegurar Segurança nos Sistemas): 5.8 (Classificação dos Dados) P09 (avaliar Riscos): 9.5 (Plano de Acção face ao Risco) AI1 (Identificar Soluções Automáticas): 1.9 (Protecções de Segurança que respeitem o equilíbrio do custo-beneficio) DS7 (Educar e Treinar Utilizadores): 7.3 (Treino na consciencialização e princípios de segurança)
Domínio : Adquirir e Implementar		
Objectivo chave do controlo	**Passos mínimos necessários para implementar o controlo**	**Referencia cruzada com processos e dos seus controlos chave no COBIT**
Considerar a segurança IT a quando do processo de procura e analise de soluções automaticas	10. Analisar de que modo as soluções automáticas podem introduzir riscos de segurança ao negocio e respectivos processos que pretendem alterar e suportar. Assegure-se que a solução é funcional e que os requisitos operacionais de segurança são especificados e são compatíveis com os	AI1 (Identificar Soluções Automáticas): 1.1 – Definição dos requisitos da informação a satisfazer pela nova solução automática

	sistemas vigentes. Obtenha conforto no que respeita à confiança da tecnologia e serviço prestado, via referencias, conselho externo, clausulas contratuais entre outras.	
Considerar a segurança a quando da aquisição e manutenção da infra-estrutura tecnológica (onde correm as aplicações)	11. Assegure-se que a tecnologia da infra-estrutura suporta de modo adequado as praticas automáticas de segurança. 12. Verifique se são necessários requisitos de segurança adicionais para a proteger a própria infra-estrutura tecnológica 13. Identifique e monitorize as fontes necessárias para manter actualizado o nível de 'patches' da sua infra-estrutura e instale-os.	AI3 (Adquira e mantenha infra-estrutura tecnológica): 3.1 – Avaliar novo hardware e software 3.2 – Manutenção preventiva para o hardware 3.3 – Segurança do software de sistema 3.4 – Instalação do software de sistema 3.5 – Manutenção do software de sistema 3.6 – Controlos na mudança do software de sistema DS8 (Assistência e Conselho aos Clientes) : 8.1 – Help-Desk PO11(Gestão da Qualidade) : 11.9 – Framework para a aquisição e manutenção de tecnologia para a infra-estrutura
Tenha em conta (consider) a segurança quando desenvolver e manter os procedimentos	14. Assegure-se que a equipa (staff) sabe como integrar a segurança nos procedimentos do dia a dia. Documente os procedimentos (actividades) e treine o Staff (A metodologia de desenvolvimento da organização deve contemplar estes outputs documentais)	AI4 (Desenvolver e manter procedimentos) : 4.2 – Manual de procedimentos para o utilizador 4.3 – Manual de Operações 4.4 – Materiais de treino DS7 (Educar e Treinar os Utilizadores) : 7.1 – Identificar necessidades de treino
Assegure-se (ensure) que todos os novos sistemas e alterações são aceites apenas após testes suficientes das funções de segurança	15. Teste o sistema ou as alterações mais significativas contra os requisitos funcionais e os procedimentos de segurança num ambiente representativo de modo a que os resultados sejam significativos. Pondere testar o modo como as funções de segurança da alteração integram com os sistemas existentes. Não teste em produção. 16. Realize a aceitação final da segurança após validar todos os resultados dos testes tendo presente os objectivos de negócio e requisitos de segurança envolvendo nesta avaliação a equipa que vai usar, correr e manter os sistemas	AI5 (Instalar e Aceitar (accredit) sistemas) 5.7 – Testar as alterações 5.11 – Teste operacional 5.12 – Passagem a produção AI5 (Instalar e Aceitar (accredit) sistemas) 5.9 – Teste final de aceitação 5.13 – Avaliação de respeito pelos requisitos dos utilizadores após entrada em produção 5.14 – Revisão de gestão após entrada em produção.

Assegure-se que todas as alterações, incluindo 'patches' suportam os objectivos da organização e são levadas a cabo de modo seguro. Assegure-se que os processos diários do negocio não sofrem com as alterações.	17. Avalie todas as alterações, incluindo os 'patches' para estabelecer o seu impacto na integridade, exposição ou perca de dados sensíveis, disponibilidade de serviços críticos e validade de transações importantes. Baseado neste impacto, realize testes adequados antes de activar a mudança. 18. Registe e autorize todas as alterações, incluindo os 'patches' As alterações de emergência devem ser também registadas mesmo que só apos a sua realização	AI5 (Instalar e Aceitar (accredit) sistemas) 5.7 – Testar as alterações AI6 (Gestão das Alterações) 6.4 – Alterações de emergencia
Domínio : Entrega e Suporte		
Objectivo chave do controlo	**Passos mínimos necessários para implementar o controlo**	**Referencia cruzada com processos e dos seus controlos chave no COBIT**
Defina e gira os aspectos de segurança dos níveis de serviço	19. Assegure-se que a gestão estabelece os requisitos de segurança e regularmente revê o respeito pelos acordos internos de nível de serviço e as obrigações contratuais com fornecedores de serviços IT externos	DS1 (Definir e gerir níveis de serviço) 1.2 – Aspectos dos acordos de níveis de serviço 1.5 – Revisão dos acordos de níveis de serviços e contratos com terceiros para os respeitar DS2 (Gestão de Serviços com Terceiros) 2.3 – Contratos com Terceiros 2.8 – Monitorização do desempenho dos Terceiros AI4 (Desenvolvimento e manutenção de procedimentos) : 4.1 – Requisitos operacionais e níveis de serviço
Gerir os aspectos de segurança dos serviços prestados por terceiros	20. Avalie a capacidade profissional das terceiras partes e assegure-se que eles fornecem contactos adequados com a autoridade para actuar de acordo com os requisitos de segurança da organização e as suas preocupações 21. Tenha em conta e contrarie a dependência dos fornecedores terceiros para os requisitos de segurança e mitigação dos riscos de continuidade, confidencialidade e direitos de propriedade intelectual, via por exemplo escrow contrats, responsabilidades legais, penalidades e recompensas	DS2 (Gestão de Serviços com Terceiros) 2.4 – Qualificações dos Fornecedores Terceiros 2.5 – Contratos de Outsourcing DS2 (Gestão de Serviços com Terceiros) 2.6 – Continuidade de Serviços 2.7 – Segurança no Relacionamento
Assegure-se que a organização é capaz de executar diariamente as suas actividades automáticas de suporte aos processos de negocio, com interrupções mínimas devidas a incidentes de segurança	22. Identifique as funções e informações criticas para o negocio e os recursos IT (aplicações; serviços prestados por terceiros; fornecedores e ficheiros) críticos para as suportar. Providencie para que estejam disponíveis no evento de um incidente de segurança de modo a manter a continuidade do serviço. Assegure-se que incidentes significativos de segurança são identificados e resolvidos em tempo. 23. Estabeleça princípios básicos para a protecção e recuperação dos serviços IT, incluindo procedimentos alternativos de processamento, como obter consumíveis e serviços numa emergência, como retornar ao processamento normal apos o incidente, e como comunicar com os clientes	DS4 (Assegurar serviço continuo) 4.2 – Estratégia e filosofia para o plano de continuidade IT 4.4 – Minimizar os requisitos para a continuidade IT 4.10 – Recursos IT criticos DS10 (Gerir problemas e incidentes) 10.1 – Sistema de gestão de problemas) 10.2 – Escalamento dos Problemas DS12 (Gestão das Facilities) 12.6- Fornecimento ininterrupto de energia electrica

	e fornecedores. 24. Em conjunto com os empregados chave, definir o que necessita ser backup up e guardado exteriormente para permitir a recuperação do negocio (ficheiros críticos; documentação e outros recursos IT) e proteja-os adequadamente. Regularmente assegure-se que os recursos salvaguardados são utilizáveis e completos.	DS4 (Assegurar serviço continuo) 4.3 – Conteúdo do plano de continuidade IT 4.9 – Processamento alternativo dos departamentos utilizadores, como salvaguarda à indisponibilidade dos serviços IT habituais DS4 (Assegurar serviço continuo) 4.6 – Teste do plano de continuidade IT 4.12 – Sitio exterior para salvaguarda de memoria DS11 (Gestão dos Dados) 11.23 – Recuperação r Salvaguarda dos Dados 11.24 – Jobs de Salvaguarda 11.25 – Salvaguarda da Memoria (Dados Programas Documentação)
Assegure-se que todos os aspectos do processamento automático da organização é utilizado apenas pessoas e sistemas autorizados para finalidades próprias do negocio.	25. Implemente regras para controlar o acesso aos serviços baseadas na necessidade do utilizador em ver, adicionar, alterar ou apagar a informação ou as transações. Tenha especial cuidado nos acessos que dá a fornecedores, prestadores de serviços e clientes. 26. Assegure-se que a responsabilidade para a gestão de todas as contas dos utilizadores e 'tokens' (passwords; cartões; dispositivos de segurança está bem definida. Periodicamente reveja e confirme os procedimentos e autoridade para a gestão destas contas e tokens. Assegure-se que não são geridos pela mesma pessoa. 27. Registe (log) violações importantes à segurança (acessos aos sistemas e redes, vírus, utilizações indevidas e software ilegal). Assegure-se que que são relatados imediatamente e existe actuação subsequente em tempo. 28. Para se assegurar que os parceiros de negocio são confiáveis e as transações são autenticas quando se utilizam sistemas electrónicos para as mesmas, verifique se as instruções de segurança são adequadas e respeitam as obrigações legais. 29. Force a utilização de software para a protecção de vírus em toda a infra-estrutura tecnológica da organização e mantenha o software anti-virus actualizado. Não use software ilegal. 30. Defina uma politica para a informação que pode entrar e sair da organização e configure os sistemas para segurança na rede (firewalls) de modo conforme. Pondere como proteger os meios de memoria fisicamente transportáveis. Monitorize as excepções e acompanhe os incidentes significativos	DS5 (Assegure a segurança dos sistemas que compõem a infra-estrutura tecnológica)) 5.3 – Segurança no acesso em l,inha aos dados 5.4 – Gestão das contas dos utilizadores DS5 5.4 - Gestão das contas dos utilizadores 5.5 – Revisão de gestão das contas dos utilizadores 5.21 – Protecção dos valores electrónicos utilizados para autenticação; execução de transações … DS5 5.7 – Vigilância de Segurança 5.11 – Tratamento de incidentes DS5 5.13 – Confiar nos parceiros de negocio 5.14 – Autorização das Transações electronicas DS5 5.19 – Prevenção detecção e correcção do software malicioso 5.20 – Arquitecturas de firewall e conexões a redes publicas DS9 (Gerir a configuração) 9.5 – Software não autorizado
Assegure-se que todos os activos	31. Assegure-se que existe um inventario regularmente actualizado do	DS9 (Gerir a configuração) :

são seguros de modo apropriado e os riscos de segurança minimizados através da consciencialização dos activos IT existentes e respectivas licenças	hardware e software da configuração 32. Regularmente reveja se todo o software está autorizado e devidamente licenciado.	9.1 – Registar a configuração 9.3 – Responsabilização pelo Estado do Inventario incluindo o histórico de cada item 9.4 – Controlo da Configuração 9.8 – Responsabilização pelo Software e Gestão de Librarias DS9 (Gerir a configuração) : 9.5 – Software não autorizado 9.8 - Responsabilização pelo Software e Gestão de Librarias
Assegure-se que todos os dados permanecem completos, fiáveis e validos durante a sua entrada, memorização e processamento e distribuição	33. Sujeite os dados a um conjunto de controlos que se assegure da sua integridade (rigor, complitude e validade) durante a sua entrada, processamento, memorização e distribuição. Controle as transações para se assegurar a sua autenticidade e que não podem ser repudiadas. 34. Distribua os 'outputs' sensíveis apenas para pessoas autorizadas 35. Defina períodos de retenção, requisitos a respeitar nos arquivos, termos para as entradas e saídas de documentos, de dados e software. Assegure-se que eles são conformes com os requisitos legais e do utilizador. Enquanto em memoria verifique continuamente a sua integridade e assegure-se que os dados não podem ser recolhidos. DS11 (Gestão dos dados) : 11.5 – Retenção dos documentos fonte (de dados) de acordo com requisitos de recuperação e legais 11.18 – Protecção de dados sensíveis que passaram à situação de não-utilizaveis (disposal) 11.19 – Gestão da memoria auxiliar (custo; requisitos de acesso; segurança) 11.20 – Períodos de retenção e termos de memorização para dados; programas; documentação; outputs; mensagens e chaves de autenticação e encriptação 11.26 – Arquivo – Politica para estabelecer responsabilidade, termos e meios que respondam a requisitos legais e de negocio.	DS11 (Gestão dos dados) : 11.3 – Recolha de documentos fonte de dados 11.4 – Tratamento de erros de dados dos documentos fonte 11.7 – Dados que originam transações devem ser verificados quanto à autorização, rigor e complitude 11.8 – Tratamento de erros no input dos dados 11.9 – Integridade no processamento dos dados 11.10 - Responsabilização pelo Software e Gestão de Librarias 11.11 – Validação e alteração (edição) dos dados a processar tão próximo qto possível da sua origem 11.14 – Balanceamento de totais nos outputs e reconciliação com os registos de trail 11.15 – Verificação dos outputs e eventual correcção 11.27 – Protecção das mensagens sensiveis 11.29 – Integridade das transações electrónicas (atomicidade da unidade de trabalho; consistência; isolamento e durabilidade) DS11 (Gestão dos dados) : 11.12 – Tratamernto e retenção dos outputs IT 11.13 – Distribuição dos outputs 11.14 - Balanceamento de totais nos outputs e reconciliação com os registos de trail 11.15 - Verificação dos outputs e eventual correcção 11.16 – Fornecimento seguro dos relatórios aos utilizadores que deles necessitam
Proteja todos os equipamentos IT de dano (damage)	36. Proteja fisicamente os activos e 'facilities' IT, especialmente os mais expostos a ameaças e se aplicável obtenha conselhos de peritos. 37. Proteja fisicamente os equipamentos de computador, incluindo os dispositivos de memoria e os moveis de dano, roubo ou perda acidental	DS12 (Gerir as Facilities) 12.1 – Protecção Fisica 12.5 – Protecção contra factores ambientais (fogo; poeira, agua; calor; humidade …) 12.6 – Fornecimento continuo de energia eléctrica.
Domínio 7 : Monitorar e Avaliar		
Objectivo chave do controlo	**Passos mínimos necessários para implementar o controlo**	**Referencia cruzada com processos e dos seus controlos**

		chave no COBIT
Monitorizar regularmente o desempenho da segurança da informação	38. Instrua a equipa a periodicamente: o Avaliar a adequação dos controlos (protecções) em função dos requisitos definidos à luz das vulnerabilidades do momento o Reavalie que excepções á segurança devem ser acompanhadas numa base diária o Avalie o desempenho dos mecanismos de segurança e verifique se existem fraquezas na detecção de intrusões, penetração, teste de stress e teste de planos de contingência o Assegure-se que as excepções são de imediato tratadas o Monitorize a conformidade com os controlos chave	M1 (Monitorização dos Processos) : 1.2 – Avaliar Desempenho via Key Performance Indicators e Critical Sucess Factors 1.3 – Avaliar a satisfação do cliente 1.4 – Relatórios para a Gestão M2 (Avaliar a adequação do controlo Interno) 2.1 – Monitorização do Controlo Interno
Ganhar confiança e acreditar na segurança através de fontes independentes capazes e reconhecidas	39. Obter quando necessário recursos externos competentes para rever os mecanismos de controlo da segurança da informação; Avaliar conformidade com leis, regulamentos e obrigações contratuais relativas à segurança IT. Aproveitar esta competência externa (conhecimento e experiência) para elevar a competência interna	M3 (Obter garantia independente) 3.3 – Avaliação independente da eficácia dos serviços IT 3.4 - Avaliação independente da eficácia dos serviços IT prestados por terceiros 3.5 - Obter garantia independente da conformidade com leis, regulamentos e obrigações contratuais 3.6 - Obter garantia independente da conformidade com leis, regulamentos e obrigações contratuais nos serviços IT prestados por terceiros 3.7 – Competência da entidade externa que executa a validação

Anexo - Checklist a partir da ISO 17799

Domínio : 3 **Política de segurança**		
Objectivo	**Controlo**	**Detalhe do Controlo**
Fornecer direcção e apoio de gestão para a segurança de informações.	**3. Política de segurança de informações** A gerência deve estabelecer uma direção política clara e demonstrar suporte a, e comprometimento com, a segurança das informações através da emissão e manutenção de uma política de segurança de informações para toda a organização	*3.1.1 Documento da política de segurança de informações –* *3.1.2 Revisão e avaliação* A política deve ter um encarregado que seja responsável por sua manutenção e revisão de acordo com um processo de revisão definido
Domínio : 4 **Segurança organizacional**		
Gerenciar a segurança das informações dentro da organização.	**4.1 Infra-estrutura para segurança de informações** Deve ser estabelecida uma estrutura gerencial para iniciar e controlar a implementação da segurança de informações dentro da organização. Foros gerenciais adequados com liderança da administração devem ser estabelecidos para aprovar a política de segurança de informações, atribuir papéis de segurança e coordenar a implementação da segurança em toda a organização. Se necessário, um canal de aconselhamento especializado em segurança de informações deve ser estabelecido e disponibilizado dentro da organização. Contatos com especialistas em segurança externos devem ser desenvolvidos para acompanhar as tendências da indústria, monitorar padrões e métodos de avaliação e prover pontos de contato adequados para quando se lidar com incidentes de segurança. Um enfoque multidisciplinar quanto à segurança de informações deve ser encorajado; por exemplo, envolvendo a cooperação e colaboração de gerentes, usuários, administradores, projetistas de aplicações, auditores e equipe de segurança e especialistas em áreas tais como seguro e gestão de riscos.	*4.1.1 Fórum gerencial de segurança de informações –* Segurança de informações é uma responsabilidade corporativa compartilhada por todos os membros da equipe gerencial *4.1.2 Coordenação da segurança de informações* Em uma organização de grande porte, pode ser necessário um fórum interfuncional de representantes das gerências de setores relevantes da organização para coordenar a implementação de controles de segurança de informação. *4.1.3 Alocação de responsabilidades pela segurança das informações* As responsabilidades pela proteção de ativos individuais e pela condução de processos de segurança específicos devem ser claramente definidas. *4.1.4 Processo de autorização para facilidades de processamento de informações* Um processo gerencial de autorização para novas facilidades de processamento de informações deve ser implantado.

		4.1.5 Aconselhamento especializado sobre segurança de informações É muito provável que um aconselhamento especializado sobre segurança de informações seja necessário em muitas organizações. Idealmente, um consultor interno experiente em segurança de informações poderia prover isto. ***4.1.6 Cooperação entre organizações*** Contatos apropriados com autoridades policiais, órgãos regulamentadores, provedores de serviços de informação e operadoras de telecomunicações devem ser mantidos para garantir que a ação apropriada seja tomada rapidamente, e obtido aconselhamento, na eventualidade de um incidente de segurança. Similarmente, deve ser considerada a afiliação a grupos de segurança e fóruns da indústria. ***4.1.7 Revisão independente da segurança das informações*** O documento sobre a política de segurança de informações (ver 3.1) estabelece a política e as responsabilidades pela segurança das informações. **Sua implementação** deve ser revisada de forma independente para fornecer garantia de que as práticas da organização refletem adequadamente a política, e que ela é viável e eficaz (ver 12.2).
Manter a segurança das facilidades de processamento de informações organizacionais e ativos de informação acessados por terceiros.	**4.2 Segurança para o acesso de terceiros** O acesso por terceiros às facilidades de processamento de informações da organização deve ser controlado. Onde houver uma necessidade do negócio para tal acesso de terceiros, deve ser efetuada uma avaliação de riscos para determinar as implicações de segurança e as exigências de controle. Os controles devem ser acordados e definidos em um contrato com a terceira parte. O acesso de terceiros também pode envolver outros participantes. Contratos que permitem o acesso de terceiros devem incluir permissão para designação de outros participantes elegíveis e as condições para o acesso	***4.2.1 Identificação dos riscos no acesso de terceiros*** **4.2.1.1** *Tipos de acesso* a) acesso físico; por exemplo, a escritórios, salas de computadores, arquivos; b) acesso lógico; por exemplo, aos bancos de dados e sistemas de informação da organização. **4.2.1.2** *Razões para o acesso*

	deles.	**4.2.1.3** *Terceiros on-site (estudantes; consultores; limpeza) – estabelecer controlos.* ***4.2.2 Requisitos de segurança para contratos com terceiros*** Os arranjos que envolvem o acesso de terceiras partes às facilidades de processamento de informações da organização devem ser baseados em um contrato formal contendo, ou referenciando, todos os requisitos de segurança para garantir a obediência às políticas e padrões de segurança da organização.
Manter a segurança das informações quando a responsabilidade pelo processamento das informações tiver sido terceirizada com outra organização.	**4.3** ***Outsourcing*** Os acordos de terceirização *(outsourcing)* devem tratar dos riscos, controles de segurança e procedimentos para sistemas de informações, ambientes de rede e/ou *desktop* no contrato entre as partes.	***4.3.1 Requisitos de segurança em contratos de outsourcing –*** Por exemplo, o contrato deve mencionar: a) como as exigências legais serão satisfeitas; por exemplo, a legislação quanto à proteção de dados; b) como a integridade e a confidencialidade dos ativos de informação da organização devem ser mantidos e testados; c) como a disponibilidade dos serviços deve ser mantida na eventualidade de um desastre; d) o direito de auditoria. ...

Domínio : **5** **Classificação e controle dos ativos**

Manter proteção apropriada para os ativos organizacionais.	**5.1 Responsabilidade pelos ativos** Todos os ativos de informação mais importantes devem ter um proprietário nominal, responsável por eles.	***5.1.1 Inventário dos ativos –*** Um inventário dos ativos ajuda a assegurar que ocorra uma proteção efetiva dos ativos, e também pode ser exigido para outros fins do negócio, tais como razões de salubridade e segurança, seguros ou razões financeiras (gestão de ativos).

	A responsabilidade pelos ativos ajuda a assegurar que seja mantida uma proteção adequada. Os proprietários devem ser identificados para todos os ativos importantes e a responsabilidade pela manutenção dos controles apropriados deve ser atribuída. A responsabilidade pela implementação dos controles pode ser delegada. A responsabili-dade final deve permanecer com o proprietário designado do ativo.	Exemplos de ativos associados com sistemas de informação são: a) ativos de informação: bancos de dados e arquivos de dados, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos operacionais ou de suporte, planos de continuidade, arranjos de *fallback*[1], informações em *archives*[2]; b) ativos de software: software aplicativo, software básico, ferramentas de desenvolvimento e utilitários; c) ativos físicos: equipamento de computador (processadores, monitores, laptops, modems), equipamentos de comunicação (roteadores, PABXs, aparelhos de fax, secretárias eletrônicas), mídia magnética (fitas e discos), outros equipamentos técnicos (geradores de energia, unidades de condicionamento de ar), móveis, acomodações; d) serviços: serviços de informática e telecomunicações, serviços públicos em geral (aquecimento, iluminação, energia, ar-condicionado).
Garantir que os ativos de informação recebam um nível de proteção adequado.	**5.2 Classificação[3] das informações** As informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de proteção. As informações apresentam graus variáveis de suscetibilidade e criticalidade. Alguns itens podem exigir um nível adicional de proteção ou tratamento especial. Um sistema de classificação das informações deve ser usado para definir um conjunto apropriado de níveis de proteção e comunicar a necessidade de medidas de tratamento especiais.	*5.2.1. Diretrizes para a classificação –* As classificações e controles associados de proteção para as informações devem considerar as necessidades do negócio quanto ao compartilhamento ou restrição das informações, e os impactos para o negócio associados com tais necessidades, por exemplo acesso não autorizado ou danos às informações. ***5.2.2 Rotulagem e manuseio de informações***

[1] N.T.: *Fallback*: o que pode ser usado quando falhar o suprimento, método ou atividade normal.
[2] N.T.: *Archive*: um conjunto de arquivos de computador compactados juntos para fins de *backup*, para serem transportados para outro local, para economizar espaço em disco ou por algum outro motivo. Um *archive* pode incluir uma simples lista de arquivos ou arquivos organizados sob uma estrutura de diretório ou catálogo.
[3] N.T.: A palavra inglesa *classification*, no contexto deste documento, significa "atribuição de grau de confidencialidade". A tradução usada, classificação, deve ser entendida da mesma forma.

		É importante que um conjunto apropriado de procedimentos seja definido para rotulagem e manuseio das informações de acordo com o esquema de classificação adotado pela organização. Esses procedimentos precisam cobrir os ativos de informação nos formatos físicos e eletrônicos. Para cada classificação, os procedimentos de manuseio devem ser definidos para cobrir os seguintes tipos de atividades de processamento de informação: a) cópia; b) armazenamento; c) transmissão pelo correio, fax e correio eletrônico; d) transmissão verbal, incluindo telefone celular, correio de voz, secretárias eletrônicas; e) destruição. As saídas geradas pelos sistemas que contêm informações classificadas como sensíveis ou críticas devem portar um rótulo de classificação apropriado (na saída).

Domínio : 6 **Segurança relacionada ao pessoal**		
Reduzir os riscos de erros humanos, roubos, fraudes ou uso indevido das facilidades.	**6.1 Segurança na definição de funções e alocação de pessoal** As responsabilidades de segurança devem ser tratadas no estágio de recrutamento, incluídas em contratos e monitoradas durante o tempo que o indivíduo estiver no emprego. Os candidatos em potencial devem ser adequadamente selecionados (ver 6.1.2), especialmente para funções sensíveis. Todos os empregados e usuários terceirizados das facilidades de processamento de informações devem assinar um contrato de confidencialidade (não divulgação).	***6.1.1 Incluindo a segurança nas responsabilidades dos serviços*** Os papéis de segurança e as responsabilidades, conforme delineados n política de segurança de informações da organização (ver 3.1), devem ser documentados onde for apropriado. ***6.1.2 Seleção e política de pessoal*** Para os empregados permanentes, no momento das propostas de emprego, devem ser efetuadas verificações de confirmação. ***6.1.3 Contratos de confidencialidade*** Contratos de confidencialidade ou não-divulgação são usados par avisar que informações são confidenciais ou secretas. Os empregado devem normalmente assinar tal contrato como parte de seus termos condições iniciais de emprego. ***6.1.4 Termos e condições de emprego*** Os termos e condições de emprego devem declarar a responsabilidad do empregado pela segurança das informações. Onde apropriado, essa responsabilidades devem continuar por um período definido após término do vínculo de emprego. Deve ser incluída a ação a se executada se o empregado desrespeitar as exigências de segurança.
Assegurar que os usuários se conscientizem das preocupações e ameaças à segurança das informações, e estejam equipados para apoiar a política de segurança organizacional no curso de seu trabalho normal.	**6.2 Treinamento dos usuários** Os usuários devem ser treinados nos procedimentos de segurança e no uso correto das facilidades de processamento de informações para minimizar os possíveis riscos de segurança.	***6.2.1 Educação e treinamento sobre segurança de informações*** Todos os empregados da organização e, onde for relevante, usuários terceirizados, devem receber treinamento apropriado e atualizações periódicas sobre as políticas e procedimentos organizacionais. Isto inclui as exigências de segurança, as responsabilidades legais controles corporativos, bem como treinamento no uso correto da facilidades de processamento de informações, por exemplo procedimento de *logon*, uso de pacotes de software, antes de serem autorizados a acessar informações ou serviços.

Minimizar os danos resultantes de incidentes de segurança e mal funcionamentos, e monitorar e aprender com tais incidentes.	**6.3 Respondendo a incidentes de segurança e mal funcionamentos** Incidentes que afetam a segurança devem ser reportados através de canais administrativos apropriados o mais rapidamente possível. Todos os empregados e contratados devem estar cientes dos procedimentos para reportar os diferentes tipos de incidente (quebra de segurança, ameaça, fraqueza ou mal funcionamento) que possam ter impacto na segurança dos ativos organizacionais. Deve ser exigido que eles reportem quaisquer incidentes observados ou suspeitados o mais rapidamente possível para o ponto de contato designado. A organização deve estabelecer um processo disciplinar formal para lidar com empregados que cometam quebras de segurança. Para que se seja capaz de tratar os incidentes adequadamente, pode ser necessário colher provas o mais cedo possível após a ocorrência (ver 12.1.7).	***6.3.1 Reportando incidentes de segurança*** Os incidentes de segurança devem ser reportados através dos canai administrativos adequados o mais rapidamente possível. Um procedimento formal para relatar os incidentes deve ser estabelecido, juntamente com um procedimento de resposta ao incidente, estabelecendo a ação a ser executada no recebimento de um relatório de incidente ***6.3.2 Reportando pontos fracos na segurança*** Os usuários de serviços de informações devem ser obrigados a anotar reportar quaisquer pontos fracos observados ou suspeitados, ou ameaças, aos sistemas e serviços. ***6.3.3 Reportando mal funcionamento de softwares*** Devem ser estabelecidos procedimentos para reportar mal funcionamento de softwares (mensagens de vírus pex) ***6.3.4 Aprendendo com os incidentes*** Devem existir mecanismos para capacitar a quantificação e o monitoramento dos tipos, volumes e custos dos incidentes e mal funcionamentos. Essas informações devem ser usadas para identificar incidentes ou mal funcionamentos recorrentes ou de alto impacto. ***6.3.5 Processo disciplinar*** Deve existir um processo disciplinar formal para empregados qu tenham violado as políticas e procedimentos de seguranç organizacionais (ver 6.1.4 e, para retenção de provas, ver 12.1.7). T processo pode atuar como um meio de intimidação para empregad que poderiam de outra forma se inclinar a desrespeitar procedimentos de segurança. Adicionalmente, ele deve tambér assegurar um tratamento justo e correto para os empregados que seja suspeitos de cometer quebras de segurança severas ou persistentes.

Domínio : 7	**Segurança física e ambiental**

Objectivo	Detalhe do Controlo
7.1. Áreas de segurança Obj: Impedir acesso não autorizado, danos ou interferência às instalações físicas e às informações da organização. Controlo: As facilidades de processamento de informações sensíveis ou críticas para o negócio devem ser localizadas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controles de entrada. Elas devem ser fisicamente protegidas contra acesso não autorizado, danos e interferências. A protecção fornecida deve ser compatível com os riscos identificados. Uma política de "mesas limpas" e "ecrãs limpos" é recomendada para reduzir o risco de acesso não autorizado ou danos a papéis, media e facilidades de processamento de informações.	*7.1.1 Perímetro de segurança física* As diretrizes e controles seguintes devem ser considerados e implementados onde apropriado: a) O perímetro de segurança deve ser claramente definido. b) O perímetro de um edifício ou *site* que contenha facilidades de processamento de informações deve ser fisicamente seguro (isto é, não deve haver brechas no perímetro ou áreas onde uma entrada forçada possa ocorrer com facilidade). As paredes externas do *site* devem ser de construção sólida e todas as portas externas devem ser adequadamente protegidas contra acesso não autorizado, com mecanismos de controle, barras, alarmes, trancas, etc. c) Deve existir uma área de recepção com atendentes ou outros meios de controlar o acesso físico ao *site* ou ao edifício. O acesso aos *sites* ou edifícios deve ser restrito apenas ao pessoal autorizado. d) As barreiras físicas devem, se necessário, ser estendidas do piso real ao tecto real para impedir entrada não autorizada e contaminação ambiental, tais como as causadas por incêndio ou inundação. e) Todas as portas corta-fogo em um perímetro de segurança devem ter alarmes e devem fechar fazendo barulho. *7.1.2 Controles para entrada física de pessoas e materiais* Os seguintes controles devem ser considerados: Visitantes nas áreas de segurança devem ser supervisionados ou conduzidos pela segurança e as datas e horários de sua entrada e saída devem ser registrados ... *7.1.3 Segurança nos escritórios, salas e instalações* Os seguintes controles devem ser considerados: a) As instalações principais devem ser situadas de modo a evitar o acesso pelo público. b) Os edifícios devem ser discretos e dar a menor indicação possível de sua finalidade, sem sinais óbvios, internos e externos, que identifiquem a presença de atividades de processamento de informações. *7.1.4 Trabalhando em áreas de segurança* Controles e diretrizes adicionais podem ser necessários para aumentar a segurança de uma área de segurança. Isso inclui controles para os funcionários ou terceiros que trabalham na área de segurança, bem como atividades terceirizadas que sejam executadas lá (limpeza; Electricidade) *7.1.5 Áreas isoladas de carga e descarga*

	a) O acesso a uma área de depósito a partir do exterior do prédio deve ser restrito a pessoal identificado e autorizado. b) A área de depósito deve ser planejada de forma que os suprimentos possam ser descarregados sem que os entregadores ganhem acesso a outras partes do edifício. c) As portas externas de uma área de depósito devem ser vigiadas quando a porta interna for aberta. d) Os materiais recebidos devem ser inspecionados quanto a possíveis perigos [ver 7.2.1d)] antes de serem transferidos do depósito para o local de uso. e) Os materiais recebidos devem ser registrados, se for o caso (ver 5.1), ao darem entrada no *site*.

7.2 Segurança dos equipamentos

Obj:

Impedir perda, danos ou comprometimento de ativos e interrupção das atividades do negócio.

Controlo:

Os equipamentos devem ser fisicamente protegidos contra ameaças à segurança e perigos ambientais. A proteção dos equipamentos (incluindo aqueles usados *off-site*) é necessária para reduzir o risco de acesso não autorizado aos dados e para proteger contra perda ou danos. Deve-se também considerar a localização dos equipamentos e sua disposição física. Controles especiais podem ser necessários para proteger contra perigos ou acesso não autorizado, e para salvaguardar instalações de apoio, tais como fornecimento de electricidade e infra-estrutura de cabelagem.

7.2.1 Disposição física dos equipamentos e protecção

Os seguintes controles devem ser considerados:

a) Os equipamentos devem ser dispostos fisicamente de forma a minimizar acessos desnecessários entre áreas de trabalho. –

b) As instalações de processamento e armazenamento de informações que lidam com dados sensíveis devem ser posicionadas para reduzir o risco de as informações serem vistas casualmente durante seu uso.

c) Itens que necessitam proteção especial devem ser isolados para reduzir o nível geral de proteção exigido.

d) Controles devem ser adotados para minimizar o risco de ameaças potenciais incluindo:

1) roubo; -
2) incêndio;
3) explosivos;
4) fumaça;
5) água (ou falha no fornecimento);
6) poeira;
7) vibração;
8) efeitos químicos;
9) interferência no suprimento elétrico;
10) radiação eletromagnética.

e) Uma organização deve considerar sua política em relação ao consumo de alimentos, bebida e cigarros nas proximidades das instalações de processamento de informações.

f) As condições ambientais devem ser monitoradas em busca de situações que possam afetar a operação das instalações de processamento de informações.

g) O uso de métodos de proteção especiais, tais como membranas para teclados, deve ser considerado para equipamentos em ambientes industriais.

7.2.2 Fornecimento de energia

Os equipamentos devem ser protegidos contra falta de energia e outras anomalias na eletricidade. Uma fonte elétrica adequada deve se provida de acordo com as especificações do fabricante do equipamento.

As opções para conseguir continuidade no fornecimento de energia incluem:

a) múltiplas alimentações para evitar um único ponto de falha no fornecimento de energia;

b) equipamento para suprimento de energia ininterrupto ("no-break");

c) gerador sobressalente.

7.2.3 Segurança para o cabeamento

Os cabos de energia e telecomunicação que transportam dados ou suportam serviços de informação devem ser protegidos contra interceptação ou danos. Os seguintes controles devem ser considerados:

a) Linhas de telecomunicação e energia dentro das instalações de processamento de informações devem ser subterrâneas, onde possível, ou sujeitas à proteção alternativa adequada.

b) O cabeamento de redes deve ser protegido contra interceptação não autorizada ou danos, por exemplo usando eletrodutos ou evitando-se rotas através de áreas públicas. Os cabos de energia devem ser segregados dos cabos de comunicação para impedir interferência.

c) Para sistemas críticos ou sensíveis, controles adicionais devem incluir:
   1) instalação de conduto blindado e salas ou caixas trancadas nos pontos de inspeção e terminação;
   2) uso de roteamento alternativo ou mídia de transmissão alternativa;
   3) uso de cabeamento de fibra ótica;
   4) iniciação de varreduras em busca de dispositivos não autorizados que possam estar sendo conectados aos cabos.

7.2.4 Manutenção de equipamentos

Os seguintes controles devem ser considerados:

a) Os equipamentos devem passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor.

b) Apenas pessoal autorizado de manutenção deve executar os reparos e a manutenção nos equipamentos.

c) Devem ser mantidos registros sobre todas as falhas ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas. ...

7.2.5 Segurança de equipamentos fora da empresa

As seguintes diretrizes devem ser consideradas:

a) Equipamentos e mídias retirados do prédio da organização não devem ser deixados desacompanhados em locais públicos. Em

viagens, os computadores portáteis devem ser transportados como bagagem pessoal e disfarçados onde possível.

b) As instruções dos fabricantes para proteção dos equipamentos devem ser sempre observadas, por exemplo proteção contra exposição a campos eletromagnéticos intensos.

c) Os controles para trabalhos em casa devem ser determinados por uma avaliação de riscos e os controles cabíveis aplicados conforme apropriado, por exemplo, armários-arquivos trancáveis, política de "mesa limpa" e controles de acesso aos computadores.

d) Cobertura de seguro adequada deve estar contratada para proteger equipamentos *off-site*.

*7.2.6 **Segurança para fim de vida ou reutilização de.***

Todos os itens de equipamento contendo mídia de armazenamento, tais como discos fixos, devem ser verificados para certificar que quaisquer dados sensíveis ou softwares licenciados foram removidos ou sobrescritos antes do descarte. Dispositivos de armazenamento danificados, que contenham dados sensíveis, podem exigir uma avaliação de riscos para determinar se tais itens devem ser destruídos, reparados ou descartados.

7.3 Controles gerais Obj: Impedir o comprometimento ou roubo de informações e de facilidades de processamento de informações. Controlo: As informações e as facilidades de processamento de informações devem ser protegidas contra divulgação, modificação ou roubo por pessoas não autorizadas, e devem ser implantados controles para minimizar perdas ou danos.	*7.3.1 Política de "mesa limpa" e "tela limpa".* As organizações devem considerar a adopção de uma política de "mesas limpas" para os papéis e media de armazenamento removível e uma política de "telas limpas" para as facilidades de processamento de informações, para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. A política deve considerar as classificações de segurança de informação (ver 5.2), os riscos correspondentes e os aspectos culturais da organização. *7.3.2 Remoção de propriedade* Equipamentos, informações ou software não devem ser retirados das instalações da organização sem autorização. Quando necessário e apropriado, os equipamentos devem ter sua saída registrada e devem ser registrados novamente quando devolvidos.
Domínio : **8 Gestão de comunicações e operações**	
8.1 Procedimentos operacionais e responsabilidades Objectivo: Garantir a operação correta e segura das facilidades de processamento de informações. Controlo: As responsabilidades e os procedimentos para a gestão e operação de todas as facilidades de processamento de informações devem ser estabelecidas. Isso inclui o desenvolvimento de instruções de operação apropriadas e de procedimentos para resposta a incidentes.	*8.1.1 Procedimentos operacionais documentados.* 8.1.2 Os procedimentos operacionais identificados pela política de segurança devem ser documentados e mantidos atualizados. Os procedimentos operacionais devem ser tratados como documentos formais e as alterações devem ser autorizadas pela gerência. Procedimentos documentados também devem ser preparados para as atividades de *housekeeping*[4] do sistema associadas com as facilidades de processamento de informações e comunicações, tais como procedimentos para iniciar e desligar o computador, *backups*, manutenção de equipamentos, gerenciamento e segurança da sala de computadores e de correio. *8.1.2 Controle das mudanças operacionais (Gestão de Alterações).* Mudanças nas facilidades de processamento de informações e nos sistemas devem ser controladas.

[4] N.T.: *Housekeeping* = procedimentos que precisam ser executados para manter um computador ou sistema operando adequadamente.

A segregação de tarefas (ver 8.1.4) deve ser implementada, onde apropriado, para reduzir o risco de utilização negligente ou má utilização deliberada dos sistemas.	Os programas operacionais devem estar sujeitos a um controle estrito das alterações. Quando programas são mudados, deve ser retido um *log* para auditoria, contendo todas as informações relevantes. Alterações no ambiente operacional podem causar impacto nos aplicativos ***8.1.3 Procedimentos para Gestão de incidentes.*** As responsabilidades e os procedimentos para gestão de incidentes devem ser estabelecidos para garantir uma resposta rápida, efetiva e ordenada aos incidentes de segurança a) devem ser estabelecidos procedimentos para cobrir todos os tipos potenciais de incidente de segurança, incluindo:. 1) falhas nos sistemas de informação e perda de serviço; 2) negação de serviço; 3) erros resultantes de dados incompletos ou inexactos; 4) violação de confidencialidade. *b) audit trails* e provas similares devem ser recolhidas (ver 12.1.7) e guardadas em segurança, conforme apropriado. d) Ação para recuperar de violações de segurança e corrigir falhas no sistema devem ser controladas de maneira formal e cuidadosa. Os procedimentos devem assegurar que: 1) apenas pessoas claramente identificadas e autorizadas tenham seu acesso permitido aos sistemas e dados "reais" (ver também 4.2.2 para acesso de terceiros); 2) todas as ações de emergência executadas sejam documentadas em detalhe; 3) a ação de emergência seja reportada à gerência e revisada de maneira ordenada; 4) a integridade dos controles e sistemas do negócio seja confirmada no menor tempo possível. ***8.1.4 Segregação de tarefas. 8.1.5 Separação das facilidades de desenvolvimento e de produção*** ***8.1.6 Gestão de instalações externas (Hosting por ex)*** A utilização de uma empresa externa contratada para gerir as instalações de processamento de informações pode introduzir uma exposição potencial de segurança, tal como a possibilidade de comprometimentos, danos ou perdas de dados no *site* da contratada.
8.2 Planejamento e aceitação de sistemas	***8.2.1 Capacity planning.***

Objetivo: Minimizar os riscos de falhas nos sistemas.	As demandas por recursos devem ser monitoradas e devem ser feitas projeções para o futuro para garantir que o poder de processamento e armazenamento adequados estejam disponíveis Eles devem identificar as tendências na utilização, particularmente em relação às aplicações comerciais ou ferramentas de gerenciamento de sistemas de informação.
Controlo: Planeamento antecipado e preparação são obrigatórios para assegurar a disponibilidade das capacidades e recursos adequados. Projeções das necessidades futuras de capacidade devem ser feitas, para reduzir o risco de sobrecarga no sistema. Os requisitos operacionais dos novos sistemas devem ser estabelecidos, documentados e testados antes de sua aceitação e uso.	*8.2.2 Aceitação de sistemas..* Os critérios de aceitação para novos sistemas de informação, *upgrades* e novas versões devem ser estabelecidos e devem ser realizados testes adequados dos sistemas antes da aceitação. Os seguintes controles devem ser considerados: a) requisitos de performance e capacidade dos computadores; b) procedimentos de reinício e recuperação de erros, e planos de contingência; c) preparação e testes dos procedimentos operacionais de rotina segundo padrões definidos; d) um conjunto acordado de controles de segurança em vigor; e) procedimentos manuais eficazes; f) arranjos para a continuidade dos negócios, conforme requerido no item 11.1; g) evidência de que a instalação do novo sistema não afetará de maneira adversa os sistemas existentes, particularmente nos horários de pico de processamento, como fim de mês; h) evidência de que foi considerado o efeito que o novo sistema terá sobre a segurança geral da organização; i) treinamento na operação ou uso dos novos sistemas.

8.3 Proteção contra software malicioso

Objectivo: Proteger a integridade de softwares e informações.

Controlo:

Precauções são necessárias para impedir e detectar a introdução de softwares maliciosos. Softwares e instalações de processamento de informações são vulneráveis à introdução de software malicioso, tais como vírus de computador, "network worms", "cavalos de Tróia" (ver também 10.5.4) e bombas lógicas. Os usuários devem ser conscientizados dos perigos relacionados com software malicioso ou não autorizado, e os gerentes devem, onde apropriado, implantar controles especiais para detectar ou impedir sua introdução. Em especial, é essencial que sejam tomadas precauções para detectar e impedir vírus em computadores pessoais.

8.3.1 Controles contra software malicioso

Os seguintes controles devem ser considerados: (com incidência nos servidores da rede)

a) uma política formal que exija obediência às licenças de software e proíba o uso de software não autorizado (ver 12.1.2.2); uma política formal para proteger contra riscos associados com a obtenção de arquivos e softwares através de redes externas, ou qualquer outro meio, indicando quais medidas de proteção devem ser tomadas (ver também 10.5, especialmente 10.5.4 e 10.5.5);

b) instalação e atualização regular de software de detecção de vírus e reparo, para varrer computadores e mídia como uma medida de precaução ou rotineiramente;

c) conduzir revisões regulares do software e dos conteúdos de dados dos sistemas que suportam processos críticos para o negócio. A presença de quaisquer arquivos não aprovados ou modificações não autorizadas deve ser formalmente investigada;

d) verificação antivírus, antes de qualquer uso, de quaisquer arquivos em mídia eletrônica de origem incerta ou não autorizada, ou arquivos recebidos de redes não confiáveis;

e) verificação contra software malicioso em quaisquer anexos de correio eletrônico e *downloads*, antes de qualquer uso. Esta verificação pode ser conduzida em locais diferentes, por exemplo em servidores de correio eletrônico, computadores *desktop* ou na entrada da rede da organização.

f) procedimentos de gerenciamento e responsabilidades para lidar com a proteção antivírus nos sistemas, treinamento sobre seu uso, como reportar e recuperar de ataques de vírus (ver 6.3 e 8.1.3);

g) planos apropriados para continuidade dos negócios para recuperar de ataques de vírus, incluindo todos os dados necessários e arranjos para *backup* e recuperação de softwares (ver tópico 11);

h) procedimentos para confirmar todas as informações relativas a software malicioso, e para garantir que os boletins de alerta sejam exatos e informativos. Os gerentes devem assegurar que sejam usadas fontes confiáveis, como publicações respeitadas, *sites* Internet confiáveis ou fornecedores de software antivírus, para diferenciar entre *hoaxes* e vírus verdadeiros. A equipe deve ser conscientizada quanto ao problema de *hoaxes(boatos)* e o que fazer quando recebê-los.

8.4 *Housekeeping*

Objectivo:

Manter a integridade e a disponibilidade dos serviços de processamento de informações e comunicações.

8.4 *Housekeeping - Controlo*

Procedimentos de rotina devem ser implantados para executar a estratégia acordada sobre *backups* (ver 11.1), fazendo cópias *backup* de dados e treinando sua restauração em tempo hábil, registrando *log* de eventos e falhas e, onde apropriado, monitorando o ambiente computacional.

8.4.1 Backup das informações – Fazer e Testar

8.4.2 Logs de operador (registos de actividade)

A equipe da operação deve manter um *log* de suas atividades. Os *logs* devem incluir, conforme apropriado:

8.4.3 Log de falhas.

As falhas devem ser reportadas e acções corretivas executadas. As falhas reportadas pelos usuários a respeito de problemas com o

		processamento de informações ou sistemas de comunicações devem ser registradas em *log*.
8.5 Gestão de redes Objectivo: Assegurar a salvaguarda de informações em redes de computadores e a proteção da infra-estrutura de apoio. Controlo: O gerenciamento da segurança em redes que podem ultrapassar as fronteiras da organização exige atenção. Controles adicionais também podem ser exigidos para proteger dados sensíveis que trafegam por redes públicas.		***8.5.1 Controles para redes.*** Especificamente, os seguintes controles devem ser considerados: a) A responsabilidade operacional pelas redes deve ser separada das operações de computador onde apropriado (ver 8.1.4). b) A responsabilidades e os procedimentos para a administração de equipamento remoto, incluindo equipamento em áreas de usuários, devem ser determinados. c) Se necessário, controles especiais devem ser estabelecidos para salvaguardar a confidencialidade e integridade dos dados que trafegam em redes públicas e para proteger os sistemas conectados (ver 9.4 e 10.3). Controles especiais também podem ser exigidos para manter a disponibilidade dos serviços de rede e computadores conectados. d) Atividades de gerenciamento devem ser cuidadosamente coordenadas para otimizar o serviço prestado ao negócio e para assegurar que controles estão aplicados de forma consistente em toda a infra-estrutura de processamento de informações..
8.6 Manuseio e segurança de mídia Objetivo: Impedir danos aos ativos e interrupções nas atividades do negócio. Mídia deve ser controlada e fisicamente protegida. Controlo: Procedimentos operacionais apropriados devem ser estabelecidos para proteger documentos, mídia magnética (fitas, discos, cassetes), dados de entrada/saída e documentação de sistemas contra danos, roubos e acesso não autorizado.		***8.6.1 Gerenciamento de mídia removível.*** Os seguintes controles devem ser considerados. a) Se não forem mais necessários, os conteúdos existentes em qualquer mídia reutilizável que for removida da organização devem ser apagados. b) Deve ser exigida autorização para remover qualquer mídia da organização e deve ser mantido um registro de tais remoções para guardar uma *audit trail* (ver 8.7.2). c) Todas as mídias devem ser armazenadas em um ambiente seguro, de acordo com as especificações dos fabricantes. ***8.6.2 Descarte de mídia.*** ***8.6.3 Procedimentos de manuseio de informações.*** Devem ser redigidos procedimentos para manusear informações, de forma consistente com sua classificação (ver 5.2), em documentos, sistemas de computador, redes, computação móvel, comunicação móvel, correio, correio de voz, comunicações de voz em geral, multimídia, serviços e facilidades postais, uso de aparelhos de fax e outros itens sensíveis, como cheques em branco e faturas

	8.6.4 Segurança da documentação dos sistemas. A documentação dos sistemas pode conter várias informações sensíveis, como descrições de processos de aplicativos, procedimentos, estruturas de dados e processos de autorização (ver também 9.1). Os seguintes controles devem ser considerados para proteger a documentação dos sistemas contra acesso não autorizado: a) A documentação dos sistemas deve ser guardada de forma segura.

8.7 Intercâmbios de informações e softwares

Objectivo: Impedir perda, modificação ou uso indevido de informações intercambiadas entre organizações.

Controlo:

Os intercâmbios de informações e software entre organizações devem ser controlados e devem obedecer à qualquer legislação relevante (ver cláusula 12).
Os intercâmbios devem ser executados com base em contratos. Procedimentos e padrões para proteger informações e mídias em trânsito devem ser estabelecidos. Devem ser consideradas as implicações para o negócio e para a segurança associadas com intercâmbio eletrônico de dados, comércio eletrônico e correio eletrônico e os controles necessários.

8.7.1 Contratos para intercâmbio de informações e softwares.

Os contratos sobre condições de segurança devem considerar:

a) responsabilidades gerenciais para controlar e notificar transmissão, expedição e recepção;

b) procedimentos para notificar o remetente, transmissão, expedição e recepção;

c) padrões técnicos mínimos para embalagem e transmissão;

d) padrões de identificação de/para *courier*;

e) responsabilidades, inclusive financeiras, no caso de perda de dados;

f) uso de um sistema de rotulagem acordado entre as partes para as informações críticas ou sensíveis, garantindo que o significado do rótulo seja entendido imediatamente e que as informações sejam protegidas adequadamente;

g) propriedade das informações e software e responsabilidades pela proteção de dados, respeito aos *copyrights* dos softwares e considerações similares (ver 12.1.2 e 12.1.4);

8.7.2 Segurança de mídia em trânsito.

8.7.3 Segurança para comércio eletrônico.

Devem ser aplicados controles para proteger o comércio eletrônico contra tais ameaças. As considerações de segurança para o comércio eletrônico incluem os seguintes controles:

a) Autenticação. Qual nível de segurança deve o cliente e o negociante exigirem quanto à identidade alegada de cada um?

b) Autorização. Quem está autorizado a definir preços, emitir ou assinar documentos comerciais importantes? Como o parceiro comercial sabe disto?

c) Processos relacionados com contratos e propostas. Quais são os requisitos de confidencialidade, integridade e prova de envio e recepção de documentos importantes e da não repudiação de contratos?

d) Informações de preços. Qual o nível de confiança que pode ser depositado na integridade da lista de preços anunciada e na confidencialidade de acordos confidenciais para descontos?

e) Transações de encomendas. Como é fornecida a confidencialidade e integridade para detalhes de manipulação de encomendas, pagamentos, entrega e confirmação de recebimento?

f) Escrutínio. Qual grau de detalhamento no exame é apropriado para checar informações de pagamento fornecidas pelo cliente?

g) Quitação. Qual é a forma de pagamento mais apropriada para resguardar contra fraudes?

h) Encomendas. Qual proteção é necessária para manter a confidencialidade e integridade das informações de encomenda, e para evitar a perda ou duplicidade de transações?

i) Responsabilidade financeira. Quem arca com o risco de transações fraudulentas?

Muitas das considerações acima podem ser tratadas com a aplicação de técnicas de criptografia esboçadas no item 10.3, levando em conta a obediência às exigências legais (ver 12.2, especialmente 12.1.6 sobre legislação de criptografia).

Os acordos de comércio eletrônico entre parceiros comerciais devem ser apoiados por um contrato documentado que compromete ambas as partes com os termos acordados do intercâmbio, incluindo detalhes sobre autorização [ver item b) acima]. Outros contratos com provedores de serviços de informação e de redes de valor agregado podem ser necessários.

8.7.4 Segurança para correio eletrônico..

8.7.4.2 *Política sobre correio eletrônico*

As organizações devem estabelecer uma política clara relativa ao uso de correio eletrônico, incluindo:

a) ataques ao correio eletrônico, como vírus e interceptação;

b) proteção dos anexos nas mensagens eletrônicas;

c) diretrizes sobre quando não usar correio eletrônico;

d) responsabilidade dos empregados em não comprometer a empresa; por exemplo, envio de mensagens eletrônicas difamatórias, utilização para assédio, compras não autorizadas;

e) uso de técnicas criptográficas para proteger a confidencialidade e a integridade das mensagens eletrônicas (ver 10.3);

f) retenção de mensagens que, se armazenadas, podem ser descobertas em casos de litígios;

g) controles adicionais para examinar cuidadosamente mensagens que não podem ser autenticadas.

8.7.5 Segurança de sistemas de automação de escritórios.

Políticas e diretrizes devem ser preparadas e implementadas para controlar os riscos para a segurança e para o negócio associados com sistemas de automação de escritórios. Estes propiciam oportunidades para disseminação e compartilhamento mais rápidos de informações comerciais usando uma combinação de: documentos, computadores, computação móvel, comunicações móveis, correio, correio de voz, comunicações verbais em geral, multimídia, serviços/facilidades postais e equipamentos de fax.

Os cuidados tomados em relação às implicações de segurança decorrentes da interconexão de tais facilidades devem incluir:

a) vulnerabilidades das informações nos sistemas de automação de escritórios, tal como gravação de telefonemas ou conferências telefônicas, confidencialidade de telefonemas, armazenagem de faxes, abertura de correspondência, distribuição de correspondência;

	b) política e controles apropriados para gerenciar o compartilhamento de informações, por exemplo o uso de *bulletin boards* eletrônicos corporativos (ver 9.1); c) excluir categorias de informações sensíveis do negócio se o sistema não fornecer um nível adequado de proteção (ver 5.2); ***8.7.6 Sistemas disponibilizados publicamente.*** Devem ser tomados cuidados para proteger a integridade de informações publicadas eletronicamente para impedir modificação não autorizada, que poderia prejudicar a reputação da organização publicadora. As informações em um sistema disponibilizado publicamente, tal como informações em um servidor de Web acessíveis via Internet, podem necessitar obedecer a leis, normas e regulamentos na jurisdição onde o sistema está localizado ou onde os negócios ocorrem. Sistemas de publicação eletrônica, especialmente aqueles que permitem *feedback* e entrada direta de informações, devem ser cuidadosamente controlados de forma que: a) as informações sejam obtidas de acordo com qualquer legislação de proteção de dados existente (ver 12.1.4); b) as informações introduzidas no sistema de publicação e processadas por ele sejam processadas inteiramente e com exatidão em tempo adequado; c) as informações sensíveis sejam protegidas durante o processo de coleta e quando armazenadas; d) o acesso ao sistema de publicação não permita o acesso não intencionado a redes em que esteja conectado. ***8.7.7 Outras formas de intercâmbio de informações.*** Procedimentos e controles devem estar implantados para proteger o intercâmbio de informações através do uso de facilidades de voz, fac-símile e vídeo-comunicações. As informações podem ser comprometidas devido à falta de conscientização, política ou procedimentos sobre o uso de tais facilidades, como por exemplo, conversas ouvidas por acaso em telefone móvel em local público, gravações em secretárias eletrônicas ouvidas por acaso, acesso não autorizado a sistemas discados de correio de voz ou enviar faxes acidentalmente para a pessoa errada.
Domínio 9 **Controle de Acesso**	
9.1 Necessidades de controle de acesso	***9.1.1 Política de controle de acesso..***

Objetivo: Controlar o acesso às informações. O acesso a informações e processos do negócio deve ser controlado com base nas necessidades de segurança e do negócio. Deve-se levar em conta as políticas para disseminação e autorização das informações.	**9.1.1.1** *Política e requisitos do negócio* Os requisitos de controle de acesso na organização devem ser definidos e documentados. As regras e direitos de controle de acesso para cada usuário ou grupo de usuários devem ser claramente definidas em uma declaração de política de acesso. Os usuários e os provedores de serviços devem receber uma declaração clara dos requisitos a serem satisfeitos pelos controles de acesso. A política deve considerar o seguinte: a) requisitos de segurança das aplicações individuais do negócio; b) identificação de todas as informações relacionadas às aplicações do negócio; c) políticas para disseminação e autorização de informações, como o princípio do "saber apenas quando necessário" e níveis de segurança e classificação de informações; **9.1.1.2** *Regras para controle de acesso* Na especificação das regras para controle de acesso, é preciso considerar com cuidado o seguinte: a) diferenciar entre regras que devem ser sempre obedecidas e regras que são opcionais ou condicionais; b) estabelecer regras baseadas na premissa "O que deve ser geralmente proibido a menos que seja expressamente permitido" em vez de usar a regra mais fraca "Tudo é geralmente permitido a menos que seja expressamente proibido"; c) mudanças nos rótulos das informações (ver 5.2) que são iniciadas automaticamente pelas facilidades de processamento de informação e aquelas iniciadas à discrição de um usuário; d) mudanças nas permissões de usuários que são iniciadas automaticamente pelo sistema de informações e aquelas iniciadas por um administrador;

9.2 Gerenciamento do acesso de usuários

Objetivo: Impedir acesso não autorizado aos sistemas de informação.

Procedimentos formais devem ser implantados para controlar a alocação de direitos de acesso a sistemas e serviços de informação.
Os procedimentos devem cobrir todos os estágios do ciclo de vida do acesso dos usuários, desde o cadastramento inicial de novos usuários até a retirada final de usuários que não mais necessitam de acesso aos sistemas e serviços de informação.
Atenção adequada deve ser dada, onde apropriado, à necessidade de controlar a alocação de direitos privilegiados de acesso, que permitem aos usuários sobrepujar os controles do sistema.

9.2.1 Cadastramento de usuários.

Deve existir um procedimento formal de cadastramento e descadastramento de usuários para a concessão de acesso a todos os sistemas e serviços de informação multiusuários.

O acesso a serviços de informação multiusuários deve ser controlado através de um processo formal de cadastramento de usuários, que deve incluir:

a) usar IDs de usuário exclusivas, de modo que os usuários possam ser relacionados com suas ações e responsabilizados por elas. O uso de IDs de grupo deve ser permitido apenas onde elas sejam adequadas para o trabalho executado;.

b) confirmar que o usuário tem autorização do proprietário do sistema para o uso do sistema ou serviço de informação. Aprovação separada para os direitos de acesso pela gerência também pode ser conveniente;

9.2.2 Gerenciamento de privilégios.

A alocação e o uso de privilégios (qualquer recurso ou facilidade de um sistema de informações multiusuário que permite ao usuário sobrepujar os controles do sistema ou aplicativo) devem ser restritos e controlados. O uso inapropriado de privilégios de sistema freqüentemente é um dos principais fatores contribuintes para a falha de sistemas que foram violados.

Sistemas multiusuários que exigem proteção contra acesso não autorizado devem ter a alocação de privilégios controlada através de procedimento formal de autorização. Os seguintes passos devem ser considerados:

9.2.3 Gerenciamento de senhas de usuário.

As senhas são um meio comum de validar a identidade de um usuário para acessar um sistema ou serviço de informações. A alocação de senhas deve ser controlada através de um processo administrativo formal, cujo enfoque deveria ser:

a) exigir que os usuários assinem uma declaração de manter confidencial as senhas pessoais e de manter as senhas de grupos somente entre as pessoas do grupo (isto poderia ser incluído nos termos e condições do contrato de trabalho, ver 6.1.4);

b) garantir, onde os usuários forem responsáveis por manter suas próprias senhas, que eles sejam providos inicialmente com uma senha temporária segura a qual eles sejam forçados a alterar imediatamente. As senhas temporárias fornecidas quando um usuário esquece sua senha devem ser fornecidas apenas após identificação positiva do usuário;

9.2.4 Revisão dos direitos de acesso dos usuários.

Para manter controle efectivo sobre o acesso aos serviços de informações, a gerência deve conduzir um processo formal, a intervalos regulares, para revisar os direitos de acesso dos usuários de forma que:

a) os direitos de acesso dos usuários sejam revisados a intervalos regulares (um período de 6 meses é recomendado) e após quaisquer alterações (ver 9.2.1)

b) as autorizações para direitos privilegiados de acesso (ver 9.2.2) devem ser revisadas a intervalos mais freqüentes; é recomendado um período de 3 meses;

9.3 Responsabilidades dos usuários

Objetivo: Impedir acesso de usuários não autorizados.

A cooperação dos usuários autorizados é essencial para a eficácia da segurança.
Os usuários devem ser conscientizados de suas responsabilidades quanto à manutenção de controles eficazes de acesso, particularmente o uso de senhas e a segurança do equipamento do usuário.

9.3.1 Uso de senhas

Os usuários devem seguir as boas normas de segurança na seleção e uso de senhas.

As senhas fornecem um meio de validar a identidade do usuário e assim estabelecer direitos de acesso aos serviços ou facilidades de processamento de informações. Todos os usuários devem ser aconselhados a:

a) manter confidenciais as senhas;

b) evitar manter anotação das senhas em papel, a menos que possam ser guardadas com segurança;

c) alterar senhas sempre que houver qualquer indicação de possível comprometimento da senha ou do sistema;

9.3.2 Equipamentos de usuário não- operado.

Os usuários devem se assegurar de que equipamentos desassistidos possuem proteção apropriada. Os equipamentos instalados nas áreas dos usuários, como estações de trabalho ou servidores de arquivos, podem exigir proteção específica contra acesso não autorizado quando deixados desassistidos por um período prolongado. Todos os usuários e contratados devem ser conscientizados dos requisitos e procedimentos de segurança para proteger equipamento não-operado, bem como de suas responsabilidades para implementação de tal proteção.

a) encerrar sessões ativas quando terminarem, a menos que elas possam ser protegidas por um mecanismo de tranca, como um protetor de tela com senha;

b) desligar *(logoff)* os computadores *mainframe* quando a sessão estiver finalizada (isto é, não apenas desligar o terminal ou o PC);

c) proteger PCs ou terminais contra uso não autorizado por meio de um *key lock* ou um controle equivalente, como acesso por senha, quando não estiverem em uso.

9.4 Controle de acesso à rede

Objetivo: Proteção de serviços que utilizam redes.

O acesso a serviços em redes internas e externas deve ser controlado.

Isto é necessário para assegurar que os usuários que têm acesso a redes e serviços em rede não comprometam a segurança de tais serviços, usando-se:

9.4.1 Política sobre o uso de serviços em rede.

Conexões inseguras com serviços em rede podem afetar toda a organização. Os usuários devem ter acesso direto apenas aos serviços que eles foram especificamente autorizados a usar. Este controle é particularmente importante para conexões de rede com aplicações sensíveis ou críticas ou para usuários em locais de alto risco, como áreas públicas ou externas que estão fora da gestão e controle de segurança da organização.

Deve ser formulada uma política relacionada ao uso de redes e de serviços em rede. Ela deve cobrir:

a) as redes e os serviços em rede cujo acesso é permitido;

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

b) mecanismos apropriados para autenticação de usuários e equipamentos;

c) controle do acesso dos usuários aos serviços de informações.

b) procedimentos de autorização para determinar quem está autorizado a acessar quais redes e serviços em rede;

c) controles e procedimentos administrativos para proteger o acesso a conexões de rede e serviços em rede.

9.4.2 Path obrigatório.

O *path* do terminal do usuário até o serviço informatizado pode precisar ser controlado. As redes são projetadas para permitir máximo escopo no compartilhamento de recursos e flexibilidade de roteamento. Esses recursos também podem propiciar oportunidades para acesso não autorizado a aplicações da organização ou uso não autorizado das facilidades de informação. Incorporar controles que restrinjam a rota entre o terminal do usuário e os serviços informatizados que o usuário está autorizado a acessar, como por exemplo criando um *path* obrigatório, pode reduzir tais riscos.

O objetivo de um *path* obrigatório é impedir quaisquer usuários de selecionar rotas que estão fora da rota entre o terminal do usuário e os serviços que o usuário está autorizado a acessar

São exemplos disto:

a) alocar linhas ou números de telefones dedicados;

b) conectar portas automaticamente com sistemas aplicativos ou *gateways* de segurança especificados;

c) limitar as opções de menus e submenus para usuários individuais;

d) impedir *roaming* de rede ilimitado;

e) para usuários externos da rede, obrigar o uso de sistemas aplicativos e/ou *gateways* de segurança especificados;

f) controlar ativamente as comunicações permitidas entre origem e destino via *gateways* de segurança, como *firewalls*;

g) restringir o acesso à rede através da implantação de domínios lógicos separados, como redes virtuais privadas, para grupos de usuários dentro da organização (ver também 9.4.6).

9.4.3 Autenticação de usuário para conexões externas (a partir do exterior)

9.4.4

Conexões externas apresentam um potencial para acesso não autorizado às informações do negócio, como por exemplo acesso através de métodos *dial-up*. Portanto, o acesso de usuários remotos deve estar sujeito à autenticação.

Autenticação de usuários remotos pode ser conseguida usando-se, por exemplo, uma técnica baseada em criptografia, *tokens* de hardware ou protocolo tipo "challenge/response". Linhas privadas dedicadas ou uma funcionalidade para checar endereços de usuário na rede também podem ser usadas para fornecer garantia da origem das conexões.

9.4.4 Autenticação de nodo (tipo telnet ...mstsc).

Um recurso para conexão automática com um computador remoto pode fornecer um meio para obter acesso não autorizado a uma aplicação da organização. Conexões com sistemas de computadores remotos devem portanto ser autenticadas. Isto é especialmente

importante se a conexão usar uma rede que está fora do controle do gerenciamento de segurança da organização.

9.4.5 Protecção de porta de diagnóstico remoto.

Acesso a portas de diagnóstico deve ser controlado de forma segura. Muitos computadores e sistemas de comunicação são instalados com um recurso de diagnóstico remoto por linha discada para uso pelos engenheiros de manutenção. Se desprotegidas, estas portas de diagnóstico propiciam um meio para acesso não autorizado.

9.4.5 Segregação em redes.

9.4.6

As redes estão cada vez mais se estendendo além das fronteiras tradicionais das organizações, à medida que são formadas parcerias comerciais que podem necessitar de interconexão ou compartilhamento de facilidades de processamento de informações e redes. Tais extensões podem aumentar o risco de acesso não autorizado aos sistemas de informação que já usam a rede, alguns dos quais podem exigir proteção contra outros usuários da rede devido à sua confidencialidade ou criticalidade. Em tais circunstâncias, a introdução de controles dentro da rede, para segregar grupos de serviços de informação, usuários e sistemas de informação, deve ser considerada.

Um método de controlar a segurança de grandes redes é dividi-las em domínios lógicos separados, como domínios das redes internas da organização e domínios das redes externas, cada um protegido por um perímetro de segurança definido.

9.4.7 Controle das conexões de rede.

Tais controles podem ser implementados através de *gateways* para a rede que filtram o tráfego utilizando tabelas ou regras predefinidas

9.4.8 Controle de roteamento da rede.

Os controles de roteamento devem ser baseados em mecanismos de verificação positiva de endereços de origem e destino. A tradução dos endereços de rede também é um mecanismo muito útil para isolar redes e impedir as rotas de propagarem da rede de uma organização para a rede de outra. Eles podem ser implementados em software ou hardware

9.4.9 Segurança de serviços em rede.

Uma vasta gama de serviços de redes públicas ou privadas está disponível, alguns dos quais oferecem serviços com valor agregado. Os serviços de rede podem ter características de segurança únicas ou complexas.

9.5 Controle de acesso ao sistema operativo das maquinas

Objetivo: Impedir acesso não autorizado a computadores.

As facilidades de segurança no nível de sistema operacional devem ser usadas para restringir o acesso aos recursos dos computadores. Estas facilidades devem ser capazes de:

a) identificar e confirmar a identidade, e se necessário o terminal ou localização, de cada usuário autorizado;

b) registrar acessos ao sistema bem-sucedidos e fracassados;

c) fornecer os meios apropriados para autenticação; se for usado um sistema de gerenciamento de senhas, ele deve garantir senhas de qualidade [ver 9.3.1 d)].

d) onde apropriado, restringir os tempos de conexão dos usuários.

Outros métodos de controle de acesso, tais como "challenge-response", estão disponíveis se forem justificáveis com base no risco para o negócio.

9.5.1 Identificação automática de terminal.

Identificação automática de terminais deve ser considerada para autenticar conexões com locais específicos e com equipamentos portáteis. Identificação automática de terminais é uma técnica que pode ser usada se for importante que a sessão possa ser iniciada apenas de um local específico ou de um terminal de computador específico.

9.5.2 Procedimentos de logon em terminais.

O acesso a serviços de informação deve ser realizado via um processo de *logon* seguro. O procedimento para conectar em um sistema de computador deve ser projetado para minimizar a oportunidade de acessos não autorizados. O procedimento de *logon* deve, portanto, divulgar o mínimo de informações sobre o sistema, de forma a evitar fornecer assistência desnecessária a um usuário não autorizado. Um bom procedimento de *logon* deve:

a) não exibir identificadores do sistema ou do aplicativo até que o processo de *logon* tenha sido completado com sucesso;

b) exibir um aviso genérico de que o computador deve ser acessado apenas por usuários autorizados;

c) não fornecer mensagens de *help* durante o procedimento de *logon* que poderiam ajudar um usuário não autorizado;

d) validar as informações de *logon* apenas após terminada toda a entrada de dados. Se ocorrer uma condição de erro, o sistema não deve indicar qual parte dos dados está correta ou incorreta;

9.5.3 Identificação e autenticação de usuários.

Todos os usuários (incluindo equipe de suporte técnico, tais como operadores, administradores de rede, programadores de sistema e administradores de banco de dados) devem ter um identificador exclusivo (ID de usuário) para seu uso pessoal, de modo que as atividades possam ser rastreadas até o responsável individual. As IDs de usuário não devem dar nenhuma indicação do nível de privilégio do usuário (ver 9.2.2), por exemplo gerente ou supervisor.

9.5.4 Sistema de gerenciamento de senhas.

Um bom sistema de gerenciamento de senhas deve:

a) obrigar o uso de senhas individuais para manter a responsabilização;

b) onde apropriado, permitir aos usuários selecionar e alterar suas próprias senhas e incluir um procedimento de confirmação para permitir corrigir erros de digitação;

c) obrigar a escolha de senhas de qualidade, como descrito no item 9.3.1;

d) onde usuários alteram suas próprias senhas, obrigar alterações de senha como descrito no item 9.3.1;

	9.5.5 Uso de utilitários do sistema. A maioria das instalações de computador tem um ou mais programas utilitários de sistema que podem ser capazes de sobrepujar controles dos sistemas e aplicativos. É essencial que o uso deles seja restrito e controlado à risca. Os seguintes controles devem ser considerados: a) uso de procedimentos de autenticação para utilitários de sistema; b) segregar os utilitários dos softwares aplicativos; c) limitação do uso de utilitários de sistema à quantidade mínima praticável de usuários autorizados e confiáveis; ***9.5.6 Alarme de coação para salvaguardar usuários.*** A provisão de um alarme de coação deve ser considerada para usuários que possam ser alvo de coerção. A decisão de se colocar um tal alarme deve ser baseada em uma avaliação de riscos. Devem ser definidas responsabilidades e procedimentos para responder a um alarme de coação. ***9.5.7 Time-out no terminal.*** Terminais inativos em locais de alto risco, por exemplo áreas públicas ou externas fora do gerenciamento de segurança da organização, ou servindo a sistemas de alto risco, devem ser desligados *(shut-down)* após um período definido de inatividade, para impedir o acesso de pessoas não autorizadas ***9.5.8 Limitação de tempo de conexão.*** Restrições nos tempos de conexão devem fornecer segurança adicional para aplicações de alto risco.

9.6 Controle de Acesso às Aplicações

Objetivo: Impedir acesso não autorizado às informações mantidas nos sistemas de informação. Os recursos de segurança devem ser usados para restringir o acesso dentro dos sistemas aplicativos.

O acesso lógico ao software e às informações deve ser restrito aos usuários autorizados. Os sistemas aplicativos devem:

a) controlar o acesso dos usuários às informações e funções do sistema aplicativo, de acordo com uma política de controle de acesso definida;

b) fornecer proteção contra acesso não autorizado para qualquer software utilitário e de sistema operacional que seja capaz de fazer *override* nos controles do sistema ou aplicativo;

c)

9.6.1 Restrição de acesso às informações.

Utilizadores de sistemas aplicativos, incluindo a equipe de suporte, devem receber acesso às informações e funções dos sistemas aplicativos de acordo com uma política predefinida de controle de acesso, baseada nos requisitos individuais das aplicações do negócio e consistente com a política organizacional de acesso a informações (ver 9.1).

9.6.2 Isolamento de sistemas sensíveis.

Sistemas sensíveis podem exigir um ambiente computacional dedicado (isolado). Alguns sistemas aplicativos são suficientemente sensíveis a perdas potenciais a ponto de exigir tratamento especial. A sensibilidade pode indicar que o sistema aplicativo deve ser executado em um computador dedicado, deve compartilhar recursos apenas com sistemas aplicativos confiáveis ou não ter limitações

9.7 Monitorando o acesso e o uso do sistema

Objetivo: Detectar atividades não autorizadas.

Os sistemas devem ser monitorados para detectar desvios da política de controle de acesso e registrar eventos monitoráveis para fornecer provas no caso de incidentes de segurança.

O monitoramento do sistema permite que a eficácia dos controles adotados seja verificada e que a conformidade com o modelo de política de acesso (ver 9.1) seja confirmada.

9.7.1 Registro de eventos em log.

Logs para auditoria, que registrem exceções e outros eventos relevantes para a segurança, devem ser produzidos e mantidos por um período acordado para auxiliar investigações futuras e monitorar controle de acessos. Os *logs* para auditoria devem incluir também:

a) IDs de usuários

b) datas e horários de *logon* e *logoff*;

c) identidade ou localização do terminal, se possível;

d) registros das tentativas de acesso ao sistema, bem-sucedidas e rejeitadas;

e) registros das tentativas de acesso a dados e outros recursos, bem-sucedidas e rejeitadas.

9.7.2 Monitorando o uso do sistema.

9.7.2.1 *Procedimentos e áreas de risco*

As áreas que devem ser consideradas incluem:

a) acesso autorizado, incluindo detalhes tais como:

1) a ID do usuário;
2) a data e o horário de eventos importantes

b) todas operações privilegiadas, tais como:

1) uso de uma conta de supervisor;

c) tentativas de acesso não autorizadas, tais como:

1) tentativas fracassadas;

d) alertas ou falhas de sistema tais como:

1) mensagens ou alertas de console;

9.7.2.2 *Factores de risco versus exame e reflexão sobre os dados recolhidos na monitorização*

O resultado do monitoramento das atividades deve ser examinado regularmente. A freqüência do exame depende dos riscos envolvidos.

9.7.2.3 *Registrando e revisando eventos*

Uma revisão do *log* de eventos envolve o entendimento das ameaças enfrentadas pelo sistema e da maneira como elas surgem. Exemplos de eventos que podem exigir investigação adicional no caso de incidentes de segurança são apresentados no item 9.7.1.

9.7.3 Sincronização de relógios.

O acerto correto dos relógios dos computadores é importante para assegurar a exatidão dos *logs* para auditoria, que podem ser exigidos para investigações ou como prova em casos legais ou disciplinares.

9.8 Computação móvel e trabalho à distância Objectivo: Assegurar segurança de informações no uso de computadores portáteis e facilidades de trabalho à distância. A protecção exigida deve ser compatível com os riscos que estes modos de trabalho específicos podem causar	***9.8.1 Computadores portáteis.*** Uma política formal deve ser adotada, levando em consideração os riscos de se trabalhar com facilidades de computação móvel, em particular em ambientes não protegidos. Por exemplo, tal política deve incluir os requisitos de proteção física, controles de acesso, técnicas criptográficas, *backups* e proteção contra vírus ***9.8.2 Trabalho à distância.*** Os controles e arranjos a serem considerados incluem: a) a provisão de equipamento e mobiliário adequados para as atividades de trabalho à distância; b) uma definição do trabalho permitido, das horas de trabalho, da classificação das informações que podem ser retidas e dos sistemas e serviços internos que o funcionário que trabalha à distância está autorizado a acessar; c) a provisão de equipamento de comunicação adequado, incluindo métodos para tornar seguro o acesso remoto; d) segurança física; e) regras e orientação sobre o acesso de familiares e visitantes ao equipamento e às informações; f) a provisão de suporte e manutenção para o hardware e o software; g) os procedimentos para *backup* e continuidade do negócio; h) auditoria e monitoramento de segurança; i) revogação de autoridade, direitos de acesso e a devolução do equipamento quando cessarem as atividades de trabalho à distância.

Domínio : **10** **Desenvolvimento e manutenção de sistemas**

Objectivo	*Detalhe Controlo Geral*
10.1 Requisitos de segurança nos sistemas Objetivo: Assegurar que a segurança seja embutida nos sistemas de informações. Isto incluirá infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelos usuários. O projeto e a implementação do processo corporativo que dá suporte à aplicação ou ao serviço pode ser crucial para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento de sistemas de informação. Todos os requisitos de segurança, incluindo a necessidade de arranjos para *fallback*, devem ser identificados na fase de requisitos de um projeto e justificados, acordados e documentados como parte do "business case" geral para um sistema de informações.	***10.1.1 Análise e especificação dos requisitos de segurança.*** f) Os relatórios com os requisitos do negócio para novos sistemas, ou melhorias em sistemas existentes, devem especificar as necessidades de controles. Tais especificações devem considerar os controles automatizados a serem incorporados no sistema e a necessidade de suportar controles manuais. Considerações similares devem ser aplicadas ao se avaliar pacotes de software para aplicações do negócio. Se considerado apropriado, a gerência pode desejar utilizar produtos certificados e avaliados de forma independente.
10.2 Segurança em sistemas aplicativos Objetivo: Impedir perda, modificação ou má utilização de dados dos usuários em sistemas aplicativos. Controles apropriados e *audit trails* ou *logs* de atividade devem ser projetados nos sistemas aplicativos, incluindo aplicativos escritos pelos usuários. Estes devem incluir a validação de dados de entrada, dados de processamento interno e dados de saída.	***10.2.1 Validação dos dados de entrada.*** A entrada de dados para os sistemas aplicativos deve ser validada para garantir que está correta e apropriada. ***10.2.2 Controle do processamento interno.*** **10.2.2.1** *Áreas de risco* Dados que foram entrados corretamente podem ser corrompidos por erros de processamento ou através de atos deliberados O projeto das aplicações deve assegurar que sejam implementadas restrições para minimizar o risco de falhas de processamento que levem a uma perda de integridade. **10.2.2.2** *Verificações e controles*

	Os controles exigidos dependerão da natureza do aplicativo e do impacto nos negócios causados por quaisquer dados corrompidos. Exemplos de verificações que podem ser incorporadas incluem os seguintes: a) controles de sessão ou de lotes, para conciliar arquivos de dados após atualizações de transações; b) fechamento dos controles, para verificar saldos inicias contra saldos finais anteriores, a saber: 1) controles de execução-para-execução 2) totais da atualização dos arquivos; 3) controles de programa-para-programa; ***10.2.3 Autenticação de mensagens*** Autenticação de mensagens deve ser considerada para aplicativos onde exista uma necessidade de segurança para proteger a integridade do conteúdo das mensagens; por exemplo, transferência eletrônica de fundos, especificações, contratos e propostas com alta importância ou outros intercâmbios de dados eletrônicos similares Autenticação de mensagens não se destina a proteger os conteúdos de uma mensagem contra divulgação não autorizada. Técnicas de criptografia (ver 10.3.2 e 10.3.3) podem ser usadas como um meio adequado de implementar autenticação de mensagens. ***10.2.4 Validação dos dados de saída.*** A saída de dados de um sistema aplicativo deve ser validada para garantir que o processamento de informações armazenadas seja correto e apropriado às circunstâncias. Geralmente, os sistemas são construídos baseado na premissa de que tendo havido validação apropriada, confirmação e testes, a saída será sempre correta. Isto não é sempre verdadeiro.

10.3 Controles criptográficos

Objetivo: Proteger a confidencialidade, autenticidade ou integridade das informações. Sistemas e técnicas criptográficas devem ser usados para a proteção das informações que sejam consideradas em risco e para as quais outros controles não propiciam proteção adequada.

*10.3.1 **Política para o uso de controles criptográficos.***

Uma organização deve desenvolver uma política sobre o uso de controles criptográficos para proteção de suas informações. Uma tal política é necessária para maximizar os benefícios e minimizar os riscos de usar técnicas criptográficas, e evitar uso inapropriado ou incorreto

10.3.2 Criptografia.

Criptografia é uma técnica que pode ser usada para proteger a confidencialidade das informações (encriptação)
Ao se implementar a política de criptografia da organização, devem ser considerados os regulamentos e as restrições nacionais que podem se aplicar ao uso de técnicas criptográficas em diferentes partes do mundo e às questões de fluxo de informações criptografadas entre países.

*10.3.3 **Assinaturas digitais.***

As assinaturas digitais fornecem um meio de proteger a autenticidade e a integridade de documentos eletrônicos

*10.3.4 **Serviços de não-repudiação.***

Serviços de não-repudiação devem ser usados, onde possa ser necessário, para resolver disputas sobre a ocorrência ou não ocorrência de um evento ou ação, por exemplo uma disputa envolvendo o uso de uma assinatura digital em um contrato ou pagamento eletrônico

*10.3.5 **Gerenciamento de chaves.***

10.3.5.1 *Proteção de chaves criptográficas*

O gerenciamento das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia

10.3.5.2 *Padrões, procedimentos e métodos.*

Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para:

a) gerar chaves para sistemas criptográficos diferentes e aplicações diferentes;

b) gerar e obter certificados de chaves públicas;

c) distribuir chaves para os usuários pretendidos, incluindo como as chaves devem ser ativadas ao serem recebidas;

d) armazenar chaves, incluindo como os usuários autorizados obterão acesso às chaves;

10.4 Segurança de arquivos do sistema

Objetivo: Assegurar que os projetos de IT e atividades de suporte sejam conduzidos de uma forma segura. O acesso aos arquivos do sistema deve ser controlado.

Manter a integridade do sistema deve ser responsabilidade da função usuária ou grupo de desenvolvimento ao qual o sistema aplicativo ou software pertence.

10.4.1 Controle de software operacional.

Deve ser fornecido controle para a implementação de software em sistemas operacionais. Para minimizar os riscos de corrupção de sistemas operacionais, os seguintes controles devem ser considerados:

a) A atualização de bibliotecas de programas operacionais deve ser executada somente por um bibliotecário indicado sob autorização da gerência apropriada (ver 10.4.3).

b) Se possível, os sistemas operacionais devem ter apenas código executável.

c) O código executável não deve ser implementado em um sistema operacional até prova de que os testes foram bem-sucedidos e de que a aceitação do usuário foi obtida, e de que as correspondentes bibliotecas-fontes de programas foram atualizadas;

10.4.2 Proteção de dados usados em teste de sistemas.

Dados de teste devem ser protegidos e controlados

10.4.3 Controle de acesso à biblioteca-fonte de programas.

Para reduzir o potencial de corrompimento de programas de computador, deve ser mantido um controle estrito sobre o acesso às bibliotecas-fontes de programas, como se segue (ver também 8.3).

10.5 Segurança nos processos de desenvolvimento e suporte

Objetivo: Manter a segurança dos softwares e das informações de sistemas aplicativos.

Os ambientes de projeto e suporte devem ser estritamente controlados.

Os gerentes responsáveis pelos sistemas aplicativos também devem ser responsáveis pela segurança do ambiente de projeto ou suporte. Eles devem assegurar que todas as alterações propostas nos sistemas sejam revisadas para verificar se elas não comprometem a segurança do sistema ou do ambiente operacional.

10.5.1 Procedimentos para controle de alterações.

Para minimizar o corrompimento dos sistemas de informação, deve existir um controle estrito sobre a implementação de alterações. Procedimentos formais para controle de alterações devem ser obrigatórios

10.5.2 Revisão técnica de alterações em sistemas operacionais.

Periodicamente, é necessário alterar o sistema operacional, por exemplo para instalar uma versão mais recente do software ou *patches* de alterações. Quando as alterações acontecem, os sistemas aplicativos devem ser revisados e testados para assegurar que não existe impacto adverso na operação ou na segurança

10.5.3 Restrições para alterações em pacotes de software.

Modificações em pacotes de software devem ser desencorajadas. Tanto quanto possível, e praticável, pacotes de software fornecidos por revendedor devem ser usados sem modificação

10.5.4 "Covert channels" e código troiano.

Um "covert channel" pode expor informações por alguns meios indiretos e obscuros. Ele pode ser ativado alterando-se um parâmetro acessível tanto por elementos seguros quanto inseguros de um sistema informatizado, ou embutindo-se informações em um fluxo de dados. Código troiano é projetado para afetar um sistema de uma forma que não é autorizada e não é prontamente percebida e não é solicitada pelo receptor ou usuário de um programa.

Onde existir preocupação com "covert channels" ou códigos troianos, os seguintes devem ser considerados:

a) comprar programas apenas de uma fonte de renome;

b) comprar programas em código-fonte apenas se o código puder ser verificado;

c) usar produtos testados e aprovados;

d) inspecionar todo o código-fonte antes do uso operacional;

10.5.5 Desenvolvimento terceirizado de software.

Onde o desenvolvimento de software for terceirizado, os seguintes pontos devem ser considerados:

a) contratos de licenciamento, propriedade do código e direitos de propriedade intelectual (ver 12.1.2);

b) certificação da qualidade e da exatidão do trabalho executado;

c) arranjos para serviços de custódia no caso de falta da terceira parte;

d) direitos de acesso para auditar a qualidade e exatidão do trabalho executado;

e) exigências contratuais para um código de qualidade;

f) testes antes da instalação para detectar código Troiano.

Domínio : 11 Gerenciamento da continuidade do negócio

11.1 Aspectos do gerenciamento da continuidade do negócio

Objetivo: Neutralizar interrupções nas atividades do negócio e proteger processos críticos do negócio contra os efeitos de grandes falhas ou

O gerenciamento da continuidade do negócio deve incluir controles para identificar e reduzir riscos, limitar as conseqüências de incidentes prejudiciais e garantir a retomada em tempo hábil das operações essenciais.

11.1.1 Processo de gerenciamento da continuidade do negócio.

Deve existir um **processo gerencial** em vigor para desenvolver e manter a continuidade do negócio em toda a organização. Ele deve

desastres. Um processo de gerenciamento da continuidade do negócio deve ser implementado para reduzir a perturbação causada por desastres e falhas de segurança (que podem ser resultantes de, por exemplo, desastres naturais, acidentes, falhas em equipamentos e ações deliberadas) a um nível aceitável através da combinação de controles preventivos e de recuperação. As conseqüências de desastres, falhas de segurança e perda de serviços devem ser analisadas. Planos de contingência devem ser desenvolvidos e implementados para assegurar que os processos do negócio podem ser restaurados dentro das réguas de tempo exigidas. Tais planos devem ser atualizados e praticados para se tornarem uma parte integral de todos os outros processos de gerenciamento.	agregar os seguintes elementos chaves do gerenciamento da continuidade do negócio: a) entender os riscos que a organização está enfrentando em termos de sua probabilidade e seu impacto, incluindo uma identificação e priorização dos processos críticos do negócio; b) entender o impacto que provavelmente as interrupções terão sobre o negócio (é importante que sejam encontradas soluções que tratarão incidentes menores, bem como incidentes sérios que poderiam ameaçar a viabilidade da organização), e estabelecer os objetivos para o negócio das facilidades de processamento de informações; ***11.1.2 Continuidade do negócio e análise de impacto.*** A continuidade do negócio deve começar pela identificação de eventos que possam causar interrupções nos processos do negócio, tais como falhas em equipamento, incêndios e inundações. Isto deve ser seguido por uma avaliação de riscos para determinar o impacto daquelas interrupções (tanto em termos de escala de danos quanto de período para recuperação). ***11.1.3 Definição e implementação de planos de continuidade.*** Devem ser desenvolvidos planos para manter ou restaurar as operações do negócio nas réguas de tempo exigidas seguintes à interrupção, ou falha, nos processos críticos do negócio ***11.1.4 Estrutura para o planejamento da continuidade do negócio.*** Deve ser mantida uma única estrutura para os planos de continuidade do negócio, para garantir que todos os planos sejam consistentes e para identificar prioridades para testes e manutenção Cada plano deve ter um proprietário específico. Procedimentos de emergência, planos de *fallback* manuais e planos de retomada devem estar dentro da responsabilidade dos proprietários dos recursos ou processos do negócio envolvidos ***11.1.5 Testes, manutenção e reavaliação dos planos para continuidade do negócio.*** *11.1.5.1 Testes dos planos* Os planos para continuidade do negócio podem falhar ao serem testados, freqüentemente devido a suposições incorretas, omissões ou mudanças em equipamentos ou pessoal **11.1.5.2** *Manutenção e reavalização dos planos* Os planos para continuidade do negócio devem passar por revisões e atualizações regulares para garantir sua eficácia continuada (ver

	11.1.5.1 até 11.1.5.3). Devem ser incluídos procedimentos dentro do programa de gerenciamento de mudanças da organização para garantir que as questões relacionadas com a continuidade do negócio sejam tratadas adequadamente. Exemplos de situações que podem exigir a atualização dos planos incluem a aquisição de novos equipamentos, ou *upgrade* de sistemas operacionais e alterações em: a) pessoal b) endereços ou números de telefone c) estratégia do negócio; d) localização, instalações e recursos;

Dominio : **12 Obediência a exigências**

12.1 Obediência às exigências legais

Objetivo: Evitar infração de qualquer lei civil e criminal, estatutária, regulamentadora ou de obrigações contratuais e de quaisquer requisitos de segurança.

O projeto, operação, uso e gerenciamento de sistemas de informações podem estar sujeitos a exigências de segurança estatutárias, regulamentadoras e contratuais.

Deve ser buscado aconselhamento sobre exigências legais específicas com os consultores jurídicos da organização, ou profissionais adequadamente qualificados. As exigências da legislação variam de país para país e para informações geradas em um país que são transmitidas para outro país (por exemplo, fluxo de dados entre países).

12.1.1 Identificação da legislação aplicável.

Todas as exigências contratuais, estatutárias e regulamentadoras relevantes devem ser explicitamente definidas e documentadas para cada sistema de informações. Os controles específicos e as responsabilidades individuais para satisfazer estas exigências devem estar similarmente definidos e documentados

12.1.2 Direitos de propriedade industrial (IPR)

12.1.2.1 *Copyright.*

Procedimentos apropriados devem ser implementados para garantir a observância de restrições legais quanto ao uso de material para o qual podem existir direitos de propriedade intelectual, tais como *copyright*, direitos de projeto e marcas registradas. Violação de *copyrights* pode levar a ações legais que podem envolver processo criminal.

12.1.2.2 *Copyright de softwares.*

Produtos de software proprietários geralmente são fornecidos sob um contrato de licenciamento que limita o uso dos produtos a máquinas especificadas e pode permitir cópias apenas para a criação de *backups*. Os seguintes controles devem ser considerados:

a) publicar uma política de obediência a *copyright* de *software*, que define o uso legal dos *softwares* e produtos de informação;

b) emitir padrões para os procedimentos de aquisição de produtos de *software*;

12.1.3 Salvaguarda de registros organizacionais.

Registros importantes de uma organização devem ser protegidos contra perda, destruição e falsificação. Alguns registros podem precisar ser guardados em segurança para satisfazer exigências estatutárias ou regulamentadoras, bem como para apoiar atividades essenciais do negócio. Exemplos destes são registros que podem ser exigidos como prova de que uma organização opera dentro das normas estatutárias ou regulamentadoras, ou para assegurar defesa adequada contra potencial ação criminal ou civil, ou para confirmar o status financeiro de uma organização com respeito a acionistas, parceiros e auditores. O período de tempo e os conteúdos de dados para retenção das informações podem ser definidos por lei ou regulamento nacional.

12.1.4 Proteção de dados e privacidade de informações pessoais.

Diversos países introduziram legislação que coloca controles no processamento e transmissão de dados pessoais (geralmente informações sobre pessoas vivas, que podem ser identificadas a partir daquelas informações). Tais controles podem impor obrigações para aqueles que coletam, processam e disseminam informações pessoais, e podem restringir a capacidade de transferir aqueles dados para outros países.

12.1.5 Prevenção de utilização indevida das facilidades de processamento de informações.

As facilidades de processamento de informações de uma organização são fornecidas para os fins do negócio. A gerência deve autorizar o seu uso. Qualquer utilização destas facilidades para propósitos não autorizados ou não relacionados ao negócio, sem aprovação da gerência, deve ser considerada como uso impróprio das facilidades. Se tal atividade for identificada pelo monitoramento ou outros meios, ela deve ser trazida à atenção do gerente individual envolvido, para a ação disciplinar apropriada.
Muitos países têm, ou estão em processo de implantar, legislação para proteger contra má utilização de computadores. Pode ser uma ofensa criminal usar um computador para propósitos não autorizados

12.1.6 Regulamentação de controles criptográficos.

Alguns países implementaram acordos, leis, regulamentos ou outros instrumentos para controlar o acesso a controles criptográficos ou o seu uso. Tais controles podem incluir:

a) importação e/ou exportação de hardware e software de computadores para executar funções criptográficas;

12.1.7 Coleta de provas.

12.1.7.1 *Regras para provas*

É necessário ter provas adequadas para apoiar uma ação contra uma pessoa ou organização. Sempre que esta ação for uma questão disciplinar interna, a prova necessária estará descrita pelos procedimentos internos.

Onde a ação envolver a lei, seja civil ou criminal, a prova apresentada deve se conformar com as regras para provas definidas na lei relevante ou nas regras do tribunal específico em que o caso será ouvido. Em geral, estas regras cobrem:

a) a admissibilidade da prova: se a prova pode ou não ser usada em tribunal;

b) o peso da prova: a qualidade e a completitude da prova;

c) comprovação adequada de que os controles funcionaram corretamente e consistentemente (isto é, prova de controle do processo) durante todo o período que a prova a ser recuperada foi armazenada e processada pelo sistema.

12.1.7.2 *Admissibilidade da prova*
Para obter a admissibilidade da prova, as organizações devem se assegurar de que seus sistemas de informações obedecem a algum padrão ou código de prática publicado sobre produção de prova admissível

12.1.7.3 *Qualidade e completitude da prova*

Para obter qualidade e completitude da prova, é necessário um sólido rastreamento da prova. Em geral, tal rastreamento sólido pode ser estabelecido sob as seguintes condições:

a) Para documentos em papel: o original é mantido em segurança e foi registrado quem o encontrou, onde foi encontrado, quando foi encontrado e quem testemunhou a descoberta. Qualquer investigação deve assegurar que os originais não foram adulterados.

12.2 Revisões da política de segurança e obediência técnica Objectivo: Garantir a obediência dos sistemas às políticas e padrões de segurança da organização. A segurança de sistemas de informações deve ser revisada regularmente. Tais revisões devem ser executadas de acordo com as políticas de segurança apropriadas, e as plataformas técnicas e os sistemas de informação devem ser auditados quanto ao cumprimento dos padrões de implementação de segurança.	*12.2.1 Obediência à política de segurança.* Os gerentes devem se assegurar de que todos os procedimentos de segurança dentro de suas áreas de responsabilidade são executados correctamente. Além disso, todas as áreas dentro da organização devem ser consideradas para revisão regular, a fim de garantir a obediência aos padrões e políticas de segurança. Estas devem incluir o seguinte: a) sistemas de informações; b) provedores de sistemas; c) proprietários das informações e activos de informação; d) usuários; e) gerência. *12.2.2 Verificação da obediência técnica* Os sistemas de informação devem ser verificados regularmente quanto à obediência aos padrões de implementação de segurança. A verificação da obediência técnica envolve o exame de sistemas operacionais para garantir que os controles de hardware e software foram correctamente implementados Este tipo de verificação de obediência exige assistência técnica especializada. Deve ser executada manualmente (apoiada por ferramentas de software apropriadas, se necessário) por um engenheiro de sistemas experiente, ou por um pacote de software automatizado que gere um relatório técnico para subsequente interpretação por um especialista técnico. A verificação da obediência cobre também, por exemplo, testes de penetração, que podem ser executados por especialistas independentes contratados especificamente para este propósito. Isto pode ser útil para detectar vulnerabilidades no sistema e para verificar quão eficazes os controles são na prevenção de acesso não autorizado devido a estas vulnerabilidades
12.3 Considerações para auditoria de sistemas Objectivo: Maximizar a eficácia do processo de auditoria de sistemas; minimizar a interferência do processo de auditoria nos negócios; minimizar interferências no processo de auditoria. Devem existir controles para salvaguardar os sistemas operacionais e as ferramentas de	*12.3.1 Controles para auditoria de sistemas.* Requisitos de auditoria e actividades envolvendo verificações em sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar o risco de perturbações nos processos do negócio. O seguinte deve ser observado: a) Requisitos de auditoria devem ser acordados com a gerência apropriada. b) O escopo das verificações deve ser acordado e controlado.

auditoria durante auditorias de sistemas. Protecção também é exigida para salvaguardar a integridade e impedir a utilização indevida das ferramentas de auditoria.	*12.3.2 **Protecção das ferramentas de auditoria de sistemas.*** O acesso às ferramentas de auditoria de sistemas, ou seja software ou arquivos de dados, deve ser protegido para impedir qualquer possível utilização indevida ou comprometimento. Tais ferramentas devem ser separadas dos sistemas operacionais e de desenvolvimento e não devem ser mantidas em bibliotecas de fitas ou áreas de usuários, a não ser que recebam um nível adequado de proteção adicional.