# SEGURANÇA INFORMÁTICA EM AUDITORIA

O objectivo deste trabalho é apresentar os aspectos mais relevantes da auditoria da segurança informática relacionando-os com os standards mais importantes. Pretende-se um documento que aborde a questão sem recorrer a designações e siglas complexas e habituais nos textos de tecnologias de informação e comunicação (TIC). O ideal seria conseguir um documento capaz de ser compreendido por todos os profissionais, mesmo que não possuam conhecimentos profundos no domínio da informática ou da auditoria.

José Maria Pedro

Julho de 2005

**INTRODUÇÃO** ..... 4

**OS ANÉIS DA INSEGURANÇA INFORMÁTICA** ..... 6

**ANÁLISE DE RISCO NA AUDITORIA DA SEGURANÇA INFORMÁTICA** ..... 10

**A AVALIAÇÃO DO CONTROLO INTERNO NA AUDITORIA DE SEGURANÇA INFORMÁTICA** ..... 15

**A segurança nos Controlos Gerais das Tecnologias de Informação (CGTI)** ..... 16
a. Comunicações e WEB (Internet, Extranet e Intranet) ..... 16
b. Utilizadores, acessos e autenticação ..... 18
c. Instalações, ambiente e segurança física ..... 19
d. Software de Sistema ..... 19
e. Hardware ..... 19
f. Negócio: Continuidade e Recuperação de Desastres ..... 20

**A Segurança nos Controlos Aplicacionais** ..... 21
a. Software aplicacional ..... 21
b. DADOS, Classificação e Controlo ..... 23

**A segurança nos Controlos de Utilização** ..... 23

**CONCLUSÃO** ..... 24

**ANEXO - OS STANDARDS DE AUDITORIA DA SEGURANÇA INFORMÁTICA** ..... 26

**CobiT – Control Objectives for Information Technology** ..... 26

**COSO - Committee of Sponsoring Organizations of the Treadway Commission** ..... 30

**ISO/IEC 17799:2000 - Code of Practice for Information Security Management** ..... 31

**ISO/IEC TR 13335** ..... 34

**ISO/IEC 15408** ..... 36

**ISO/IEC 21827:2002(E)** ..... 37

**ITIL** ..... 39

**NIST 800-14** ..... 41

**OECD's Guidelines for the Security of Information Systems** ..... 42

**TickIT** ..... 43

**BIBLIOGRAFIA** ..... 45

**LOCAIS A VISITAR NA INTERNET.....46**

# Introdução

De todas as mudanças empresariais até agora, nenhuma foi tão significativa para os profissionais de controlo como a provocada pelas TIC nos últimos trinta anos. O aparecimento da Internet e a sua utilização generalizada para efectuar transacções, na sua maior parte com significado, quer sejam financeiras quer sejam de qualquer outra natureza, condicionaram decisivamente o trabalho dos profissionais de auditoria.

Tomando a banca como exemplo, é hoje possível para um cliente realizar movimentos entre as suas contas mediante o acesso a um website. O cliente pode estar em qualquer parte do globo sem limites geográficos, políticos, físicos ou legais. Também empresas das mais variadas áreas de negócio se servem das tecnologias de informação para integrar os seus sistemas internos e proporcionar interfaces aos seus parceiros que permitam todo o tipo de transacções.

Os circuitos de informação flexibilizaram-se, tornaram-se mais virtuais e deixaram de ser tão fixos como eram conhecidos tradicionalmente. Os suportes de informação tornaram-se voláteis, a fiabilidade dos documentos sobre papel ou electrónicos é mais questionável actualmente.

Nesta fase os profissionais de auditoria sem competências profissionais no domínio das tecnologias de informação perdem a possibilidade de contacto com os suportes de informação e com os dados que eles contêm. A vida complica-se seriamente para os agentes de controlo pouco qualificados!

Entre nós e de acordo com o Banco de Portugal[1], os dados da utilização dos instrumentos de pagamento, de 1989 a 2002, revelam uma tendência muito favorável para os instrumentos electrónicos de pagamento. O rácio "notas e moedas/PIB" variou de 7% para 3,5%, aproximadamente, a parte das transacções por cheque no total variou de 80% para cerca de 30% e a parte das transacções por cartão de pagamento evoluiu de 2% para 57%. Estes

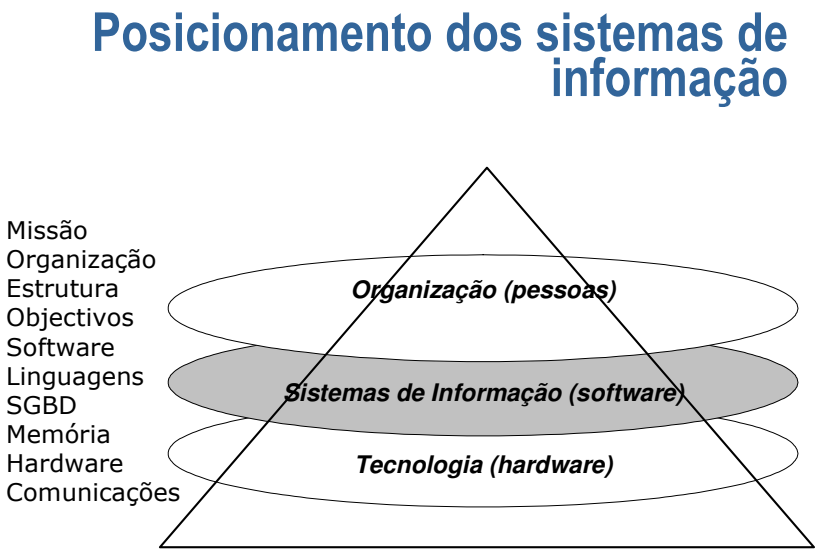
[1] Consulte http://www.bportugal.pt/; http://www.oecd.org/, http://www.ine.pt/ e http://epp.eurostat.cec.eu.int/ para mais dados sobre esta questão;

números significam uma revolução nos suportes da informação relativos às transacções e um acréscimo nas dificuldades de auditar e certificar transacções.

Esta realidade não é exclusivamente portuguesa, segundo a literatura da especialidade, actualmente as maiores empresas mundiais e cerca de metade das grandes corporações internacionais estão centradas na segunda fase do negócio pela Internet (transacções) obtendo grandes benefícios.

O comércio electrónico é um tema incontornável na economia mundial que afecta Instrumentos Legais associados às transacções económicas, Normas e Metodologias Contabilísticas, Normas e Metodologias de Auditoria.

A visão tradicional da empresa associando-a a um simples organigrama, está hoje modificada pela presença das TIC, a estrutura organizacional suporta maior dispersão das pessoas devido aos meios de comunicação disponíveis, apresenta-se mais difusa e assenta sobre softwares que são sistemas de informação submersos em tecnologia que recolhe, processa, guarda e transporta a informação através de toda a organização. Podemos perspectivar esta nova realidade no seguinte esquema:



Os procedimentos de auditoria direccionados apenas ao nível organizacional superior através de contactos pessoais são insuficientes para obter a evidência suficiente na formação da opinião do auditor porque ignoram o software e o hardware, ou seja, os sistemas de informação e a tecnologia.

A segurança informática é uma consequência desta nova realidade, um aspecto particular da maior importância porque está ligada a todos os sistemas de informação na empresa. Constitui uma preocupação maior na actualidade e continuará a condicionar a fiabilidade dos dados no futuro.

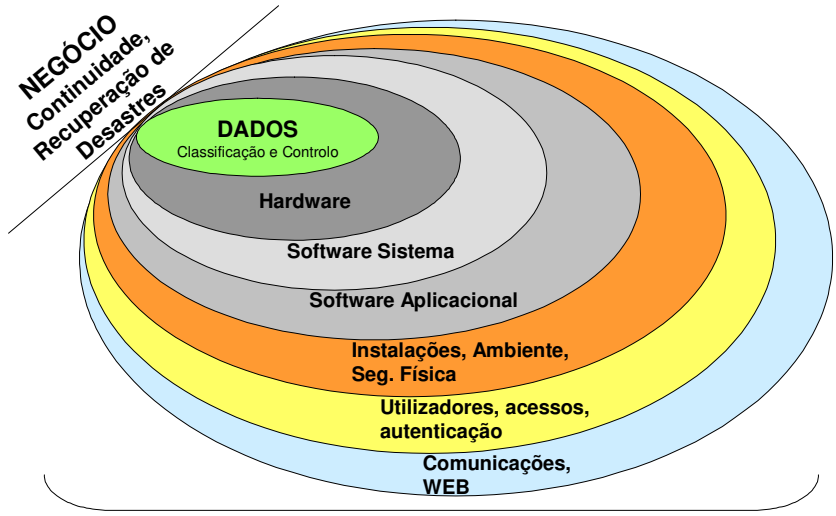
A análise dos aspectos mais relevantes e actuais da segurança informática relacionando-a com a auditoria obriga-nos a apresentar de forma sumária em primeiro lugar os standards de segurança informática. Com efeito a auditoria faz-se de competências profissionais e de standards de referência aceites de forma generalizada.

## Os Anéis da Insegurança Informática

Naturalmente que ao falar de informática estamos a referir-nos a informação automática que flúi através de uma sucessão de camadas ou anéis que começam quando alguém entra em contacto com uma dada empresa ou organização e acabam nos dados relativos a todos os factos relevantes que ocorrem. Incluímos neste conceito todos os circuitos de informação bem como a infraestrutura que os suporta.

Para ilustrar esta ideia de forma clara, apresentamos o seguinte esquema onde o negócio aparece sustentado por anéis sucessivos que condicionam a segurança e fiabilidade dos dados e podem afectar seriamente a continuidade do negócio ou mesmo a sobrevivência da empresa quando o recurso às TIC é generalizado.

**Figura 1 – Os Anéis da Segurança Informática**




Cada um destes anéis coloca problemas particulares que importa analisar para compreender até que ponto a auditoria deve ir. Por sua vez, todo este conjunto de anéis é condicionado pelas políticas e princípios de segurança adoptados na organização em causa e pelos graus de conformidade com os standards, com a legalidade e com princípios de gestão de risco usados como referencial.

Para entender a ideia de sustentação do negócio pelos anéis é preciso raciocinar com base em organizações onde a actividade operacional não pode funcionar sem as TIC. Lembre-se do sector financeiro (bancos e seguros) onde é praticamente impossível o funcionamento quando as TIC falham. Um banco pode ir à falência se a confiança nos seus sistemas for abalada de forma sistemática.

De acordo com Ernst Jan Oud[2] podemos organizar os standards de TIC mais conhecidos em nove títulos principais:

- **Gestão de TI** (COBIT[3], BS15000, Microsoft Operations Framework e ITIL);

[2] Auditor de SI certificado pela associação americana ISACA. Publicou um artigo recente "The value to IT of Using International Standards, in Informations Systems Control Journal da ISACA, Vol 3, 2005;

- **Gestão de Projectos** (PRINCE2 e PMBOK);
- **Gestão de Segurança** (ISO13335, ISO13569 para os serviços financeiros, ISO17799/BS7799-2 muito traduzidos e adaptados por esse mundo fora, ITBaseline Protection Manual alemão, ACSI-33[4] australiano, numerosos da NIST[5] americana, COBIT Security Baseline, ENV12924 para SI médicos, Information Security Fórum *Standard of Good Pratice[6]);*
- **Gestão da Qualidade** (ISO9001, EFQM e Baldrige National Quality Plan);
- **Desenvolvimento de Software** (TickIT, Capability Maturity Model Integration – Software Engineering Institute);
- **Governo de TI** (COBIT, IT Governance Implementing Guide, COSO Internal Control – Integrated Framework, e AS8015-2005 australiano);
- **Gestão de Risco** (AS/NZS4360 australiano[7]);
- **Planos de Continuidade de Negócio** (PAS-56 da British Standards Institution e HB221-2004 Australiano).

Nem todos são utilizados da mesma forma e com a mesma frequência, alguns têm maior divulgação.

A gestão da segurança está intimamente ligada à gestão do risco empresarial e não é possível abordar o tema sem uma visão universal do que existe actualmente sobre a matéria. As propostas mais defendidas actualmente pelos profissionais de TIC baseiam-se em diversos modelos aceites internacionalmente. A teoria dos anéis que apresentamos anteriormente é uma síntese simplificadora da enorme variedade de fontes que existem. A tabela abaixo apresenta uma lista dos referenciais internacionais mais conhecidos e mais utilizados.

**ALGUNS REFERENCIAIS INTERNACIONAIS USADOS EM SEGURANÇA INFORMÁTICA[8]**

---

[3] www.bsi-global;
[4] www.dsd.gov.au/infosec/publications/acsi33.html - instruções para a segurança das comunicações electrónicas Australianas;
[5] www.nist.gov;
[6] www.isfsecuritystandard.com;
[7] www.standards.com.au
[8] SINFIC - Newsletter Sinfic Insight n.º15 - ERM (Enterprise Risk Management);

| Referência | Objectivo | Audiência Alvo | Entidade Emitente |
|---|---|---|---|
| CobiT | Objectivos de Controlo de Governação de TIC (uso diário) | Gestores de Topo, Gestores de TIC, Utilizadores e Auditores | IT Governance Institute[9] |
| COSO | Gestão e Controlo do Risco das Organizações | CIO, CEO, CFO, CxOs, Utilizadores e Auditores Internos | Committee of Sponsoring Organizations of the Tradeway Comission (COSO), USA |
| ITIL | Abordagem para Fornecedores de Serviços de Gestão de TIC | Pessoas Responsáveis por Serviços de Gestão de TIC | British Office of Government Commerce (OCG) UK. |
| ISO/IEC 17799:2000 | Orientações para Implementação da Segurança da Informação | Pessoas Responsáveis pela Segurança da Informação | International Organizational for Standardization and International Electrotechnical Comission Joint Technical Committee (ISO/IEC JTC 1), Switzerland |
| ISO/IEC TR 13335 | Orientações sobre aspectos da Gestão da Segurança de TIC | Gestores Seniores e Pessoas Responsáveis pela Medição da Segurança de TIC | International Organizational for Standardization and International Electrotechnical Comission Joint Technical Committee (ISO/IEC JTC 1), Switzerland |
| ISO/IEC 15408 | Definição de Critérios para Avaliação da Segurança da Informação | Consumidores, Programadores e Avaliadores | International Organizational for Standardization and International Electrotechnical Comission Joint Technical Committee (ISO/IEC JTC 1), Switzerland |
| NIST 800-14 | "Baseline" para o Estabelecimento e Revisão de Planos de Segurança de TIC | Terceiras Partes Responsáveis pela Segurança de TIC para Organizações Governamentais | Computer Security Resource Centre (CSRC), National Institute of Standards and Technology (NIST), US Department of Commerce, USA |
| OCDE | Orientações para a Segurança dos Sistemas de Informação | Gestores, CIO, CEO, CFO, utilizadores | OCDE |
| TickIT | Sistemas de Gestão da Qualidade para Desenvolvimento de Software e Critérios de Certificação | Clientes, Fornecedores e Auditores | TickIT Office, British Standards Institute (BSI), UK |

Os profissionais de auditoria informática, na prática escolhem um destes standards ou uma parte deles em função das necessidades de cada missão. O ISO/IEC 17799[10] e o COBIT são talvez os mais utilizados actualmente.

A Comissão Europeia está a proceder à alteração do Reg EC nº 1663/95 com regras detalhadas relativas aos procedimentos de aprovação das contas do FEOGA Garantia e Orientação, exigindo uma certificação de segurança dos sistemas de informação além da tradicional certificação de contas anual. Esta certificação de segurança dos sistemas de informação não se dirige exclusivamente à tecnologia e deverá ser efectuada com base num dos referenciais internacionais de segurança informática combinado com uma escala de níveis feita com o CMM (Capability Maturity Model)

As normas referenciais sugeridas foram o ISO/IEC17799, o BSI (norma alemã do tipo do ISO/IEC 17799, mas mais pormenorizada) e o COBIT. Até ao momento o ISO/IEC17799 foi preferido pela maioria das autoridades de pagamento dos estados europeus para efectuar esta

[9] O COBIT tem sido amplamente patrocinado pela associação americana Information Systems Auditing and Control Association (www.isaca.org);
[10] ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission)

certificação de segurança dos sistemas de informação. A adopção deste standard pelos estados europeus dar-lhe-á maior divulgação e projecção internacional. Por outro lado, os estados poderão vir a adoptar a mesma exigência para acompanhar a certificação das contas públicas.

Trata-se de uma exigência forte em termos de sistemas de informação, o standard ISO17799 é bastante exigente e se for combinado com os níveis de maturidade do CMM, dá chumbo certo a qualquer sistema de informação de perfil mediano nas empresas portuguesas. Provavelmente, tendo em conta a tendência dos portugueses para a intuição e aversão a sistemas rígidos, só o sector financeiro estará em condições de situar os seus processos de TIC acima do nível 2 do CMM.

Mostramos em anexo uma síntese de cada um destes standards, embora sem grande profundidade, para fornecer uma ideia objectiva do seu conteúdo a usar na opção por cada um deles durante o processo de auditoria.

## Análise de Risco na Auditoria da Segurança Informática

Apesar da existência de uma infinidade de standards em permanente actualização que acompanham o ritmo de evolução das tecnologias de informação e comunicação, ainda não existe uma metodologia aceite generalizadamente para a auditoria da segurança informática.

A maior parte dos textos de auditoria informática abordam a questão do risco quando se fala em segurança. Isto acontece porque os riscos têm incrementado em espiral nos sistemas de informação desde que as tecnologias de informação foram adoptadas generalizadamente. A análise de risco está sempre orientada para proteger alguém, pode proteger o auditor ou pode proteger a empresa.

Actualmente existem várias correntes metodológicas, mas podemos reduzir todo o conjunto a duas grandes lógicas de acção, uma dirigida à protecção do auditor e outra à protecção da organização. Assumimos então que existem em auditoria informática duas visões do risco:

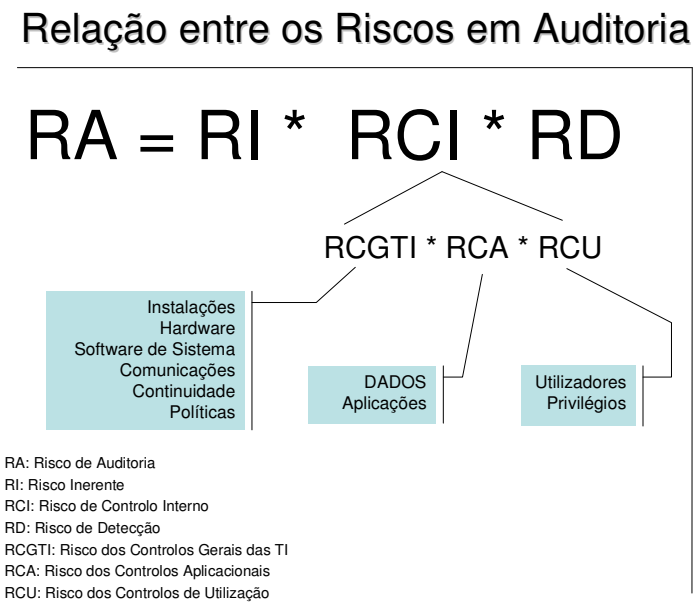
a. **Análise de Risco da Auditoria:** orientada para redução do risco do auditor poder emitir uma opinião incorrecta. A primeira preocupação do auditor é obter informação suficiente para emitir uma opinião adequada. Para além do risco de auditoria, o auditor está também exposto a perdas e danos no exercício da sua actividade profissional resultante de litígios, publicidade adversa ou outros eventos, que surjam em conexão com a informação que ele examinou e sobre as quais emitiu uma opinião;

b. **Análise de Risco da Organização:** orientada para os riscos que a empresa corre ao depender em absoluto de sistemas de informação automatizados. A primeira preocupação da empresa é funcionar sem acidentes de percurso e sem falhas dos sistemas de informação que são essenciais aos objectivos do negócio. Os riscos são analisados nos processos associados à função informática na empresa, discutindo as exigências que podem ser feitas aos sistemas de informação e aos recursos envolvidos. O COBIT é o melhor exemplo desta corrente.

Vamos abordar a perspectiva da Análise de Risco da auditoria (protecção do auditor). Durante a minha experiência de ensino na área de auditoria informática, um dos processos mais fáceis de explicar a profissionais de informática o que se faz em auditoria, foi a utilização do Standard de Auditoria relativo à análise de risco. Por um lado, os profissionais de auditoria captam facilmente o problema dos anéis quando é apresentado na lógica da análise de risco porque a conhecem bem. Por outro lado, os profissionais de informática gostam de esquemas, usam-nos no seu dia-a-dia com tanta frequência que acabam por apreender rapidamente os conceitos transmitidos por esta via.

Observe o esquema seguinte preparado com base na norma dedicada à Avaliação do Risco em Auditoria, pode vê-la no site da Ordem dos Revisores Oficiais de Contas (OROC)[11]:

[11] http://www.cidadevirtual.pt/croc/index.html




Esta norma/standard de auditoria proporciona orientação aos profissionais de auditoria[12] na avaliação do risco de auditoria e seus componentes: risco inerente, risco de controlo e risco de detecção[13].

A norma coloca em primeiro plano o risco da auditoria para o auditor que é a entidade a proteger. A norma não é dirigida ao risco da organização na perspectiva global do COSO que refere o risco empresarial nos seguintes termos:

*"Gestão do risco empresarial é um processo, levado a efeito pelo quadro de directores de uma entidade, gestores e outro pessoal, aplicado na definição da estratégia em toda a empresa, desenhado para identificar potenciais acontecimentos que podem afectar a entidade, e para gerir o risco mantendo-o em níveis aceitáveis, tendo em vista oferecer segurança razoável relativamente à concretização dos objectivos da entidade"*[14]

[12] os ROC são um exemplo destes profissionais
[13] A fórmula apresentada pela OROC, que traduz um dos modelos existentes para a avaliação do risco de revisão/auditoria, descreve o risco de revisão/auditoria não nos três componentes de risco aqui apresentados, mas através de quatro componentes do risco. O risco de detecção é dividido em duas componentes: o risco dos procedimentos analíticos e outros relevantes testes substantivos poderem falhar na detecção de distorções iguais às distorções toleráveis e o risco tolerável de aceitação incorrecta para os testes substantivos de pormenor.
[14] O texto original é o seguinte: "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"

A necessidade de determinação do risco vem referida no parágrafo 15 das Normas Técnicas de Revisão/Auditoria seguidas pelos ROC: *"15. O revisor/auditor deve planear o trabalho de campo e estabelecer a natureza, extensão, profundidade e oportunidade dos procedimentos a adoptar, com vista a atingir o nível de segurança que deve proporcionar e tendo em conta a sua determinação do risco da revisão/auditoria e a sua definição dos limites de materialidade."*

O que se pretende dizer com o esquema é, em primeiro lugar, que o risco da auditoria provém de três fontes principais que podem ser decompostas noutras dimensões específicas como veremos mais à frente. Uma adaptação das definições com base no conceito de "susceptibilidade" na norma para a auditoria informática, ampliando o conteúdo de "dados financeiros" para "qualquer informação produzida por qualquer sistema de informação", pode resultar nas seguintes definições:

- **Risco de auditoria**: é a susceptibilidade do auditor dar uma opinião de auditoria não apropriada quando uma informação produzida pelo sistema esteja distorcida de forma materialmente relevante.

- **Risco inerente**: é a susceptibilidade de uma informação conter uma distorção que possa ser materialmente relevante, considerada individualmente ou quando agregada com distorções em outros dados, assumindo que não existem os respectivos controlos internos.

- **Risco de controlo interno**: é a susceptibilidade de uma distorção, que possa ocorrer numa informação e que possa ser materialmente relevante, considerada individualmente ou quando agregada com distorções em outros dados, não vir a ser prevenida ou detectada e corrigida atempadamente pelo sistema de controlo interno. "*O conceito de controlo interno faz parte do processo de gestão. É constituído pelas acções tomadas pela gestão para planear, organizar e dirigir as suficientes acções que providenciem adequada certeza que os seguintes objectivos são atingidos:*

    - *cumprimento de metas estabelecidas para os programas e operações;*
    - *uso económico e eficiente dos recursos;*
    - *salvaguarda de recursos;*

- *fiabilidade e integridade da informação;*
- *conformidade com as políticas, planos, procedimentos, leis e regulamentos" (Institutr of Internal Auditors)*[15].

- **Risco de detecção**: é a susceptibilidade dos procedimentos substantivos executados pelo auditor não virem a detectar uma distorção que exista numa informação que possa ser materialmente relevante, considerada individualmente ou quando agregada com distorções em outros dados.

Não estamos preocupados em analisar as TIC como instrumento de auditoria. Interessa-nos sobretudo a análise das TIC como fonte de risco para a auditoria.

As TIC intervêm como instrumento na avaliação de qualquer destes três tipos de risco associados ao risco de auditoria nos termos em que o definimos. As TIC são determinantes como condicionantes do risco em qualquer dos três tipos de risco (inerente, controlo, detecção), mas onde assumem um papel verdadeiramente decisivo é no controlo interno.

O controlo interno, montado tradicionalmente com base em encontros e desencontros de documentos nos circuitos de informação, ou através da comparação dos dados de várias fontes e circuitos, passou progressivamente para dentro do software e hardware. A célebre comparação da guia de entrada em armazém com a factura para autorizar a emissão do cheque, em muitos casos, já não pode ser feita com recurso ao papel porque o que existe actualmente são transacções gravadas pelo software em estruturas de dados complexas.

Hoje, não é possível avaliar adequadamente o controlo interno sem ter em conta as TIC, porque os dados circulam electronicamente e são tratados por software posto em acção por utilizadores autorizados pelo seu user/password que alguém deve gerir. Actualmente, há poucos sistemas de informação que não recorram a algum hardware e software.

A análise dos referenciais internacionais usados em segurança informática é da máxima importância para quem precisar de fundamentar a sua opinião. Como os standards nasceram de motivações diferentes, algumas pouco relacionadas com a auditoria, revelam muitas zonas de sobreposição e várias perspectivas de abordagem em função das preocupações de cada grupo que as desenvolveu.

A abrangência e actualidade são determinantes na escolha de um standard para aplicar. O ISO/IEC 17799 tem-se mostrado irresistível porque é amplo e surgiu relativamente cedo na sequência de publicação e divulgação dos standards. O COBIT tem sido defendido pela associação americana Information Systems and Control Association[16] que se sustenta em milhares de auditores certificados de sistemas de informação (os CISA e os CISM[17]) e pela utilização de recursos electrónicos bastante ricos para os seus membros espalhados por todo o mundo.

## A avaliação do controlo interno na auditoria de segurança informática

Por necessidade de organização do trabalho de auditoria, separamos os anéis[18] relativos à segurança informática em vários componentes relevantes para avaliar o risco de controlo interno:

- Controlos Gerais das Tecnologias de Informação (CGTI): compreendem tudo o que diz respeito à infraestrutura das TIC bem como a continuidade de negócio e recuperação de desastres nas TIC, políticas e princípios de segurança organizacional, conformidade, legalidade e gestão de risco.

- Controlos Aplicacionais (CA): compreendem a análise do software aplicacional e dos respectivos dados. Naturalmente que a análise de dados feita no âmbito dos controlos aplicacionais se destina a recolher evidência sobre conformidade, a análise substantiva será efectuada posteriormente;

- Controlos de Utilização (CU): compreendem as questões directamente relacionadas com os utilizadores dos sistemas de informação[19]. Podemos incluir neste ponto as questões relacionadas com as necessidades e a utilidade da informação;

---

[15] veja www.theiia.org
[16] veja www.isaca.org
[17] CISA = Certified Information Systems Auditor; CISM = Certified Information Security Manager

***A segurança nos Controlos Gerais das Tecnologias de Informação (CGTI)***

De acordo com o esquema da Figura 1 – Os Anéis da Segurança Informática, os CGTI são a base dos mecanismos de controlo interno porque incluem aspectos de infraestrutura. Funciona como o esqueleto da segurança e controlo das TIC numa organização. Vamos tentar mostrar a importância de cada um dos anéis e a forma como podem condicionar a segurança e o risco da auditoria.

***a. Comunicações e WEB (Internet, Extranet e Intranet)***

Nenhuma organização pública ou privada pode funcionar e ser eficiente sem comunicação entre os seus colaboradores. Actualmente, a redução de custos está irremediavelmente associada aos meios de comunicação aplicados aos diferentes processos na cadeia de valor das empresas.

Há um papel crescente desempenhado pelas redes e pelos sistemas de informação na actualidade que importa conhecer e proteger porque estamos a assistir a muitos modos de condicionamento destes meios por indivíduos sem qualquer responsabilidade social espalhados pelo globo. Sempre existiram pessoas deste género, mas nunca tiveram tanto poder para afectar tanto a sociedade.

As consequências são dramáticas para algumas empresas, a indisponibilidade temporária dos sistemas, as falhas de desempenho ou o funcionamento incorrecto, condicionam negativamente os processos de negócio afastando os clientes das empresas que dependem destes meios de comunicação.

Algumas organizações tomaram iniciativas no sentido de prevenir esta ameaça:

---

[18] Veja o esquema dos anéis de insegurança que apresentámos no início deste trabalho.

[19] Alguns autores incluem os controlos de utilização nos controlos aplicacionais. Esta opção pode ser útil em alguns casos, mas em regra é melhor separar a utilização porque cobre aspectos relacionados com a necessidade de informação para determinadas funções e processos de negócio

- **OCDE**: Em Setembro de 2002, depois dos acontecimentos do 11 de Setembro publicou as *Guidelines for the Security of Information Systems* manifestando as preocupações neste domínio;

- **ENISA**[20]: Foi criada pela União Europeia para responder às preocupações com as infraestruturas de comunicação na Europa.

A segurança das telecomunicações compreende várias dimensões:

- Segurança no acesso interno às redes
- Segurança no acesso externo às redes
- Segurança no envio de informação
- Segurança de circuitos

Começando com o acesso interno às redes, de forma controlada com autorização de alguém responsável pela segurança, com registo e análise periódica dos acessos. Convém lembrar que segundo algumas estatísticas, mais de metade dos acessos indevidos e intrusão são originados a partir do interior das organizações.

A segurança no acesso externo às redes é outra grande preocupação quando existem entidades externas à organização que acedem à rede. Todos os acessos concedidos devem ser autorizados e atribuídos pelo responsável de segurança com análise periódica de quem entrou. Além da verificação de *login*, é conveniente estabelecer outros tipos de verificações que permitam identificar eventuais piratas informáticos.

O serviço de Internet deve ser devidamente protegido, tal como o envio de informação e a transferência de dados para fora da rede com encriptação de dados confidenciais.

Outro grande problema actual é a multiplicidade de vírus produzidos diariamente que entram através das ligações de rede. Ter um antivírus eficaz e actualizado instalado nos servidores da rede e em todos os computadores pessoais é uma condição base de sobrevivência de toda a rede.

[20] ENISA = European Network and Information Security Agency. Veja em http://europa.eu.int/agencies/enisa/index_en.htm

A segurança de circuitos com meios de protecção adequados, designadamente contra software *"peer-to-peer*" que consegue por um computador pessoal a comunicar com outro de outra rede sem qualquer controlo da nossa rede, é um problema maior para a segurança. A moda de troca de músicas e filmes fez divulgar este tipo de software de uma forma incrível. A instalação de software de *firewall* que destrua os pacotes associados a estas aplicações é uma solução cada vez mais adoptada.

Os sistemas de *Firewall* instalados nas redes e nos computadores pessoais foram uma esperança para todos os responsáveis de segurança, mas a habilidade dos piratas parece imbatível. Criaram outros meios de acção como o *Spyware* e outro software do mesmo tipo que se instala sorrateira e disfarçadamente nos computadores e capta dados importantes como *passwords* de acesso.

***b. Utilizadores, acessos e autenticação***

A gestão de utilizadores e respectivas *passwords* é um aspecto de primeiríssima importância. Quando alguém é recrutado e entra na empresa, é necessário criar-lhe uma identificação na rede com os direitos de acesso adequados à sua função.

Quando um utilizador sai da empresa para trabalhar noutra organização, pode ser, por exemplo, um concorrente, é necessário eliminar a sua identificação na rede de origem para evitar que continue a usar os privilégios de acesso que detinha. Os meios de autenticação de utilizadores na rede devem estar activos a 100% para que um estranho não a possa usar.

A gestão de *passwords* de acesso à rede e às aplicações é uma matéria sempre actual, é a melhor protecção dos dados da empresa. Por isso é essencial que sejam alteradas periodicamente. O ideal é configurar os servidores para forçarem a alteração periódica de *password*, porque se algum pirata estiver na posse da identificação e *password* de um empregado, ficará sem poder entrar na rede quando a *password* for alterada.

### *c. Instalações, ambiente e segurança física*

As instalações também merecem cuidados especiais de segurança, embora pareça que não. Muitas empresas colocam os servidores na cave o que é uma vantagem porque evita acesso de curiosos, mas pode ter uma enorme desvantagem perante inundações porque a água corre para os pisos inferiores e pode entrar nos servidores destruindo todo o seu conteúdo incluindo os dados gravados nos seus discos.

### *d. Software de Sistema*

Para o software de sistema todo o cuidado é pouco. Especialmente porque algum deste software pode intervir nas aplicações em exploração e respectivos dados. A maioria das aplicações actuais é desenvolvida sobre sistemas de gestão de base de dados (ORACLE, SQLServer, etc.) que dispõem de ferramentas de alteração directa dos dados sem passar pelos controlos aplicacionais.

As responsabilidades pelo desenvolvimento e pela operação de software devem ser segregadas. Quem desenvolve software não deve ter acesso às aplicações que estão já em exploração para não poder fazer alterações sem controlo e autorização.

Os sistemas abertos que estão hoje em voga e em expansão tornar-se-ão um perigo devido à facilidade da sua alteração. Obrigando por isso a esquemas apertados de controlo e autorização nas alterações.

### *e. Hardware*

Quanto ao hardware, embora pareça que é menos importante que o software, convém ter em atenção que os componentes dos computadores são cada vez mais pequenos e mais portáveis. O disco de um servidor pode ser retirado ou copiado facilmente. Por outro lado, o acesso ao hardware de sistema pode ter consequências se for permitido livremente.

A gestão de contratos de assistência técnica é importante porque os custos vão aumentando com a idade do hardware e porque deixa de haver componentes de substituição nos últimos anos de vida dos servidores.

### *f. Negócio: Continuidade e Recuperação de Desastres*

Nos últimos anos houve um grande crescimento na utilização das TIC nas organizações. Algumas empresas ficaram completamente dependentes das TIC, por exemplo os bancos, as companhias aéreas, as seguradoras, etc. Uma paragem de um dia pode significar a falência! Por isso e dada a falibilidade e riscos associados às TIC agravados pelos acontecimentos dos últimos tempos (terrorismo, *hackers*, vírus, …) tornou-se indispensável dispor de controlos adequados (CGTI) e especialmente de bons planos de contingência, testados periodicamente e a funcionar em pleno. Um Plano de Contingência deve tratar pelo menos os seguintes conteúdos:

- Objectivos do plano de contingência;
- Estratégia e metodologia adoptadas;
- Limitações do plano;
- Processos de negócio críticos e sistemas envolvidos;
- Cenários de falha dos sistemas e impactos na actividade;
- Medidas de contingência e acções necessárias à sua operacionalização;
- Responsabilidades por cada fase do processo de recuperação e pela actualização do plano de contingência.

Por ocasião do ano 2000, houve uma enorme preocupação com este tipo de planos devido às preocupações que se generalizaram quanto aos riscos de falha dos sistemas. Hoje, já todos esquecemos esta euforia de prevenção e estamos a viver alegremente como se não existissem riscos.

As empresas que usam as TIC de forma extensiva devem proceder a auditorias periódicas à segurança e continuidade de funcionamento dos seus sistemas de informação com incidência especial nas áreas de segurança de acessos, continuidade de funcionamento e recuperação de

desastres. Os controlos gerais das tecnologias de informação devem merecer atenção especial em contextos inseguros como existem actualmente.

### *A Segurança nos Controlos Aplicacionais*

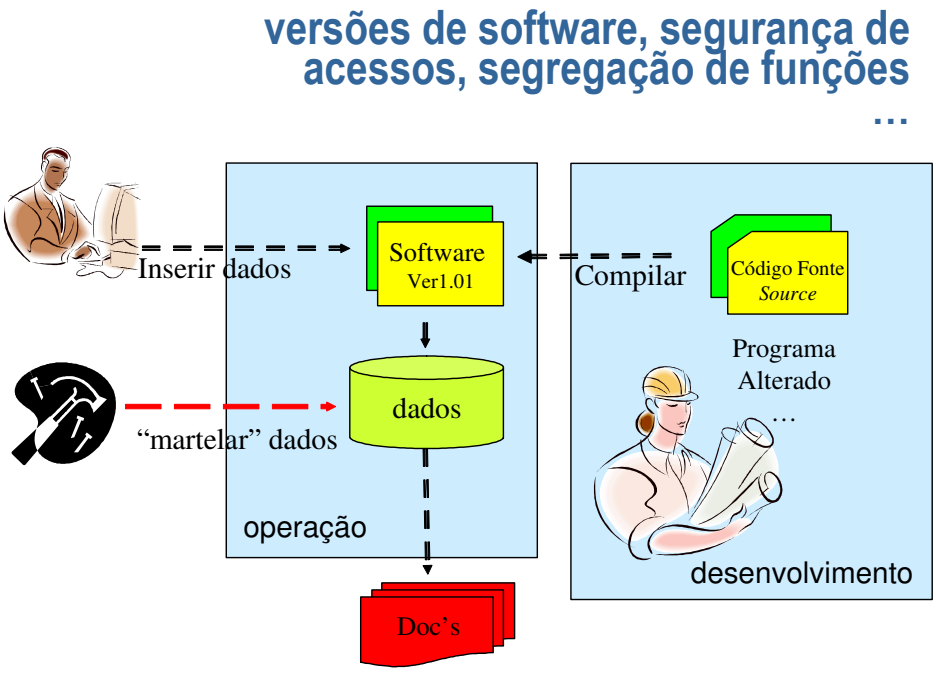
A avaliação dos controlos aplicacionais é uma tarefa difícil que obriga a análise do software e dos dados. A experiência diz-nos que a maior parte das aplicações dispõe apenas de versões executáveis nas empresas que as usam. Os fornecedores de software guardam as linhas de código para si (*sources*) porque são a sua garantia de não haver cópia.

O facto de não dispormos do código fonte e sendo tão extenso quando existe, inviabiliza a análise do software. Resta a hipótese de reprocessar os dados para avaliar a qualidade do software e analisar os dados através de software especializado como WinIdea ou ACL.

De facto, porque a auditoria intervém em regra depois do processamento, nunca temos certezas quando avaliamos controlos aplicacionais. Os dados de input podem ser alterados, o software que processou pode ter usado várias versões, os dados de output podem ter sido modificados. Os dados podem ter sido martelados. Pode não existir segregação de funções entre a operação dos sistemas centrais e o desenvolvimento de software.

#### *a. Software aplicacional*

Certo é que nunca poderemos certificar documentos produzidos a partir de um sistema de informação sem avaliar os controlos gerais e aplicacionais.




A melhor abordagem aos controlos aplicacionais faz-se após a avaliação do Controlos Gerais das Tecnologias de Informação, dirigindo-nos aos dados que consideramos críticos ou sensíveis para a segurança, através do percurso seguinte:

- Autorização de Input
- Verificação de Dados depois de inseridos e antes do processamento
- Controlo de erros de Input
- Controlo de processamento em lotes (Batch) ou on-line
- Controlo de Ficheiros
- Controlo sobre output electrónico ou de papel

A existência de sistemas empresariais (ERP – Enterprise Resouce Planning) do tipo SAP traz alguma tranquilidade porque têm componentes de auditoria que podem ser postos em acção.

***b. DADOS, Classificação e Controlo***

Com a modificação dos suportes preferenciais, do papel para os electrónicos, verificou-se uma grande transformação. Até aqui, praticamente só um incêndio ou uma inundação podiam destruir os dados da empresa. A partir deste ponto tudo se complicou porque além destes acidentes juntaram-se outros riscos que foi necessário considerar. Acessos indevidos, vírus, avaria nos discos, facilidade de cópia, rapidez de processamento para outras utilizações, etc.

Um bom software de *Data Mining* pode facilitar a segmentação de clientes e reduzir custos de marketing e publicidade por evitar desperdícios com campanhas desajustadas aos interesses dos clientes.

Os gestores das empresas tomaram consciência da importância que os dados têm e passaram a classificá-los e a protegê-los. Por isso o controlo de acesso aos dados se tornou tão importante nos nossos dias.

***A segurança nos Controlos de Utilização***

Controlos de utilizador são avaliados relativamente aos controlos de aplicação. Por exemplo quando há um controlo de aplicação que produz uma lista de erros, deve existir um procedimento de utilização para lidar com estes erros. Se os utilizadores não estão empenhados no controlo do sistema então é provável que existam falhas desconhecidas dos responsáveis pelos sistemas.

O envolvimento dos utilizadores no desenvolvimento e manutenção dos sistemas é do maior interesse porque pode reduzir custos em diversas tarefas e melhorar a segurança. Um utilizador mal informado sobre a importância de um sistema é um risco sério na maior parte dos casos.

Neste sentido, o relacionamento dos utilizadores com o sistema deve ser cuidado através de treino e a sua satisfação relativamente ao Sistema de Informação que usa deve ser conhecida.

## Conclusão

Como se referiu, tanto o sector público como o sector privado, dispõem de sistemas de informação que funcionam através de software variadíssimo, sobre computadores e circuitos de comunicações dispersos, torna-se pouco aconselhável que alguém se pronuncie sobre um mapa em papel sem previamente saber quem produziu os dados que contém, por onde passaram, quem os guarda e para onde foram enviados.

Assim, em nosso entender, a certificação de informação relativa a um período de tempo, pressupõe uma avaliação da qualidade e do controlo dos sistemas que a processam. A dispersão dos sistemas e a facilidade de alteração e cópia dos dados é tal que o auditor deve acautelar a sua opinião.

A tendência dos sistemas de informação da generalidade das entidades é para a interligação com outros, formando macrosistemas de informação que importa conhecer, controlar e auditar. Por exemplo, os grandes grupos económicos dispõem de contabilidades interligadas e controladas internamente com possibilidade de balancear diariamente os resultados previstos, podendo actuar sobre os preços de transferência dos produtos e serviços em função das conveniências. Ao nível do Estado temos também os sistemas de controlo da receita, tesouraria e despesa pública que incluem, designadamente, vários serviços e subsistemas, algumas dezenas de programas de contabilidade espalhados pelas entidades.

Assim, a avaliação do controlo interno quando existem meios informáticos nos sistemas de informação auditados, só pode ser levada a cabo por auditores que saibam valorizar o efeito desses meios na respectiva fiabilidade e integridade dos dados. A ideia de que é possível auditar à volta do computador, ou que basta introduzir dados de teste nos sistemas e observar os resultados, é considerada hoje demasiado simplista para ser usada isoladamente em auditoria.

Ainda que actualmente se defenda, numa óptica de análise de custo-benefício no curto prazo, que é preferível contratar serviços externos para cobrir esta necessidade, existem pelo menos três razões que aconselham alguma prudência nessa abordagem:

- ✓ Quem contrata serviços deve saber sempre o que está a contratar (uma entidade responsável pelo controlo financeiro, não deve depender de outra para saber o que deve contratar para executar a sua missão);

- ✓ O auditor responsável pela opinião emitida deve primeiro entender / compreender / conhecer, para depois saber valorizar o que lhe é transmitido (isto é, mesmo que alguém contrate os serviços especializados por ele, isso não dispensa a capacidade técnica para os integrar na sua opinião);

- ✓ Os serviços contratados externamente são, em regra, extremamente caros e o conhecimento adquirido com cada intervenção perde-se, porque fica no exterior da organização, não sendo possível a sua reutilização em idênticas acções de auditoria no futuro.

# Anexo - OS STANDARDS DE AUDITORIA DA SEGURANÇA INFORMÁTICA

***CobiT – Control Objectives for Information Technology*[21]**

Foi desenvolvido pela associação americana ISACA (Information Systems Audit and Control Association).

O Cobit é um modelo orientado para a gestão das tecnologias de informação. A sua visão sustenta que a sobrevivência das organizações depende da gestão efectiva da informação e da tecnologia associada a quatro problemas actuais:

- O aumento da dependência da generalidade das organizações relativamente às TIC[22];
- Aumento das vulnerabilidades e ameaças, muito conhecidas actualmente em alguns sectores de actividade, por exemplo, o sector bancário que não pode deixar de usar as TIC;
- Escala de custos com os SI. Todas as empresas investem somas consideráveis nas suas TIC independentemente do sector de actividade onde actuam;
- Potencial das TIC. Há um grande potencial associado à utilização adequada das TIC em todos os processos organizacionais desde os recursos, à produção e às vendas e apoio ao cliente.

Este standard ou modelo assenta da ideia de que o negócio determina as necessidades de informação e esta determina as necessidades de tecnologia[23].

[21] Information Systems Audit and Control Association (ISACA) got its start in 1967, when a small group of individuals with similar jobs—auditing controls in the computer systems that were becoming increasingly critical to the operations of their organizations—sat down to discuss the need for a centralized source of information and guidance in the field. In 1969, the group formalized, incorporating as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

[22] Para os americanos o conceito de sistemas de informação inclui os circuitos de informação e as TIC. Na Europa usa-se ainda o conceito de sistema de informação independente do de TIC.


É muito fácil entender a lógica deste modelo, talvez seja por isso que tem tanto êxito: a estratégia e os correspondentes processos de negócio definem as necessidades de informação bem como as condições da sua utilização; a informação e as condições em que deve ser tratada determinam os recursos a afectar.

As exigências a considerar nos sistemas de informação para que possam fornecer a informação necessária ao negócio são as seguintes:

- ***Eficácia**: a informação deve ser relevante, pertinente, entregue a tempo, correcta, utilizável e consistente;*
- ***Eficiência**: os recursos são aproveitados de modo óptimo para a sua produção;*
- ***Confidencialidade**: a informação deve ser protegida de acessos não autorizados;*
- ***Integridade**: a informação deve ser completa e correcta;*

[23] Houve alguns tempos em que parecia o contrário, isto é, primeiro compravam-se os computadores e o software, porque estava na moda, e depois decidia-se para que serviam. Esta visão é considerada muito errada nos nossos dias.

- ***Disponibilidade****: a informação deve estar disponível quando necessário. Afectar recursos que garantam a continuidade da disponibilidade;*
- ***Conformidade****: Respeita as normas e exigências legais, ou contratuais do negócio;*
- ***Fiabilidade:*** *a informação dever ser fiável relativamente às fontes, aos circuitos e conteúdos para permitir tomar decisão de qualidade.*

Os recursos são tratados de uma forma abrangente, incluindo os seguintes tipos:

- ***Dados*** *- Sentido amplo (estruturados, não-estruturados, vídeo, som, gráficos, …);*
- ***Aplicações*** *- Procedimentos manuais e automáticos;*
- ***Tecnologia*** *- Hardware, Sistemas Operativos, Rede, Sistemas de Gestão de Base de Dados (SGBD) ... ;*
- ***Instalações*** *- Recursos necessários para alojar e suportar os SI, edifícios, ar condicionado, energia, …;*
- ***Pessoas*** *- Competências necessárias para motivar, planear, organizar, adquirir, entregar, suportar e monitorar os SI e serviços associados.*

Uma vez clarificados os objectivos relativos à informação e os recursos a afectar este standard considera quatro domínios da gestão das TIC desde o planeamento até a monitorização do seu funcionamento:

- ***Planeamento e Organização****: Estratégia; Identificação do modo com a função IT vai contribuir para os objectivos do negócio;*
- ***Aquisição e Implementação:*** *A realização da estratégia. Identificação das soluções IT adequadas, aquisição ou desenvolvimento e integração nos processos de negócio;*
- ***Disponibilização e Suporte:*** *Preocupa-se com a continuidade das operações, a sua segurança e o treino das equipas de TIC;*
- ***Monitorização****: Todos os processos IT necessitam de avaliação regular da sua qualidade e conformidade com os requisitos de controlo e de negócio.*

Cada um destes domínios inclui diversos processos, num total de 34, a avaliar através dos níveis do CMM como já se referiu. Para cada processo IT é possível obter informação de

apoio à auditoria muito pormenorizada a partir do Cobit-Online no site da associação ISACA[24] sobre:

- Framework (enquadramento metodológico do modelo);
- Control Objectives (explicação dos objectivos de controlo);
- Audit Guidelines (orientações de auditoria);
- Key Goal Indicators (indicadores chave dos objectivos de controlo a usar);
- Key Performance Indicators (indicadores chave de performance);
- Critical Success Factors (factores críticos de sucesso);
- Maturity Models (níveis de maturidade ajustados do CMM);

O Cobit On-line está preparado para filtrar o material aplicável a uma missão de auditoria e fornecê-lo por via electrónica.

A associação ISACA tem vindo a expandir o número de utilizadores em todo o mundo. Em 2005 candidataram-se mais de 20000 profissionais à certificação em todo o mundo[25]. Oferece actualmente dois tipos de certificação profissional com algumas exigência de formação continua para quem quiser manter o título:

- **CISA - Certified Informations Systems Auditor.** Obriga a exame em matérias como Processo de Auditoria de Sistemas de Informação, Gestão, Planeamento e Organização dos SI, Insfraestrutura Tecnológica e Práticas Operacionais, Protecção de Activos de Informação, Recuperação de Desastres e Continuidade de Negócio, Desenvolvimento de Sistemas Aplicacionais, Aquisição, Implantação e Manutenção e Avaliação de Processos de Negócio e Gestão de Risco;

- **CISM - Certified Information Security Manager.** Obtido com exame de certificação sobre Gestão da segurança, Gestão de risco e Gestão de programas de segurança da informação. Além disso deve aderir à associação ISACA, ter cinco anos de experiência em segurança informática e três anos de gestão da segurança informática.

[24] www.isaca.org – naturalmente que só os membros têm acesso à informação mais detalhada.

***COSO - Committee of Sponsoring Organizations of the Treadway Commission***[26]

O comité COSO é uma organização privada americana, foi formada inicialmente em 1985 para apoiar a National Commission on Fraudulent Financial Reporting, uma iniciativa independente do sector privado que estudou as causas da publicação de relatórios financeiros fraudulentos e desenvolveu recomendações para as empresas privadas e seus auditores, para a SEC (Stock Exchange Comission) e outros reguladores e instituições de edução.

Esta Comissão Nacional Americana (COSO) foi patrocinada por cinco grandes associações profissionais dos Estados Unidos da América, American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, Institute of Internal Auditors e National Association of Accountants (hoje Institute of Management Accountants). A comissão funcionava independente dos patrocinadores e incluía representantes da indústria, da contabilidade pública, de empresas de investimento e da Bolsa de Nova York (New York Stock Exchange).

Trata-se de um modelo global de gestão de risco empresarial que embora não seja totalmente aplicado à segurança informática e auditoria, pode ser útil no desenho do enquadramento para a auditoria das tecnologias de informação e comunicação. A definição adoptada para gestão de risco é a seguinte:

*"Gestão do risco empresarial é um processo, levado a efeito pelo quadro de directores de uma entidade, gestores e outro pessoal, aplicado na definição da estratégia em toda a empresa, desenhado para identificar potenciais acontecimentos que podem afectar a entidade, e para gerir o risco mantendo-o em níveis aceitáveis, tendo em vista oferecer segurança razoável relativamente à concretização dos objectivos da entidade"*[27]

No entendimento do COSO, as premissas subjacentes à gestão de risco empresarial são que qualquer entidade existe para fornecer valor aos seus donos (*stakeholders*). Todas as

---

[25] Consulte www.isaca.org
[26] http://www.coso.org
[27] O texto original é o seguinte: "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to

entidades enfrentam incerteza, o desafio de gestão é determinar quanta incerteza pretende aceitar para ampliar o valor da empresa. A incerteza é constituída em simultâneo por risco e oportunidade, com potencial para criar ou destruir valor. A gestão de risco empresarial permite aos gestores lidar eficazmente com a incerteza e risco associado, melhorando a capacidade de criar valor.

A gestão de risco empresarial propõe:

- Alinhar a apetência por risco com as alternativas estratégicas;
- Melhorar as decisões de resposta ao risco;
- Reduzir surpresas operacionais e perdas;
- Identificar e gerir riscos múltiplos e cruzados em toda a empresa ou nos seus departamentos;
- Recolher oportunidades a partir dos eventos potenciais;
- Melhorar a rentabilidade do capital.

### *ISO/IEC 17799:2000 - Code of Practice for Information Security Management*[28]

Foi desenvolvido pela ISO (the International Organization for Standardization) e IEC (the International Electrotechnical Commission) com base num standard inicial desenhado pelo BSI (British Standard Institute).

É um standard detalhado de segurança[29]. Está organizado em dez secções, cada uma cobre uma área ou tópico relevante:

- Politica de Segurança

---

identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"

[28] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

[29] http://www.ansi.org/, www.bsi.gov.uk, www.iso.org

- Segurança Organizacional
- Classificação e Controlo
- Segurança Pessoal
- Segurança Física e de Ambiente
- Gestão de Comunicações e de Operação
- Controlo de Acessos
- Desenvolvimento e Manutenção de Sistemas
- Gestão de Continuidade de Negócio
- Conformidade

Existem variadíssimas entidades certificadas para avaliar a conformidade com este standard, o facto de ter sido muito divulgado, ser bastante pormenorizado e de ter aparecido num momento oportuno, tornaram-no bastante popular entre os profissionais de TIC.

Trata-se de um standard bastante exigente e completo como podemos verificar pelos tópicos abrangidos em cada uma das áreas ou anéis de segurança no conceito que estamos a seguir:

*Politica de Segurança* – refere-se à documentação das políticas de segurança da informação e avaliação.

*Segurança Organizacional* – trata a gestão, coordenação e atribuição de responsabilidades na segurança de informação. Inclui também a cooperação entre organizações, riscos de acesso por terceiros e *outsourcing*.

*Classificação e Controlo* - Inventário de activos de informação, regras de classificação, catalogação e movimentação de informação.

*Segurança Pessoal* – versa a inclusão de segurança de informação nas responsabilidades funcionais, nas políticas de selecção de pessoal e condições de emprego, educação e treino em segurança de informação. Inclui ainda o relato de incidentes, fraquezas, deficiências de funcionamento no software bem como as consequências disciplinares.

*Segurança Física e de Ambiente* – trata da segurança física, especialmente controlos físicos de entrada em instalações, salas e escritórios, isolamentos indispensáveis e localização.

Inclui também fornecimento de energia, segurança de cablagem, garantias e manutenção e remoção de equipamento.

*Gestão de Comunicações e de Operação* – trata os procedimentos de operação, incidentes, segregação de funções e de instalações de desenvolvimento e operação, planeamento de capacidade. Inclui ainda regras de backup, protecção contra vírus, intrusão nas redes, gestão e circulação de suportes de informação e documentação dos sistemas. Considera também a segurança relativa a acordos de troca de software e informação, comércio electrónico, correio electrónico, escritório electrónico.

*Controlo de Acesso* – trata a política de controlo de acessos, registo de utilizadores, gestão de privilégios, *passwords* de utilizadores, direitos de acesso. Políticas de utilização de serviços de rede, circuitos obrigatórios, autenticação de utilizadores em ligações externas. Inclui o diagnóstico remoto de protecção de portas, a segregação em redes, controlo de conexões de rede, de *routing* e segurança de serviços de rede. Trata também identificação automática de terminal, *logon* via terminal, uso de utilitários de sistema, *time-out* de terminal e limitação de tempo de conexão, monitorização do uso do sistema, sincronização de relógio, computação móvel e teletrabalho

*Desenvolvimento e Manutenção de Sistemas* – versa a especificação de requisitos de segurança, validação de dados de Input, controlo de processamento interno, validação de dados de Output, uso de controlos de criptografia, assinaturas digitais e gestão de chaves. Inclui o controlo de software operacional, de acessos a livrarias de programas fonte e procedimentos de alterações de controlo. Inclui também a verificação técnica de alterações de sistema operativo, de *packages* de software e *outsourcing* de desenvolvimento de software

*Gestão de Continuidade de Negócio* – refere-se ao processo de gestão, análise de impacto, teste, manutenção e reavaliação de planos de continuidade de negócio.

*Conformidade* – considera a identificação de legislação aplicável, direitos de propriedade intelectual, salvaguarda de registos organizacionais, protecção de dados e privacidade na informação pessoal. Inclui ainda a regulamentação de controlos de criptografia, de recolha de

evidência. Trata também a conformidade com a política de segurança, os testes de conformidade técnica e a auditoria de controlos de sistema.

O Standard ISO/IEC 17799:2000 está em revisão e é esperado para finais de 2005 a conclusão. A alteração maior será na estrutura de controlos, para distinguir claramente entre requisitos, orientação de implantação e posterior informação. Prevê-se alguma racionalização e aditamento de novos controlos.

A seguir à publicação da parte 2 deste Standard BS 7799-2:2002 em Setembro de 2002, surgiu ainda um maior interesse em todo o globo com um aumento de certificações em todo o mundo. A parte 2 explica o que uma organização ou um consultor precisa de fazer para obter a certificação neste standard.

Provavelmente haverá ainda no futuro uma parte 3 deste standard para melhoramento contínuo[30].

### *ISO/IEC TR 13335[31]*

Foi desenvolvido pela ISO (the International Organization for Standardization) e IEC (the International Electrotechnical Commission).

É constituído por um conjunto de orientações genéricas de gestão da segurança das TI, com 5 partes produzidas nos últimos oito anos:

2004 - Parte 1: Conceitos e modelos para a segurança de TI

1997 - Parte 2: Gerir e planear a segurança de TI

[30] Consulte a história do Standard 7799 em http://www.gammassl.co.uk/bs7799/history.html

[31] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

1998 - Parte 3: Técnicas de gestão da segurança de TI

2000 - Parte 4: Selecção de protecção

2001 - Parte 5: Orientações de gestão na segurança de redes

A parte 1 deste standard oferece uma visão de alto nível da gestão. É adequada para gestores e para quem tem responsabilidades na segurança das TIC. Foca a atenção em conceitos e modelos de gestão, planeamento, implantação e operações da segurança das TIC e contém:

- Definições aplicáveis em todo o standard;
- Descrição dos elementos de segurança mais importantes e do seu relacionamento no âmbito da segurança das TIC;
- Objectivos de segurança da empresa, estratégias e políticas necessárias para tornar efectiva a segurança das TIC;
- Organização da segurança eficaz, modelos de responsabilização e atribuição explícita e conhecimento das responsabilidades;

A informação fornecida pelo ISO/IEC 13335-1 pode não ser directamente aplicável a todas as organizações, especialmente as mais pequenas poderão não possuir todos os recursos necessários para executar plenamente as funções determinadas pelo standard. Nestas situações é importante que os conceitos base sejam postos em prática de forma adequada à sua dimensão.

A Parte 2 (ISO/IEC 13335-2 refere-se às técnicas de gestão de risco apropriadas na segurança das tecnologias da informação

As partes 3, 4 e 5 são documentos técnicos. A parte 4 refere a selecção de protecções e o modo como pode ser suportada pelo uso de controlos e como se complementa com a parte 2

A Parte 5 refere-se a orientação de gestão da segurança de redes e comunicações para quem for responsável pela gestão da segurança. Esta orientação suporta a identificação e análise dos factores relacionados com comunicações a ter em conta no estabelecimento da segurança de redes.

### *ISO/IEC 15408*[32]

Foi desenvolvido pela ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission).

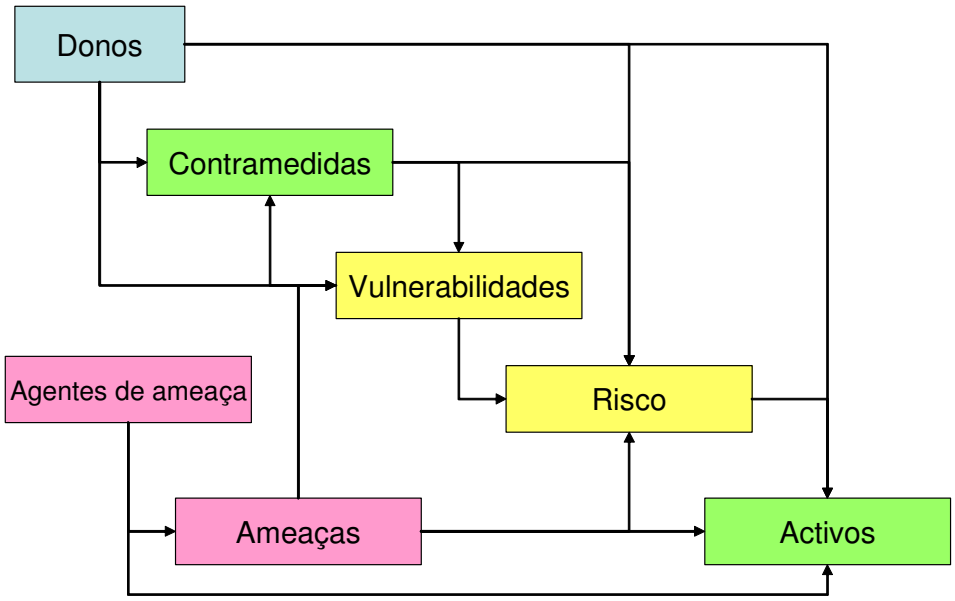
ISO/IEC 15408 consiste nas seguintes partes subordinadas ao título geral de Tecnologias de Informação – Técnicas de Segurança – Critérios de avaliação da segurança das TI:

> Parte 1: Introdução e modelo geral - define conceitos gerais e princípios do modelo geral de avaliação também apresenta objectivos de segurança para selecção de requisitos;
>
> Parte 2: Requisitos funcionais de segurança - estabelece um conjunto de componentes funcionais como meio de exprimir requisitos funcionais catalogados em famílias e classes;
>
> Parte 3: Requisitos de certificação de segurança - estabelece um conjunto de componentes de certificação com critérios de avaliação e escalas para nivelar;

Este standard é pouco utilizado entre nós. O esquema de conceitos e relacionamento deste standard pode ilustrar-se da seguinte forma:

[32] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

Esquema de conceitos usado no standard ***ISO/IEC 15408***




***ISO/IEC 21827:2002(E)***[33]

Foi desenvolvido pela ISO (the International Organization for Standardization) e IEC (the International Electrotechnical Commission).

Trata-se de um standard de avaliação de maturidade dos sistemas de segurança: Tecnologias de Informação — Engenharia de Sistemas de Segurança — Capability Maturity Model (SSE-CMM).

[33] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

O modelo considera seis níveis de maturidade que vão desde a não existência de segurança até ao nível mais elevado quando o sistema está plenamente seguro e optimizado:

0 – Não existente
1 – Inicial ou *ad hoc*
2 – Repetível mas intuitivo
3 – Processo definido
4 – Gerido e mensurável
5 – Optimizado

Um vasto número de entidades pratica a engenharia de segurança no desenvolvimento de software de sistemas operativos, gerindo e reforçando as funções de protecção. São necessários métodos adequados e boas práticas de referência.

O SSE-CMM® é um modelo de referência de processo. Foca-se nos requisitos para implantar a segurança num sistema ou série de sistemas de Tecnologias de Informação. Pode sugerir um processo específico para uma organização em particular.

O seu âmbito considera:

- A engenharia das actividades do sistema de segurança para um produto seguro ou um sistema de confiança, tratando o ciclo de vida completo desde a definição do conceito, análise de requisitos, desenho, desenvolvimento, integração, instalação e operação, manutenção e desactivação;

- Requisitos para programadores de software, programadores de sistemas seguros e integradores, organizações que forneçam serviços de segurança de computadores ou construção de computadores;

- Aplica-se a todos os tipos e tamanhos de organizações de engenharia de segurança, comerciais ou estatais

### *ITIL*[34]

Foi produzido pelo *Office of Government Commerce (OGC*) um serviço com autonomia funcional inserido no Ministério das Finanças do Reino Unido que reporta ao *Chief Secretary to the Treasury*.

O ITIL é um conjunto de boas práticas em gestão de TI, desenvolvido pelo OGC e sustentado em publicações, certificados de qualificação e por um grupo de utilizadores internacionais.

Pretende apoiar as organizações no desenvolvimento de um *framework* para ajudar gestores de *outsourcing* a controlar a qualidade e os custos. O ITIL destina-se a fornecedores de serviços de TI, directores de TI e CIOS (Chief Information Officers), gestores, clientes e utilizadores finais.

Os seus promotores dizem que o ITIL oferece uma aproximação sistemática e profissional à gestão das TI que permite reduzir custos, melhorar os serviços de TI devido ao uso das melhores práticas nos processos, melhorar a satisfação dos clientes, orientar, estandardizar e melhorar a produtividade entre outras vantagens.

A aplicação deste standard a todos os processos internos de uma organização obriga a combinar diferentes tipos de informação, desde o inventário da infraestrutura, o impacto das ocorrências tecnológicas nos serviços e processos de negócio, até à reiteração de ocorrências associadas a um determinado componente. O ITIL suporta a maior parte dos processos tratados no COBIT. Distribui-se por oito documentos principais:

- Serviços e apoio
- Serviços de disponibilização
- Planeamento de implantação da gestão do serviço
- Gestão de aplicações
- Gestão de infra-estruturas de TIC
- Gestão da segurança
- Gestão dos activos de software

[34] Para obter mais informação consulte http://www.ogc.gov.uk e http://www.itil.co.uk

- Perspectiva de negócio: A abordagem dos sistemas de informação na disponibilização de serviços ao negócio

Estão previstos três níveis de certificação profissional no esquema do ITIL:

- *Foundation Certificate* – Certificado em Fundamentos de Gestão de Serviços TI. Oferece um nível basilar de conhecimento em gestão TI e é destinado a todos os profissionais que pretendem estar familiarizados com as melhores práticas ITIL. Teste de uma hora realizado em papel ou via Web, consistindo em quarenta perguntas com resposta de escolha múltipla. Não requer qualquer certificação prévia;

- *Practitioner's Certificate* – Certificado de Praticantes em Gestão de Serviços de TI. Destinado a todos os profissionais com responsabilidades pelo desenho de processos relativos à gestão de TI. O exame consiste em dois testes de três horas. Os examinandos devem já possuir o Certificado em Fundamentos de Gestão de Serviços TI.;

- *Manager's Certificate* – Certificado de Gestores em Gestão de Serviços de TI. Destina-se aos profissionais que gerem as TI. Certificado de Gestores em Gestão de Serviços de TI. O exame consiste em dois testes de três horas. Os examinandos devem já possuir o Certificado em Fundamentos de Gestão de Serviços TI.

A certificação ITIL, tal como noutros standards garante que os seus detentores são tecnicamente qualificados para usar as melhores práticas ITIL. A certificação é atribuída por um grupo de certificação constituído por representantes do próprio OGC, do itSMF e vários institutos examinadores. Actualmente, os institutos que oferecem formação profissional são:

- ISEB (The Information Systems Examination Board), uma subsidiária da British Computer Society;
- ISEB ITIL Service Management training;
- ISEB ITIL Infrastructure Management training;
- EXIN - the Examination Institute for Information Science in the Netherlands;
- EXIN accredited trainers.

O OGC trabalhou em ligação com o BSI (British Standard Institute) e itSMF (IT Service Management Forum )[35] na elaboração da sua documentação de modo a que o *BSI Management Overview* (PD0005), BS15000-1 (especificações para gestão de serviços), BS15000-2 (código de prática para a gestão de serviços) e os documentos ITIL façam parte de uma estrutura lógica. O documento *BSI Management Overview* serve como uma introdução de gestão aos guias detalhados ITIL[36]

O BS15000 consiste em duas partes:

- BS15000-1 com 10 secções: âmbito, termos e definições, requisitos para um sistema de gestão, plano e implantação do serviço de gestão, planeamento e implantação de novos serviços ou serviços modificados, processos de disponibilização de serviços, processos de relacionamento, processos de resolução, processos de controlo e processos de desafectação;

- BS15000-2 oferece assistência às organizações que esperam ser auditadas contra o standard BS15000-1 ou planeiam melhorar os serviços.

***NIST 800-14[37]***

Esta norma foi produzida pelo National Institute of Standards and Technology - Technology Administration - U.S. Department of Commerce. Foi-lhe atribuída a designação "*Generally Accepted Principles and Practices for Securing Information Technology Systems"*.

Este standard aborda os princípios e práticas, bem como os relacionamentos entre princípios. Tem preocupações com a audiência e terminologia a usar nos princípios de segurança de

---

[35] A *it*SMF - IT Service Management Forum - é uma organização independente e sem fins lucrativos, que reúne cerca de 3 mil organizações em todo o mundo nos sectores das Tecnologias de Informação, Administração Pública, Retalho, Banca, Telecomunicações e Grande consumo. Em Portugal desde 2003, esta organização representa um importante passo no processo de desenvolvimento e promoção dos standards e Melhores Práticas nos Serviços de Gestão de TI. Consulte http://www.itsmf.pt/

[36] Para mais informação sobre o BS15000 visite http://www.bs15000.org.uk/index.htm

[37] NIST = **National Institute of Standards and Technology - Technology Administration - U.S. Department of Commerce.** Generally Accepted Principles and Practices for Securing Information Technology Systems

sistemas geralmente aceites. Trata-se de um documento com intenções semelhante aos princípios contabilísticos ou de auditoria geralmente aceites.

Sustenta que a segurança dos computadores suporta a missão da organização e é um elemento integral da gestão sólida moderna. As responsabilidades devem ser tornadas explícitas e avaliadas regularmente de forma integrada e compreensiva tendo em conta que a segurança é muito influenciada actualmente por factores sociais. Há quem crie problemas de segurança nas redes pelo prazer de conseguir fazer algo difícil!

As políticas são um aspecto chave, tal como a gestão do risco, identificação de ameaças e a sua mitigação. A segurança é vista como um processo que deve ser controlado desde a fase de planeamento à fase de monitorização, tal como se faz no Cobit.

O standard NIST trata ainda de diversos domínios comuns como a gestão de utilizadores, contingência, recuperação de desastres com cenários alternativos hipotéticos, gestão de incidentes, treino dos utilizadores, identificação, autenticação e gestão de *passwords* e *encriptação*. O *Audit Trail* é também uma preocupação saliente do standard,

***OECD's Guidelines for the Security of Information Systems***

A OCDE procurou intervir nas questões emergentes de insegurança decorrentes da adopção generalizada das TIC. Publicou as seguintes recomendações:

*Responsabilização (Accountability)* – As responsabilidades e a responsabilização de proprietários, fornecedores e utilizadores de sistemas de Informação e outras partes … devem ser explícitas;

*Prevenção (Awareness)* - Proprietários, fornecedores e utilizadores devem estar alinhados quanto antes, com a manutenção da segurança, para obterem conhecimento apropriado e estarem informados sobre a existência e extensão geral de medidas… para a segurança de sistemas de informação;

*Etica (Ethics)* – Os sistemas de informação e a segurança dos sistemas de informação devem ser disponibilizados e usados de modo a respeitar os direitos e interesses legítimos dos outros.

*Multidisciplinariedade (Multidisciplinary)* – As medidas, práticas e procedimentos para a segurança dos sistemas de informação devem mencionar e ter em conta todos as considerações e pontos de vista…

*Proporcionalidade (Proportionality)* – Níveis de Segurança, custos, medidas, práticas e procedimentos devem ser adequados e proporcionais ao valor e ao grau de fiabilidade dos sistemas de informação e à severidade, probabilidade e extensão dos danos potenciais…

*Integração (Integration)* – Medidas, práticas e procedimentos para a Segurança dos sistemas de Informação devem ser coordenadas e integradas entre si e com outras medidas, práticas e procedimentos da organização de modo a criar um sistema de segurança coerente

*Oportunidade (Timeliness)* – As partes públicas e privadas ao nível nacional e internacional, devem actuar de modo oportuno e coordenado para prevenir e responder às brechas na segurança dos sistemas de informação.

*Reavaliação (Reassessment)* – A segurança dos sistemas de informação deve ser reavaliada periodicamente, à medida que os sistemas de informação e requisitos de segurança variam ao longo do tempo.

*Democracia (Democracy)* – A Segurança dos sistemas de Informação deve ser compatível com o uso legítimo de fluxos de dados e informação numa sociedade democrática.

### *TickIT*[38]

O programa TickIT foi criado pelo governo do Reino Unido para assegurar um método de registo do desenvolvimento de software baseado no standard ISO 9000-3. O esquema foi desenvolvido conjuntamente pelo United Kingdom Department of Trade and Industry (DTI) e British Computer Society.

[38] TickIT Office at BSI (Floor 8E), 389 Chiswick High Road, London W4 4AL.

O standard TickIT é mantido e gerido por um Departamento dentro do BSI Standards (British Standards Institute), um departamento com responsabilidades por todos os aspectos de standardização de sistemas de informação e comunicações.

O grande propósito do TickIT, suportado pela indústria de software do Reino Unido e também da Suécia, é estimular os programadores de software de sistema a pensar e aceitar:

- Que a qualidade existe no contexto dos processos de desenvolvimento de software;
- Que pode ser conseguida a qualidade;
- Que podemos melhorar continuamente os sistemas da gestão da qualidade.

Embora seja exigida a certificação na ISO 9001 aos fornecedores de software de sistemas, em certas áreas do mercado justificam-se maiores preocupações de qualidade. Relativamente à certificação neste standard, são objectivos da indústria:

- Melhorar a confiança em sistemas de terceiros através de esquemas de certificação no sector do software;
- Melhorar as práticas profissionais entre os auditores de sistemas de gestão da qualidade no sector do software;
- Publicar orientações para todos os interessados.

# Bibliografia

SOBEL, Paul J.; Auditor's Risk Management Guide: Integrating Auditing & ERM 2005 Edition

HUNTON, James E. & BRYANT, Stephanie M. & BAGRANOFF, Nancy A.; Core Concepts of Information Technology Auditing

HALL, James A. (2000); Information Systems Auditing and Assurance, South-Western;

WEBER (1999); Information Systems Control and Audit;

KRIST (1999); A Standard for Auditing Computer Applications;

IT Governance Institute; Governance of the Extended Enterprise: Bridging Business & IT Strategies

HILES, Andrew; Enterprise Risk Assessment and Business Impact Analysis

HICKMAN; Practical IT Auditing;

MONTEIRO, Edmundo & Boavida, Fernando; Engenharia de Redes Informáticas, 3ª edição, FCA, ISBN 972-722-203-X

Handbook of International Auditing, Assurance, and Ethics Pronouncements, 2005 Edition; International Federation of Accountants

International Standards on Information Systems

## Locais a visitar na Internet

http://www.oit.nsw.gov.au/content/2.3.16-Security-Pt1.asp -

.NET Development (General)

ADO Code Examples in Microsoft Visual Basic

ASP diversos

Extensible Markup Language (XML)

Extensible Markup Language Version 1.0 Part I Syntax

HTML com registos

MSN

Open and Close Methods Example (VB)

WDVL PHP - Aprender

XML.com XML From the Inside Out -- XML development, XML resources, XML specifications

ACTIVE Information - ISO 9000 Compliance Checklists - ISO 9000 Software

Assinatura electrónica

British Standards Institution

BS 7799 Taxonomy of Reference Documents

BS7799 Taxonomy - Queries

BSI-DISC website for BS 7799

Buy Products -- Customer Profile

Certipor - Sociedade Portuguesa de Certificados Digitais, S.A.

Cisco Secure PIX Firewall FTP Vulnerability

Como Funciona o PGP

Direct Hit Web Search network security

Ecora

Global Information Assurance Certification

Guide to Enabling Secure Payment Processing on Your Site

Hackers

ICSA 2000 WE SECURE THE WEB !

MCSE Braindumps, all you'll ever need to get certified!

Microsoft TechNet Security

Net Detective people search utility software- HDP Corporate Website

Network Associates Downloads - Updates

Network Associates Products - NAI Survey

NIST Computer Security Special Publications

O Lado Negro da WEB - Tecnologia e Extras

SANS Resources - The Twenty Most Critical Internet Security Vulnerabilities (Updated)

SecurityFocus

Seguritec Lda

The ITIL ® Toolkit

Vigias - The Web Information Company

VNC - Virtual Network Computing from AT&T Laboratories Cambridge

What is firewall

whatis.com

Windows 2000 Security Technical Overview [Microsoft Windows 2000 Server, security, distributed security services, authenticat

ACL para Windows

ANACOM - Autoridade Nacional de Comunicações

Audit Methodology

Auditing & Fraud Examination

Auditoria Informática - BS 7799 Popular Products

COSO

ecommerce - Novo

EDI

EESSI-Assinatura Electrónica

EUROPA - MISSOC - Comparative Tables on Social Protection in the Member States

FEE Homepage - English

Guideline Menu - NSW Department of Commerce da Australia

History of BS 7799

IASB - International Accounting Standards Board

IASPlus Home Page - News about International Financial Reporting

IFAC - The International Federation of Accountants

INTOSAI EDP Directory

ISACA Chapter Seminar Schedule by Location

ISO 17799 - The Information Directory for ISO17799

NetDetective 7.0

Office of the Auditor General of Canada - Bureau du vérificateur général du Canada

Pleier Corporation - ADM PLUS Audit Management System, CD-DVD production, Web design, multimedia.

PowerPoint in the Classroom

Rational Unified Process - Metodologia

Regras AntiSPAM - Pathway Communications

RIA -- Handbook of IT

SCRIPTS VMware -- Virtual Computing Throughout the Enterprise

Spam Remedy

SPAMM Pew Internet & American Life Project

Spreadshet Templates

Symantec Security Response - W32.Klez Removal Tool

The United States General Accounting Office

UK National Audit Office home page

What is monte carlo simulation

Win32 Scripting.... Everything you need to get up and running

Word of Mouth Connection - A Background Research Tool