ISO/IEC 27001

A norma das normas em Segurança da Informação

Henrique Manuel Dinis dos Santos
Departamento de Sistemas de Informação
Universidade do Minho

"The nice thing about standards is that there are so many of them to choose from."
Andrew S. Tanenbaum

A evolução das Tecnologias de Informação e Comunicação (TIC) é um fenómeno sem precedentes na história da humanidade. Com efeito, a sua banalização tem permitido o desenvolvimento de novos modelos económicos e sociais, com vantagens óbvias ao nível da eficiência e da flexibilidade em todas as áreas de actividade e a um ritmo impressionante. Mas esta tendência tem sofrido alguns reveses, por vezes devido a inadequações, mas muito frequentemente porque a segurança das TIC não tem sido acautelada devidamente, optando-se normalmente por reagir em vez de prevenir. Atendendo à dimensão deste problema e ao seu crescente impacte negativo na actividade das organizações, na última década têm surgido diversas normas e guias de boas práticas que procuram dar resposta a essas necessidades. Contudo, essas recomendações aparecem demasiado orientadas para aplicações específicas ou seguem modelos de desenvolvimento diferentes, dificultando a criação de uma base de conhecimento comum sobre a área da Segurança de Sistemas de Informação. A norma ISO/IEC 27001 vem procurar exactamente responder a essa dificuldade, propondo uma linguagem comum que poderá servir de suporte para a aplicação, devidamente adequada, de várias outras normas mais específicas.

É hoje universalmente aceite que a segurança da informação é muito mais do que a aquisição, instalação e configuração de alguma infra-estrutura tecnológica, por mais eficiente que ela pareça ser. Com efeito, sem o adequado suporte de uma metodologia de gestão da segurança que aborde todo o processo de geração, processamento e armazenamento da informação, no contexto real da organização, dos seus objectivos e das suas práticas de trabalho, não é possível garantir um nível de segurança da informação adequado. E sem estes indicadores qualquer investimento em segurança pode ser sempre questionado [1]. A determinação daquele nível e a avaliação da sua adequabilidade carecem de uma análise do risco a que a informação está sujeita, quer por agentes internos quer por agentes externos. A mitigação efectiva dos riscos obrigam à definição de várias medidas de controlo e uma reavaliação contínua de todo o processo, que acompanhe a contínua evolução organizacional. Estas características conferem a esta actividade o estatuto de metodologia de gestão, surgindo assim, naturalmente, o conceito de Sistema de Gestão da Segurança da Informação, ou ISMS (*Information Security Management System*).

No âmbito da Segurança dos Sistemas de Informação diversas normas e metodologias associadas têm vindo a ser discutidas e utilizadas, umas orientadas para classes de organizações específicas, como é o caso da norma HIPAA [2][8], publicada em 1996 nos EUA, outras mais genéricas como a OCTAVE [3][9], ou a COBIT [4][10], por vezes integrando explicitamente as questões de segurança com as actividades de gestão convencionais. Das várias normas publicadas neste contexto realçam-se a BS 7799 e a ISO/IEC 17799, que se complementam de uma forma interessante. A primeira define um conjunto de requisitos que um sistema de segurança deve

respeitar com vista à sua certificação, a segunda inclui importantes recomendações relativas fundamentalmente à implementação e gestão das tecnologias de segurança. Estas normas são utilizadas na grande maioria das metodologias propostas mas, dado o seu âmbito de aplicação restrito, dificilmente essas metodologias suportam um ISMS completo. Isso mesmo pode ser constatado observando um modelo deduzido da norma ISO/IEC 17799 – que se encontra ilustrado na figura 1, sendo apresentado e discutido em [5] – e verificando que a norma se centra essencialmente nas recomendações relativas às diversas medidas (ou controlos) de segurança.

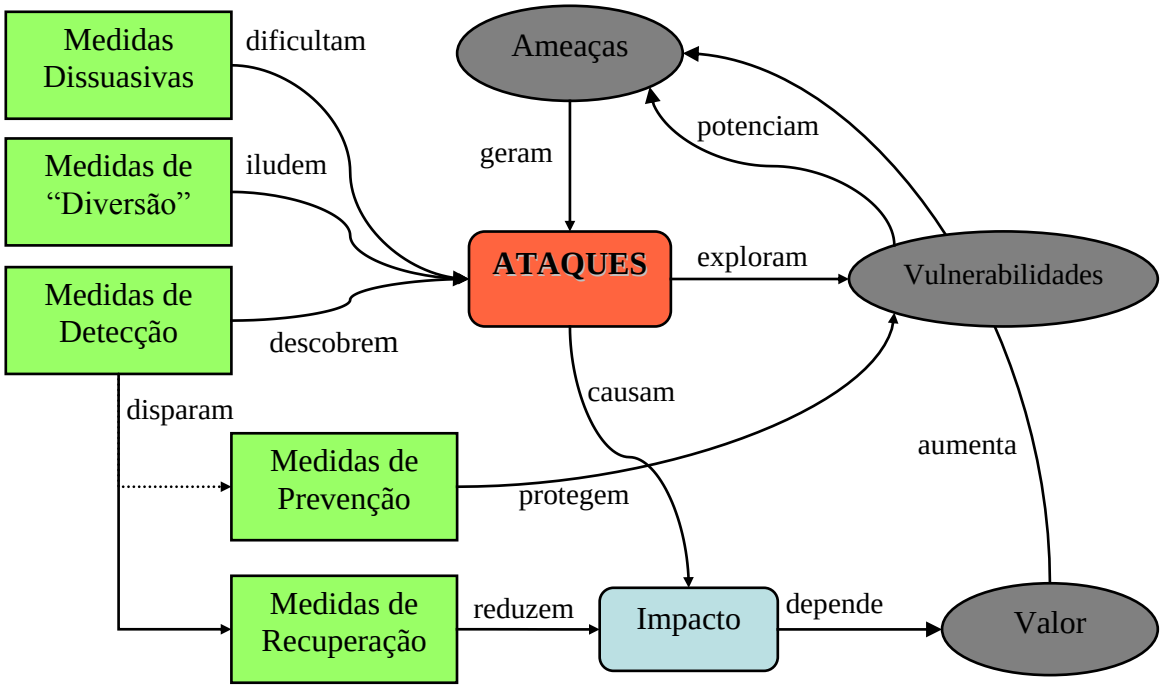

Figura 1 – Modelo de suporte à norma ISO/IEC 17799

Mas as funções de gestão da segurança ausentes nestas normas não foram esquecidas. Bem pelo contrário, à medida que a sua importância foi aumentando, também o foi o reconhecimento da necessidade de normalização. Em resposta e no meio de diversos guias de boas práticas, apareceram, entre outras, as normas ISO/IEC 13335 e a ISO/IEC 15408. A primeira define um conjunto de procedimentos associados ao que é assumido como boas práticas na gestão do risco dos sistemas de informação, desde a sua análise e avaliação até à forma de mitigação; a segunda, destinada essencialmente a definir um conjunto de critérios que permita avaliar um sistema de segurança (base de um processo de certificação e algo que a BS 7799, segunda parte, também já fazia). Convém ainda realçar que a ISO/IEC 15408 é uma adaptação directa de uma outra norma, conhecida por CC (*Common Criteria*), cuja segunda versão, a que deu origem à ISO/IEC 15408, foi publicada em 1999. Por sua vez, a CC resultou de um notável esforço de concertação de diversos países que inicialmente adoptaram diferentes versões de uma norma anterior, a TCSEC (*Trusted Computer System Evaluation Criteria*), criada sob os auspícios do Departamento da Defesa dos EUA.

Apesar de muito estreitamente relacionadas, todas estas normas acabaram por criar modelos alternativos e, por vezes, terminologias diferentes na mesma área da Segurança dos Sistemas de Informação. Esta realidade compromete seriamente qualquer esforço de criar uma cultura comum e globalmente percebida sobre a área, para além de aumentar significativamente o esforço de implementação de um ISMS, tarefa que acaba por se revelar demasiadamente complexa e, consequentemente, onerosa. Justifica-se assim a tentativa de uniformizar ou alinhar as diferentes

normas, o que encontra uma das suas expressões máximas na recente criação da família de normas ISO/IEC 27000.

Adopção de normas de Segurança da Informação

Antes de abordar aquela norma convém ainda realçar a importância que, neste domínio, assumem os grupos de trabalho ou redes de utilizadores que incentivam e ajudam a criar um clima propício à adopção de determinadas práticas ou regras, cuja natureza assume um carácter mais ético. Ao contrário da privacidade, um direito facilmente caracterizado e alvo de legislação adequada, a Segurança dos Sistemas de Informação é algo muito mais abrangente e difuso, onde a regulamentação é muito difícil, se não mesmo impossível. É verdade que em domínios mais limitados como a assinatura digital ou a factura electrónica até é possível promover legislação e obrigar a garantir algumas propriedades de segurança. Mas na grande maioria das actividades organizacionais, mormente naquelas que passam pela utilização de meios de comunicação abertos, como é o caso da internet, ou que estão relacionadas com processos de gestão internos perfeitamente estabelecidos, isso é muito difícil de fazer e só mesmo as pressões sociais e a criação de uma consciência ética/profissional podem obrigar à adopção de determinadas regras ou procedimentos, conducentes a níveis adequados de segurança. Podemos aqui reconhecer duas vias principais para abordar esta questão: a divulgação do conhecimento desenvolvido sobre a Segurança dos Sistemas de Informação, orientada à criação de uma consciência social alargada sobre a sua necessidade, e o envolvimento das organizações no processo de análise, avaliação e construção das normas e guias de boas práticas.

De entre as diversas estratégias que é possível idealizar para atingir tais objectivos, uma que tem demonstrado particular eficiência é a criação de grupos de trabalho ad-hoc (semelhante a redes sociais) que integrem especialistas independentes e representantes de organizações com interesse na área em questão, envolvendo-os em tarefas de estudo, análise, implementação e definição das normas e guias de boas práticas. Um bom exemplo desta estratégia é o grupo de trabalho ISMS *Internationa User Group* (ISMS IUG) [11], criado em 1997 pela comunidade de organizações que assimilaram as normas BS 7799 e/ou ISO/IEC17799, com o objectivo de partilhar informação relativa à implementação daquelas normas, e que actualmente promove a adopção da nova família de normas ISO/IEC 27000.

É igualmente nesta linha de actuação que em 2004, por iniciativa do Instituto de Informática (II) e do Instituto Português da Qualidade (IPQ), foi criada a Comissão Técnica em Segurança da Informação (CT 163). Respondendo a uma necessidade crescente da adopção das normas internacionais já criadas, esta CT apoia o IPQ na sua função como Organismo Nacional de Normalização, no âmbito da segurança da informação, ao mesmo tempo que procura criar um grupo de trabalho que divulgue e incentive a adopção das normas e guias de boas práticas.

A ISO/IEC 27000

A família de normas ISO/IEC 27000 é uma tentativa de estabelecer uma linguagem comum, independentemente da natureza da organização, para a abrangente área da segurança da informação. Por essa via será possível compreender rapidamente o que é a política de segurança de uma organização, promovendo assim um ambiente de maior confiança no estabelecimento de relações entre organizações e indivíduos no que concerne à segurança da informação que necessita de ser partilhada. Embora este seja um esforço assumido pelo Subcomité SC 27, do Comité Técnico Conjunto ISO/IEC JTC1 (mais propriamente o seu grupo de trabalho WG1), ele conta com a colaboração de diversas outras organizações com trabalho similar, por vezes em áreas mais restritas,

como é o caso do instituto ITU-T no domínio das telecomunicações. Uma parte importante dos conceitos e procedimentos incluídos nesta família de normas foi herdada de normas bem conhecidas e já anteriormente referidas, como a BS 7799 e a ISO/IEC 17799. Por isso, não é de estranhar a clara ligação entre estas normas e os componentes homólogos dentro da família 27000. Com efeito, o plano de trabalho do SC27 relativos à família de normas ISO/IEC 27000 refere os seguintes documentos:

- ISO 27000 ISMS *Fundamentals and vocabulary*
- ISO/IEC 27001 ISMS – *Requirements* (publicado em Outubro de 2005 e que vem substituir a BS 7799 *Part 2:2002*)
- ISO/IEC 27002 (publicado em Junho de 2005 e que substituirá a ISO/IEC 17799 depois de 2007)
- ISO/IEC 27003 ISMS *Implementation guidance*
- ISO/IEC 27004 *Information security management measurements*
- ISO/IEC 27005 *Information security risk management*

Como se pode constatar a única norma publicada até à data é a ISO/IEC 27001, que define os requisitos necessários para a implementação de um ISMS e sobre a qual nos iremos debruçar no resto deste artigo.

A norma ISO/IEC 27001 [6] assenta na utilização de um modelo de processo conhecido como PDCA (*Plan-Do-Check-Act*), à semelhança do que é adoptado nas normas ISO 9001 e ISO 14001, o qual se encontra ilustrado na figura 2. Aliás, a correspondência com estas normas é tão acentuada neste aspecto, que justificou um anexo da ISO/IEC 27001 apenas dedicado à identificação dos itens correspondentes na estrutura de cada uma das normas. Como na grande maioria dos modelos deste tipo, é preconizado um ciclo de actividades que, no seu conjunto, define a forma de estabelecimento de um sistema de gestão de segurança da informação (ISMS), a sua implementação e operação, a sua monitorização e revisão e, finalmente, a sua optimização em função dos resultados obtidos em cada iteração do processo. Refira-se ainda que a adopção do modelo PDCA alinha esta norma com as recomendações gerais da OCDE sobre a segurança das redes e dos sistemas de informação [7].

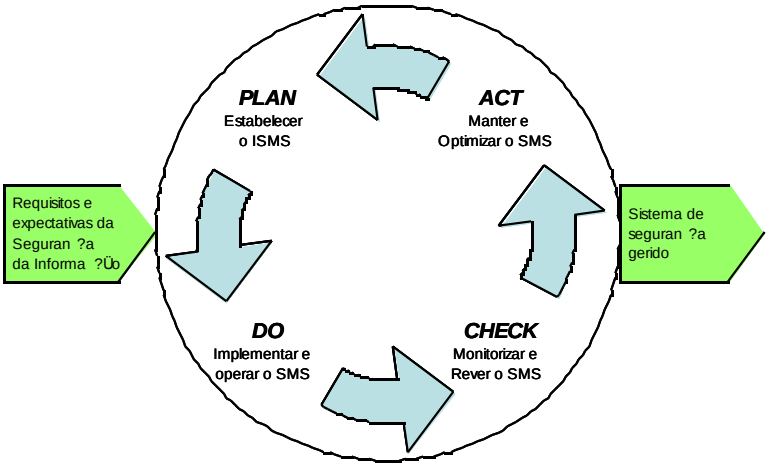

Figura 2 – Modelo PDCA para um ISMS

Na ISO/IEC 27001 estão igualmente incluídas recomendações com vista à identificação e avaliação do risco de segurança, assim como as opções de gestão genéricas para a mitigação do risco. Contudo, não se encontram aqui detalhados os processos ou métodos de implementação dessas recomendações, sendo para tal indicadas as normas complementares. Assim, no que diz respeito à

avaliação do risco, é indicada a norma ISO/IEC TR 13335-5, enquanto que relativamente à implementação de medidas como forma de mitigação do risco, é indicada a norma ISO/IEC 17799. Esta organização reflecte bem o principal objectivo da ISO/IEC 27001, que é sobretudo o de definir requisitos com vista à certificação. Nesta matéria a ISO/IEC 27001 herda muitas das recomendações de uma outra norma similar, utilizada também apenas para esse propósito nos últimos anos, a norma BS 7799 *Part* 2:2002, que passa então a ser preterida pela anterior.

Do ponto de vista da estrutura e no que respeita à sua componente central – a criação de um ISMS – a ISO/IEC 27001 encontra-se dividida em cinco secções, cada uma delas endereçando um aspecto específico da sua construção: o estabelecimento e gestão de um ISMS, a gestão da responsabilidade, a auditoria interna do ISMS, o processo de revisão do ISMS e o processo de melhoria. Cada uma dessas secções será abordada em seguida, realçando os aspectos considerados mais relevantes.

Estabelecimento e gestão de um ISMS

Esta é sem dúvida uma fase crucial de todo o processo e é sobre ela que recai a maior parte da atenção da ISO/IEC 27001. A norma define claramente a necessidade de um documento de fundo para suporte ao estabelecimento do ISMS, no qual devem constar, entre outros, os seguintes detalhes:

– Sobre o estabelecimento de um ISMS

- Definição do âmbito e as fronteiras do ISMS em termos do negócio e da organização (incluindo recursos, tecnologias, etc.). Na prática significa que é necessário proceder a uma análise do modelo de negócio e identificada a informação, os processos e os recursos que podem interferir com a segurança da informação. Qualquer excepção deve ser devidamente justificada por facilmente introduzir vulnerabilidades que podem afectar todo o sistema.
- Definição da política do ISMS em termos das características do negócio, da organização, da sua localização, recursos e tecnologias. Neste ponto o maior desafio é conseguir expressar claramente os objectivos da segurança, tendo em conta não só a cultura da organização, mas também a realidade dos seus parceiros, bem como o enquadramento legislativo. Não menos importante é conseguir especificar um critério que possibilite a quantificação do risco. Naturalmente, a estratégia da segurança da informação deve estar alinhada com a estratégia da organização e deve ser reconhecida ao mais alto nível da gestão.
- Definição da forma como será feita a avaliação do risco (incluindo a metodologia de avaliação e o critério de aceitação dos níveis de risco). Neste domínio as recomendações expressas na ISO/IEC 27001 são manifestamente insuficientes, sendo necessário o recurso a outra norma, como seja a ISO/IEC TR 13335-3.
- Identificação dos riscos (componente central da análise de risco), que exige a identificação dos recursos alvo (informação, tecnologias, imóveis, etc.), das suas vulnerabilidades, das ameaças que sobre eles pendem e ainda do impacte negativo que eventuais quebras de segurança possam implicar. As propriedades de segurança dos recursos que, no mínimo, devem ser analisadas são a confidencialidade, a integridade e a disponibilidade, muito embora outras sejam muito relevantes em determinados contextos como, por exemplo, a autoria, no caso das organização de saúde ou no comércio electrónico.
- Análise e quantificação do risco (incluído igualmente na análise de risco), o que implica a obtenção de valores para o impacte de quebras de segurança, da probabilidade da ocorrência de incidentes e de um valor final para o risco. Por vezes não é fácil quantificar esta matéria, sendo apenas possível usar estimativas ou recorrer a uma

análise mais qualitativa. Mais ainda, tipicamente não se chega a um valor de risco isolado, mas a um conjunto de valores associados a diferentes recursos. A análise desses valores, com base nos critérios de aceitação do risco definidos anteriormente, permite identificar os recursos que carecem de algum tipo de intervenção.
• Identificação das opções de mitigação dos riscos – tradicionalmente passa por aplicar medidas de controlo ou, conscientemente, aceitar o risco ou evitar o risco ou, ainda, transferir o risco para terceiros. O custo de cada uma das hipóteses deve ser determinado. No caso da aplicação de medidas de controlo devem seleccionar-se as medidas adequadas segundo os objectivos e requisitos definidos durante a avaliação e análise do risco. Deve ainda ter-se em conta os aspectos legais e contratuais que podem impor restrições. A ISO/IEC 17799 contém um conjunto detalhado dessas medidas que, naturalmente, devem incluir as medidas de detecção, correcção, dissuasão, diversão e prevenção. Por seu lado, a ISO/IEC 27001 inclui em anexo uma lista com algumas dessas medidas de controlo, consideradas obrigatórias e que devem ser consideradas como um conjunto mínimo.

– Sobre a implementação e operação do ISMS

• Criação de um plano de acção com base nos riscos de segurança, que identifique os procedimentos, recursos envolvidos e responsabilidades de gestão. Devem incluir-se igualmente os aspectos financeiros e a atribuição das funções de segurança ao pessoal envolvido, não esquecendo a necessidade de eventuais acções de formação e outras formas de disseminação do plano.
• Identificação dos parâmetros necessários para medir a eficiência das medidas de segurança estabelecidas (isoladas ou em grupo), assim como a identificação da forma como essas medições serão utilizadas na avaliação do respectivo desempenho. Estes parâmetros são essenciais para se proceder à avaliação futura da qualidade do plano e da correcção das opções tomadas.

– Sobre a monitorização e revisão do ISMS

• Definição de mecanismos que garantam que os procedimentos de monitorização e controlo são executados, permitindo detectar rapidamente erros de processamento, quebras de segurança ou mesmo simples tentativas e falhas na execução das medidas de segurança previamente definidas. O resultado desta monitorização permitirá medir a eficiência das medidas de segurança, usando os parâmetros acima identificados.
• Planificação de verificações periódicas à eficiência do ISMS (incluindo as políticas e os objectivos, bem como a revisão das medidas de controlo), tendo por base os resultados de auditorias de segurança, relatórios de incidentes, medidas de eficiência, sugestões e o *feedback* das pessoas envolvidas. O próprio processo de gestão do ISMS deve ser alvo da revisão, assim como o conjunto de requisitos inicialmente estabelecidos.
• Revisão periódica da avaliação do risco (ou em resposta a um evento estranho que a tal obrigue), tendo em particular atenção eventuais alterações da organização, das tecnologias, dos objectivos e estratégias do negócio, das ameaças, da eficiência das medidas de segurança implementadas e alterações externas, desde regulamentos a disposições legais.

– Manutenção e melhoria do ISMS

• Definição de mecanismos que garantam a implementação das melhorias ou modificações identificadas nos dois pontos anteriores. Estes mecanismos deverão ter

em conta as lições apreendidas das experiências de segurança da própria organização ou de outras organizações.
• Comunicação das acções e melhorias introduzidas a todos os parceiros, com um nível de detalhe adequado às circunstâncias e, quando relevante, prever eventuais reacções.

Tal como foi referido inicialmente, a ISO/IEC 27001 exige que todo o processo de estabelecimento e gestão do ISMS esteja documentado. Para além disso, muitas das tarefas de gestão derivadas dos requisitos anteriormente descritos exigem também documentação de suporte. Não admira, portanto, que a ISO/IEC 27001 inclua também alguns requisitos quanto à própria documentação. Nomeadamente, deverão existir todos os registos das decisões de gestão por forma a garantir que é possível estabelecer uma ligação entre estas e as acções que estão na sua origem, assim como a possibilidade de recriar todo o processo. É ainda importante demonstrar as relações entre as medidas de segurança e os resultados da avaliação do risco que lhe estão na origem e, subsequentemente, com a política e objectivos do próprio ISMS. Para tal a norma identifica um conjunto de documentos, sendo de realçar as declarações relevantes acerca dos objectivos e política do ISMS, assim como do seu âmbito, a descrição do método de avaliação do risco e o plano de acção para o risco de segurança da informação.

Dado a sua natureza, os documentos exigidos pelo ISMS devem ser protegidos e controlados. Naturalmente a ISO/IEC 27001 considera ainda vários procedimentos de manuseamento com o objectivo de garantir a autenticidade e integridade dos documentos e registos. O processo de gestão do ISMS deve contemplar cuidadosamente a execução desses procedimentos.

Gestão da responsabilidade de um ISMS

Um dos requisitos naturais relativamente à responsabilidade sobre o ISMS diz respeito ao empenhamento claro e inequívoco da gestão. Desde a definição dos objectivos, passando pela atribuição de recursos, pela delegação de responsabilidades aos indivíduos ligados directamente à implementação do ISMS, pela definição do critério de aceitação do risco e terminando na supervisão das auditorias e consequentes processos de melhoria, o envolvimento da gestão tem que ser permanente. Isto só é possível se a gestão do ISMS for encarada como uma verdadeira actividade de gestão e a Segurança da Informação for tida como um investimento.

Em particular no que respeita à atribuição dos recursos, deve ser cuidadosamente avaliada a adequabilidade das competências de cada elemento da organização a quem for atribuída cada uma das funções definidas no ISMS. Como é óbvio, os recursos (humanos, técnicos e financeiros) devem ainda ser em quantidade suficiente para implementar completamente o ISMS. Outro aspecto importante a ter em conta, ainda relativamente aos recursos humanos, é a sua formação, o desenvolvimento de competências e a consciencialização relativa à importância das funções associadas ao ISMS. Esta consciencialização deve estender-se a toda a organização através da divulgação necessária para que o ISMS seja naturalmente integrado com o modelo de negócio da organização. Tudo isto são requisitos sobre os quais devem aparecer evidências para uma eventual certificação à luz da ISO/IEC 27001.

Auditoria interna de um ISMS

A organização deve promover a realização de auditorias internas periódicas para determinar se os objectivos, os processos e procedimentos definidos no ISMS estão conformes. Quanto aos objectivos do ISMS, esta conformidade diz respeito aos requisitos acima identificados e, caso existam, alguns requisitos externos impostos por legislação ou outros regulamentos gerais. Quanto aos processos e procedimentos, é necessário verificar se eles estão efectivamente a ser executados conforme planeado e se o seu resultado está conforme as expectativas.

A forma como a auditoria deve decorrer, desde a escolha dos auditores até aos critérios a utilizar e o âmbito da sua acção, tudo deve estar devidamente explicitado. Da mesma forma, os responsáveis pelas áreas auditadas devem estar preparados para facultar a informação necessária, nomeadamente os resultados da monitorização (por exemplo, relativamente à ligação à internet, o responsável pela segurança da rede deve garantir que estão disponíveis os *logs* das *firewalls* ou de outros recursos envolvidos). É ainda um requisito que os resultados das auditorias fiquem devidamente registados.

Processo de revisão de um ISMS

A área de segurança dos sistemas de informação está em permanente transformação. Não só devido à evolução tecnológica, mas também devido às frequentes mudanças do meio em que se inserem as organizações, condicionado por sociedades abertas, com cada vez mais conhecimentos e meios de comunicação muito flexíveis. Tudo isto obriga a uma elevada atenção relativamente à necessidade de alterações no ISMS ou, simplesmente, às oportunidades de melhoria. A ISO/IEC 27001 recomenda que este processo de revisão ocorra, no mínimo, uma vez por ano e que seja dirigido sobretudo para os objectivos da segurança e para as políticas de segurança. Como nas restantes secções da ISO/IEC 27001, é um requisito obrigatório guardar os registos de toda a actividade ligada a este processo de revisão, obedecendo às regras definidas para o resto da documentação do ISMS.

Este processo de revisão é alimentado por informações de várias fontes, como sejam os resultados das auditorias internas, o *feedback* proveniente de colaboradores ou parceiros, o anúncio de novas técnicas e tecnologias, a experiência de operação do próprio ISMS, relatório ou *surveys* publicados por organizações que estudam a evolução da segurança da informação e qualquer outra fonte de informação que se julgue relevante. No que respeita aos resultados esperados do processo de revisão e dependendo obviamente dos factores que impõem modificações, é de esperar (tipicamente):

- actualizações ao documento que define o ISMS;
- uma reavaliação da análise de risco e, eventualmente, das opções de mitigação do risco;
- modificações aos procedimentos e controlos das medidas de segurança implementadas;
- modificações aos parâmetros e forma de obtenção das medidas de avaliação;
- realocação de recursos.

Com vista a uma maior eficiência na avaliação e controlo do processo de melhoria resultante da revisão, a ISO/IEC 27001 prevê a utilização de dois tipos de instrumentos: acções correctivas e acções preventivas. Ambas deverão ser consubstanciadas num documento que deve incluir as causas da acção, uma avaliação das medidas a executar, nomeadamente quanto à sua efectiva utilidade para evitar uma futura recorrência, um plano de aplicação e o registo das características mensuráveis que permitam avaliar o efeito dessas medidas. A grande diferença entre estes dois tipos de acções consiste no momento em que é percebida a não-conformidade. As acções correctivas aplicam-se após o reconhecimento da ocorrência, altura em que é necessário corrigir o seu efeito, enquanto que as acções preventivas aplicam-se quando existe a percepção de que poderá verificar-se a ocorrência de uma não-conformidade e que a mesma deve ser prevenida. Quando aplicado de uma forma continuada e devidamente controlada, este processo de revisão deve conduzir a uma melhoria efectiva do ISMS.

Certificação no futuro

Dado o nível de proliferação das TIC e das alterações que tal provocou no seio das organizações, sobretudo no que toca à necessidade de troca de informação rápida e segura, é hoje crítico ter uma forma de avaliação rápida da qualidade do ISMS de uma organização.

Aparentemente, tal apenas pode ser garantido por um mecanismo de certificação, o qual carece da definição de um conjunto comum de regras ou normas, assim como do seu processo de avaliação que, em última análise, estabelecerá um nível de certificação.
A família de normas ISO/IEC 27000 vai procurar criar as condições para esse grande objectivo, sendo a ISO/IEC 27001 a primeira componente a ser publicamente distribuída para adopção. Na realidade, esta norma apenas vem definir um conjunto de requisitos essenciais para estabelecer um ISMS numa organização. Contudo, esses requisitos obrigam à implementação de um processo contínuo de melhoria, onde é possível medir a qualidade do próprio ISMS. Estão assim criadas as bases necessárias para desencadear, desde já, os processos de certificação.
Do ponto de vista operacional, a ISO/IEC 27001 contém um detalhe reduzido, não servindo só por si para pôr a funcionar um ISMS. Para tal é necessário recorrer a outras normas, como as ISO/IEC 17799, 13335, 15408 e a BS 7799, esta última já largamente usada para certificação, conforme pode ser constatado em [11]. Mas à medida que estas e outras normas forem integrando formalmente a família de normas ISO/IEC 27000, estarão então criadas as condições para dispor realmente de uma base comum que permita regular a complexa e vasta área da Segurança dos Sistemas de Informação.

Bibliografia

1. Dhillon, G., *Principles of Information Systems Security: Texts and Cases*. 2006: Wiley.
2. Amatayakul, M., et al., *Handbook for HIPAA Security Implementation*. 2003: MLA, AMA Press.
3. Alberts, C. and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*. The SEI Series in Software Engineering. 2003: Addison-Wesley Professional. 512.
4. Lahti, C., S. Lanza, and R. Peterson, *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*. 2005: Syngress. 450.
5. Santos, H.D. *O Combate Electrónico - Ataques e Defesas sobre a Rede*. in *Seminário: A Evolução Tecnológica na Protecção da Informação em Sistemas Distribuídos*. 2002. Instituto de Defesa Naciona, Lisboa: Gabinete Nacional de Segurança.
6. ISO/IEC, *Information technology — Security techniques — Information security management systems — Requirements*. 2005, ISO copyright office: Geneva, Switzerland.
7. OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. 2002: Paris.
8. HIPAA.ORG, Março de 2006, http://www.hipaa.org/
9. OCTAVE® Information Security Risk Evaluation, Março de 2006, http://www.cert.org/octave/
10. COBIT, Março de 2006, http://www.isaca.org/cobit
11. ISMS International User Group, Março de 2006, http://www.xisec.com/