43 – Outubro de 2002

Por que falam tanto da Norma ISO17799?

Para que serve uma norma ISO? Muitos de nós nunca fizemos esta pergunta, apesar de estarmos cotidianamente em contato com produtos certificados, empresas que que possuem o reconhecimento de organismos certificadores e, em alguns casos, relações comerciais business to business que só ocorrem pela presença mútua de conformidade com determinada norma. Sendo didático, podemos dizer que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço.

Mas por que é que tantas empresas buscam adesão a essas normas? Em uma economia tradicional e saudável, as empresas representam engrenagens de um sistema complexo onde há trocas constantes de bens e serviços, através da utilização da moeda, para concretizar as relações financeiras. Diante disso, é saudável que todas as empresas procurem uma base comum que facilite a interação e a confiança entre elas e, oportunamente, busquem elementos que as projetem mais, conquistando diferenciais competitivos. Essa é a lei de mercado.

As normas surgiram para sugerir bases comuns, cada qual com a sua especificidade, como vemos na ISO9001 – Qualidade e a ISO14000 – Meio Ambiente. São exemplos de critérios, padrões e instrumentos de controle, aplicáveis parcialmente ou totalmente em função da natureza de cada negócio, que acabaram formando cultura e recebendo o reconhecimento mundial de segmentos específicos.

À medida que os negócios passaram a aplicar tecnologia da informação para suportar processos importantes da empresa e, muitas vezes, os mais críticos e representativos para a sobrevivência e continuidade operacional, a proteção da informação passou a ser fator crítico de sucesso.
A tecnologia da informação deixou de ser coadjuvante e passou à protagonista no desenvolvimento corporativo, servindo de base comum para a troca eletrônica de informações e para a intermediação de transações comerciais. Estamos falando de um parque tecnológico cada vez mais integrado, porém heterogêneo, que mantém custodiadas informações de seus parceiros da cadeia produtiva, informações de clientes, fornecedores e ainda informações estratégicas da empresa.

O mercado atingiu um nível de automação, de compartilhamento de informações e de dependência tal que motivou a elaboração e compilação de uma norma específica para orientar a padronização de uma base comum voltada para a gestão de segurança da informação. A ela dá-se o nome de BS7799: parte 1, que possui uma versão brasileira, a NBR /ISO17799:1.
Para os que desconhecem o assunto, a primeira parte da Norma Britânica BS7799 deu origem à versão ISO17799:1 após avaliação e proposição de pequenos ajustes. Em seguida, foi traduzida e disponibilizada pela ABTN – Associação Brasileira de Normas Técnicas.

Tem o objetivo de definir na parte 1 um Código de Prática para a Gestão de Segurança da Informação. São ao todo 10 domínios reunidos em 36 grupos que se desdobram em um total de 127 controles. Por se tratar de um código de prática, esta parte da norma não é objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação.

Domínios

1. Política de Segurança
2. Segurança Organizacional
3. Classificação e Controle dos Ativos de Informação
4. Segurança de Pessoas
5. Segurança Física e do Ambiente
6. Gerenciamento das Operações e Comunicações
7. Controle de acesso
8. Desenvolvimento e Manutenção de Sistemas
9. Gestão da Continuidade do Negócio
10. Conformidade

Por hora, a parte 2 da BS7799, que especifica um framework de segurança chamado SGSI – Sistema de Gestão de Segurança da Informação, está em consulta pública a fim de gerar a versão ISO correspondente e será, quando concluída, a base para a certificação das empresas. Enquanto isso não ocorre, a alternativa é buscar a conformidade e a certificação da BS7799, que já poderia representar uma pré-certificação para a ISO17799.

É notório que uma norma não ganha respeito e adesão automática pelo simples fato de existir. O processo é lento, mas pode se tornar tão rápido sobretudo quando temos em mente que, a exemplo do que aconteceu com a ISO 9001, aderir pode significar um importante diferencial competitivo para as organizações.

Marcos Sêmola *é Mestrando em Economia Empresarial, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente Nacional de Produtos e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br