

# GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A adoção de um modelo corporativo de gestão de segurança da informação permite à organização equacionar os desafios de sua proteção. Entretanto, os procedimentos de segurança não devem ser implementados sem uma política formalmente definida. Essas políticas devem fornecer claramente todas as orientações necessárias para a condução segura dos negócios da organização. A segurança da informação abrange, além

de aspectos técnicos, aspectos humanos, fazendo com que seja necessária uma abordagem de gestão que considere a cultura, a educação e a conscientização dos envolvidos acerca dos meios adequados para se usarem as ferramentas de TI. **Alberto Luiz Albertin**, professor titular da FGV-EAESP, e **Luis Hernan Contreras Pinochet**, doutorando em Administração de Empresas na FGV-EAESP, recomendam os seguintes livros:



- **WRITING INFORMATION SECURITY POLICIES.** Scott Barman. Indianapolis, IN: New Riders Publishing, 2002. 216 páginas.

A obra afirma que as políticas de segurança da informação representam uma função crítica na defesa de sistemas em rede. Explica por que e como deve ser escrita uma política de segurança, discutindo o processo, observando as diferentes áreas envolvidas na segurança, as direções do discurso da política, e oferece exemplos para uma maior percepção da importância de sua prática. São apresentadas algumas sugestões para coordenar e entender o desenvolvimento de uma política de segurança da informação.



- **INFORMATION SECURITY, POLICIES AND ACTIONS IN MODERN INTEGRATED SYSTEMS.** Mariagrazia Fugini e Carlo Bellettini. Hershey, PA: Idea Group Inc, 2004. 341 p.

Os autores destacam que os sistemas de informação nas empresas estão se tornando heterogêneos, pois os dados e as aplicações envolvem vários locais e diferentes plataformas tecnológicas. Os problemas de segurança nesses sistemas vão desde a privacidade e confidencialidade de dados até a confiança que os usuários possuem nos processos e na autenticidade dos dados, na segurança física, e em questões organizacionais. A obra apresenta recentes pesquisas que aproximam os sistemas integrados das novas necessidades de segurança da informação.



- **INFORMATION SECURITY, POLICIES, PROCEDURES, AND STANDARDS: Guidelines for Effective Information Security Management.** Thomas Peltier. Boca Raton: Auerbach Publications – CRC Press LLC, 2002. 297 p.

O livro cobre três seções principais: as políticas, os procedimentos e os padrões. Cada seção inicia com a definição de terminologias, conceitos e a apresentação de estruturas de documentos. A obra contém *checklists*, modelos de políticas, procedimentos, padrões, diretrizes, e um resumo do Padrão Britânico 7799 e da ISO 17799, além de uma pesquisa desenvolvida na indústria indicando as melhores práticas que podem ser personalizadas às necessidades de qualquer organização.



- **MANAGING A NETWORK VULNERABILITY ASSESSMENT.** Thomas R. Peltier, Justin Peltier e John A. Blackley. Boca Raton: Auerbach Publications – CRC Press LLC, 2003. 291 p.

A obra fornece uma estrutura formal de segurança da informação, buscando eliminar ameaças em rede, e aborda passos como processos administrativos, o desenvolvimento de um escopo, a compreensão do uso de uma metodologia de avaliação, a criação de um time de avaliação especialista, e a produção de um valioso relatório administrativo. Também apresenta críticas relacionadas com as políticas de segurança fundadas na ISO 17799, revisões sobre as exigências dos padrões internacionais, e discute como delegar e avaliar a segurança de componentes tecnológicos e organizacionais.



- **SEGURANÇA DA INFORMAÇÃO: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** Adriana Beal. São Paulo: Atlas, 2005. 175 p.

A proteção dos ativos de informação adquire o *status* de questão estratégica para as organizações, tanto pelo alto valor associado a esses ativos quanto pelos impactos negativos que a destruição, alteração ou divulgação indevida de informações ocasiona na organização. A obra oferece subsídios para o tratamento da questão da segurança da informação num contexto global. Com base nos princípios de melhores práticas, as organizações poderão desenvolver estratégias eficazes para uma proteção mais abrangente de seus ativos.