1.O modelo PDCA

O modelo PDCA (Plan-Do-Check-Act), também chamado de ciclo de qualidade de Deming, forma a base para determinar, implementar, monitorar, controlar e manter o sistema de gerenciamento da segurança da informação (ISMS).

A ISO 27001:2005 exige o modelo PDCA como a base geral para a implementação e a manutenção do ciclo de gestão.

Na ISO 27001:2013 isso mudou. A ISO percebeu que a maioria das empresas e organizações com ou sem fins lucrativos já possui seu próprio ciclo de gestão de negócios, sendo ou não baseado no PDCA. PDCA nem sempre é compatível com o ciclo de gestão adotado por uma empresa em particular. Por essa razão, na ISO 27001:2013 o texto mudou para a obrigação da organização estabelecer, implementar, manter e melhorar continuamente o sistema de gerenciamento da segurança da informação, em conformidade com os requisitos dessa norma internacional. É claro que a norma apresenta requisitos para estabelecer o ISMS. No entanto, a obrigação de utilizar o ciclo PDCA desapareceu.

1.2 Projetar o ISMS (Planejar)

Na fase de projeto, é desenvolvida e documentada a política de segurança da informação. Aqui os objetivos da segurança da informação, os processos relevantes e os procedimentos são definidos; isso assegura que os riscos sejam gerenciados. Esses objetivos devem, é claro, apoiar os objetivos de negócios da organização. As medidas de segurança podem ser adotadas com base em uma análise de riscos e de custo-benefício. A fase de planejamento se aplica não só à política principal, mas também a todos os documentos de políticas que apoiam e as regulamentações subjacentes.

1.3 Implementar o ISMS (Executar)

Nesta fase, a política de segurança da informação e os procedimentos e medidas subjacentes são implementados. As responsabilidades são alocadas a cada sistema e/ou processo de informação.

1.4 Monitorar e checar o ISMS (Checar)

Nesta fase, são realizados controles utilizando uma autoavaliação e, onde possível, medições são realizadas para ver se a política de segurança da informação é executada corretamente. Um relatório sobre o assunto é emitido para gerência responsável e para o Diretor Corporativo de Segurança da Informação (CISO).

1.5 Manter e ajustar o ISMS (Agir)

Nesta fase final, são realizadas correções e são tomadas medidas preventivas com base nos resultados da auditoria interna. O ISMS é atualizado à luz de quaisquer

descobertas particulares. O ciclo PDCA é contínuo. Isso está descrito em um manual ISMS.