ISO 27001: Sistema de Gestão da Segurança de Informação

O referencial ISO 27001 estabelece uma nova forma de lidar com a informação, consolidando um conjunto das melhores práticas da gestão de segurança da informação. A implementação da mesma consubstancia-se num Sistema de Gestão de Segurança da Informação (SGSI).

A norma ISO/IEC 27001 (evolução da antiga BS 7799-2:2002) certifica as organizações em termos de gestão de segurança da informação. A certificação demonstra que estas organizações possuem um sistema de gestão que protege a sua informação com mecanismos de controlo adequados às suas necessidades e realidades, verificados por uma entidade externa (em Portugal por instituições como APCER, LUSAENOR, BVQ e SGS, entre outros, devidamente acreditados pelo IPQ - Instituto Português da Qualidade). Através da avaliação e gestão do risco este sistema procura garantir a continuidade de negócio e diminuir o impacto de eventuais incidentes de segurança.

Uma organização ao ser certificada em termos de Gestão da Segurança da Informação obtém, além de outros, os seguintes benefícios:

- Credibilidade comercial;

- Redução de custos de incidentes;

- Cumprimento de leis e regulamentos;

Figura 1: Componentes principais de um sistema de gestão da segurança da informação