SICUREZZA DELLE INFORMAZIONI

VALUTAZIONE DEL RISCHIO
I SISTEMI DI GESTIONE
LA NORMA ISO/IEC 27001:2013

Cesare Gallotti

Versione 10 giugno 2014

Indice

Presentazione e ringraziamenti

Pensino ora i miei venticinque lettori che impressione dovesse fare sull'animo del poveretto, quello che s'è raccontato.

Alessandro Manzoni, *I promessi sposi*

Nel 2002 scrissi il libro *Sicurezza delle informazioni - Analisi e gestione del rischio* per la FrancoAngeli [28] e mi ero divertito molto a scriverlo. Mi ha fatto anche molto piacere incontrare in questi anni più di 25 persone, che l'avevano letto e apprezzato; purtroppo, spesso, l'avevano preso in prestito da una biblioteca e questo non ha aiutato ad aumentare le vendite.

Va detto che non speravo assolutamente di guadagnare alcunché da quella operazione. Speravo solo di ripagarmi del toner e della carta utilizzati per stampare e correggere le bozze.

Dopo più di dieci anni ho voluto rimettere su carta (elettronica) le idee maturate durante i corsi di formazione, le presentazioni, le discussioni con colleghi e amici, gli incontri a livello nazionale e internazionale per scrivere la ISO/IEC 27001:2013. In alcuni casi, alcune delle convinzioni del 2002 sono cambiate, grazie ai tanti audit e progetti di consulenza fatti in questi anni.

Si tratta quindi più di una raccolta di appunti che di un vero e proprio saggio:

- la prima parte riporta le basi per descrivere la sicurezza delle informazioni e un sistema di gestione per la sicurezza delle informazioni;
- la seconda parte descrive la valutazione del rischio, con un'ampia parte teorica, bilanciata da molti esempi; i calcoli presentati non sono necessari per comprendere appieno i concetti esposti;
- la terza parte descrive i controlli di sicurezza ed è stata ricavata dagli appunti, basati sulla ISO/IEC 27002, che utilizzo per le attività di audit e di consulenza;