

Abstract

This article concisely describes the freshly released ISO/IEC 27000:2009 introducing its contents, explaining its importance and illustrating the normative context in which it will stand including the main details about related standards.

Famiglia 27000: Definizioni di Sicurezza

La ISO/IEC 27000:2009 è l'ultima norma nata nella "famiglia 27000", che sta prendendo forma in seno al SC27 (IT Security techniques) del JTC1. Questa norma, alla sua prima edizione assoluta, rientra nella categoria dei "vocabolari" ma, come vedremo più in dettaglio, non si limita solo a questo, siccome fornisce anche una panoramica delle norme ad essa legate. La capostipite della famiglia in questione è la ISO/IEC 27001:2005, che stabilisce i requisiti di un Sistema di Gestione per la Sicurezza delle Informazioni (in breve SGSI), fortemente ma non esclusivamente legato al mondo IT. La ISO/IEC 27001:2005 è stata elevata da norma nazionale (BS 7799) a internazionale. Durante questo passaggio si è pensato, vista la complessità e l'estensione della materia, di creare tutto un insieme di documenti ad essa collegati. Con questa intenzione è stato riservato lo spazio di numerazione tra 27000 e 27040. Al momento della stesura del presente articolo (agosto 2009) sono state pubblicate 6 norme in questa numerazione mentre ben altre 17 si trovano in un variegato stato di sviluppo, come è possibile osservare nello schema seguente.

IS	Non IS
27000:2009	27003 FDIS
	27004 FDIS
	27007 CD
27001:2005	27008 WD
	27010 WD
	27013 WD
	27014 WD
27002:2005	27015 WD
	27031 CD
	27032 WD
27005:2008	27033-1 CD
	27033-2 WD
	27033-3 CD
27006:2007	27034 CD
	27035 CD
	27036 WD
27011:2008	27037 WD

La maggior parte delle norme legate alla ISO/IEC 27000:2009 sono delle linee guida per l'implementazione di SGSI in settori specifici quali le aziende di telecomunicazioni (27011) e per l'esecuzione di processi da inerenti la sicurezza, primi tra tutti l'IT risk management (27005) e le misurazioni di efficacia e performance (27004). A queste si aggiungono poi norme dedicate a tematiche specifiche quali la continuità operativa (27031) e la sicurezza delle applicazioni (27034).

La ISO/IEC 27000:2009 è nata per assolvere un ruolo comune rispetto a questa nascente costellazione normativa, rispecchiando la funzione di glossario e di introduzione che la ISO 9000:2005 ha per la più nota "famiglia 9000", capostipite dei sistemi di gestione. Un'ulteriore particolarità che contraddistingue questa nuova norma deriva dalla decisione del SC27 di distribuirla gratuitamente, visto il suo carattere generale e introduttivo. Questa scelta non è molto comune in ambito ISO¹ ma serve anche a facilitare e rafforzare la

¹ Per l'elenco delle norme ISO liberamente disponibili si visiti l'indirizzo:

<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

divulgazione della norma e dell'intera famiglia.

Nella ISO/IEC 27000:2009, dopo una breve premessa, sono raccolti tutti i termini e le relative definizioni applicabili alla sicurezza delle informazioni. Prima della sua uscita queste definizioni si dovevano reperire con difficoltà saltando continuamente tra la ISO/IEC 27001:2005 e la complementare ISO/IEC 27002:2005. Segue un'introduzione ai sistemi di gestione e alla sicurezza delle informazioni, preludio di una spiegazione più dettagliata dei processi e delle attività legate alle principali fasi del ciclo di vita di un SGSI. Di particolare interesse quindi i fattori critici di successo e i principali benefici derivanti dall'adozione di questo tipo di sistema di gestione. Nella parte finale del documento è fornita una carrellata sulle norme della famiglia, nel loro insieme e singolarmente.

Va infine segnalato che per questa norma sarà molto probabilmente prevista una revisione nel prossimo futuro, al fine di mantenerla allineata sia con l'espansione della famiglia sia per renderla immediatamente parlante con la ISO/IEC 27001:2005, attualmente in revisione e la cui uscita è prevista per il 2010.

E' singolare notare come, nonostante nel settore IT e ancora di più nella sua sicurezza le norme riscuotano un'attenzione limitata, si rilevi una così forte attività normativa. Attualmente la "famiglia 27000", nata per essere applicata a qualsiasi tipo di organizzazione, ha ben pochi eguali nel panorama internazionale. Basti pensare che le aziende certificate ISO/IEC 27001, le quali sono solo una piccola minoranza rispetto a quelle che la adottano, sono oltre 5600 a livello mondiale e 140 a livello italiano².

L'uscita della ISO/IEC 27000:2009 aggiunge un importante tassello verso la definitiva affermazione e il completamento di questo importante sistema normativo, a cui anche altri schemi, quali ad esempio ISO/IEC 20000, stanno iniziando a riferirsi in modo esplicito e diretto.

Fabio Guasconi

Impegnato dal 2003 come consulente per la sicurezza delle informazioni, con particolare attenzione per le tematiche di analisi del rischio, gestione della sicurezza e verso le norme internazionali, a cui contribuisce attivamente tramite UNINFO e ISO, ha ottenuto le qualifiche di CISA e CISM. E' lead auditor qualificato con significativa esperienza sullo schema ISO/IEC 27001 (della cui traduzione in italiano è stato editor) e ha una conoscenza approfondita delle diverse attività di verifica e miglioramento della sicurezza. Laureatosi in Informatica a Torino, presiede attualmente il comitato italiano SC27 per la sicurezza delle informazioni di UNINFO ed è responsabile della Divisione Sicurezza Informazioni presso @ Mediaservice.net S.r.l.

² Dato rilevato a fine Agosto 2009