

Norme ISO e Sicurezza Informatica

Revisione dell'omonimo articolo uscito su "ICT Security" n.52 Gennaio-Febbraio 2007

L'ISO (International Organization of Standardization) è l'ente di riferimento per la normazione a livello mondiale, include delegazioni da 156 paesi e ha una produzione di oltre 1200 norme all'anno tra revisioni e nuovi documenti.

Descrivere la struttura di questa grande fucina globale esula dagli scopi di questo articolo, ma basti sapere che uno dei suoi comitati (l'ISO/SC27) si occupa di IT, e in particolare di Gestione della Sicurezza delle Informazioni. Questo comitato si è di recente incaricato della redazione della ISO 17799:2005, ereditiera delle sorti della famosa BS 7799 e della norma complementare ISO 27001:2005.

La cadenza delle riunioni di questo comitato, composto da professionisti del settore provenienti da tutto il mondo, è normalmente semestrale e gli ultimi eventi si sono tenuti a Glenburn Lodge (Sud Africa) e tra Mosca e S.Pietroburgo.

La famiglia 27000

Quando i delegati non sono riuniti a seguire i gruppi di lavoro dedicati alle singole norme, si istruiscono delle sessioni plenarie per

decidere delle questioni di maggiore importanza riguardanti tutto il comitato. Centrale durante il convegno madrileño è stata la discussione sullo sviluppo di quella che si è deciso di chiamare "famiglia" (invece di serie) 27000.

Una delle ultime norme che sono entrate a fare parte della famiglia è logicamente la ISO 17799:2005 la quale dagli ultimi mesi del 2007 (data slittata rispetto ad Aprile per dare più tempo agli enti nazionali) sarà ufficialmente nota come ISO 27002:2005, cosa che rende ancora più evidente il suo legame con la capostipite ISO 27001:2005; quest'ultima rimarrà comunque documento principale e requisito certificativo tra le nuove norme.

La maggior parte di queste ultime sarà costituita da guide implementative o metodologiche legate ai sistemi di gestione per la sicurezza delle informazioni (SGSI o ISMS che dir si voglia).

Vediamo nomi e titoli delle principali:

- ISO 27000: Fundamentals & Vocabulary
- ISO 27001: ISMS Requirements
- ISO 27002: Code of Practice for ISM
- ISO 27003: ISMS Implementation Guidance
- ISO 27004: Measurements
- ISO 27005: Risk Management
- ISO 27006: Requirements for the Accreditation of Certification Bodies
- ISO 27007: Guidelines for ISMS auditing

A queste primi membri della famiglia, che sono in un avanzato stadio di sviluppo, se

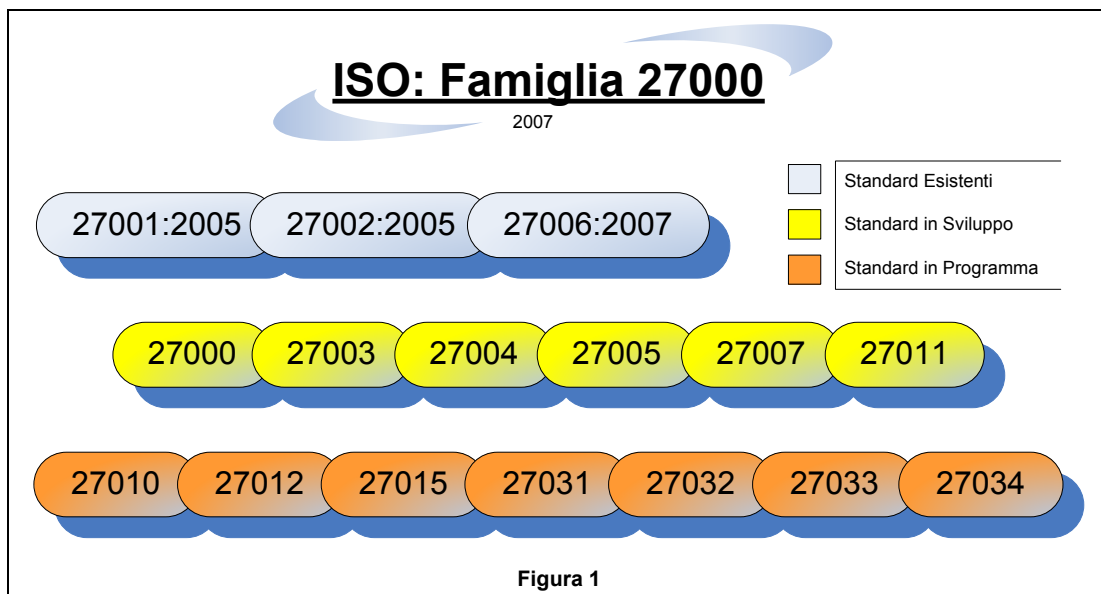


Figura 1

ne aggiunge una nutrita schiera composta da linee guida per l'implementazione degli ISMS, espressamente sviluppate per specifici settori di interesse. Tale gruppo collocherà la sua numerazione probabilmente tra la 27010 e la 27020 e la capostipite sarà probabilmente la ISO 27011: ISMS Guidelines for TLC seguita "a ruota" da quella per il settore Automotive (ancora priva di numerazione). Questi numeri non sono però ancora da considerarsi definitivi.

Attualmente è inoltre allo studio l'uso della numerazione tra 27020 e 27040 per altri standard legati alla sicurezza delle informazioni ma non facenti strettamente parte del gruppo "ISMS", alcuni dei quali sono già esistenti. In particolare le aree di interesse individuate sono IDS, Incident Management, Cybersecurity e i servizi di disaster recovery.

Un riassunto visivo dello stadio di sviluppo della famiglia (nel suo ramo più legato agli ISMS), a fine 2006, è riportato per chiarezza in Figura 1 (la 27002 sarà ancora ufficialmente 17799 fino agli ultimi mesi del 2007).

ISO 27004 – Measurements

Entrando nel dettaglio delle singole norme, la 27004 è una di quelle a cui l'autore ha dedicato più tempo ed attenzioni. Tale norma è dedicata ad un argomento che recentemente sta attirando molto interesse ma sul quale le opinioni sono ancora decisamente divergenti (quando non drasticamente opposte!).

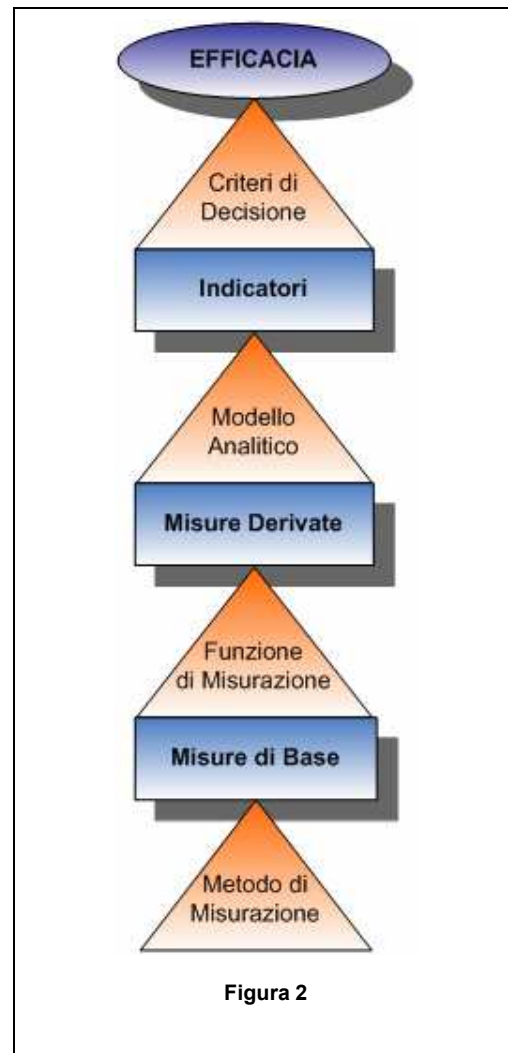
Prima di descriverne il contenuto è opportuno premettere un paio di concetti fondamentali:

- 1) questa norma è una linea guida pertanto ciò che si trova al suo interno sono delle "best practices". Il fatto che in pratica moltissimi si atterranno ad esse è un altro discorso ...
- 2) lo scopo della norma è di rendere possibile la misura dell'efficacia sia dei singoli controlli che di gruppi di essi fino a considerare tutto l'ISMS; essa no

n è rivolta al benchmarking, se non in minima parte, ma al miglioramento dell'ISMS stesso.

La 27004 imposta una serie di linee guida su come scegliere, sviluppare, implementare, raccogliere, verificare e utilizzare le misurazioni, installando un ciclo di PDCA integrato con quello dell'ISMS vero e proprio.

La stessa norma invita inoltre a considerare solo i controlli più rilevanti per l'organizzazione in base ad una scala di priorità predefinita, non tutti i controlli (è auspicabile una progressiva estensione delle misurazioni ad un numero sempre crescente di essi).



Entrando nel vivo del documento vengono definiti due tipi di misurazioni: di conformità e di prestazione.

Le prime riguardano la distanza fra un'implementazione e le policy aziendali inerenti mentre le seconde misurano l'efficacia dei controlli di sicurezza.

Ogni misurazione in generale deve soddisfare alcuni requisiti di base quali: essere gestita, avere dei responsabili, dei destinatari ed una documentazione completa (è incluso in allegato il fac-simile di una scheda dettagliata simile a quella del NIST SP800-55). I metodi di misurazione possono variare di molto anche tra organizzazioni simili, potendosi basare su dati che possono spaziare dalle più complesse statistiche ai più classici questionari.

Il funzionamento del processo di misurazione in generale, schematizzato in Figura 2, parte dall'applicazione di un *metodo di misurazione* da cui si ottengono delle *misure di base* (i dati veri e propri), che possono essere aggregati in differenti *funzioni di misurazione* che portano infine ad avere delle *misure derivate*.

Una volta giunti a questo livello attraverso l'applicazione di *modelli analitici* si ottengono gli *indicatori*, che stanno alla base dell'intero processo decisionale supportato dalle misurazioni. Tale processo è volto a stabilire l'efficacia di ISMS, obiettivi di controllo o semplici controlli, basandosi sui *criteri di decisione* prestabiliti nell'organizzazione.

Una parte di particolare interesse per i professionisti del settore sarà l'allegato B, dove verranno raccolte numerose reali misurazioni esemplificative. Un rapido esempio ispirato da questa sezione, per dare una dimensione concreta a quanto esposto finora, può essere la misurazione di prestazione riguardante il controllo 10.4.1 (codice dannoso o malware); essa è definita come la percentuale di eventi legati al codice dannoso che hanno provocato degli incidenti di sicurezza rispetto al totale di quelli che sono stati bloccati dalle contromisure e non.

Per il resto la norma ricalca i principi generali, già evidenziati nella 27001, di coinvolgimento della Direzione, formazione

del personale e in generale di buona governance. Sul sito ISO è da segnalare che è acquistabile il FCD (final committee draft) della norma.

ISO 27005 – Risk Management

Questa norma, seguita attivamente dall'autore, è in sviluppo da un periodo di tempo decisamente maggiore rispetto alla precedente, essendo nata originalmente come quarta parte della famiglia ISO 13335 (meglio nota come Guidelines for the Management of IT Security o GMITS) e successivamente "spostata" nella famiglia 27000. Per questo motivo il suo stadio di lavorazione è ben più avanzato rispetto alla 27004 e vedrà la luce tempo prima di essa; va sottolineato che entrambe sono definite come linea guida.

Molti dei termini citati nel seguito sono spesso utilizzati (e/o tradotti) con altre accezioni, pertanto può essere d'aiuto fare un po' di chiarezza sulla terminologia prima di procedere, onde evitare possibili cantonate.

Dalle definizioni riportate al suo interno:

- *Identificazione dei Rischi* – identificazione di asset, minacce, vulnerabilità, impatti e controlli di sicurezza attivi
- *Stima dei Rischi* – calcolo del rischio attraverso la valorizzazione di quanto individuato nell'identificazione e dei controlli di sicurezza attivi
- *Classificazione dei Rischi* – comparazione dei valori di rischio ottenuti con i criteri di valutazione prestabiliti al fine di determinare le azioni da intraprendere

Nella 27005 il processo di gestione dei rischi viene schematizzato in due macro fasi: *valutazione* (Risk Assessment) e *trattamento* (Risk Treatment) dei rischi, a cui si aggiungono quale "collante" la *comunicazione dei rischi* e l'*accettazione* degli stessi quale stadio finale. Propedeutica a tutto il processo è la definizione dell'ambito, ovvero dell'estensione dell'analisi in termini di processi, risorse etc.

Com'è possibile osservare in Figura 3, la *valutazione dei rischi* è a sua volta

composta dall'*analisi dei rischi* (Risk Analysis) e dalla *valorizzazione dei rischi* (Risk Evaluation). Durante l'*analisi dei rischi* vengono identificati gli asset, le minacce e le vulnerabilità rilevanti per il perimetro del Sistema, quindi si procede all'adeguata valorizzazione degli elementi identificati, la quale può essere qualitativa (e.g. alto, medio, basso) o quantitativa (e.g. in euro o basata su statistiche).

La *valorizzazione dei rischi* prevede la comparazione dei livelli di rischio individuati con i criteri di valutazione definiti.

Questa particolare analisi è un'attività sempre più riconosciuta come necessaria in tale ambito e la sua importanza è esplicitamente sottolineata nel documento. Osservando la stessa figura è possibile notare quanto anche in questa norma legata agli ISMS sia pervasivo il concetto di miglioramento continuo e di ciclicità degli stadi.

Una volta terminata l'articolata fase di *valutazione dei rischi*, si passa a quella di *trattamento dei rischi*; tale fase include fondamentalmente le quattro possibili azioni che possono essere esercitate sui rischi:

- 1) Evitare, grazie a modifiche al processo o all'ambiente
- 2) Trasferire, ad altre società (outsourcing o assicurazioni)
- 3) Ridurre, applicando contromisure o controlli opportuni
- 4) Accettare

Un singolo rischio può passare diverse volte attraverso questa fase se si sceglie l'azione di ridurre, ritornando nuovamente alla *valutazione dei rischi* una volta che le contromisure opportune sono state applicate.

Le prime tre azioni generano un rischio residuo, il quale passa in seguito attraverso una decisione finale sulla sua accettazione, che può a sua volta rimandare il rischio ad una delle fasi precedenti in caso sia di tipo negativo.

La riduzione dei rischi è, prevedibilmente, l'attività più "interessante" e nella norma vengono descritti alcuni vincoli che possono influenzare la scelta di una contromisura rispetto ad un'altra, derivanti non solo da fattori tecnici od economici, ma anche

ambientali, etici, legali, legati al personale etc.

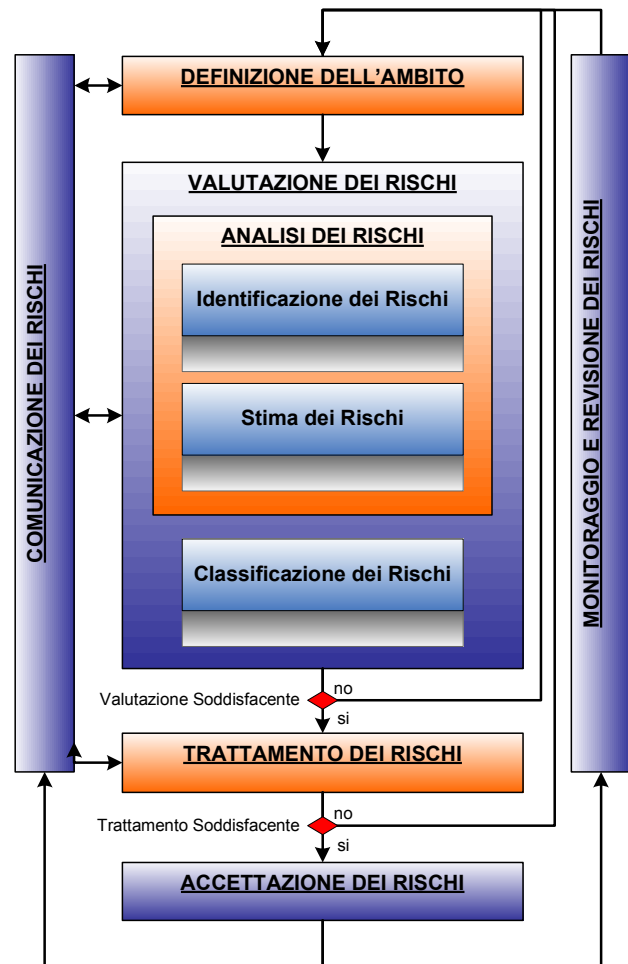


Figura 3

Come già osservato per la 27004, anche qui viene posta particolare enfasi nelle attività di monitoraggio e di revisione e in particolare nella loro continuità temporale.

La norma è particolarmente ricca di allegati, che comprendono tipologie di asset, elenchi di minacce, vulnerabilità e spunti di carattere metodologico. Anche di questa norma, sul sito ISO, è acquistabile il FCD (final committee draft) provvisorio.

ISO 27000, 27003, 27006, 27007

Tra le altre principali norme in sviluppo, la 27000 andrà a coprire un ruolo di "collante" per tutta la famiglia; in essa saranno indicati

i concetti alla base dei sistemi per la gestione della sicurezza delle informazioni e saranno riportate le definizioni generali di maggiore rilievo. Questa norma ricoprirà in pratica lo stesso ruolo della ISO 9000.

La 27003 è la norma della famiglia che si trova in uno stadio più arretrato ma inizia comunque a prendere forma. Il suo fine è quello di fornire una guida implementativa per il ciclo PDCA, di fondamentale importanza per gli ISMS e per diverse norme correlate che ne fanno uso come la 27004. In pratica è un walk-through della norma di riferimento (27001), espandendo in dettaglio tutte le principali attività del punto 4 di quest'ultima e definendo ad ogni passo:

- precondizioni ed obiettivi
- chi deve essere coinvolto
- come fare cosa
- risultati

Per quanto riguarda la 27006 invece il discorso è decisamente più interessante: tale norma è nata originalmente come revisione dell'EA-7/03 che definiva le linee guida per l'accreditamento degli enti di certificazione per gli ISMS.

Inizialmente sviluppata come 27015, questa norma definisce, a differenza delle altre, dei requisiti e non delle linee guida, acquisendo un'importanza assai maggiore.

Al suo interno sono inizialmente definiti i principi su cui si devono basare gli enti di certificazione e successivamente i requisiti a cui devono sottostare, organizzati in maniera più chiara e sintetica rispetto all'EA-7/03. Sono inoltre presenti quattro allegati con calcoli e tabelle esemplificative sul calcolo dei tempi di audit, sulla classificazione dei controlli da verificare, etc. La 27006 è stata approvata a Febbraio di quest'anno dopo un iter rapidissimo ed è ora un punto di riferimento importante per gli organismi di certificazione e per gli auditor degli ISMS.

A chiudere la serie di linee guida direttamente relazionate all'ISMS vi è il recente inizio dei lavori sulla 27007, il cui contenuto ancora in fase di definizione verterà principalmente sulle tecniche e modalità consigliate per condurre un audit su un ISMS. Particolare attenzione sarà

concentrata sui contenuti dei documenti focali quali il SoA e il report della valutazione dei rischi.

Altre norme dal SC27

I cinque gruppi di lavoro (WG) del SC27 sono inoltre impegnati nello sviluppo di diverse altre norme di tutto interesse, non direttamente legate alla famiglia 27000, tra cui vale la pena notare la nuova 29100: Privacy Framework e la 27031: ICT Readiness for Business Continuity.

Conclusioni

Terminata questa abbondante carrellata normativa può venire spontaneo chiedersi il perché di questo grande impiego di carta, ma in un ambito fortemente dinamico e in cui spesso un'opinione altamente soggettiva gioca ancora un ruolo decisivo come quello della sicurezza informatica, la presenza di norme e linee guida sviluppate e riconosciute internazionalmente può essere un punto di appoggio importante. La lunga evoluzione dalla BS 7799 fino alla ISO 17799, oggi 27001, sta facendo guadagnare a questo tipo di approccio verso la sicurezza delle informazioni sempre più supporto internazionale, persino in paesi tradizionalmente "lontani" da questo iter come gli Stati Uniti d'America.

Una certificazione ISO 27001 può rappresentare un'importante riconoscimento finale dell'attività svolta e della buona gestione di un'azienda se condotta seguendo i criteri definiti dalle norme della famiglia opportunamente calati nella realtà in questione.

L'Italia non è attualmente né fanalino di coda né vagone trainante di questo processo, ma diverse organizzazioni di rilievo quali Poste Italiane, Ferrovie dello Stato (RFI Spa), San Paolo, Siemens, SIA, Telecom Italia e TIM hanno iniziato a sensibilizzarsi e a certificare porzioni (più o meno estese) dei loro sistemi informativi [fonte: Sincert].

Questa base, abbinata ad una maturata visione del processo di certificazione, potrebbe, e il condizionale è d'obbligo, innescare un ciclo virtuoso per le imprese

italiane, con benefici tangibili sul bilancio (minori spese dovute ad incidenti informatici e maggiore efficacia delle contromisure) e sull'immagine (minori incidenti quindi pubblicità positiva oltre a un più significativo riconoscimento ISO di cui fregiarsi).

Quanto prima le aziende italiane decideranno di muoversi in questa direzione, tanto più grande sarà il vantaggio d'immagine che avranno sulla concorrenza nel breve periodo e maggiore sarà l'esperienza nella gestione della sicurezza che potranno avere più avanti nel tempo.

Come considerazione finale, una partecipazione di più personalità del panorama italiano della sicurezza informatica ai comitati ISO pertinenti, quali l'SC27, è decisamente auspicabile. In tal modo si potrebbero arricchire le norme internazionali con l'esperienza e le conoscenze maturate in ambito nazionale. Paesi come Cina e Giappone presentano delegazioni di dieci-venti persone in ogni campo e i loro commenti sono sempre numerosi. Stati Uniti, Gran Bretagna e i paesi nordici in genere hanno una presenza consolidata in ogni gruppo di lavoro. Sicuramente più creatività dal bel paese non guasterebbe oltre al fatto che, più concretamente, comporta uno sforzo decisamente inferiore adottare norme internazionali che sono più vicine alle "best practices" nazionali.

Giugno 2007

Fabio Guasconi,
Consulente per la Sicurezza delle
Informazioni
tel. 329.46.56.930
fabio.guasconi@poste.it