ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

La sicurezza delle informazioni e le Norme ISO 27000

Attilio Rampazzo, Antonio Piva, David D'Agostini

1. Introduzione

Il 5 aprile scorso è entrata in vigore la Legge 18 marzo 2008 n. 48, con la quale l'Italia ratifica la Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001; tale accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche, rappresentò il primo tentativo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata, che consenta di combattere il crimine informatico in maniera coordinata.
La legge citata introduce importanti modifiche al Codice penale, al Codice di procedura penale, al d.lgs. 231/2001 sulla responsabilità amministrativa delle persone giuridiche e al d.lgs. 196/2003 sul trattamento dei dati personali. Si aggiunge così un nuovo tassello alla legislazione applicabile in materia di sicurezza delle informazioni già corposa ed articolata.
Il quadro normativo è in costante e rapida evoluzione, in funzione ovviamente della crescente importanza che il bene "informazione" sta assumendo non solo in ambito economico, ma anche in ambito sociale e politico. Di conseguenza per le aziende, le pubbliche amministrazioni e gli enti "*no profit*" diventa sempre più complesso gestire in modo efficiente, efficace e soprattutto economico la crescente mole di informazioni in appropriata sicurezza e rispettando la normativa applicabile. Termini come Information *Security Compliance* ma meglio *Information Security* Governance sono all'ordine del giorno.
L'International *Organization for Standardization* (ISO), sempre attenta alle evoluzioni, da alcuni anni ha costituito un gruppo che sta emanando una serie di norme nell'ambito della Sicurezza delle Informazioni che tendono ad aiutare le organizzazioni a ben cimentarsi nell'*Information Security Governance* e a migliorare la fiducia nelle relazioni tra azienda e azienda (B2B - *Business to Business*) o tra azienda e cliente (B2C - *Business to Consumer*). Pertanto da alcuni anni sono aumentate in maniera significativa le disposizioni, seppur sempre volontarie, che prospettano una nuova visione di Gestione dell'*Information Tecnology* come elemento dominante del *Business* dell'organizzazione. La capostipite di queste norme è la ISO/IEC 27001:2005 - Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.

2. Origine ed evoluzione della Norma ISO/IEC 27001

La realizzazione della norma risale agli inizi degli anni '90 quando il *Department of Trade and Industry* (DTI) britannico istituì un gruppo di lavoro finalizzato a fornire alle aziende una guida per la gestione della sicurezza del loro patrimonio informativo. Il gruppo pubblicò nel 1993 una rac-

colta di best practice (intitolata *Code of practice for information security management*) che costituì la base per lo standard vero e proprio pubblicato dal *British Standard Institution* (BSI) nel 1995. Questo standard, essendo opera del BSI, è stato identificato con la sigla BS 7799.
Nel 1998 fu aggiunta una seconda parte allo standard (intitolata *Specification for information security mangement systems*) che fu poi sottoposta a una revisione complessiva conclusasi con la pubblicazione, nell'aprile del 1999, di una nuova versione delle sue due parti. Nel 1999 lo standard BS7799 viene sottoposto all'approvazione dell'ISO/IEC per farlo diventare standard internazionale.
La parte prima dello standard BS7799 diventa standard internazionale ISO/IEC 17799 alla fine del 2000. La parte seconda viene sottoposta a nuova revisione nel 2002 al fine di armonizzarla rispetto agli altri Sistemi di Gestione certificati (ISO 9001, ISO 14001).Nel frattempo, il 15 luglio 2005, la ISO/IEC 17799 viene aggiornata ed implementata mentre anche la seconda parte del BS7799 viene presa in considerazione dall'ISO. Il 15 ottobre 2005 vede l'approvazione la ISO/IEC 27001 da alcune modifiche della BS 7799-2:2002 ed In luglio 2007 la ISO 17799:2005 è stata rinumerata ISO 27002.
Si dà vita così a una nuova famiglia, la ISO 27000 series che tratterà tutti gli standard sulla Gestione dei Sistemi di Sicurezza delle Informazioni.
Lo standard ISO/IEC 27001 è entrato in vigore e pubblicato in Italia in data 28/03/2006 come UNI CEI ISO/IEC 27001:2006 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti. Nell'autunno 2007 l'UNI pubblica la versione in lingua italiana della norma curata da UNINFO, ente di formazione federato all'UNI che si interessa di tecnologie informatiche e loro applicazioni.

3. ISO/IEC 27001:2005 e ISO/IEC 27002:2005

La differenza tra le due norme è data dai differenti obiettivi.
La Norma ISO/IEC 27002 ha l'obiettivo di fornire delle regole di buon comportamento sulla gestione della sicurezza nell'organizzazione: usa sempre il verbo *should* (dovresti) e mai *shall* (devi) nel condurre un'azione per raggiungere la conformità al requisito normativo. La ISO/IEC 27001, invece, ha l'obiettivo di specificare i requisiti per la realizzazione di un Sistema di Gestione della Sicurezza delle Informazioni: usa sempre il verbo *shall* (devi). La ISO/IEC 27001:2005 è la norma utilizzata per certificare il Sistema della Sicurezza delle Informazioni (SGSI)[1] degli Enti e delle aziende.

4. La Norma ISO/IEC 27001:2005

La Norma copre tutte le tipologie di Organizzazioni (imprese commerciali, agenzie governative, organizzazioni senza scopo di lucro). Lo sviluppo di un Sistema di Gestione per la Sicurezza delle Informazioni secondo la ISO/IEC 27001 consente tra le altre cose di gestire al meglio i requisiti della normativa applicabile allo specifico caso aziendale, contribuendo a salvaguardare l'organizzazione stessa da eventuali conseguenze negative di carattere giuridico, economico e di immagine. La ISO/IEC 27001 non pretende di essere il rimedio a tutti mali della Sicurezza delle Informazioni, ma costituisce il punto di partenza per impostare un efficace Sistema Organizzativo che comprenda tutti gli aspetti della Sicurezza e che si inserisca in un contesto di IT Governance[2].
Quando si parla di sicurezza delle informazioni si pensa subito alla sicurezza informatica: antivirus, firewall, backup, password ecc.. Si corre quindi il rischio di considerare la sicurezza delle informazioni, e le norme di riferimento quali la Norma ISO 27001, come un'attività tecnica, o come una norma "tecnica", di esclusiva competenza degli "informatici".Contrariamente, invece, la Norma ISO/IEC 27001 propone un modello organizzativo, più che uno standard tecnico: non "come" fare, ma "cosa" fare.
Per evitare pericolosi fraintendimenti, le caratteristiche in sintesi sono le seguenti:
- la ISO/IEC 27001 è uno standard gestionale (e non tecnico) nel campo del "management" e non dell'"ingegneria". I sistemi di gestione della sicurezza delle informazioni considerano infatti, oltre agli aspetti informatici, anche (e soprattutto) gli aspetti inerenti la gestione delle risorse

[1] SGSI corrispondente all'inglese ISMS – Information Security Management System.

[2] Si pensi per esempio a ITIL, ISO 20000; Cobit, CoSO - Enterprise Risk Management.

umane, la gestione dei processi organizzativi e la gestione degli spazi fisici. Paradossalmente un'organizzazione potrebbe essere dotata di sistemi informatici di ultima generazione, ma non aver sensibilizzato il proprio personale a non lasciare scritta sul post-it in bella vista la password di accesso ai sistemi oppure a non discutere per cellulare di argomenti delicati.

❑ La ISO/IEC 27001 riguarda la gestione in sicurezza di tutto il patrimonio informativo aziendale, indipendentemente dai supporti utilizzati per immagazzinare i documenti e i dati, supporti che possono essere elettronici ma anche cartacei.

❑ La ISO/IEC 27001 definisce la sicurezza delle informazioni in termini di preservazione di integrità, disponibilità e riservatezza delle stesse. Ciò premesso, la ISO/IEC 27001 ha una struttura molto agile e gli aspetti "burocratici" di sistema sono ridotti al minimo. La norma eredita i nove principi dell'OCSE (emessi in occasione della sessione del Consiglio dell'OCSE del 25 luglio 2002) nei quali si afferma che:

- i Governi hanno il compito di diffondere la cultura della sicurezza;
- tutti (anche gli utenti occasionali) devono contribuire all'attuazione ed alla gestione della sicurezza;
- rispetto dei principi etici e democratici, libera circolazione delle informazioni, protezione adeguata dei dati personali, apertura e trasparenza.

La ISO/IEC 27001 è strutturata macroscopicamente in tre blocchi di requisiti:

❑ fino al capitolo 3 - requisiti introduttivi e di spiegazione della norma (come quasi tutte le Norme ISO);

❑ dal capitolo 4 al capitolo 8 - requisiti applicativi del SGSI;

❑ appendici (o allegati) normativi e descrittivi a supporto di quanto citato nei capitoli precedenti.

I capitoli compongono la parte alta che contiene i requisiti che armonizzano la norma con gli altri schemi di certificazione (ISO 9001, ISO 14001) utilizzando il ciclo *Plan-Do-Check-Act* (o di *Deming*). Gli appendici o allegati sono tre:

❑ l'Allegato A ricopre un ruolo fondamentale nelle fasi di implementazione operativa e *audit*;

❑ l'Allegato B (informativo) contiene integrazione dei principi OECD rispetto al modello PDCA;

❑ l'Allegato C indica la corrispondenza tra ISO 9001:2000, ISO 14001:2004 e questo standard.

Essenzialmente la Norma ISO 27001 prende in considerazione, oltre agli aspetti di sistema, i seguenti aspetti inerenti la Gestione della Sicurezza delle Informazioni:

❑ identificazione del perimetro aziendale che il S.G.S.I[3]. deve proteggere. Il perimetro può essere di natura fisica (per esempio, sito o siti aziendali), di natura organizzativa (per esempio, funzioni aziendali) o di natura logica (reti informatiche e sistemi informativi);

❑ definizione di Politica e Obiettivi per la sicurezza delle informazioni, ovviamente in funzione della missione strategica aziendale e del relativo assetto organizzativo;

❑ identificazione dei beni (per esempio, relativi a sistemi informativi, sistemi informatici, sistemi di comunicazione, archivi cartacei ecc.) entro i confini del perimetro da proteggere nonché valutazione del valore dei beni stessi per l'Azienda;

❑ identificazione delle vulnerabilità inerenti i beni (per esempio, carenza di controlli, insufficiente formazione del personale, accessi fisici incustoditi, luoghi soggetti a incendi e inondazioni ecc.);

❑ identificazione delle minacce che possono sfruttare le vulnerabilità (per esempio, furti, avarie, incendi, inondazioni, picchi o interruzioni di energia elettrica, errori umani, atti dolosi ecc.);

❑ stima delle probabilità del verificarsi delle minacce individuate (eventi);

❑ stima della gravità dell'impatto delle minacce sui beni in termini di integrità, disponibilità e riservatezza delle informazioni;

❑ calcolo del rischio in funzione delle probabilità e degli impatti;

❑ scelta di come affrontare il rischio calcolato. Si può scegliere di accettarlo consapevolmente, di evitarlo, di eluderlo mediante trasferimento a soggetti terzi, per esempio, con contratti di assicurazione, oppure di ridurlo mediante applicazione di opportuni controlli;

❑ scelta ed attuazione dei controlli per diminuire il rischio. I controlli possono essere di natura organizzativa, fisica o logico-informatica.

L'allegato A della ISO/IEC 27001 si sviluppa in 11 sezioni (clausole, domini o aree di intervento), identificando per ciascuna gli obiettivi del controllo (in totale 39, ove il termine "controllo" va inteso in senso lato come "strumento di gestione") e i controlli stessi da implementare (per un totale di 133).

[3] S.G.S.I. Sistema di Gestione della Sicurezza delle Informazione traduzione del termine inglese I.S.M.S. *Information Security Management System*.

Le 11 aree di intervento:
1. Politica di sicurezza – l'obiettivo è fornire una guida e supporto alla direzione per la sicurezza delle informazioni.
2. Sicurezza Organizzativa – standard, norme e metodologie; definizione dei compiti e relative responsabilità anche quando l'elaborazione delle informazioni è affidata in outsourcing.
3. Gestione degli *asset* – l'obiettivo è garantire anche la gestione delle informazioni abbia un appropriato livello di protezione attraverso la classificazione delle informazioni stesse per una corretta valutazione del rischio associato.
4. Sicurezza delle risorse umane – l'obiettivo è ridurre i rischi di errore, furto, frode, o abuso da parte degli operatori accertandosi che gli stessi siano informati delle possibili minacce riguardanti la sicurezza delle informazioni, sostenendo così la politica sulla sicurezza della società nello svolgimento del loro lavoro.
5. Sicurezza fisica e ambientale – si vuole impedire l'accesso, il danneggiamento e l'interferenza dei non autorizzati, interni o esterni, proteggendo il flusso delle informazioni del business aziendale impendendone manomissioni o furto delle informazioni.
6. Gestione delle operazioni e delle comunicazioni – accertarsi del corretto funzionamento dei sistemi di elaborazione delle informazioni, minimizzare i rischi di guasti, mantenere l'integrità e la validità dei processi di elaborazione dell'informazione e comunicazione, garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto.
7. Controllo degli accessi – l'obiettivo è impedire l'accesso non autorizzato e gestire un appropriato il sistema di autenticazione.
8. Acquisizione, sviluppo e mantenimento dei sistemi informativi – le attività di sviluppo e manutenzione devono essere gestite, controllate e tracciate.
9. Gestione degli incidenti di sicurezza delle informazioni – garantire che le debolezze ed i relativi eventi legati alla sicurezza siano segnalati per permettere efficaci azioni correttive.
10. Gestione della continuità operativa – obiettivo è impedire interruzioni alle attività ed ai processi critici del business aziendale dovuti a causa di eventi accidentali o fraudolenti.
11. Rispetto normativo – obiettivo è di garantire la conformità ai requisiti di legge (rispetto delle leggi civili, penali, patti contrattuali) e dei requisiti di sicurezza e delle policy: va cioè garantito il rispetto di tutto quanto può essere definito "cogente".
I controlli proposti sono una precisa descrizione a livello funzionale delle misure di protezione richieste per gestire la Sicurezza delle Informazioni. Ciononostante è importante sottolineare che l'elenco dei 133 controlli presente nell'allegato A è per esplicita ammissione non esaustivo: possono essere introdotti un numero maggiore di controlli a discrezione dell'organizzazione o possono essere eliminati controlli che non sono necessari[4].
I controlli devono essere realizzati:
- attraverso soluzioni hardware o software (di autenticazione, protezione crittografica, chiave digitale, monitoraggio software delle modifiche sul sistema ecc.) nel caso dei controlli attuabili mediante misure di sicurezza di tipo logico;
- attraverso l'installazione di sistemi anti intrusione, antifurti volumetrici e/o perimetrali, telecamere, casseforti, allarmi a distanza, armadi ignifughi, porte blindate, accesso fisico con badge magnetico, nel caso dei controlli che richiedono misure di sicurezza di tipo fisico;
- attraverso la definizione di precise procedure e la creazione di apposite strutture o cariche aziendali, per la messa in atto dei controlli di tipo procedurale (per esempio, l'istituzione del Comitato della Sicurezza per la gestione della sicurezza dell'informazione, la gestione delle risorse, la definizione dei requisiti di sicurezza da inserire nei contratti con le terze parti, le procedure di controllo degli accessi fisici, le registrazioni di manutenzione sui server, costanti audit interni sulla sicurezza ecc.); in questo caso si tratta di misure organizzative.

5. La famiglia ISO 27000 e normativa vigente

La ISO/IEC 27001 è uno standard **certificabile e auditabile** (**attraverso i requisiti**), mentre tutte le altre norme che costituiranno la famiglia ISO 27000 sono dei consigli, delle guide di supporto alla ISO/IEC 27001 quindi non sono oggetto

[4] La scelta dei controlli per ciascuna sezione di appartenenza deve essere sempre individuata attraverso un processo formale di valutazione dei rischi. L'output del processo di valutazione dei rischi è costituito dall'insieme dei controlli prescelti ed è formalizzato nella Dichiarazione di Applicabilità (S.O.A. - *Statement of Applicability*).

di certificazione ma vengono utilizzate per supportare l'attuazione di un Sistema di Gestione della Sicurezza delle Informazioni.
Attualmente la famiglia ISO 27000 è costituita da:
- ISO/IEC 27001:2005 - Sistema di Gestione per la Sicurezza delle Informazioni – Requisiti;
- ISO/IEC 27002:2005 - S.G.S.I. Consigli pratici;
- ISO/IEC 27005:2008 - S.G.S.I. Gestione del Rischi;
- ISO/IEC 27006:2007 - S.G.S.I. Linee guida per Enti di Certificazione Accreditati.

Nel corso dei prossimi anni sono previste le pubblicazioni ulteriori norme generali (tabella 1)[5] ed inoltre i vari gruppi del comitato ISO/IEC JTC 1/SC27 stanno lavorando a specifiche norme che trattano di applicazioni settoriali (sanità, finanza e banche, *automotive*, manifatturiero ecc.) o aspetti tecnici quali *incident management, network security*, IDS (tabella 2).
Quando si parla di Sicurezza delle Informazioni si pensa subito alla normativa sulla "privacy", ovvero al *Dlgs. n. 196 del 30 giugno 2003* "*Codice in materia di protezione dei dati personali*"[6]. Si corre quindi il rischio di considerare la norma ISO/IEC 27001 come un inutile "doppione " della legge sulla "privacy" e del relativo Documento Programmatico sulla Sicurezza (quest'ultimo può essere effettivamente integrato nel S.G.S.I. ma non viceversa!).
In realtà gli standard volontari di gestione (come la ISO/IEC 27001, la ISO 9001, la ISO 14001) hanno, tra le altre finalità, quella di supportare l'Azienda a gestire in modo sistematico, efficiente ed efficace i requisiti posti da specifiche norme cogenti di legge. Questo anche in considerazione del fatto che la legislazione inerente la sicurezza delle informazioni è piuttosto corposa e va ben oltre il codice sulla "privacy": si pensi per esempio al d.lgs. 8 giugno 2001 n. 231 "Responsabilità Amministrativa delle Persone Giuridiche", alla normativa in materia di tutela del diritto di autore (copyright)[7], di commercio elettronico e tutela dei consumatori, di accesso agli atti amministrativi, di reati informatici[8], di digitalizzazione della PA[9] ecc..
La normativa cogente di legge in materia di sicurezza dei dati è in genere finalizzata a tutelare gli interessi dei terzi mentre lo standard ISO 27001 è esplicitamente finalizzato a tutelare innanzitutto gli interessi dell'Organizzazione (nonché dei suoi legali rappresentanti e/o responsabili di gestione). Paradossalmente, un'Organizzazione potrebbe, per esempio, essere "tendenzialmente" in linea con la "privacy" e cessare di esistere perché i suoi dati più vitali (brevetti, specifiche di produzione ecc.) sono stati trafugati! Per non parlare dei dati di natura economico-finanziaria

• ISO/IEC 27000 S.G.S.I. - Fondamenti e vocabolario (FCD)
• ISO/IEC 27003 S.G.S.I. - Guida all'implementazione
• ISO/IEC 27004 S.G.S.I. - Misurazioni e metriche (FCD)
• ISO/IEC 27007 Linee Guida per l'Audit di un S.G.S.I. (WD)
• ISO/IEC 27008 Linee Guida per l'Audit dei Controlli

TABELLA 1
Norme della famiglia 27000 di prossima pubblicazione

• ISO/IEC 27011 Information security management guidelines for telecommunications (FDIS)
• ISO/IEC 27031 ICT readiness for business continuity
• ISO/IEC 27032 Guidelines for cybersecurity
• ISO/IEC 27033 Guidelines network security (revisione della ISO/IEC 18028-1:2006))
• ISO/IEC 27034 Guidelines for application security
• ISO/IEC 27799 Security Management in Health using ISO/IEC 27002 (pubblicata 12/6/2008)
• ISO/IEC 24762 Disaster recovery services (pubblicata 31/1/2008)

TABELLA 2
Specifiche nome settoriali o tecniche, previste o pubblicate

[5] Pur non appartenenti alla famiglia delle ISO 27000, per quanto riguarda la sicurezza informatica si ritiene doveroso menzionare anche le Norme ISO 20000 - Sistemi di Gestione dei Servizi IT - e le BS 25999 - Sistemi di Gestione di Business Continuity.

[6] Per una completa trattazione si rinvia al numero 2 del giugno 2008, al numero 2 di giugno 2007, al numero 1 di marzo 2004, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

[7] Si rinvia al numero 3 del settembre 2004, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

[8] Si rinvia al numero 2 del giugno 2004 ed al numero 4 di dicembre 2006, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

[9] Si rinvia al numero 3 del settembre 2005 ed al numero 4 di dicembre 2005, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

che, essendo relativi all'Organizzazione, non sono il fulcro centrale della tutela derivante dalla normativa sulla "privacy" (la quale si concentra soprattutto sui dati personali relativi a terzi trattati dall'Organizzazione).
Pertanto gli adempimenti cogenti inerenti la sicurezza dei dati e dei sistemi informatici (art. 31 del *Codice della privacy*) sono finalizzati a ridurre al minimo i rischi di distruzione o perdita dei medesimi, ovvero di accesso non autorizzato, di trattamento non consentito o non conforme alla finalità della raccolta, l'adozione di idonee misure di sicurezza in relazione al progresso tecnologico ed alle specifiche caratteristiche del trattamento di dati trattati, le prescrizioni sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice*), la tenuta di un aggiornato documento programmatico sulla sicurezza e l'attuazione delle misure minime di sicurezza (*Allegato B del Codice della Privacy denominato "Disciplinare tecnico in materia di misure minime di sicurezza"*) devono essere effettuate al fine di prevenire le sanzioni amministrative, civili e penali derivanti dal Codice della Privacy.
L'identificazione e l'aggiornamento costante dei processi riguardanti il controllo della sicurezza fisica, logica ed organizzativa, l'analisi dei rischi per l'identificazione delle misure idonee di sicurezza, la gestione di opportune procedure ed istruzioni operative frequentemente aggiornate, il monitoraggio dei processi aziendali anche attraverso costanti verifiche interne tecnico-organizzative e *audit*, come previsto dalle norme volontarie internazionali ISO/IEC 27001[10], riguardanti i Sistemi di Gestione della Sicurezza delle Informazioni, sono utili strumenti per supportare l'azienda oltre che nella gestione la Sicurezza informatica e Privacy[11], anche e soprattutto per tutelare e garantire il business dell'organizzazione.

Organismo di Certificazione	Certificati ISO/IEC 27001:2005
TUV	85
DNV	61
RINA	13
IMQ	35
CERTIQUALITY	14
CERMET	4
Totali	212

TABELLA 3

Diffusione in Italia: situazione certificati ISO/IEC 27001 rilasciati da Organismi Italiani accreditati SINCERT
(Fonte SINCERT data : 30/6/2008)

6. La diffusione della certificazione ISO/IEC 27001

A livello internazionale le certificazioni ISO/IEC 27001 aumentano di oltre mille ogni anno con un significativo incremento a conferma del continuo interesse a questo *framework* come supporto organizzativo per la gestione della Sicurezza delle Informazioni: a fine luglio 2008 sono stati emessi 4426 certificati ISO/IEC 27001[12].
L'Italia si trova alla dodicesima posizione per certificati rilasciati e riconosciuti dall'International *Register of ISMS Certificates* ed anche se lentamente, la consapevolezza di dotarsi volontariamente, di un metodo di trattamento sicuro delle informazioni sta avanzando.
Dal sito del Sincert si evince che a fine giugno 2008 in Italia sono 212 i certificati ISO/IEC 27001:2005 rilasciati a circa un'ottantina di aziende, con un incremento di raddoppio dal 31 marzo 2006 termine del periodo di transizione della precedente norma BS 7799-2:2002 (Tabella 3). Un risultato significativo che con tutta certezza nei prossimi anni dovrebbe sicuramente ancora aumentare.

7. Conclusioni

"*La sicurezza è un processo, non un prodotto*". Questa è l'affermazione di Bruce Schneier, noto autore di libri sulla crittografia e sulla sicurezza informatica, che riassume la filosofia

[10] Ivi inclusi le citate aree di intervento, obiettivi di controlli ed i controlli stessi previsti dalla norma.

[11] Ci si potrebbe porre il dubbio su come operativamente sarebbe possibile essere a posto con le misure minime ed idonee di sicurezza imposte dal Codice della Privacy senza un'appropriata e costante gestione di tutti i processi relativi alla sicurezza come suggerito dalla norma ISO/IEC 27001.

[12] Fonte www.iso27001certificates.com version 182 July 2008; nella tabella **A** a p. 65 si riportano, in percentuale, le certificazioni rilasciate suddivise per settore.

che sta alla base dello standard ISO/IEC 27001. Non è sufficiente progettare un modello di sicurezza focalizzato sui soli aspetti tecnologici, ma è necessario tenere in considerazione anche le carenze legate all'organizzazione e alle procedure interne. Lo standard ISO/IEC 27001 attribuisce anche a questi ultimi aspetti una notevole importanza. Un Sistema di Gestione di Sicurezza delle Informazioni conforme allo standard ISO/IEC 27001 è uno strumento attraverso il quale un'organizzazione può dimostrare di essere capace di tutelare in modo globale il proprio patrimonio informativo (o quello di terzi a lei affidato). Se ne deduce che ormai dotarsi di un Sistema di Gestione della Sicurezza delle Informazioni è un'esigenza e non una "*tendenza del momento*" come ancora alcuni pensano.

Settore	Percentuale
Telecomunicazioni	25
Finanza	21
Servizi Terze Parti	17
Industria	15
Manifatture	11
Organizzazioni Governative	7
Utilities	4

TABELLA A

Certificazioni rilasciate suddivise per settore (in percentuale)

Bibliografia

[1] Quaderno AICQ n. 22 - *Gestione della Sicurezza delle Informazioni: guida alla lettura della Norma ISO 27001*.

[2] Quaderno Clusit - *Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni*.

[3] UNI CEI ISO/IEC 27001:2006 *Tecnologia delle informazioni -Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti*.

[4] ISO/IEC 27002:2005 *Information technology -- Security techniques -- Code of Practice for Information Security Management*.

[5] Piva A., D'Agostini D.: Sicurezza informatica e privacy nella scuola. *Mondo Digitale*, n. 2 - giugno 2008, p. 55-60. Felician L., D'Agostini D., Piva A.: 10 anni di Privacy: la protezione dei dati personali tra passato e futuro. *Mondo Digitale*, n. 2 giugno 2007, p. 65-74. Piva A., D'Agostini D.: La tutela dei dati personali nell'era digitale: il Codice sulla privacy tra vecchi e nuovi adempimenti. All'interno della rubrica ICT e Diritto di *Mondo Digitale*, n. 1 marzo 2004, p. 57-60.

Attilio Rampazzo, consulente di Sistemi Informativi e Sicurezza delle Informazioni in AlmavivA Finance Spa. Ha maturato un'esperienza più che trentennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. ÈVice Presidente del Comitato AICQ "Qualità del Software e dei Servizi IT", valutatore Sistemi di Sicurezza delle Informazioni R.G.V.I. (AICQ_SICEV certificato n.3), socio AIPSI-Associazione Italiana Professionisti Sicurezza Informatica.
E-mail: attilio@rampazzo.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

David D'Agostini avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it