CRITERI DI VALUTAZIONE E CERTIFICAZIONE DELLA SICUREZZA DELLE INFORMAZIONI.

CESARE GALLOTTI
MILANO, 14 MAGGIO 2004

Questo documento va inteso come una raccolta di appunti correlati alla presentazione dallo stesso titolo.

1 Introduzione

L'*informazione* è un'aggregazione ed elaborazione di dati elementari di interesse per uno o più destinatari importante per il processo decisionale presente e futuro. L'aggregazione e l'elaborazione sono affidate al *sistema informativo*.

Per l'ISO 9000:2000:

- *informazione*: dati significativi (ossia che hanno significato per qualcuno)
- *documento:* informazioni con il loro mezzo di supporto (IT e/o non-IT).

Mezzo di supporto può essere: carta, elettronico, radiografie, fotografie, eccetera. Vanno anche considerati i cervelli delle persone fisiche.

Per *sicurezza delle informazioni* si intende l'attività volta a definire, conseguire e mantenere le seguenti proprietà: riservatezza, integrità, disponibilità, autenticità, non ripudiabilità. Autenticità e Non ripudio sono viste dagli standard come problemi di Integrità, perché visti come problemi di "mancanza di firma".

La sicurezza si garantisce attraverso processi organizzativi e prodotti adeguati. Buoni processi organizzativi portano a scegliere ed usare buoni prodotti perché saranno frutto di una pianificazione, un'attenta scelta requisiti, la conseguente scelta del prodotto ottimale, un'adeguata formazione del personale addetto per la configurazione e manutenzione.
Non è vero l'inverso: per esempio, non garantiscono sicurezza firewall ottimi ma non adeguati (firewall SOHO per grandi reti) o mal configurati o mal gestiti nel tempo.

2 Valutazione dei prodotti

TCSEC: http://www.radium.ncsc.mil/tpep/library/rainbow/
ITSEC e Common Criteria: http:\\www.commoncriteria.org. Sul sito dei Common Criteria sono presentate diverse linee guida per la preparazione alla certificazione di prodotto, un software per aiutare nella preparazione del Security Target e tutti i Protection Profile attualmente certificati.

TCSEC è stato sviluppato in ambito governativo negli USA. ITSEC fu sviluppato in Europa con un'ottica più legata alla certificazione di prodotti commerciali.
I Common Criteria sono simili a ITSEC e ne sono un'evoluzione sviluppata dai Paesi autori di questo con Canada e Stati Uniti.

Può essere utile considerare anche gli standard legati alla gestione dello sviluppo del software, anche se non riguardano la certificazione di un singolo prodotto:

- Sofware Capability Maturity Model (CMM, 1993, Software Engineering Institute (SEI) della Canergie Mellon University; reperibile su http:// www.sei.cmu.edu/cmm/cmms/cmms.html).
- SSE-CMM (System Security Evaluation CMM, 1997, evoluzione del Software CMM per la sicurezza, reperibile su http://www.sse-cmm.org)
- ISO 90003 (applicazione dell'ISO 9001:2000 al software, aggiornata nel 2003)
- ISO/IEC 12207 (sul ciclo di vita del software)
- ISO/IEC 15288 (System life cycle)
- ISO 15504 (SPICE, software process assessment)
- ISO/IEC 14764 (Software Maintenance)

Il Software Capability Maturity Model propone cinque livelli di maturità per un'azienda, basati sulla sua capacità di gestire i progetti software e il loro miglioramento:

1. iniziale: il successo dei progetti dipende dall'impegno di alcuni;

2. ripetibile: è definita una disciplina basata su pianificazione, calcolo dei costi e supervisione dei progetti, per ripeterne i successi;
3. definito: vi è uno standard aziendale per la gestione dello sviluppo (associabile all'ISO 9001:1994 e al BS 7799:1999);
4. gestito: sono attuati controlli quantitativi della gestione dei processi di sviluppo del software;
5. ottimizzato: sono in atto strategie di miglioramento progressivo e continuo dei progetti di sviluppo (associabile all'ISO 9001:2000 e al BS 7799:2002).

Il Technical Report dell'ISO 15504:1998 (detto anche SPICE) riprende i concetti del CMM.

Legate alla qualità del singolo prodotto software sono le due seguenti guide (non standard "certificabili") dell'ISO:

- ISO 9126 (caratteristiche di qualità di prodotti software)
- ISO/IEC 14598 (Software Evaluation, riguarda le attività di test anche legate all'ISO 9126)

L' ISO 9126:2001 riguarda la valutazione della qualità del software. I requisiti di valutazione sono divisi in famiglie:

- funzionalità: funzioni che soddisfano i bisogni per i quali il software è progettato;
- affidabilità: capacità del software di mantenere le prestazioni entro le condizioni indicate;
- usabilità: sforzo richiesto agli utenti per l'utilizzo;
- efficienza: relazione tra prestazioni del software e risorse impegnate;
- manutenibilità: lavoro occorrente per apportare successive modifiche;
- portabilità: possibilità di trasferire il software da un ambiente informatico a un altro (per esempio: un ambiente Win 2000 è potenzialmente diverso da un Win 2000 con Service pack 1 o 2, perché alcune dll sono modificate e possono incidere sul software installato).

Per quanto riguarda i prodotti di sicurezza fisica (resistenza agli incendi REI 60 o 120, allo scasso per un tempo variabile, agli urti, eccetera), ci sono norme UNI.

2.1 Cosa si valuta

Nell'ambito degli standard di valutazione ITSEC e Common Criteria, l'oggetto di valutazione è detto TOE (Target of Evaluation) e può essere un sistema o un componente del sistema. I sue standard distinguono tra:

- Sistema: specifica installazione informatica, con un determinato scopo e presente in un ambiente definito
- Prodotto: pacchetto hardware e/o software acquistabile in un negozio e incorporabile in più sistemi.

2.2 Cos'è la sicurezza

Per descrivere cos'è la sicurezza per il TOE, vanno definiti, dopo un'analisi dei rischi basata sull'individuazione delle minacce che possono riguardare il TOE, gli *obiettivi di sicurezza* per contrastare tali minacce. Vanno quindi definite le *funzioni di sicurezza* atte a realizzare gli obiettivi. La realizzazione della funzionalità prende il nome di *meccanismo* e può essere costituito da parti di codice software, componenti hardware con software embedded.

La descrizione di obiettivi e funzionalità possono essere esplicitate in due tipologie di documenti:

- Protection Profile: espressione di requisiti di sicurezza per una famiglia di TOE (es. firewall, database, sistemi operativi, sofware di gestione PKI, smart card), coerenti con gli obiettivi di sicurezza stabiliti
- Security Target: espressione di requisiti di sicurezza per uno specifico TOE (es. database Oracle, s.o. Win 2000 o HP UX), più dettagliati rispetto a quelli espressi dal PP, perché devono descrivere nel dettaglio le scelte operate per la realizzazione.

In termini di valutazione, quella della funzionalità (Security Target o Protection Profile) può avere risultato positivo o negativo (1, 0) e stabilisce se le funzioni di sicurezza soddisfano gli obiettivi.

I Protection Profile non sono previsti da TCSEC, perché questo stabilisce già le funzionalità per specifici livelli di sicurezza. Queste non sono quindi più liberamente definibili dallo sviluppatore. Le funzionalità richieste da TCSEC sono relative a sistemi operativi e applicativi gestionali. Tra di queste, da un certo livello in poi, vi è il controllo accessi mandatario.

ITSEC, al posto dei Protection Profile, prevede la definizione di *classi di funzioni* per famiglie di TOE.

2.3 Realizzare le misure

Dopo aver valutato le funzionalità, gli standard richiedono di valutare la correttezza di realizzazione dei meccanismi.

I Common Criteria prevedono 7 livelli crescenti (EAL 1 ... EAL 7) di valutazione della correttezza. L'attribuzione di un livello di correttezza dipende dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo: più la documentazione è estesa e formale, più si ha la garanzia che il processo di sviluppo è stato rigoroso.

Per la valutazione della correttezza si guardano anche i compilatori, la gestione delle versioni del TOE, l'accuratezza dei manuali, i parametri di default, le modalità di consegna.

Il livello EAL1 non richiede la valutazione della documentazione utilizzata, dell'ambiente di sviluppo e del codice sorgente. Gli altri sì, e richiedono la collaborazione degli sviluppatori. ITSEC non prevede il livello EAL 1.

TCSEC assegna ad ogni livello di correttezza (D, C1, C2, B1, B2, B3, A1) funzioni via via più robuste.

2.4 Garantire la sicurezza nel tempo

Parte dei requisiti per la valutazione della correttezza riguardano la gestione del ciclo di vita del TOE e della gestione dei fix.

Lo standard, però, non garantisce il mantenimento del livello di sicurezza per versioni successive del TOE perché non si sa a priori che parti di codice sono state modificate. Non è quindi consigliabile l'uso dei Common Criteria per la certificazione un sistema informatico: lo standard non è adatto per queste cose proprio perché richiede la collaborazione degli sviluppatori del codice sorgente. Questo standard, inoltre, non riguarda aspetti di gestione organizzativa, fondamentali per il mantenimento del livello di sicurezza di un sistema informatico.

3 Valutazione dell'organizzazione della sicurezza

Standard di riferimento sono:

- ISO 9001:2000
- BS 7799-1:1999 (ISO 17799:2000, "Code of practice for information security management") e BS 7799-2:2002 ("Information security management systems — Specification with guidance for use)
- Cobit 3rd edition (scaricabile da www.isaca.org)
- ISO TR 13335: Guidelines for the management of IT security (GMITS)

Per quanto riguarda la parte 1 del BS 7799, si tratta di una lista di *controlli* di sicurezza soprattutto di tipo gestionale (organizzativo) intesa come "best practice": non tutto va realizzato e può essere un valido spunto per le attività di sicurezza. I controlli sono divisi in 10 capitoli:

3. Security policy
4. Organizational security
5. Asset classification and control
6. Personnel security
7. Physical and environmental security
8. Communications and operations management
9. Access control
10. Systems development and maintenance
11. Business continuity management
12. Compliance

Lo standard ha il pregio di essere stato il primo a toccare in modo così evidente gli aspetti organizzativi della gestione delle informazioni, non limitandosi solo all'ambito informatico. Come difetti, è facile vedere come i controlli provengono da fonti diverse e sono quindi descritti con linguaggi eterogenei tra controllo e controllo e in molti casi la stessa misura viene ripetuta in più punti; alcune misure sono spiegate in modi molto pratici, altre in modi molto teorici.

Sono anche suggeriti degli Starting Points "normativi" (sui dati personali, registrazioni, diritto d'autore) e organizzativi (Politiche di Sicurezza delle informazioni, ruoli e responsabilità, formazione e sensibilizzazione, gestione degli incidenti, piano di continuità).

La seconda parte dello standard è quella che indica i requisiti per la certificazione.

La prima parte è nata nel 1995, revisionata nel 1999 ed è stata recepita dall'ISO nel 2000. La seconda parte è nata nel 1998, adeguata alla revisione della prima parte nel 1999 ed è stata rivista nel 2002 per allinearsi alla ISO 9001:2000. Non è stata ancora recepita dall'ISO (http://www.iso.ch) e quindi non esiste ancora certificazione ISO17799, ma solo BS 7799-2.

3.1 Cosa si valuta: lo scopo

È il perimetro delle attività ed è un passo fondamentale per le attività di certificazione, perché in esso si deduce l'ampiezza delle attività.

Vanno identificate le caratteristiche di business e dell'organizzazione, le risorse fisiche, IT, non IT, umane e procedurali entro le quali valutare l'ISMS. Vanno anche definite le relazioni con l'esterno: clienti, fornitori, partner, case madri, ...

Nell'ambito del ciclo delle attività, lo scopo andrebbe definito dopo le politiche di sicurezza. Infatti queste hanno valenza per tutta l'azienda e possono influenzare l'ampiezza dello scopo di certificazione.

Il BS 7799 promuove l'approccio per processi per pianificare, realizzare, mantenere in opera, controllare e migliorare l'efficacia dell'ISMS.

Processo è un'attività che usa risorse e viene gestita per trasformare elementi in entrata in elementi in uscita. Vanno quindi definiti i processi:

- risorse (chi lo fa, chi ne è responsabile)
- input (quali informazioni si ricevono)
- attività o fasi
- output (il risultato)
- interdipendenze tra attività (da quale processo si ricevono indicazioni e a quale sono destinate gli elementi in uscita, considerando anche processi esterni, quali quelli relativi a clienti, fornitori, partner)
- controllo di gestione (indicatori di processo)

L'analisi delle interdipendenze è importante: se cambia un processo, la modifica può riflettersi anche sugli altri collegati. Esempio banale: la ristrutturazione dell'ufficio acquisti coinvolge anche i clienti, fosse solo per comunicare loro i nuovi numeri di telefono e nominativi a cui fare riferimento.

L'approccio per processi è collegato al principio di *approccio sistemico*: "identificare, capire e gestire (come un sistema) i processi relativi alla sicurezza delle informazioni tra loro correlati, contribuendo all'efficacia ed efficienza di un'organizzazione nel conseguire i propri obiettivi".

La definizione dello scopo è fondamentale e in alcuni casi da esso dipende il successo di un processo di certificazione. Questo perché obiettivi troppo ambiziosi sono impossibili da raggiungere in un solo passo ed è preferibile un'estensione graduale del campo valutazione.

In alcuni casi, è preferibile certificare una parte del sistema informativo piuttosto che niente: può servire da prototipo e aumenta la cultura aziendale in merito allo sviluppo e gestione dei sistemi informativi.

3.2 Il ciclo PDCA

Al fine di dare una lettura diversa del BS 7799 da quella già proposta nella presentazione, viene qui descritto il ciclo PDCA.

3.2.1 Pianificare

Politica per la sicurezza delle informazioni
Le politiche devono riportare:

- una definizione di sicurezza delle informazioni,
- uno schema per stabilire gli obiettivi e i principi da seguire,
- un'indicazione per dare un orientamento alle attività e chiarire l'impegno della direzione,
- i requisiti di business e i vincoli legali e contrattuali da rispettare,
- definizione delle responsabilità.

Esse sono uno strumento per evidenziare l'impegno della Direzione nella sicurezza delle informazioni.

Si osservi come il BS 7799 presenti una definizione di politiche più estesa di quella proposta dall'ISO 9001. In effetti, questa intende come politica i principi da seguire, mentre richiede la presenza di un *manuale* nel quale far confluire il restante della documentazione.

Responsabilità
Alcune figure proposte dal BS 7799 sono:

- Management information security forum
- Information security co-ordination
- Responsabili delle risorse (asset, informazioni)
- Amministratori di sistema
- Responsabili di processo
- Responsabile della sicurezza delle informazioni
- Responsabili per l'ampliamento del sistema informativo
- Auditor (interno, esterno)
- Custode delle password

Scopo
È il perimetro delle attività.

Identificazione e valutazione del rischio (risk identification and assessment)
L'approccio per la valutazione del rischio deve basarsi su un metodo (ripetibile!) e identificare i livelli di rischio accettabili. Vanno documentati i seguenti dettagli:

- Identificazione del rischio, ossia identificazione delle risorse (asset) e dei loro responsabili (owners), delle minacce a queste risorse, delle vulnerabilità e degli impatti nel caso queste risorse perdano di riservatezza, integrità, disponibilità.
- Valutazione del rischio, ossia la valutazione dei danni all'azienda per problemi di sicurezza correlata agli impatti di cui sopra, della probabilità di accadimento di tali problemi correlata alle minacce e vulnerabilità di cui sopra oltre che dei controlli già in opera, valutazione del livello di rischio.
- Determinare se il rischio è accettabile.

La ripetibilità del metodo si basa sulla descrizione delle scale di valutazione utilizzate.

Vanno quindi fatte delle scelte in merito al trattamento del rischio:

- Valutare le opzioni di trattamento del rischio: contrastare, trasferire, evitare, accettare.
- Selezionare i controlli, giustificandoli sulla base della valutazione del rischio e delle opzioni di trattamento scelte.
- Preparare una dichiarazione di applicabilità dei controlli scelti (Statement of Applicabiliy, equivalente ad una lista di correlazione dei controlli attuati con quelli proposti dalla parte 2 della norma).
- Ottenere l'approvazione del management sul rischio accettato e per l'implementazione dei controlli (riesame).
- Pianificare le attività: azioni del management, responsabilità e priorità.

L'analisi del rischio non ha come scopo l'individuazione dei controlli da realizzare, così come descritti dalla seconda parte dello standard. Infatti questi sono descritti in modo troppo generico per poterli ignorare. L'analisi del rischio deve portare all'individuazione delle misure di dettaglio per realizzare tali controlli, che possono richiedere impegno diverso a seconda del rischio individuato (per esempio, un controllo degli accessi alle risorse può richiedere il DAC o il MAC o l'RBAC a seconda del livello di rischio).

Piano di gestione del rischio (risk treatment)
Una volta scelte le misure da realizzare, è necessario pianificare i tempi da rispettare, le risorse da allocare e le modalità per verificarne l'efficacia.

Dichiarazione di applicabilità
Lo Statement of applicability (SOA) deve riportare i controlli proposti dalla seconda parte dello standard (descritti in modo molto più sintetico e generico rispetto alla prima parte) e i dettagli relativi alla loro realizzazione o le motivazioni della loro esclusione. Il SOA dovrebbe riportare i riferimenti alle eventuali procedure correlate.

Il SOA è utile all'auditor esterno, che deve riferirsi ad una sola tassonomia di misure di sicurezza; internamente l'azienda può usarne altre, come quelle proposte dal Cobit, dal GMITS, eccetera. Il SOA deve riportare le modifiche apportate tra le diverse versioni, anche per aiutare l'auditor per fargli vedere cosa è cambiato e che deve vedere nel corso delle verifiche di mantenimento.

Lo standard lascia la possibilità di estendere anche un Summary of Controls (SOC), ossia una versione semplificata del SOA senza riferimenti troppo approfonditi e che può essere fatto vedere a clienti, partners, eccetera.

3.2.2 Fare

Allocare risorse
Per la realizzazione del piano vanno allocate le risorse necessarie in termini di personale, tempo e denaro per:

- garantire e migliorare l'efficacia dell'ISMS,
- seguire l'evoluzione dei vincoli legali e contrattuali,
- garantire la correttezza dei controlli applicati,
- condurre revisioni e reagire ai risultati,

Formazione e sensibilizzazione
Il personale, con responsabilità relative alla sicurezza, deve essere competente e consapevole (formato e sensibilizzato).
Vanno definite le competenze necessarie per il personale coinvolto nell'ISMS.
Deve essere valutata l'efficacia delle attività di formazione.

Gestione dei documenti
Va predisposta una procedura documentata per la gestione dei documenti e una per la gestione delle registrazioni.

I documenti esplicitamente richiesti dalla norma sono:

a. Politica e obiettivi
b. Scopo dell'ISMS
c. Relazioni in merito alla valutazione del rischio, alle scelte di trattamento e al piano di gestione
d. Statement of applicability
e. Procedura per la gestione dei documenti
f. Procedura per la gestione delle registrazioni
g. Procedura per la gestione delle verifiche ispettive interne
h. Procedura per la gestione delle azioni correttive
i. Procedura per la gestione delle azioni preventive

3.2.3 Verificare

Controlli tecnici
Possono essere

- Continui: riconciliazioni, quadrature, controlli incrociati. Non vanno dimenticati quelli organizzativi, come per esempio la gestione dei reclami.
- Allarmi: da IDS, programmi di monitoraggio, rilevatori presenze, segnalazioni di incidenti.
- Confronti: mailing list (cert cc, bugtraq), conferenze, periodici, articoli, Forze dell'ordine

Visite ispettive
Vanno condotte visite ispettive interne periodiche. I criteri di pianificazione, conduzione e riporto vanno definiti in una procedura documentata.

Devono basarsi su evidenze oggettive e non devono avere carattere punitivo.

Le visite servono anche per avere dei ritorni da parte del personale (documenti, moduli, pratiche "difficili") e per poter allineare il tutto anche alle loro esigenze.

Riesame della direzione
Va condotto regolarmente (almeno una volta all'anno) un riesame della direzione dell'ISMS. Deve essere documentato e con opportuni elementi in entrata e in uscita (input e output) la cui estensione minima è descritta dalla norma.

Sulla base di queste analisi vanno rivisti i criteri di accettabilità del rischio.

Indicatori di processo

La norma (4.2.3.a.3) stabilisce che è necessario monitorare le procedure e i controlli al fine di consentire alla direzione di determinare se le attività delegate ad altri sono condotte come previsto ("obiettivi" oggettivi e misurabili).

L'ISO 9001 (8.2.3) chiede di "adottare adeguati metodi per monitorare e, ove applicabile, misurare i processi del sistema di gestione [...]. Questi metodi devono dimostrare la capacità dei processi ad ottenere i risultati pianificati. Qualora tali risultati non siano raggiunti, devono essere adottate correzioni ed intraprese azioni correttive, come opportuno [...]".
Convenzionalmente, si dice che le misure dei processi sono basate su *indicatori*.

Gli “indicatori di processo” dell’ISO 9001:2000 rappresentano un grosso cambio di direzione rispetto all’ISO 9001:1994 tanto che il tempo di transizione tra le due norme è stato stabilito di tre anni. E’ possibile vedere come tale innovazione si rifletta anche tra BS 7799:1999 e BS 7799:2002.

Gli indicatori di processo riguardano le attività di carattere gestionale (non tecnico per le analisi del rischio quantitative!). È possibile riferirsi al Cobit per averne degli esempi.

Gli indicatori di processo devono essere utili al personale operativo perché possa vedere quanto bene lavora e devono essere utili alla direzione per stabilire se il processo funziona (non per valutare il personale).

L’analisi degli indicatori di processo può permettere la soluzione dei problemi prima che si verifichino incidenti o non conformità.

Possono essere utili anche gli indicatori tecnologici (come gli allarmi IDS), tenendo però conto che questi rilevano problemi “individuati”, non quelli effettivamente subiti. Per esempio, se il firewall segnala meno attacchi del solito, può anche essere che sia mal configurato o non aggiornato, non che i “cattivi” sono andati a riposare o a dedicarsi ad altro.

N.B: L’interpretazione oggi consolidata del BS 7799-2:2002 non prevede la presenza di tali indicatori, a differenza dell’ISO 9001:2000. Va però considerata perché tale aspetto sarà presumibilmente specificato nel futuro.

3.2.4 Agire

Questa parte del ciclo di Deming si focalizza sulla gestione delle azioni correttive e preventive.

Una *non conformità* è:

- l’assenza di uno o più requisiti dell’ISMS,
- una situazione che pone il dubbio sull’efficacia dell’ISMS rispetto agli obiettivi.

Una non conformità può essere individuata nel corso delle diverse attività di verifica sopra descritte. Una volta evidenziata un’area di non conformità, vanno poste in atto attività per risolvere il problema, ossia *azioni correttive.* Nel caso in cui la non conformità non si è manifestata ma si ritiene comunque di prevenirla, si parla di *azioni preventive*.

Le azioni correttive e preventive devono eliminare la causa di una [possibile] non conformità e devono essere quindi previste delle analisi successive per valutare l’efficacia di tali azioni.

Molte volte, è possibile vedere le azioni correttive e preventive come progetti interni all’azienda. Le modalità della loro gestione devono essere descritte in una procedura documentata.

3.3 Percorso di certificazione

Per certificazione si intende la verifica ed attestazione, da parte di enti terzi indipendenti e competenti (organismi di certificazione), della conformità ai requisiti previsti dalla normativa di riferimento.

Le attività di certificazione, oltre ad essere utili in termini di immagine, rappresentano per l’azienda anche un’opportunità di confrontarsi con un organismo esterno e raccogliere spunti per eventuali miglioramenti.

In linea di principio un certificato può essere rilasciato da chiunque, anche senza l'opportuna indipendenza e qualifica. Per questo sono in atto procedure di accreditamento per dimostrare la correttezza, trasparenza e professionalità dell'attività dell'organismo di certificazione.

L’accreditamento avviene su specifici standard e settori industriali ed ogni organismo può essere accreditato per più standard e settori.

In Italia il compito di accreditare gli organismi di certificazione è affidato al Sincert (http://www.sincert.it).

L’accreditamento avviene su specifici schemi emanati dall'ISO (guide 62) o dal CEN (EN 45012) o da altri basati sui sistemi di gestione qualità.

Per il BS 7799 sono di riferimento le Guidelines for Certification- EA 7/03 (del 2000).

Il compito dell'organismo di accreditamento è anche quello di uniformare l'approccio di valutazione degli organismi di certificazione. In Europa, il lavoro degli enti di accreditamento viene coordinato dall'EA.

Il sistema di accreditamento e certificazione ha come protagonisti quattro gruppi di attori:

- gli enti normatori, come l'ISO, il BSI (British Standard Institute) o l'UNI (Ente Nazionale Italiano di Unificazione), che emettono standard;
- gli enti di accreditamento; in Italia sono il Sincert (per gli organismi di certificazione), il Sinal (per i laboratori) e il Sit (per i centri taratura);
- i soggetti accreditati, ossia organismi di certificazione, laboratori e centri di taratura;
- i consumatori finali, intesi come aziende ed imprese.

Quando un'azienda vuole certificarsi rispetto ad una specifica norma, deve contattare l'organismo di certificazione che pianifica una visita di ispezione ai fini della valutazione. Nel caso del BS 7799, è possibile prevedere la divisione di questa prima visita in 3 parti, da condurre in periodi distinti:

RIESAME DELLA DOCUMENTAZIONE	AUDIT INIZIALE - FASE 1	AUDIT INIZIALE - FASE 2
▪ Documentazione ISMS ▪ Politiche ▪ Scopo ▪ Descrizione ambiente IT ▪ Descrizione ambiente non IT ▪ Dichiarazione di Applicabilità ▪ Valutazione del rischio ▪ Piano di continuità	▪ Riesame della documentazione a seguito della fase precedente. ▪ Valutazione tecnica iniziale	▪ Riesame di quanto emerso dalla fase 1 ▪ Valutazione dell'ISMS realizzato ▪ Validazione della conformità ai requisiti della norma
Risultato ▪ Rapporto	Risultato ▪ Rapporto ▪ NC da chiudere prima della fase 2	Risultato ▪ Rapporto ▪ NC da chiudere prima dell'emissione del certificato ▪ Proposta di Certificazione

Se la visita dovesse avere esito positivo, l'organismo di certificazione rilascia un certificato di validità pluriennale (generalmente tre anni) e pianifica delle visite periodiche meno esaustive della prima per avere la conferma del mantenimento dei requisiti. Le verifiche periodiche sono condotte almeno una volta all'anno.

Alla scadenza del certificato, riprende l'iter con una visita completa da parte dell'organismo per il rinnovo del certificato.

Nel caso in cui l'organismo di certificazione riscontri delle non conformità rilevanti, prima di confermare la validità del certificato, deve essere effettuata una verifica straordinaria per avere la garanzia che l'azienda ha risolto il problema ed è nuovamente conforme a quanto dettato dalla normativa di riferimento.

4 Bibliografia

In Italia i testi di sicurezza delle informazioni di carattere non tecnico sono due:

1. Carducci Giulio, La tutela dei dati aziendali. Come integrare gli aspetti giuridici, organizzativi e tecnici per proteggere i dati, Franco Angeli, Milano, 1999.
2. Gallotti Cesare, Sicurezza delle informazioni – Analisi e gestione del rischio, Franco Angeli, Milano, 2003.

Altri testi in commercio (anche all'estero) riguardano principalmente aspetti tecnici. In molti casi, tali testi propongono uno o più capitoli dedicati ad aspetti gestionali. Tra questi ritengo utile segnalare lo storico

3. Zwicky Elisabeth D., Cooper Simon, Chapman D. Brent, *Building Internet Firewall, 2nd edition*, O'Reilly, Sebastopol, CA, USA, 2000.

Come fonte autorevole di documentazione è certamente da segnalare il sito del NIST (http://csrc.nist.gov). Nella pagina dedicata alle Special Pubs, è possibile trovare i testi proposti da questo ente, sia di carattere più tecnico che gestionale.

Infine, è da segnalare il penultimo libro dell'odierno guru della sicurezza informatica (anche se oggi sta allargando il proprio campo di interesse):

4. Schneier Bruce, *Secrets and Lies : Digital Security in a Networked World*, John Wiley & Sons, New York, USA, 2000.

Da un punto di vista gestionale, può essere utile il:

5. Marco Tagliavini, Aurelio Ravarini, Donatella Sciuto, *Sistemi per la gestione dell'informazione,* 2003, Apogeo, Milano.