



**LA SICUREZZA DELLE INFORMAZIONI  
SECONDO LO STANDARD DELLA NORMA  
BS 7799**

di

**CRISTIAN ERCOLANO**

Estratto dalla Rivista «Il Nuovo Diritto» n. X-XI – 2005

[www.ilnuovodiritto.com](http://www.ilnuovodiritto.com)

# DIRITTO DELLA GESTIONE DIGITALE DELLE INFORMAZIONI

(a cura di Cristian Ercolano)

---

## LA SICUREZZA DELLE INFORMAZIONI SECONDO LO STANDARD DELLA NORMA BS 7799\*

### 1. *La sicurezza delle informazioni*

“*Information is an asset which, like other important business assets, has VALUE to an Organization and consequently needs to be suitably PROTECTED*” (ISO/IEC 17799:2000). Spesso si dimentica di annoverare, fra i beni che costituiscono il capitale aziendale (ad es.: immobili, macchinari, strutture tecnologiche ed informatiche) le risorse intellettuali, identificabili nella enorme mole d'informazioni custodite e trattate. Anche questo bene, in quanto economicamente valutabile, deve essere adeguatamente tutelato dai diversi tipi di rischi che possano metterlo in pericolo, minacciando così l'operatività dell'azienda. Queste osservazioni sono tanto più vere se si considera che il modo in cui una organizzazione tratta le proprie informazioni può costituire uno dei parametri attraverso cui dare evidenza di sicurezza, fiducia, credibilità verso il mercato.

Questo risultato si consegue solo attraverso una corretta gestione operativa che garantisca non solo il massimo grado di sicurezza delle informazioni ma anche e soprattutto, in un'ottica globale, una corretta politica di continuità del business. Ed è per questo che la gestione delle informazioni deve essere effettuata in modo integrato, adottando strategie di prevenzione che siano di supporto costante alle attività di gestione delle emergenze e di controllo, monitoraggio e vigilanza: ovvero un processo costituito da attività sistematiche, integrate nelle prassi e nei comportamenti aziendali che, attraverso un *feed-back* continuo derivante dall'esito delle misure adottate, porta l'azienda ad analizzare la situazione in continua evoluzione, inclusa l'identificazione dei nuovi rischi insorgenti e a valutare i danni potenziali e la necessità di nuove contromisure<sup>1</sup>.

### 2. *Information Security Management System*

L'ISMS<sup>1</sup>, o anche SGSI (Sistema di Gestione della Sicurezza delle Informazioni) è il *framework*<sup>2</sup> che realizza la gestione della Sicurezza delle Informazioni in una organizzazione. Esso riguarda tutta l'azienda coinvolgendo, allo stesso livello di importanza, gli aspetti legati ai sistemi informativi<sup>3</sup>, al

---

\* Articolo pubblicato sulla Rivista scientifica “Il Nuovo Diritto”, n. X-XI - 2005, p. 995.

<sup>1</sup> I rischi - intesi come possibilità che, a seguito di eventi non del tutto prevedibili e contrastabili, si verifichino danni ad una organizzazione o ad un'azienda - sono diventati un elemento dal quale una corretta politica di gestione aziendale non può prescindere. Ciò ha fatto nascere una branca di analisi e di gestione delle criticità denominata *Risk Management*.

<sup>1</sup> Information Security Management System.

<sup>2</sup> Processo o insieme di processi.

<sup>3</sup> Per sistema informatico / informativo si intende l'insieme dei processi che realizzano la gestione delle informazioni utilizzando mezzi informatici.

## DIRITTO DELLA GESTIONE DIGITALE DELLE INFORMAZIONI

personale ed ai processi operativi attraverso una serie di *controlli* che verifichino e garantiscano il livello di sicurezza raggiunto attraverso i più vari strumenti: policy, prassi, procedure, strutture organizzative, strumenti software.

Una corretta politica di gestione delle informazioni trova il suo presupposto nell'esigenza dell'azienda stessa che, resasi conto dell'importanza delle proprie informazioni e definiti i *propri specifici obiettivi di sicurezza*, cerchi poi di raggiungerli. Tali obiettivi di sicurezza possono – anzi devono – essere quantificati e definiti dall'organizzazione stessa in base alle proprie strategie ad alle caratteristiche del proprio *business*, ma devono necessariamente essere rapportati e valutati in base a parametri universalmente riconosciuti<sup>4</sup>: parliamo, in questo caso, di *standard di sicurezza*.

Le prime normative nel campo della sicurezza delle informazioni furono formalizzate negli USA degli anni '70: questi standard<sup>5</sup> definivano “classi” di sicurezza per prodotti (in particolare: sistemi operativi). Negli anni '80, il settore ebbe un notevole impulso con la definizione degli standard TCSEC<sup>6</sup>, ITSEC<sup>7</sup>, ed i Common Criteria<sup>8</sup>. La caratteristica di tali norme è, però, quella di considerare solo l'aspetto tecnologico del problema sicurezza, consentendo di certificare solo un sistema o un prodotto. Negli anno '90, infine, la sicurezza comincia ad essere considerata e gestita come un processo integrato: nasce così la norma BS 7799.

### 3. La norma BS 7799

Il documento, abbozzato nel 1993 nella forma di best practice<sup>1</sup> dal DTI (Department of Trade and Industry) britannico, costituì la base per lo standard vero e proprio, formalizzato dal BSI<sup>2</sup> nel 1995 (BS 7799-1, “Code of practice for information security management”) e seguito, nel 1998, da una seconda parte (BS 7799-2, “Specification for Information Security Management Systems”), prima di essere entrambi ritirati e riemessi, in una nuova versione riveduta e corretta, nel 1999. La Norma ebbe così tanto successo al di fuori dei confini britannici da essere immediatamente recepita dall'ISO/IEC<sup>3</sup> quale standard internazionale (almeno nella sua prima parte, divenuta ISO/IEC 17799). Nel 2002 il BSI ha rilasciato una nuova versione della Parte 2, che a breve<sup>4</sup> sarà recepita anch'essa dall'ISO/IEC, con il nome di ISO 27001 (già pubblicata in

---

<sup>4</sup> Che possano, quindi essere utilizzati un numero infinito di volte all'interno dell'azienda e per un numero infinito di aziende diverse.

<sup>5</sup> primo esempio l'Orange Book.

<sup>6</sup> TCSEC: Trusted Computing Security Evaluation Criteria (i criteri di valutazione statunitensi, risalenti al 1985).

<sup>7</sup> ITSEC: Information Technology Security Evaluation Criteria (i criteri di valutazione europei, del 1992).

<sup>8</sup> Common Criteria: primo vero standard internazionale riconosciuto: ISO/IEC 15408, del 1999.

<sup>1</sup> Ovvero una “guida” per la gestione della sicurezza delle informazioni nelle aziende.

<sup>2</sup> British Standard Institute.

<sup>3</sup> ISO: International Organization for Standardization; IEC: International Electrotechnical Commission.

<sup>4</sup> Si dice entro il 2006.

## DIRITTO DELLA GESTIONE DIGITALE DELLE INFORMAZIONI

versione draft, bozza), dando luogo alla nuova categoria delle ISO 27000 ovvero la famiglia dei SGSI<sup>5</sup>.

La prima parte della Norma (BS7799-1 Code of practice for information security management) contiene gli elementi di base (raccomandazioni, requisiti e linee guida) per implementare e gestire correttamente l'ISMS. La seconda parte (BS7799-2 Specification for Information Security Management Systems), invece, specifica ed identifica gli elementi necessari per il conseguimento della Certificazione dell'ISMS aziendale o di una parte di esso<sup>6</sup>. Contiene, inoltre, la descrizione delle attività necessarie per implementare il processo di ISMS e l'elenco dei controlli, degli obiettivi di sicurezza e delle contromisure da adottare.

L'oggetto principale della Norma è l'informazione, sotto qualsiasi forma o supporto, per la quale devono essere garantiti i seguenti requisiti:

- **riservatezza:** *la proprietà delle informazioni in base alla quale ad esse accedere solo chi è autorizzato a conoscerle;*
- **integrità:** *quella caratteristica che, con riferimento al loro livello di alterazione o danno, richiede che le informazioni devono essere trattate in modo che siano difese da manomissioni o modifiche non autorizzate;*
- **disponibilità:** *la circostanza che le informazioni siano sempre disponibili per l'accesso alle persone autorizzate, quando necessario.*

attraverso un approccio integrato all'*information security* che, seguendo il classico modello PDCA (*Plan, Do, Check, Act*), sia in grado di guidare l'organizzazione nelle seguenti attività:

- a) impostare, implementare e amministrare, controllare e migliorare il Sistema di Gestione della Sicurezza delle Informazioni;
- b) selezionare le appropriate contromisure ritenute necessarie per la riduzione del rischio a livelli ritenuti accettabili dall'azienda;
- c) implementare correttamente le contromisure individuate.

#### 4. I criteri della norma BS 7799

La norma BS 7799 richiede la soddisfazione di numerosi requisiti, molti di essi non vincolanti né esaustivi ma dipendenti dalla realtà aziendale, identificabili nei seguenti elementi:

- **controlli:** si tratta di raccomandazioni normative da soddisfare per raggiungere il livello di sicurezza prefissato dallo Standard, in rapporto alla realtà aziendale;
- **policy:** rappresentano le linee guida per la salvaguardia dei sistemi e delle informazioni, indirizzate a tutto il personale dell'azienda;
- **procedure:** stabiliscono i criteri di comportamento dei vari operatori per il mantenimento del livello di sicurezza prefissato.

Tali requisiti operano in diverse aree di intervento<sup>1</sup> e sono organizzati in 6 fasi di analisi adeguatamente documentate, attraverso le quali deve emergere il

<sup>5</sup> Che si affianca, così, alla ISO 9000 ovvero la famiglia dei SGQ (Sistemi di Gestione della Qualità).

<sup>6</sup> Si può certificare, infatti, l'intero ISMS aziendale o quello relativo ad uno specifico settore o sistema.

## DIRITTO DELLA GESTIONE DIGITALE DELLE INFORMAZIONI

grado di conformità aziendale alla Norma, le eventuali lacune, le vulnerabilità ed i rischi che possono concretizzarsi in un danno effettivo per l'azienda.

### 5. La certificazione BS 7799

La certificazione BS 7799<sup>1</sup> è una dichiarazione pubblica che ha lo scopo di dare evidenza alla capacità di gestire la sicurezza delle informazioni all'interno di un'azienda.

Il valore della certificazione stessa è di alto livello, anche se per nulla cogente: la BS 7799 non è obbligatoria in base ad alcuna normativa nazionale né comunitaria, e l'adesione ad essa è assolutamente volontaristica. Il livello di sicurezza che essa garantisce è, però, un elemento fondamentale per aumentare la competitività aziendale, proprio perché ufficializzato da un organismo *super partes* che si basa, nella sua analisi, su norme universalmente valide e riconosciute.

La Certificazione BS7799 vanta, tra i propri benefici, la capacità di dimostrare all'opinione pubblica l'affidabilità e la credibilità dell'azienda ma anche e soprattutto la capacità di tutelare l'organizzazione in caso di contenziosi sorti in ragione di normative cogenti o requisiti contrattuali. Quest'ultima prerogativa le deriva dalla circostanza di assorbire, nel proprio sistema, anche specifici obblighi vincolanti nei vari Paesi in cui essa è applicata: in Italia, ad esempio, non si può essere certificati se non si rispettano preventivamente determinate rilevanti prescrizioni di legge come, a puro titolo esemplificativo: il Codice in materia di protezione dei dati personali (D.Lgs 196/03), la legislazione in materia di crimini informatici (L. 547/93), in materia di diritto d'autore (L. 633/1941 e successive modifiche), di responsabilità amministrativa degli enti e società (D.Lgs 231/2001) e, non ultimi, eventuali vincoli contrattuali stipulati dall'organizzazione in base all'ordinamento vigente.

In conclusione, l'ottenimento della certificazione alla BS 7799 rappresenta un forte segnale verso un mercato sempre più sensibile alle problematiche della gestione sicura delle informazioni.

**CRISTIAN ERCOLANO**

---

<sup>1</sup> La norma ne identifica 10: 1) politica di sicurezza; 2) organizzazione per la sicurezza; 3) controllo e classificazione delle risorse; 4) sicurezza del personale; 5) sicurezza fisica ed ambientale; 6) gestione dell'operatività e delle comunicazioni; 7) controllo degli accessi alle informazioni; 8) sviluppo e manutenzione dei sistemi; 9) gestione della business continuity; 10) conformità legale.

<sup>1</sup> Lo schema di certificazione prevede: una valutazione iniziale (c.d. pre-audit, seguito da una verifica ispettiva in azienda); il rilascio – da parte di un ente accreditato presso il SINCERT (ente accreditatore) - di un certificato di conformità alla norma valido 3 anni; verifiche periodiche di convalida durante il triennio e verifiche alla sua scadenza ai fini del rinnovo.