diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 18/02/2010

All'indirizzo http://www.diritto.it/docs/28936-i-piani-di-sicurezza-secondo-lo-standard-di-riferimento-bs7799

Autore: Guzzo Antonio

I piani di sicurezza secondo lo standard di riferimento BS7799

I piani di sicurezza secondo lo standard di riferimento BS7799 (a cura del Dottor Antonio Guzzo – Responsabile CED – Sistemi Informativi del Comune di Praia a Mare)

Il piano di sicurezza è un documento che seguendo lo standard BS (British Standard) 7799 (ISO 17799) – Code of Practice for Information Security Management fornisce un insieme di linee guida organizzative che possono riguardare una pubblica amministrazione e/o un'azienda. Nell'ambito di ciò che si definisce sicurezza si è soliti comprendere quattro settori specifici:

.1 Norme funzionali relative ai prodotti, aventi come scopo principale la ricerca della interoperabilità dei sistemi informatici

.2 Criteri di valutazione dell'assurance, ossia della fiducia riponibile nella sicurezza realizzata da sistemi e prodotti informatici

TC SEC (Applicato in USA)

IT SEC (Applicato in Europa)

ISO/IEC 15408 (Common Criteria – evoluzione ed integrazione di entrambi)

.3 Norme relative al sistema di gestione della sicurezza

ISO 9000 (solo di riflesso – Analisi del rischio)

ISO/IEC TR 13335 (parti 1, 2, 3, 4)

BS 7799 parte1 – Code of practice

BS 7799 parte2 – Verifica

ISO/IEC 17799 (che recepisce la parte 1 delle BS7799

.4 Norme legali

Legge 675/96

D.lgs 196/2003

DPR 318/99

Altre leggi e direttive nazionali ed europee.

La certificazione di sicurezza, attualmente, ritenuta la migliore e più completa è la BS 7799 emessa dal BSI (British Standard Institution). Essa infatti rappresenta una normativa che comprende le policies di best practice (miglior pratica) ed una serie di 127 controlli da effettuare cercare di rendere il proprio sistema informativo il più sicuro possibile. Le BS7799 affrontano il problema sicurezza ad alto livello, indipendentemente dalla tecnologia, concentrandosi principalmente sulla gestione della sicurezza. Le norme introducono nel settore della sicurezza il concetto di "**Sistema di Gestione**" che permette di tenere sotto controllo nel tempo i processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, di procedure formali e di canali di comunicazione. Principale obiettivo di un sistema di sicurezza è la salvaguardia delle informazioni. A tal proposito è fondamentale individuare quali informazioni proteggere e quale livello di protezione assegnare a ciascuna di esse. Si parla di "possibile" e non di "certo" poiché un "un computer sicuro è un computer spento e inabissato in fondo all'oceano", bisogna sempre ricordare l'assunto che la sicurezza al 100% non esiste. Tutto ciò che gravita attorno alla sicurezza è sempre legato ai mezzi usati per attuarla ma anche agli esseri umani che usano le risorse da proteggere e si sa che, anche ammettendo di avere dei mezzi perfetti, gli uomini non lo sono. Pensiamo ad un impiegato, egli può essere: ricattabile, corruttibile, distratto, ingenuo, frustrato ecc. ecc. Quindi anche se si spendono milioni di euro per proteggersi, non si potrà mai avere garanzie che gli uomini saranno sempre il punto debole. Uno degli assunti fondamentali della sicurezza è:

"*una catena è forte quanto il suo anello più debole*" quindi tutto quello che bisogna fare per mettersi al sicuro, il più possibile, è rafforzare al massimo l'anello più debole. Un'altra politica fondamentale è:"*tutto ciò che non è espressamente permesso è vietato*" Quest'ultima affermazione è, a volte, troppo conservativa, e spesso adottarla significa rendere la vita complicata, pensiamo se si dovesse adottare una politica così restrittiva negli aeroporti o nelle aziende, si formerebbero situazioni insostenibili. D'altro canto non si può adottare la politica: "*tutto ciò che non è vietato è permesso*" poiché troppo "aperta", quindi, come sempre, la sicurezza, va adeguatamente bilanciata, sia con gli investimenti economici sia con le politiche, in modo da non rendere la vita troppo difficile. Il successo della BS 7799 è dato dall'armonizzazione con gli Standard relativi a Qualità ed Ambiente, ed il miglioramento delle fasi relative alla verifica ed il controllo, tramite la definizione del modello "PDCA" (Plan Do Check Act) rappresentato nel diagramma sottostante.

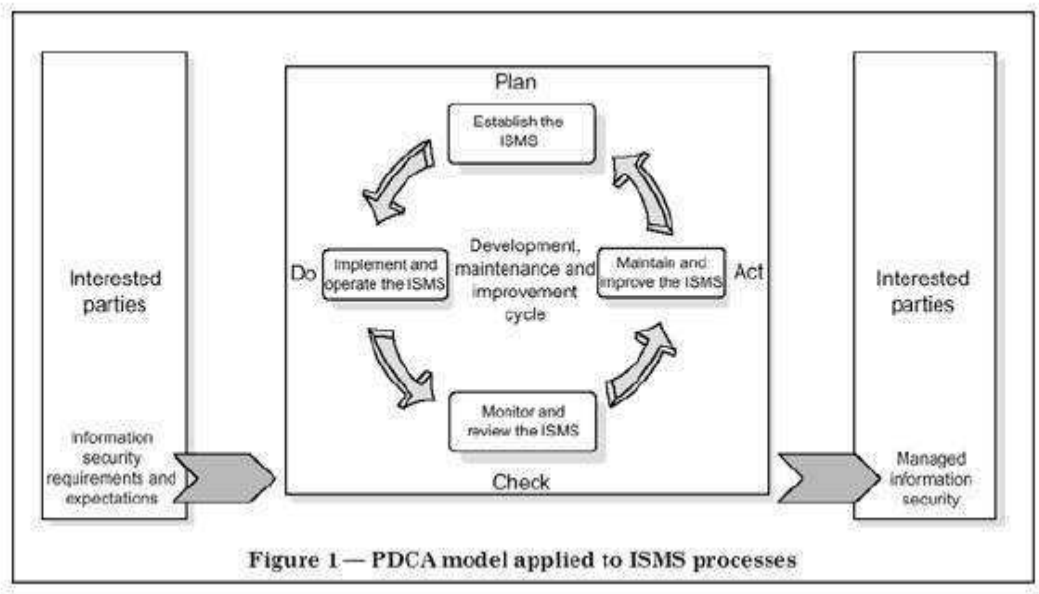

Figure 1 — PDCA model applied to ISMS processes

Lo standard segue un approccio simile a quello degli standard della serie ISO9000 per la certificazione di qualità di un'azienda. I concetti di politica di qualità e di sistema di gestione della qualità sui quali tali serie si basa, sono sostituiti da quelli di politica di sicurezza dell'informazione e di sistema di governo della sicurezza dell'informazione o ISMS (Information Security Management System) o SGSI (Sistema di Gestione della Sicurezza dell'Informazione). La politica di sicurezza è la specificazione ad alto livello degli obiettivi di sicurezza (espressi,come di consueto in termini di volontà di salvaguardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce) che l'organizzazione si propone di conseguire. L'ISMS, è la serie di procedure e contromisure adottate per mantenere fede alle politiche di sicurezza adottate. La Parte 2 dello standard BS 7799 propone il modello di ISMS schematizzabile come in **Fig. 1**. Si tratta di un modello dinamico nel quale vengono individuate 6 fasi di analisi e gestione del problema. I risultati delle analisi e le scelte di gestione vengono permanentemente messe in discussione in modo da garantire la capacità dell'azienda di mantenere nel tempo la sicurezza del proprio patrimonio informativo anche in presenza degli inevitabili cambiamenti dovuti a fattori esterni o interni all'azienda stessa.

Fig. 1 - Il modello di ISMS proposto dallo standard BS7799

La Parte 1 dello standard è un elenco di funzioni di sicurezza (controlli) di tipo organizzativo, logico, fisico, che costituiscono la prassi corrente per garantire la sicurezza dell'informazione in ambito industriale. Lo standard propone un insieme di 127 controlli/contromisure raggruppate in 10 categorie:

• Security policy (Politica di sicurezza);

• Security organization (Organizzazione per la sicurezza);

• Asset classification and control (Controllo e classificazione delle risorse);

• Personnel security (Sicurezza del personale);

• Physical and environmental security (Sicurezza materiale e ambientale);

• Communications and operations management (Gestione operativa e comunicazione);

• Access control (Controllo degli accessi);

• System development and maintenance (Sviluppo e manutenzione dei sistemi);

• Business continuity management (Gestione della continuità delle attività);

• Compliance (Conformità).

L'insieme dei controlli prescelti costituisce una sorta di regolamento di sicurezza che l'azienda si impone di rispettare. I controlli prescelti dovranno, pertanto, essere realizzati: attraverso meccanismi hardware o software (sistemi di autenticazione tramite password e/o smart-card, prodotti per la protezione crittografica dei dati, firewall, etc.), nel caso dei controlli attuati mediante misure di sicurezza di tipo tecnico; attraverso l'installazione di sistemi anti-intrusione, telecamere, casseforti, contenitori ignifughi, etc. nel caso dei controlli che richiedono misure di sicurezza fisiche; attraverso la creazione di apposite strutture o cariche aziendali e la definizione di precise

procedure per la messa in atto dei controlli di tipo procedurale (ad esempio l'istituzione del forum aziendale per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di indottrinamento periodico del personale, le procedure per l'accettazione di visitatori all'interno dell'azienda, etc.).