

Compliance e organizzazione Gestione dei sistemi informativi Sicurezza delle informazioni

I progetti di **compliance (adeguamento a norme e modelli)** saranno sempre più importanti, anche per le organizzazioni che operano in Italia. La produzione legislativa in materia è copiosa, a volte sovrapponibile e talvolta contraddittoria, ma il rispetto delle normative deve essere un'occasione per ottimizzare le risorse aziendali - in primo luogo quelle immateriali come informazioni e know-how - e presentarsi su mercati sempre più concorrenziali con credenziali maggiori.

Proponiamo un approccio comprensivo alla compliance, comprendendo sì la gestione degli aspetti tecnici (sicurezza informatica) ma anche di quelli organizzativi e di gestione delle risorse umane, di quelli economici-finanziari.

In Italia la **normativa sul trattamento dei dati personali** ("privacy") impatta la sicurezza delle informazioni, ma il suo campo di applicazione è relativamente limitato. Ci sono però molti motivi oltre al fatto di rispettare norme imperative per adottare dei modelli di gestione riconosciuti. **La responsabilità penale degli enti introdotta dal D. Lgs. 231/01** impone ormai anche in Italia l'adozione di modelli organizzativi sofisticati e formalizzati.



Negli Stati Uniti dal 2002 esiste il Sarbanes-Oxley Act ed il relativo modello di gestione della sicurezza da questa imposto (COSO) e modelli di gestione riconosciuti a livello internazionale come Cobit (di ISACA) e CMMI.

Le norme **ISO** standard della serie **27000** - la cui ispirazione e impostazione sono coerenti con quelle ad esempio della **serie 9000 sulla qualità** (gestione per processi, analisi dei rischi, approccio PDCA, gestione delle non conformità, azioni correttive...) - forniscono un modello di riferimento importante per la gestione dei rischi legati alla gestione delle informazioni, assieme alla **ISO 20000** (derivata dal modello ITIL) per la gestione dei servizi ICT. L'adozione delle normative ISO - e la possibile certificazione - anche se per ora imposta solo in particolari casi, diventerà sempre più importante, essendo riconosciuta a livello mondiale.

Facciamo alcuni esempi pratici di quanto ampio sia il patrimonio informativo aziendale da proteggere, anche nelle organizzazioni più piccole, dividendolo per funzioni aziendali:

Direzione: report strategici, piani di affari, contratti, corrispondenza elettronica e cartacea...

Risorse umane: fascicoli dei collaboratori, informazioni su compensi fissi e variabili (bonus, stock option), contratti, dati sensibili anche ai soli fini privacy, valutazioni delle posizioni e dei rendimenti...

Produzione: piani di produzione, distinte base, ricette di produzione e formule (magari nascoste e distribuite sui sistemi di automazione e supervisione non protetti adeguatamente), software proprietario...

Le leggi

D.Lgs. 196/03 - Testo unico Privacy
D.Lgs. 231/01 - Responsabilità penale
L. 262/05 - Antiriciclaggio

Le norme internazionali

ISO 27001 - Sicurezza delle informazioni
ISO 20000 - Gestione servizi IT
ISO 9000 - Gestione della qualità
ISO 15408 - Valutazione della sicurezza
ISO 13335 - Gestione della sicurezza IT

I framework di gestione

CMMI
CoBIT
COSO
ITIL

Ricerca e sviluppo: progetti, know-how, proprietà intellettuali in genere (brevetti...)
Amministrazione: dati finanziari e contabili, bilanci, budget periodici, elenchi di clienti...

Marketing: dati di vendita, programmi, dati relativi ai clienti o di loro proprietà, budget e previsioni di vendita...

La perdita o la sottrazione di queste informazioni può essere molto onerosa per l'azienda sia in termini economici che di immagine, oltre che legali. Esiste quindi la necessità di **prevenire:**
l'investimento sarà ripagato nel futuro dall'abbattimento dei rischi e dalla maggiore efficienza dell'organizzazione.

Contatti per maggiori informazioni e :

StudioAG - Consulting & Engineering

Via Giacomo Zanella, 166

I 36010 Cavazzale – VI

Tel. +39 0444 945523

Fax. +39 0444 298549

studio@studioag.eu

www.studioag.eu

Membro ISACA - Information Systems Audit and Control Association

Membro CLUSIT - Associazione italiana per la sicurezza informatica

Membro UNINFO - Comitato italiano per le norme ISO relative alla sicurezza delle informazioni

