PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 16 - numero 3230 di giovedì 09 gennaio 2014

La gestione della sicurezza delle informazioni e della privacy nelle PMI

Indicazioni per la realizzazione di un Sistema di gestione per la sicurezza delle informazioni (SGSI) che integri le varie misure di sicurezza e costituisca un quadro di riferimento per mantenerle e migliorarle nel tempo.

È disponibile online il quaderno "**La gestione della sicurezza delle informazioni e della privacy nelle PMI**" realizzato dal Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000 come libera iniziativa volta principalmente a diffondere la cultura dell'uso pratico degli standard relativi alla sicurezza delle informazioni in contesti di qualsiasi dimensione e non solo nelle grandi aziende.

Pubblichiamo un estratto del quaderno relativo al PLAN (ciclo PDCA: Plan, Do, Check, Act).

2.3.1.1 Ruoli e responsabilità

Il primo passaggio propedeutico alla creazione di un **Sistema per la gestione della sicurezza delle informazioni**, compresi i dati personali, una volta definita in modo preliminare la sua estensione rispetto ai processi aziendali, consiste nell'individuare un membro della Direzione con adeguate competenze relative al tema della privacy e della sicurezza delle informazioni, a cui assegnare la responsabilità di coordinamento (d'ora innanzi citato come Responsabile del sistema o del SGSI).

Questa figura, a seconda delle dimensioni e della complessità dei trattamenti di dati personali e dell'azienda, può essere dedicata completamente o meno a questo compito. Può però capitare, specie nelle PMI, che non esistano all'interno dell'azienda figure di competenza adeguata. In questo caso si presentano due possibili alternative:

- assegnazione della responsabilità ad una persona interna, che si appoggia, anche con continuità, ad un esperto esterno;
- assegnazione della responsabilità ad un esperto esterno, che opera con continuità e piena visibilità all'interno dell'azienda.

Qualunque sia la scelta adottata, non dovrà mancare al Responsabile il pieno sostegno della Direzione e la necessaria autorità per garantire una corretta ed efficace gestione del sistema. Il primo passo è la formalizzazione della sua nomina.

Va sottolineato che non dovrà mai mancare da parte della Direzione, che ha comunque la titolarità dei trattamenti, un adeguato e visibile supporto anche economico alle azioni proposte dal Responsabile del sistema, un continuo monitoraggio del suo operato e una costante condivisione degli obiettivi e delle finalità del SGSI.

In molte realtà, è d'uso associare alla nomina di Responsabile del sistema la nomina a Responsabile del trattamento. Poiché al Responsabile del sistema potrebbe non essere assegnato alcun particolare trattamento, tale scelta può essere intesa come non prevista dal Codice. Cionondimeno, il comma 2 dell'articolo 29 [1], in virtù dell'elevato livello di responsabilità assegnato al soggetto, rende giustificata la prima interpretazione. Si ricorda inoltre che la nomina del Responsabile del sistema, anche ai sensi del comma 3 dell'articolo 29 del Codice, non impedisce la nomina di altri Responsabili del trattamento, mediante opportuna suddivisione dei compiti.

Ulteriori responsabilità, ricoperte dal Responsabile di sistema in contesti aziendali di ridotte dimensioni o da personale a suo supporto, possono essere introdotte in base alla dimensione e alla complessità dei trattamenti effettuati e comprendono:

- verifica periodica (audit interno) dello stato di conformità del SGSI;

· gestione della documentazione del SGSI e del suo aggiornamento;
· supporto all'applicazione delle procedure del SGSI
· erogazione di interventi di formazione e consapevolezza;
· gestione delle comunicazioni in materia di privacy con gli interessati;
· risposta alle richieste di informazione, cancellazione o modifica di dati personali da parte degli interessati (esterni e interni all'azienda);
· sorveglianza dei nuovi obblighi normativi e delle sentenze in materia.

Gli altri ruoli aziendali normalmente coinvolti nella sicurezza delle informazioni sono il responsabile del Sistema informativo, il responsabile dell'Ufficio personale e, nel caso ci siano trattamenti di dati personali che presentano rischi specifici o per i quali è richiesta la notifica (ad es. carta fedeltà, gestione automezzi con GPS, ecc.), i responsabili delle aree aziendali coinvolte da tali trattamenti (eventualmente anche loro nominati Responsabili di tali trattamenti, ai sensi dell'art. 29 del Codice).

È importante sottolineare che non devono necessariamente essere coinvolti tutti i responsabili delle funzioni aziendali, ma solo coloro che sono specificamente dedicati a garantire, in vari modi e con diverse professionalità, la sicurezza delle informazioni e la protezione dei dati personali. In altri termini, l'organigramma della sicurezza non deve necessariamente replicare la struttura dell'organigramma aziendale. E' indispensabile però che il Responsabile del sistema sia un efficace canale di comunicazione con la Direzione aziendale che, a sua volta, deve fornire tutto il proprio appoggio affinché i diversi Responsabili dei trattamenti abbiano risorse e autorità adeguate a garantire un efficiente funzionamento del sistema.

2.3.1.2 Documentazione per la sicurezza delle informazioni
Definire e documentare una Politica per la gestione della sicurezza delle informazioni e dei dati personali, finalizzata a definire gli indirizzi e le regole generali da applicare in materia all'interno di tutta l'azienda è la base di partenza di tutto il sistema di gestione. La politica, sintetica ed estremamente comprensibile nella sua stesura, deve includere:
· una definizione di cosa si intende come sicurezza delle informazioni, dei suoi obiettivi e della sua importanza, in linea con gli obiettivi aziendali e la normativa sulla privacy;
· un indirizzo generale e i principi di azione concernenti la protezione dei dati personali;
· la descrizione dei processi necessari alla gestione della sicurezza delle informazioni e dei dati personali;
· la formalizzazione di ruoli e responsabilità;
· i criteri rispetto ai quali ponderare i rischi.

Tale Politica deve essere riesaminata almeno con cadenza annuale e venire approvata dalla Direzione affinché sia garantito e visibile il necessario appoggio.
Alla Politica deve essere associato un Elenco della documentazione aziendale (procedure) rilevante sul tema.

Il Documento programmatico per la sicurezza, se già presente, può essere convenientemente aggiornato e inserito nel suddetto elenco, anche se non più richiesto dall'attuale normativa privacy. Si raccomanda comunque di descrivere in un documento i meccanismi di sicurezza implementati.

Le procedure operative che guidano in maniera puntuale l'attuazione di quanto indicato nella politica possono essere definite in modo informale nelle aziende di più ridotte dimensioni mentre, con il crescere del numero delle persone, delle sedi e della complessità del business, aumenta la necessità di averle formalizzate all'interno di un unico documento o come oggetti separati per un più facile aggiornamento. Anche tali procedure dovrebbero essere riesaminate con cadenza annuale, in occasione degli audit interni.

I temi da trattare nelle procedure sono legati alla realtà aziendale e ai rischi che incombono su di essa. Quelli più frequentemente indirizzati sono:
· gestione della documentazione;
· gestione degli asset;
· controllo degli accessi fisici e logici;
· gestione delle utenze;
· gestione degli incidenti;
· back-up e ripristino;
· modalità di conduzione degli audit interni.

E' opportuno sottolineare come le procedure siano funzionali all'esecuzione di azioni specifiche, sovente legate a flussi

operativi. In tale prospettiva possono anche essere formalizzate in modo estremamente schematico indicando la sequenza delle attività e i corrispondenti ruoli degli attori coinvolti.
Si ricorda che l'Allegato B del D.lgs. 196/03 richiede esplicitamente la descrizione scritta di alcune attività: si raccomanda di includerle nelle procedure sopra elencate.

Si raccomanda inoltre di documentare per iscritto le regole per la corretta gestione delle informazioni e dei dati personali e degli strumenti aziendali connessi al loro trattamento. Esse dovrebbero essere mantenute aggiornate e distribuite a tutti gli incaricati o ai soggetti interessati dove rilevante. Tali regole, aggregabili anche in un solo documento, possono includere:

- le modalità di classificazione e etichettatura dei dati (vanno ad esempio identificati i dati personali di natura sensibile o le informazioni rilevanti per garantire la loro disponibilità, integrità o riservatezza) considerando i diversi supporti (per esempio, cartacei ed elettronici) su cui possono essere mantenuti;
- le regole di trattamento di informazioni e dati personali lungo tutto il loro ciclo di vita;
- le regole di accesso fisico e logico e le relative richieste ed assegnazioni dei diritti di accesso alle informazioni;
- le regole per l'uso di Internet e della posta elettronica;
- le regole per l'uso di computer, telefoni e altre tecnologie in dotazione.

Le suddette regole dovrebbero trovare applicazione nelle procedure operative.

L'**indice** del documento:

UNINFO - La gestione della sicurezza delle informazioni e della privacy nelle PMI (formato PDF, 727 kB).

RPS

[1] D.lgs. 196/03 (Codice in materia di protezione dei dati personali)