

## La sicurezza delle informazioni

La sicurezza delle informazioni si occupa di definire e organizzare la difesa contro una o più minacce o eventi dannosi, allo scopo di assicurare la continuità del business aziendale. In un primo tentativo di cogliere la nozione di sicurezza delle informazioni, possiamo dire che essa è l'attività volta a definire, perseguire e mantenere le proprietà di riservatezza, integrità, e disponibilità.

La **riservatezza**, mira a prevenire l'accesso non autorizzato alle informazioni, in quanto l'informazione deve essere accessibile soltanto al personale autorizzato, i possibili danni derivanti dalla fuga di informazioni possono nei casi più gravi essere:

- ✓ furto di segreti aziendali
- ✓ furto di credenziali di autenticazione per l'accesso a servizi (codici carte di credito)
- ✓ furto di informazioni strategiche per l'azienda (dati clienti -fornitori)
- ✓ diffusione di informazioni sensibili

Quindi ci sono di ogni tipo, rischi in termini economici, legali e di immagine. E' importante rendersi conto dell'importanza delle vostre informazioni, ogni informazione è importante e ogni informazione non è innocua, è anche importante pensare che alle vostre informazioni (anche semplicemente la posta elettronica), può essere interessato chiunque, dal vostro concorrente di mercato interessato alla vostra strategia al/vostro/a partner che mira semplicemente a curiosare nelle vostre mail per scoprire eventuali scappatelle.

L'**integrità** dei dati mira a prevenire l'alterazione non autorizzata delle informazioni, nessuno deve cioè, a vostra insaputa, modificare le informazioni in vostro possesso, modificare contratti, buste paghe, indirizzi, etc... Una volta salvati i dati occorre avere la sicurezza che questi siano immutabili, e quindi non modificabili né cancellabili dai non autorizzati. In questi caso è anche opportuno parlare dei gruppi di continuità, e cioè di quegli apparati che in caso di black-out permettono uno spegnimento corretto dei sistemi preservando l'integrità dei dati.

La **disponibilità** dei dati garantisce l'accessibilità alle informazioni agli autorizzati. Chi è autorizzato cioè deve poter accedere ai dati in qualunque momento, è quindi importante organizzare i back-up, ed assicurarsi della disponibilità dei dati archiviati (backup).

Per assicurarsi la riservatezza, l'integrità e la disponibilità dei dati rispettando i principi di riservatezza e necessità del Codice della Privacy (art. 1, 2 e 3) è quindi fondamentale avere delle adeguate "policy" (**politiche**) di **sicurezza**, avere cioè conoscenza (**formazione**) dei problemi e delle soluzioni in tema di privacy e sicurezza, quindi, implementare in ogni contesto aziendale delle **procedure** atte a rendere operativa la politica di sicurezza, ed infine, l'ultimo requisito fondamentale è la **disciplina**, tutti gli addetti/impiegati, devono sempre seguire la politica di sicurezza, e operare sempre secondo le procedure.

Proprio questo piccolo vademecum insieme al D.P.S. vuole essere una piccola guida sulla politica della sicurezza delle informazioni in azienda. (quindi il primo passo è fatto !!, mancano solo formazione, procedure e disciplina...). Invito comunque ogni azienda a dotarsi di un suo "piano di sicurezza" con scopi, principi, compiti, responsabilità e procedure.

## La legge sulla privacy e l'ambito oggettivo di applicazione

La legge sulla privacy è il primo concreto tentativo di assicurare la sicurezza delle informazioni in campo aziendale.

L'**ambito di applicazione oggettivo** del Codice della Privacy è rappresentato da qualsiasi trattamento di dati personali, cioè di qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Particolari misure devono essere prese per quello che riguarda i "dati giudiziari" e i "dati sensibili", cioè i dati personali idonei a rivelare:

- ▶ origine razziale ed etnica;
- ▶ le convinzioni religiose, filosofiche o di altro genere;
- ▶ le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale;
- ▶ nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

## Ambito soggettivo di applicazione

Le norme del Codice della Privacy riguardano tutti i soggetti privati e pubblici, le figure individuate dal Codice della Privacy sono:

- ▶ l'**interessato**, il soggetto al quale occorre rendere l'informativa, il titolare dei dati trattati
- ▶ il **titolare**, il soggetto a cui si riferiscono **sempre** tutti gli obblighi e doveri previsti dal Codice, il titolare è sempre il responsabile del trattamento
- ▶ il **responsabile** è una persona fisica che **può** (facoltativo) essere nominato dal titolare
- ▶ l'**incaricato** è la persona fisica nominata per iscritto e autorizzata dal titolare a compiere operazioni di trattamento dati

## Adempimenti

Gli adempimenti del Codice della Privacy a cui le aziende devono adempiere sono:

- Notificazione preventiva al Garante, va fatta solo in alcuni casi particolari
- Informativa agli interessati, deve precedere qualsiasi trattamento di dati e può essere fatta anche oralmente (ma la prova è difficile)
- Consenso, bisogna ottenerlo prima di effettuare i trattamenti (anche oralmente), ma non è richiesto quando il trattamento è necessario per eseguire obblighi derivanti da un contratto, e

quando riguarda dati relativi allo svolgimento di attività economiche trattati nel rispetto della vigente normativa in materia di segreto aziendale.

- Autorizzazione del Garante, solo per dati sensibili, salvo le autorizzazioni generali recentemente rinnovate fino al 30 giugno 2007
- Nomina per iscritto degli incaricati
- Nomina per iscritto dei responsabili (facoltativa)

Misure minime di sicurezza

Documento programmatico sulla sicurezza.

Nella pratica le uniche misure a cui una piccola-media deve adempiere sono l'adeguamento alle misure minime di sicurezza (di cui qui sotto una sintesi), il D.P.S., la nomina per iscritto degli incaricati e l'informativa agli interessati. Raramente le piccole-medie aziende sono obbligate ad altri adempimenti.

## Misure minime di sicurezza

Per quanto riguarda le misure minime a cui attenersi queste riguardano quelle procedure di cui si parlava al primo capitolo. Ogni incaricato/addetto dovrebbe leggere con attenzione questo capitolo (e il D.P.S.).

1. **Sistema di autenticazione informatica**, ogni volta che si accede ad una risorsa informatica, ad una base di dati su un computer, occorre accedervi con un username ed una password, ogni incaricato deve avere le sue credenziali di autenticazione. Custodire le credenziali in busta chiusa.
2. Se necessario se si gli incaricati trattano dati diversi occorre stabilire profili di autorizzazione diversi (raramente accade nelle piccole-medie aziende)
3. Proteggere i dati informatici tramite **antivirus, firewall** (anche software),
4. **Aggiornare** i propri software
5. Programmare **backup** almeno settimanali, ed assicurarsi della disponibilità dei dati archiviati (backup).
6. **Distruggere o comunque rendere inutilizzabili i supporti rimovibili** di memorizzazione.

## Altre misure di sicurezza non obbligatorie

Altre misure consigliate, ma non obbligatorie, per la sicurezza dei dati sono:

- Dotarsi di **gruppo di continuità** per proteggersi da black-out improvvisi
- Utilizzo di **caselle di posta filtrate**
- **Software di controllo** dei sistemi

- **cifratura dei dati** persistenti e dei dati trasmessi
- **firma digitale**
- controlli e registrazione degli accessi
- Filtraggio di tutto il traffico da internet (impossibilità di scaricare codice ostile)

## Altre buone abitudini per la sicurezza e la privacy in azienda

Sarebbe opportuno **classificare i propri dati**, classificare sia i dati trattati correntemente (ma questo viene già fatto dal DPS), sia i dati archiviati (backup), questo in modo da avere piena coscienza delle risorse informativi disponibili da proteggere. La classificazione inoltre aiuta a gestire vari livelli di riservatezza delle informazioni (qualcosa di simile ai regimi autorizzativi del DPS), determinando quali dati sono confidenziali, quali personali, quali a semplice rilevanza interna e quali pubblici.

Se avvengono **richieste di informazioni dall'esterno** occorre sempre verificare con delle procedure precise l'identità del richiedente e il suo status. Mai diffondere informazioni se non si è certi dell'identità.

Usare i computer solo per scaricare posta fidata (caselle di posta filtrate da antivirus) e per consultare siti "fidati", **diffidare dei programmi** per lo scambio di file, e dei programmi di messaggistica, far configurare i propri sistemi informatici per la massima sicurezza.

Se possibile, evitare di installare **punti di accesso wireless** (senza fili) ed impedire connessioni (abusive) da pc portatili.

Per i comuni incaricati/dipendenti evitare di usare **account "root", "admin"** o comunque con poteri di amministrazione. Non permettere l'installazione di software e l'uso di floppy-cd agli incaricati/dipendenti.

**Verificare ogni volta le informazioni** ricevute dall'esterno o inviate all'esterno.

L'ultima buona abitudine è come sempre un invito a fare formazione, ad investire in conoscenza, formazione e conoscenza per l'uso dei mezzi informatici e per sfruttare al meglio i sistemi e le informazioni che contengono.