

## **Misure di sicurezza per il trattamento dei dati (D Lgs 196/03 e successivi Provvedimenti del Garante - GDPR 2016/679)**

### ***Premessa***

Le norme in materia di sicurezza si caratterizzano per i seguenti parametri:

- sono di tipo organizzativo e di tipo tecnico
- si distinguono per la tipologia dei dati (classificati ex art. 4)
- si distinguono per la dimensione aziendale e, in genere, la varietà e complessità delle operazioni
- sono in divenire attraverso nuovi Provvedimenti nazionali o europei

**Aspetti tecnici (gli stessi temi sono anche oggetto di una relazione di tipo "organizzativo" a completamento)**

### **Schema di riferimento (per procedura controllo ex art. 32 lett. d GDPR 2016/679)**

#### **1. Gestione password (sistema di autenticazione) (D. Lgs 196/03 All. B1-11)**

- a. principi
  - i. lunghezza minima 8 caratteri
  - ii. scadenza (manuale o automatica) periodica
  - iii. differenza strutturale e di contenuti fra pw successive
  - iv. memorizzazione di tutte le versioni successive
- b. tipologia
  - i. di stazione di lavoro
  - ii. di salvaschermo
  - iii. di rete
  - iv. di amministratore di sistema
  - v. gerarchiche
  - vi. di accesso a specifici servizi (es. posta elettronica, web generico, altro)
  - vii. per specifici applicativi (accesso)
- c. modalità di gestione
  - i. chi può fare cosa
  - ii. log degli interventi

#### **2. Autorizzazioni/profili (D. Lgs 196/03 All. B12-14)**

- a. legate a stazioni di lavoro
- b. legate a specifici ID/PW
- c. legate a specifiche operazioni di sistema
- d. legate a specifiche basi dati
- e. legate a specifiche funzioni di applicativi
- f. chi può fare cosa
- g. memorizzazione interventi

**3. Operazioni di back up (D. Lgs 196/03 All. B 18 e 20-22)**

- a. modalità di esecuzione (automatica/manuale/locale/remoto, ecc.)
- b. frequenza
- c. autorizzazioni
- d. modalità di esecuzione
  - i. solo alcuni file con caratteristiche specifiche
  - ii. tutti i file in specifiche cartelle e/o specifici hw
  - iii. back up completo o incrementale
  - iv. supporti utilizzati (rimovibili) con relative caratteristiche

**4. Operazioni di ripristino (D. Lgs 196/03 All. B23)**

- i. modalità esecuzione
- ii. frequenza
- iii. test validità

**5. Crittografazione dati (D. Lgs 196/03 art. 22 c. 6 e All. B24)**

- a. presenza o meno di un obbligo di legge
- b. automatismi per specifiche basi dati
- c. attivazione successiva e/o da esterno /v. soluzioni Partner)
- d. autorizzazioni relative

**6. Analisi di Vulnerabilità/Penetration test (D. Lgs 196/03 All. B16)**

- a. da attacchi esterni
- b. da errori interni

**7. Utilizzo mail (D. Lgs 196/03 art. 154 1c - Provv. 1.3.07, art. 7 Statuto dei lavoratori 1970)**

- a. presenza mail individuali o di gruppo e relative autorizzazioni
- b. controlli automatici per prevenire intrusioni, malware, spam, ecc.
- c. controlli per bloccare invii non autorizzati
- d. controlli per evitare download indesiderati
- e. controlli per allegati indesiderati (input/output)
- f. modalità memorizzazione e conservazione

**8. Utilizzo web generico (non siti per servizi specifici) (v. sopra)**

- a. limitazione accessi
- b. cronologia accessi (da remoto)
- c. limitazione attivazione servizi esterni

d. regolamentazione e controllo aggiornamento dati

**9. Privacy siti (L. 70/03)**

- a) informazioni su home
- b) privacy policy

**10. Videosorveglianza (Prov. 29.11.00, 22.9.09, 8.4.10)**

- a. impianto autonomo o gestito via PC
- b. supporto e modalità di registrazione (continua, ad immagini in movimento, in sovrapposizione, ecc.)
- c. durata immagini
- d. riproducibilità

**10. Apps su mobile aziendali (guide e documenti vari sito Garante)**

- i. utilizzo di apps dal mercato
  - 1. verifica pertinenza dati eventualmente raccolti e loro utilizzo
  - 2. verifica Terms of Service del fornitore di apps
  - 3. modalità e registrazione dai raccolti
  - 4. possibilità di controllo degli stessi
  - 5. durata mantenimento dati (anche dopo cancellazione servizio/funzione)
- ii. utilizzo apps proprie
  - 1. c.s.
  - 2. NA
  - 3. c.s.
  - 4. c.s.
  - 5. c.s.