ISMAR ANCONA

Incontro di aggiornamento sulle misure minime sulla sicurezza informatica con il personale.

Ancona, 29 giugno 2011

a cura di
Rocco De Marco
rocco.demarco@an.ismar.cnr.it

Programma dell'incontro

- Durata: ca. 1 ora
- Argomenti trattati:
  - Cenni sul trattamento dei dati personali, il nostro dps
  - Sicurezza degli accessi (password)
  - Sicurezza dei dati (backup)
  - Norme generali di comportamento

I dati sensibili

- I dati personali sensibili sono quelli che riguardano: Sesso, salute, soldi, sindacati, religione, razza.
- Con la semplificazione:
  - *"Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B) (...)"*

In altre parole

- La semplificazione ha eliminato l'obbligo di presentazione del DPS nei casi consentiti, ma non la necessità di rispettare i requisiti delle misure minime di sicurezza
- L'ismar ha comunque presentato il dps poiché:
  - Tratta dati personali sensibili (schede sanitarie dipendenti, certificazioni mediche concorsi)
  - Effettua attività di monitoraggio del traffico dati

Misure minime di sicurezza informatica

- Fonti normative: D.lgs 196/03, D.l. 25/6/08 n.112 e convertito in legge il 6/8/08, n133
- Art. 31: Obblighi di Sicurezza
  - I dati personali vanno conservati prevenendo rischi di:
    - Distruzione
    - Perdita
    - Accesso non autorizzato
    - Trattamento illecito

Gli adempimenti: la sintesi

- I dati sono accessibili solo previa autenticazione
- Gli utenti sono tenuti ad impiegare password di sufficiente robustezza
- *“chiunque essendovi tenuto omette di adottare tutte le misure previste dall'articolo 33 è punito con l'arresto fino a 2 anni e con un'ammenda da 10.000 a 50.000 €”*

La password

- Lunghezza minima: 8 caratteri
- Almeno una cifra
- Almeno una maiuscola
- Almeno un carattere speciale
- Esempio valido: Bx34$rtZ, ma anche Birb0,99
- NOSTRA PROMESSA: una persona, una password per tutti i servizi della sede.

Norme di comportamento

- NON usare email istituzionali per comunicare informazioni sensibili
- NON usare email istituzionali per intrattenere rapporti non attinenti alla attività
- USARE email private per le attività individuali (es. gmail, yahoo, etc.)
- NON usare i sistemi dell'istituto per memorizzare immagini, testi o file personali contenenti dati sensibili: immagini di famiglia, curricula dei familiari, etc.