Privacy e sicurezza informatica

Concetti, principi ed indicazioni pratiche

http://eos.pi.it/Approfondimenti/Sicurezza/PrivacyPacinotti/slides.pdf

Marzo 2008

Manlio Morini

Sommario

Normative e linee guida
- Disciplinare tecnico
- Normative ISO/IEC
- Direttive CNIPA

Concetti fondamentali
- ISO/IEC
  - Disponibilità
  - Integrità
  - Riservatezza
- Testo Privacy
  - Misure minime
  - Misure idonee

Sistemi di autenticazione
- Credenziali di autenticazione
- Gestione password
- Dispositivi di autenticazione

Cosa fare, cosa evitare
- E-mail
- Web
- Backup

Normative e linee guida

Allegato B (artt. da 33 a 36 D.Lgs 196/2003)
(Disciplinare Tecnico in materia di misure minime di sicurezza)

- Autenticazione, codici identificativi e password
- Profili di autorizzazione
- Disposizioni varie
- Adozione di sistemi di cifratura
- Backup
- Interventi formativi

Sottoinsieme

ISO/IEC 17799:2005
(Information Technology – Security Techniques)

Perfezionamento

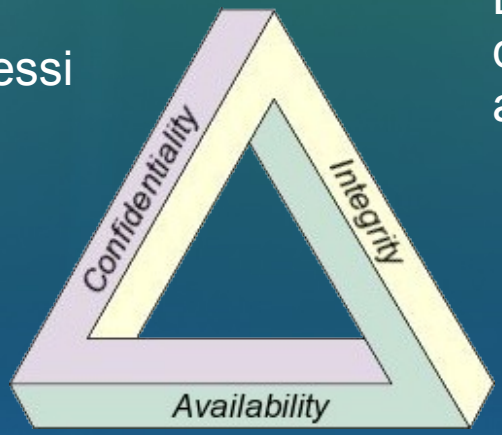
ISO 27001
(Information security management systems)

Concetti fondamentali 1

(ISO/IEC)

Riservatezza

Le informazioni non devono essere consultabili da parte di utenti / processi non autorizzati



Integrità

Le informazioni ed i processi devono essere protetti da modifiche accidentali o non autorizzate

Disponibilità

Garanzia che un sistema informatico sia sempre utilizzabile dagli utenti legittimi.

Concetti fondamentali 2

("Testo unico sulla Privacy")

- Misure minime (dati personali)
  - Definizione di una procedura per il trattamento tecnico/organizzativo dei dati personali e dell'organigramma della sicurezza (DPS e lettere di incarico). Aggiornamento almeno annuale.
  - Politiche di backup (settimanale).
  - Formazione degli incaricati al trattamento dati.
  - Installazione ed aggiornamento software antivirus / software per prevenire le vulnerabilità e correggere i difetti (ogni 6 mesi).

Concetti fondamentali 3

("Testo unico sulla Privacy")

- Misure per dati sensibili / giudiziari
  - Tecniche per la custodia dei supporti rimovibili, la distruzione controllata e la cancellazione (e.g. *sanitizzazione DoD 5220.22-M*).
  - Crittografia.
  - Contingency plan.
- Misure idonee
  - Ciò che va oltre le misure minime.
  - La mancata adozione delle misure minime comporta responsabilità penali. L'adozione di misure idonee ci tutela da responsabilità civili.

Sistema di autenticazione informatica 1

(punti da 1 a 11)

Autenticazione
Identificazione sicura dell'utente.

Identità verificata

Integrità
Riservatezza

Credenziali di autenticazione
I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati.

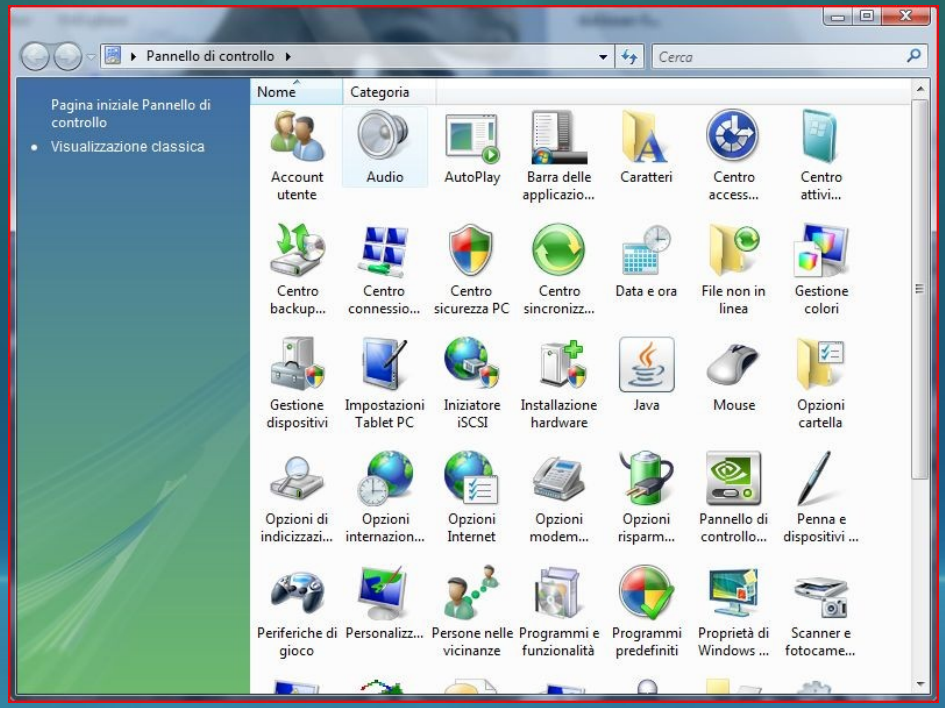
Sistemi di autenticazione informatica 2

(credenziali di autenticazione)

- Qualcosa conosciuto solo dall'utente (e.g. parole d'ordine, PIN)... *what a person knows*
- Dispositivi posseduti dall'utente (e.g. carte, chiavi)... *what a person has*
- Attributi dell'utente (e.g. impronte digitali, geometria della mano, caratteristiche della retina/iride, voce, viso)... *what a person is*

Sistemi di autenticazione informatica 3

(settaggio account utente con Windows Vista)

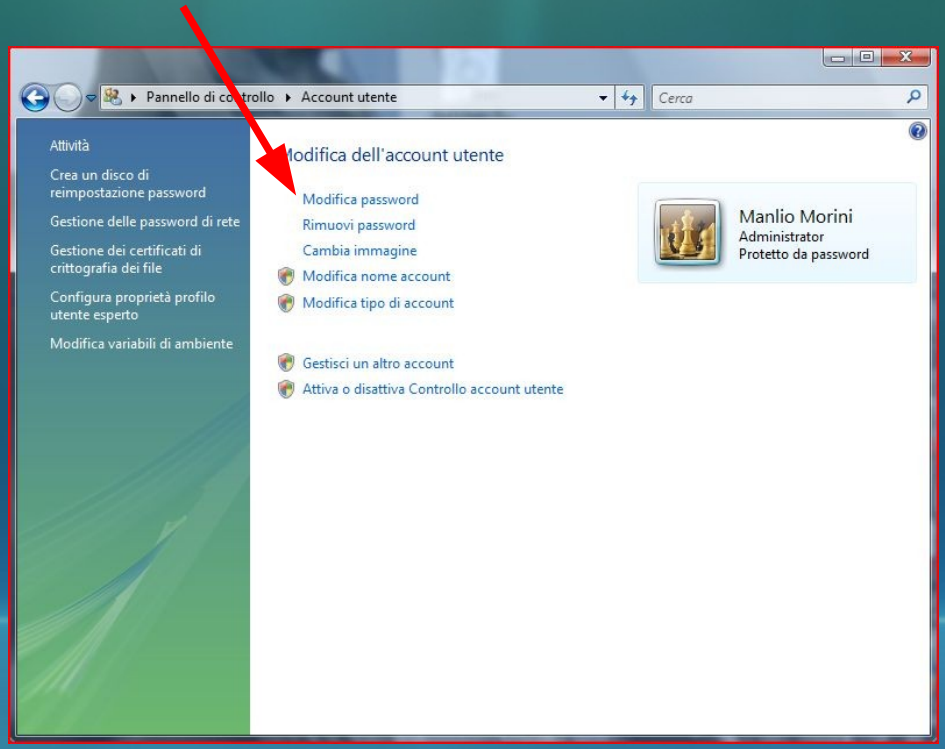


- Pulsante Start (barra delle applicazioni, tasto in basso a sinistra).
- Voce “Pannello di controllo”.

Sistemi di autenticazione informatica 4

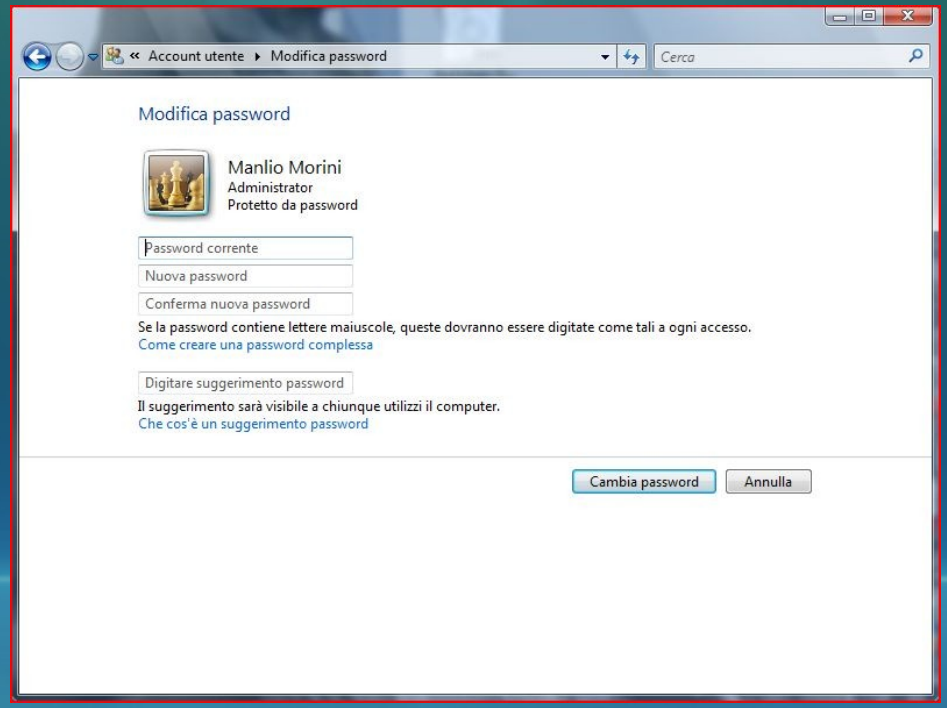
(settaggio account utente con Windows Vista)

- Modifica password.
- Modifica tipo account.



Sistemi di autenticazione informatica 5

(settaggio account utente con Windows Vista)



- Formato della password.
- Modifica periodica.
- Problema del default.
- Segretezza delle credenziali.
- Custodia delle credenziali.

The big lie of computer security is that security improves by imposing complex passwords on users. In real life, people write down anything they can't remember. Security is increased by designing for the way humans actually behave

Jakob Nielsen

Sistemi di autenticazione informatica 6

(credenziali di autenticazione alternative / supplementari)

- Impronta digitale, smartcard, scansione dell'iride, geometria della mano... Molte di queste tecnologie sono economicamente accessibili, ma presentano il problema della memorizzazione di dati biometrici.

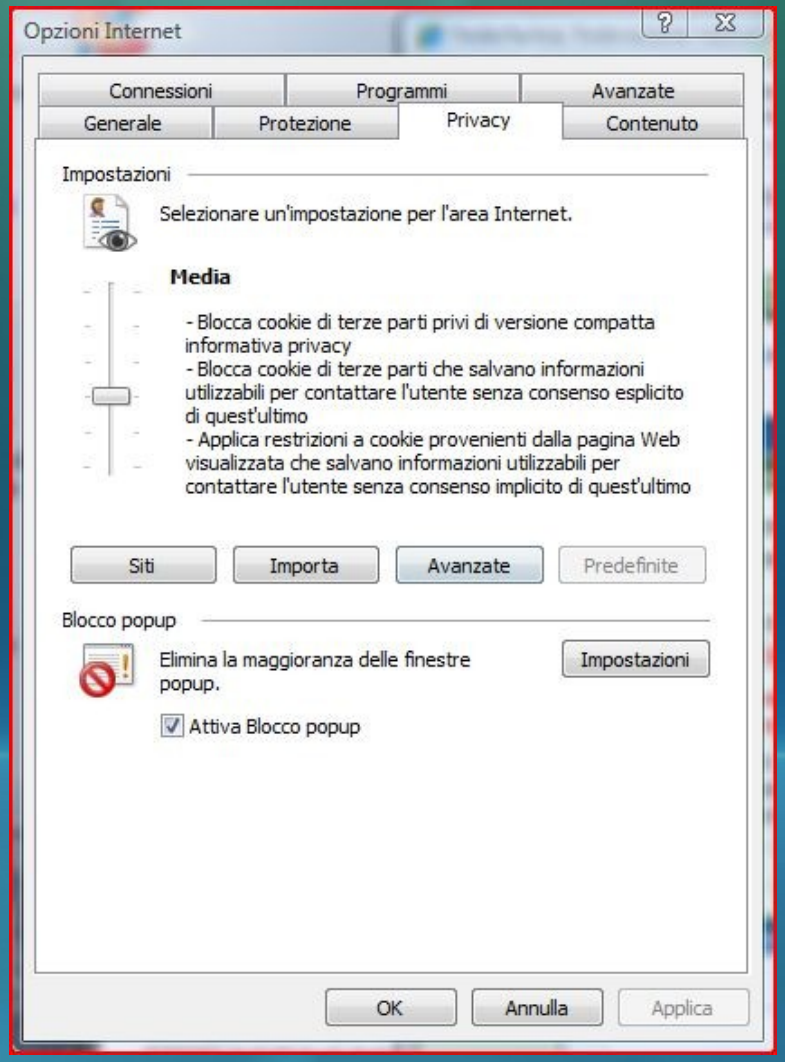
Cosa fare, cosa evitare 1

(e-mail)

- La posta elettronica tradizionale NON è sicura!
  - Per il mittente
    - I messaggi viaggiano in chiaro
    - Tempi ed instradamento sono indefiniti
    - Non esiste certezza di recapito
  - Per il destinatario
    - Il mittente non è certo
    - Il messaggio può esser stato alterato od essere falso (spoofing, phishing)
  - Problema spamming
    - Non rispondere ai messaggi!

Cosa fare, cosa evitare 2

(web)

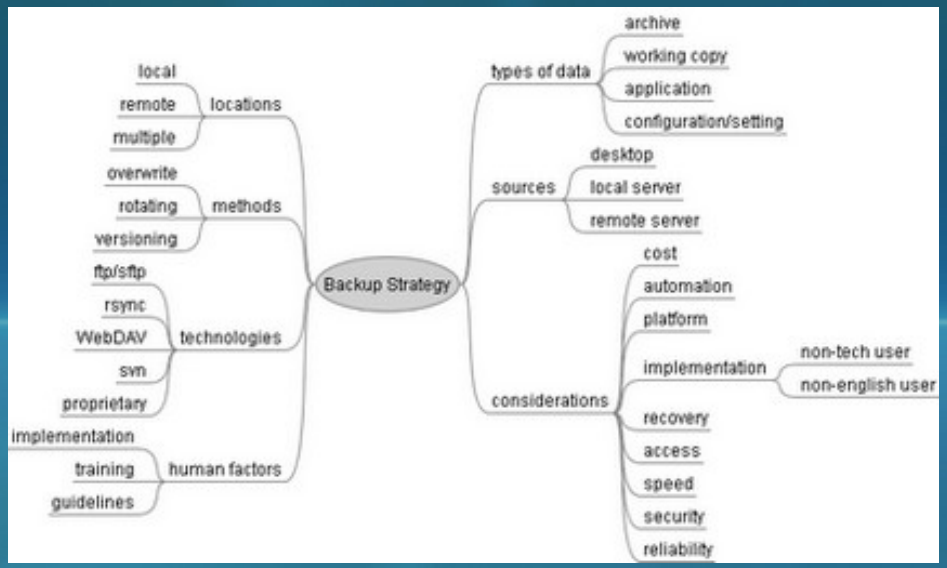


- Non utilizzare il meccanismo di accesso automatico ai siti.
- Verificare il livello di sicurezza del proprio browser (voci strumenti/opzioni internet/protezione e strumenti/opzioni internet/privacy): almeno medio/medio-alto.
- Non scaricare software/certificati da fonti non attendibili
- NON FIDARSI!

Backup

The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered and his States and all their clans are preserved.

Confucio



- Le procedure di backup vanno modificate e migliorate nel tempo
  - Quante copie?
  - Cosa copiare?
  - Con quale frequenza?
  - Su quali dispositivi?
  - Come conservarle?
- Ripristino di prova periodico (efficienza / efficacia)
- Eliminazione di supporti memorizzazione, elaboratori e dispositivi elettronici (sanitizzazione)

Approfondimenti

- Libri / collegamenti
  - http://eos.pi.it/Approfondimenti/ (sezione sicurezza per consigli, posta elettronica certificata, firma digitale, crittografia, backup, dati...)
  - http://www.garanteprivacy.it
  - http://www.cnipa.gov.it
  - http://www.clusit.it
  - “L'arte dell'inganno” - Kevin Mitnick
- Software
  - http://www.ccleaner.com ('pulizia' del sistema)
  - http://www.free-av.com (antivirus gratuito)
  - http://www.safer-networking.org (anti spyware gratuito)
  - http://www.truecrypt.com (archivi cifrati)
  - http://www.gnupg.org (crittografia a chiave pubblica)

Domande