Carlo Carlesi
Istituto di Scienza e Tecnologie dell'Informazione “A. Faedo”

STeP

Analisi dei principali adempimenti di carattere organizzativo e procedurale

PRINCIPALI ADEMPIMENTI DI CARATTERE ORGANIZZATIVO E PROCEDURALE

- Sicurezza fisica e logica dei dati
- Le misure di sicurezza minime richieste dal Dlgs 196/2003
- Il Documento Programmatico della Sicurezza (DPS)

SICUREZZA

- **Nel linguaggio corrente, per sicurezza si intende una “misura di protezione” e si definisce sicuro “ciò che è esente da pericoli”**

SICUREZZA INFORMATICA

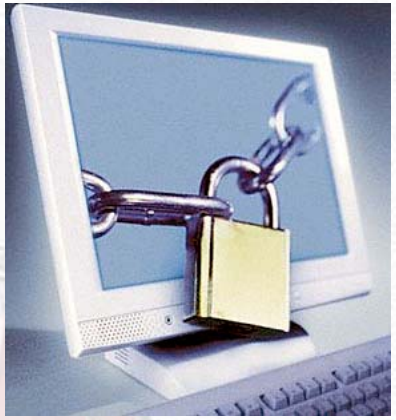
- Un sistema informatico è considerato sicuro quando è in grado di garantire determinati requisiti di sicurezza in termini di:
  - Disponibilità
  - Integrità
  - Riservatezza
  - Autenticità e non ripudio
- Lo standard ISO 27001:2005 è una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nel settore informatico

REQUISITI

- **Requisisto di disponibilità**
  - **Il sistema deve garantire la disponibilità delle informazioni a ciascun utente autorizzato nei modi e nei tempi previsti (politiche aziendali)**
- **Requisito di integrità**
  - **Il sistema deve impedire e comunque rilevare alterazioni dirette o indirette delle informazioni da parte di utenti o procedure non autorizzati o a causa di eventi accidentali**

REQUISITI

- **Requisito di riservatezza**
  - Nessun utente deve poter acquisire o dedurre, dal sistema, informazioni che non è autorizzato a conoscere
- **Requisito di autenticità e non ripudio**
  - Avere la certezza che una data informazione appartenga da chi dice di averla generata (autenticità)
  - Chi ha generato una data informazione non deve poter negare di averlo fatto (non ripudio)



IL RIPUDIO DI AGAR
Francesco Ruschi (1610-1670)
Olio su tela

COSA È LA SICUREZZA

- La ”Sicurezza Informatica” è l’insieme delle misure di carattere organizzativo, tecnologico e procedurale mirate ad assicurare la protezione dei sistemi informatici e delle informazioni in essi contenuti riguardo a determinate minacce

SICUREZZA INFORMATICA

- NIST – Recommended Security Controls for Federal Information System
  - Information Security (October 2006)

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

MINACCE

- Possibili condizioni, azioni o eventi in grado di modificare o alterare le normali funzionalità di un sistema

- Minacce:
  - Guasti hardware
  - Errori Software
  - Errori umani
  - Intrusioni
  - Cause accidentali ed imprevedibili (allagamenti, incendi, black-out etc)
  - Vulnerabilità (di infrastruttura, di progetto, di sistema, rete)

VULNERABILITÀ

- La sicurezza totale nella realtà è un'astrazione
- Non esiste un sistema informatico totalmente sicuro

Vulnerabilities reported

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2006

Year	2000	2001	2002	2003	2004	2005	Q1-Q3,2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	5,340

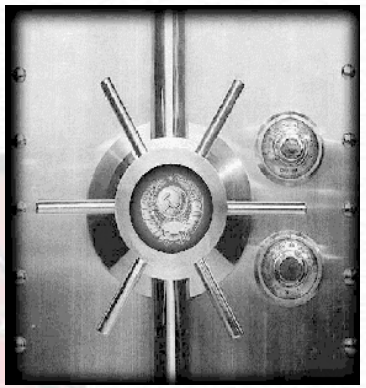
Total vulnerabilities reported (1995-Q3,2006): **28,056**

OBIETTIVI DELLA SICUREZZA

- Scopo principale della sicurezza informatica è quello di proteggere i “beni informatici” (ASSET)
  - Riducendo i rischi, a cui sono esposti
  - Limitando gli effetti causati dall’eventuale occorrenza di una minaccia (rischio residuo)

SICUREZZA FISICA/PASSIVA

- Sicurezza perimetrale
  - Protezione accesso ai locali
    - Porte blindate, serrature sicurezza
  - Registrazione e controllo degli accessi
  - Vigilanza e/o videosorveglianza
  - Dispositivi di autenticazione
    - Badge di accesso, dispositivi biometrici
  - Sistemi di allarme e anti intrusione
  - Sistemi anti-incendio
  - Gruppi di continuità elettrica



Sicurezza logica/organizzativa

- Definizione dei ruoli e dei compiti
- Definizione delle responsabilità
  - Dei dati
  - Dei sistemi
- Definizione di procedure e diritti di accesso ai dati e ai sistemi
- Analisi dei rischi e misure di sicurezza
- Sicurezza dei sistemi e della rete
  - Controllo del software di sistema
  - Controllo del software applicativo
  - Controllo del traffico di rete
  - Controllo degli accessi remoti
  - Controllo dispositivi “hardware”

CONCETTO DI RISCHIO

- **Fibonacci e Cartesio**
  - **Studiano in termini probabilistici la connessione tra rischio e gioco**

Probabilità di vittoria rispetto a quella di perdita

- **Concetto di rischio**
  - **Eventualità di subire un danno**

CONCETTO DI RISCHIO

- Rischio come un evento di cui è incerto il verificarsi
  - Conseguenze positive
  - Conseguenze negative

- L'analisi del rischio è un prerequisito essenziale per la progettazione razionale dei sistemi di protezione

CONCETTI COMUNI

- **Rischio**
  - Eventualità che una *minaccia* possa trasformarsi realmente in danno, comportando così un determinato *impatto*
- **Minaccia**
  - Evento di natura dolosa o accidentale che sfruttando una *vulnerabilità* del sistema, potrebbe provocare un *danno*

CONCETTI COMUNI

- **Vulnerabilità**
  - Debolezza, intrinsica o dovuta a condizione di esercizio, che può essere sfruttata da una minaccia per arrecare un danno
- **Danno**
  - Conseguenza negativa del verificarsi di un rischio o dell'attuarsi di una minaccia

CONCETTI COMUNI

- **Impatto**
  - **Il concetto è lo stesso di danno in termini di misura o entità del danno ma alcune metodologie indicano che l'impatto deve tenere conto anche di possibili responsabilità civili o penali, (es. Il D.Lgs. 196/2003) quindi l'effetto reale del danno sul sistema (azienda)**

FASI DELL'ANALISI DEI RISCHI

- **Adozione di una metodologia/approccio**

1. **Preparazione e pianificazione**
   Identificazione degli Asset, architettura di rete, dispositivi fisici, applicativi e processi aziendali

2. **Identificazione e stima dei rischi**
   Determinare le minacce e le conseguenze (check-list)

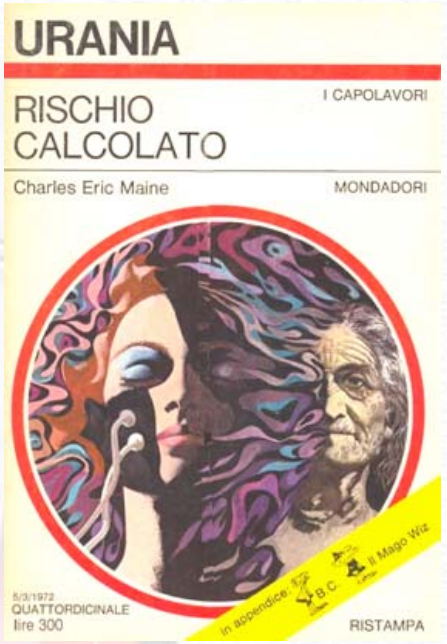
3. **Valutazione dei rischi**
   Classificare la gravità/criticità e identificare le misure di protezione ritenute più appropriate

ANALISI DEI RISCHI

- Alcuni strumenti/metodologie
  - BSA
  - CRAMM
  - CETRA
  - COBIT
  - EBIOS
  - ISO21827
  - OCTAVE
  - FIRM
  - SARA
  - .....

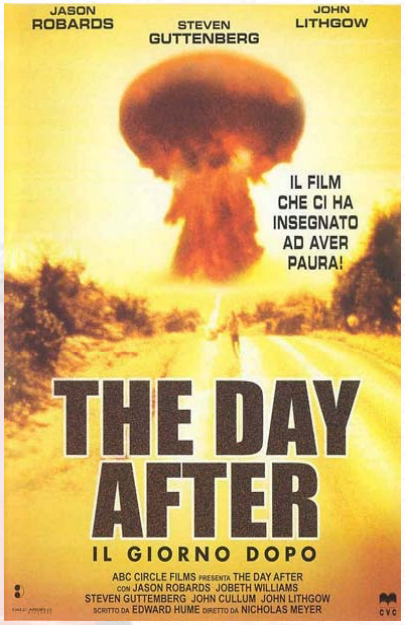
APPROCCIO ALLA VALUTAZIONE DEI RISCHI

- **Metodo qualitativo**
  - Prevede una valutazione del rischio su una scala qualitativa
    - Alto, medio, basso
- **Metodo quantitativo**
  - Valutazione della perdita economica derivante dal verificarsi del rischio
- **Metodo semi-quantitativo**
  - Compromesso tra i primi due



APPROCCIO ALLA GESTIONE DEI RISCHI

- Approccio reattivo
  - Al verificarsi di un evento si tenta di contenere il problema e di ripristinare il sistema il più presto possibile limitando i disagi
  - Successivamente si risale alle cause e si attivano nuove protezioni
- Appproccio preventivo
  - Cerca di ridurre la possibilità che si verifichino problemi



GESTIONE E VALUTAZIONE DEI RISCHI

- **Obiettivi:**
  - **Gestione dei rischi**
    - Gestire tutti i rischi e portarli ad un livello accettabile
    - Programmazione continua
  - **Valutazione dei rischi**
    - Identificare i rischi e definirne le priorità
    - Programmazione in base alle necessità

LIVELLO DI MATURITÀ (AZIENDA)

0 Inesistente

Non esiste un criterio di analisi dei rischi e/o non sono conosciuti

1 Ad-hoc

Non esistono criteri e procedure documentate ed il processo non è ripetibile

2 Ripetibile

Il processo è ripetibile ma non ancora completamente documentato (maturo)

3 Processo definito

Adozione di procedure di gestione formalizzate

4 Gestito

Il processo di gestione è ben definito e assistito da strumenti tecnologici

5 Ottimizzato

Il processo di gestione è ben identificato e significatamente automatizzato

BENI INFORMATICI

- Sistemi + Informazioni + Servizi
  - Sistemi (Hardware & Software)
    - Personal computer, workstation, server, main frame, supporti di memorizzazione
    - Apparecchiature di rete (locali e geografiche), sistemi di comunicazione elettronica, router, switch
  - Informazioni
    - Banche dati e documenti digitali
      - Dati finanziari/marketing
      - Dati aziendali/personali
      - Piani strategici
      - Dati personali sensibili
    - Dati in transito sui sistemi di comunicazione
  - Servizi
    - Posta elettronica
    - Server WEB
    - Sportelli elettronici

PERICOLI COMUNI

- **Persone malintenzionate**
  - Dipendenti insoddisfatti, negligenti, disonesti; hacker e pirati informatici
- **Persone non malintenzionate**
  - Dipendenti/utenti non informati
- **Eventi catastrofici**
  - Incendi, inondazioni, terremoti, nubifragi, valanghe, …
- **Problemi tecnici**
  - Guasti hardware, interruzione servizi di rete, dell'alimentazione, incidenti edili

Vulnerabilità comuni

- Fisiche
  - Accesso alle strutture non presidiato
  - Progettazione dei locali non adeguata
  - Materiali di costruzione infiammabili e sistema anti-incendio insufficiente
- Naturali
  - Edifici in prossimità di zone soggette ad inondazioni e/o altre calamità naturali
- Hardware/Software
  - Firmware non aggiornati e/o sistemi obsoleti
  - Software non aggiornato, mancanza di antivirus, errori di configurazione, applicazioni scritte in modo non corretto
- Umane
  - Furto di credenziali
  - Procedure definite in modo insufficiente o non rispettate

ANALISI DEL RISCHIO (CONT.)

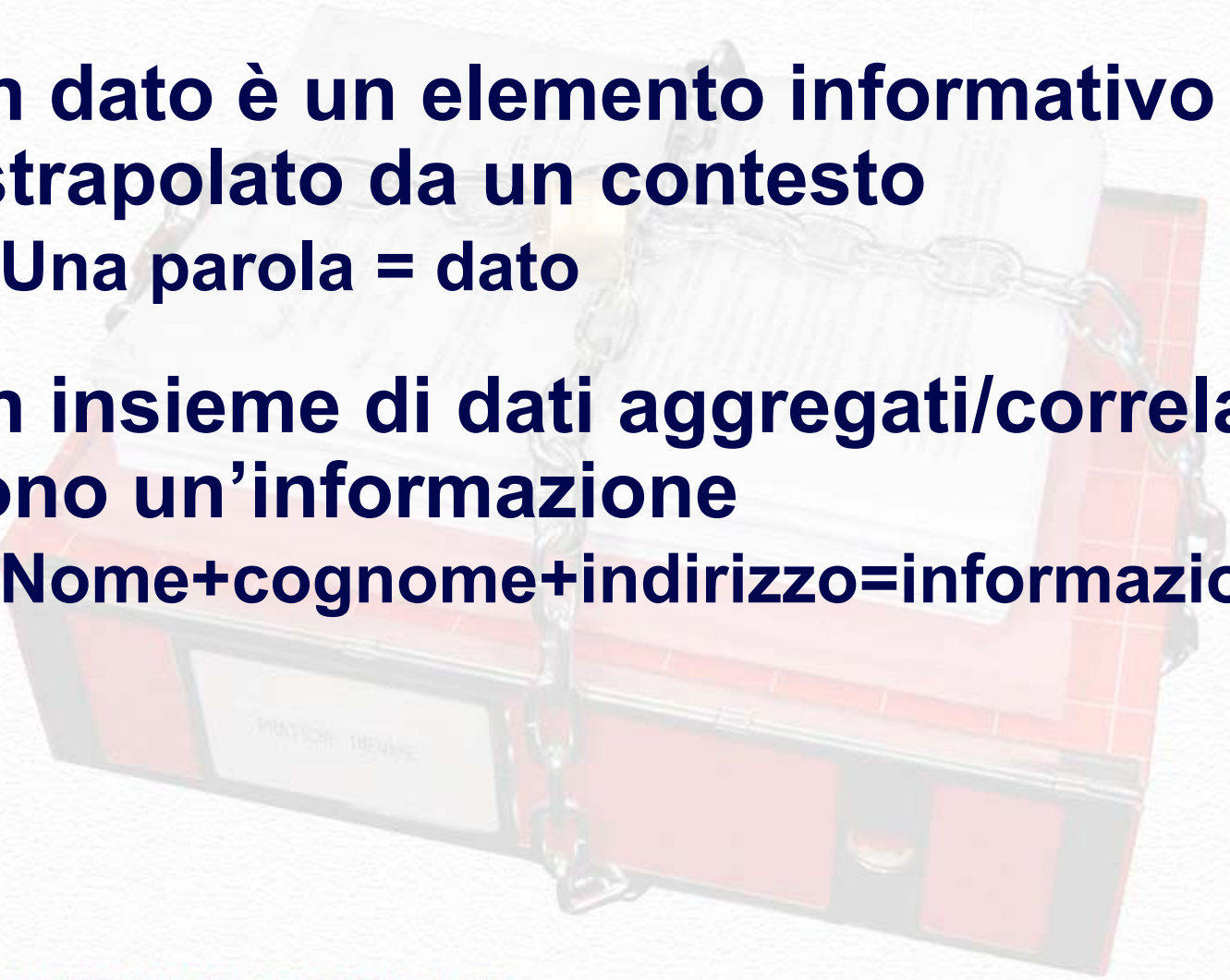
- Obiettivo del Codice
  - Art 1. garantire “il rispetto dei diritti e delle libertà fondamentali ... e al diritto alla protezione dei dati personali”
- La legge considera i rischi che potrebbero ledere tali diritti (art. 31)
  - Distruzione o perdita anche accidentale dei dati
  - Accesso non autorizzato
  - Trattamento non consentito o non conforme alle finalità della raccolta

SCENARIO NORMATIVO

- D. Lgs. 231/2001 - in materia di responsabilità amministrativa
- D. Lgs. 518/92. D. Lgs. 70/2003, L. 128/2004 'Decreto Urbani' - in materia di diritto d'autore
- D. Lgs. 196/2003 - misure per la tutela dei dati personali
  - Impone esplicitamente di documentare un'analisi dei rischi con il DPS

DATO E INFORMAZIONE

- Un dato è un elemento informativo estrapolato da un contesto
  - Una parola = dato
- Un insieme di dati aggregati/correlati sono un'informazione
  - Nome+cognome+indirizzo=informazione



DATO E INFORMAZIONE

- **DIGITALI**
  I dati trattati attraverso sistemi informatici e mantenuti su supporti digitali (dischi magnetici, ottici, etc)

- **CARTACEI**
  I dati contenuti/espressi su carta e/o altro supporto diverso dal digitale (microfilm, pellicola fotografica, etc.)

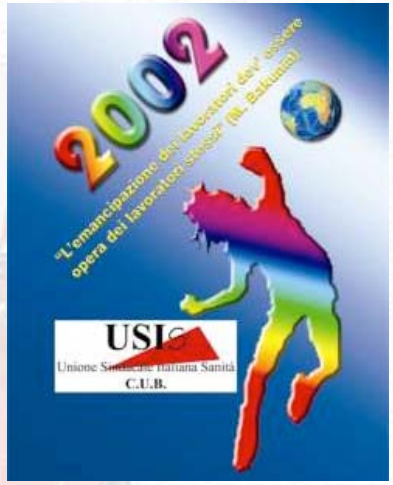
- **In entrambi i casi sono "documenti" che necessitano di cure e di attenzioni**

TIPOLOGIA DI DATI (D. LGS. 196/2003)

- **DATI PERSONALI**
  - Art 4 Definizioni (…)
  - b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
  - c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

TIPOLOGIA DI DATI (D. LGS. 196/2003)

- **DATI SENSIBILI E GIUDIZIARI**
  - Art 4 Definizioni (…)
  - d) “dati sensibili”, i dati personali idonei a rivelare l'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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
  - e) “dati giudiziari”, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;



MODALITÀ DI TRATTAMENTO

1. I dati personali oggetto di trattamento sono:
   a. trattati in modo lecito e secondo correttezza;
   b. raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   c. esatti e, se necessario, aggiornati;
   d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

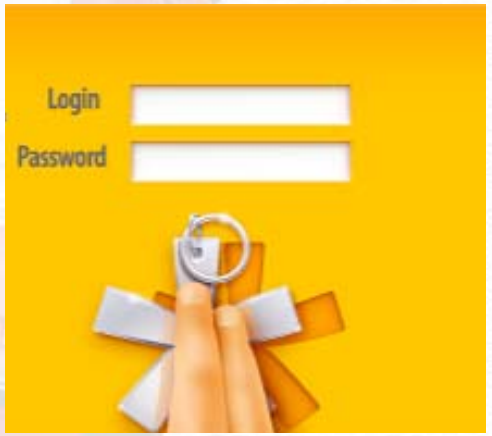
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati

MISURE DI SICUREZZA (D. LGS. 196/2003)

- **Art. 31. Obblighi di sicurezza**
  1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

MISURE DI SICUREZZA (D. LGS. 196/2003)

- **Art. 33 Misure minime**
  - 1. ..., adottare le misure minime ....., volte ad assicurare un livello minimo di protezione dei dati personali
- **Art. 34. Trattamenti con strumenti elettronici**
  - 1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
    a) autenticazione informatica;
    b) adozione di procedure di gestione delle credenziali di autenticazione;
    c) utilizzazione di un sistema di autorizzazione;



MISURE DI SICUREZZA (D. LGS. 196/2003)

- **Art. 34. - continuo**

  d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

  e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

  f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

  g) tenuta di un aggiornato documento programmatico sulla sicurezza;

  h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

MISURE DI SICUREZZA (D. LGS. 196/2003)

- **Art. 35 - Trattamenti senza l'ausilio di strumenti elettronici**
  1. **Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:**
     - **(…)**
     - **b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti**
     - **c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.**

ALLEGATO B

- **Trattamenti con strumenti elettronici**
  - **Sistema di autenticazione informatica**
    1. **Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti; ... (2 -11)**
  - **Sistema di autorizzazione**
    12. **Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione; ... (13-14)**
  - **Altre misure di sicurezza**
    16. **I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di ...**

DPS
DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

- **Cosa è il DPS?**
  - E' un documento scritto che traccia gli interventi che si prevede di adottare nell'anno in merito alla sicurezza nel trattamento dei dati personali
- **A cosa serve?**
  - A capire come funziona il nostro sistema di trattamento dei dati personali
    - Strumenti, sistemi di accesso, programmi, locali, etc
    - Quali trattamenti vengono effettuati
    - Quali sono le misure di sicurezza veramente adottate
    - Se sono conformi ai requisiti della legge
- **Come si redige?**
  - Esiste una "Guida operativa per redigere il DPS" pubblicata dal Garante

DPS
DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

- **Cosa contiene?**
  - **Sulla base del punto 19 del disciplinare tecnico in materia di misure minime di sicurezza (all. B al Dlgs. 196/2003) contiene idonee informazioni riguardo:**

    19.1 Elenco dei trattamenti di dati personali
    19.2 Distribuzione dei compiti e delle responsabilità
    19.3 Analisi dei rischi che incombono sui dati
    19.4 Misure in essere e da adottare
    19.5 Criteri e modalità di ripristino della disponibilità dei dati
    19.6 Pianificazione degli interventi formativi previsti
    19.7 Trattamenti affidati all'esterno
    19.8 Cifratura dei dati o separazione dei dati identificativi
      - **Dati idonei a rilevare lo stato di salute e la vita sessuale trattati da organismi sanitari ed esercenti le professioni sanitarie**

DPS
DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

- Chi è obbligato a farlo?
  - Il DPS è obbligatorio per tutti coloro che trattano dati personali con l'impiego di elaboratori elettronici (art.34 lett. g) (senza distinzione di tipologia)
- Chi lo deve compilare?
  - Il titolare del trattamento anche attraverso il Responsabile (se designato)
- Quando deve essere fatto?
  - Entro il 31 marzo (data prevista a regime) a partire dal 2005
  - Periodicità: 1 anno
- Cosa si rischia?
  - L'omessa adozione di misure indispensabili ("minime") costituisce reato che prevede l'arresto sino a 2 anni o l'ammenda da 10 mila a 50 mila euro

ALLEGATO B

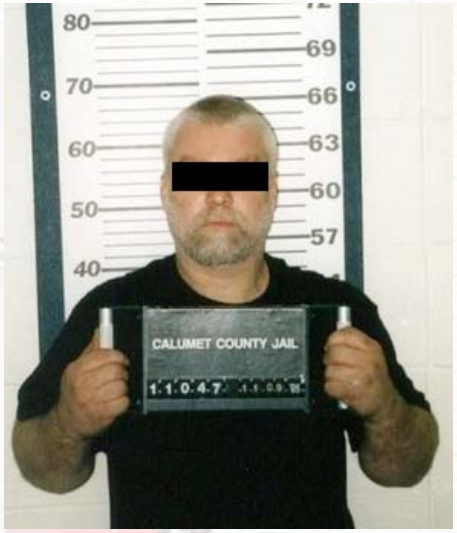
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

- **Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

  20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici

  21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti

  22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili

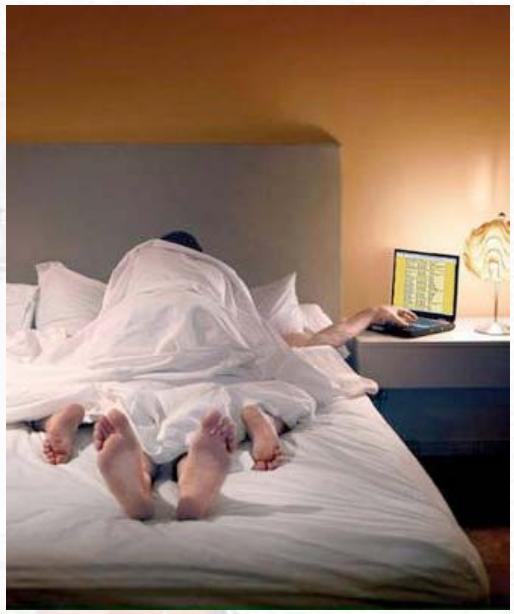


ALLEGATO B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato



ALLEGATO B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

- **Trattamenti senza l'ausilio di strumenti elettronici**

  27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali...

  28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento ..., i medesimi atti e documenti sono controllati e custoditi ... in maniera che ad essi non accedano persone prive di autorizzazione, ...

  29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate

SISTEMA DI GESTIONE DELLA SICUREZZA

- Politica della sicurezza
- Analisi e gestione dei rischi
- Sicurezza fisica ed ambientale
- Gestione della continuità operativa
  - Capacità di reazione ad interruzioni operative, disastri ed incidenti rilevanti
- Controllo degli accessi alle informazioni
- Selezione & formazione del personale
- Sviluppo e manutenzione delle applicazioni
- Conformità alle leggi e a regolamenti pertinenti

CONCLUSIONI

- **Formazione e Cultura: possono contribuire a trasformare la sicurezza da costo ad investimento**
  - **Educare gli utenti all'adozione di misure di sicurezza**
    - **Comprendere le vulnerabilità, i pericoli, i rischi che si corrono utilizzando servizi in rete e le possibili soluzioni**
    - **Proteggere, conservare ed accrescere il patrimonio informativo aziendale**
  - **Formare nuove figure professionali di addetti alle misure di sicurezza**
    - **Raggiungere e garantire adeguati assetti di sicurezza logica, fisica e organizzativa**
    - **Prevenire maggiormente gli abusi, le frodi e gli incidenti ai danni dei sistemi informativi o fatti attraverso i sistemi informatici**
    - **Proteggere, conservare ed accrescere la qualità del patrimonio informativo aziendale**