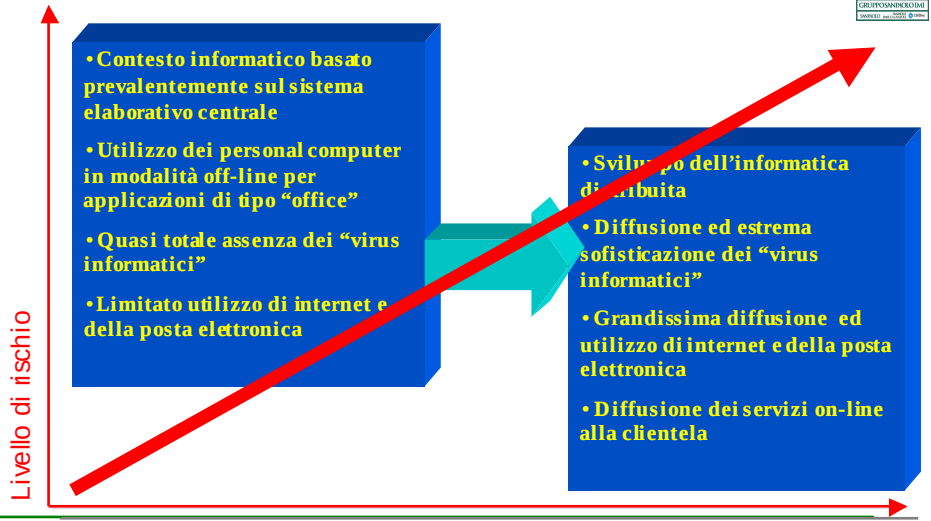

# LA CERTIFICAZIONE BS7799 UN ANNO DOPO

**Milano, 11 febbraio 2004**

*Gian Paolo Vella*

# LA CERTIFICAZIONE BS 7799 RAPPRESENTA L'ULTIMO PASSO DEL PROCESSO AZIENDALE DI EVOLUZIONE DELLA SICUREZZA INFORMATICA


Evoluzione del contesto tecnologico
Evoluzione del contesto normativo e legislativo
NUOVA VISIONE DELLA SICUREZZA


Livello di rischio
• Contesto informatico basato prevalentemente sul sistema elaborativo centrale
• Utilizzo dei personal computer in modalità off-line per applicazioni di tipo "office"
• Quasi totale assenza dei "virus informatici"
• Limitato utilizzo di internet e della posta elettronica
• Sviluppo dell'informatica distribuita
• Diffusione ed estrema sofisticazione dei "virus informatici"
• Grandissima diffusione ed utilizzo di internet e della posta elettronica
• Diffusione dei servizi on-line alla clientela

Legge 15 marzo 1997, n. 59

**"Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"**

Pubblicata nella *Gazzetta Ufficiale* n. 63 del 17 marzo 1997

Art. 15.

1…….

2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. ……

- Decreto Legge n.518 (Tutela giuridica dei programmi per elaboratore
- Legge 547 (Modifiche al Codice di Procedura Civile in tema di criminalità informatica)
- (Legge 675)
- (DPR 318)
- Decreto Legislativo 30 giugno 2003, n. 196 (Codice in Materia di Protezione dei Dati Personali)

# DECRETO LEGISLATIVO 30 giugno 2003, n. 196
# CODICE
# IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

## Titolo V
## SICUREZZA DEI DATI E DEI SISTEMI

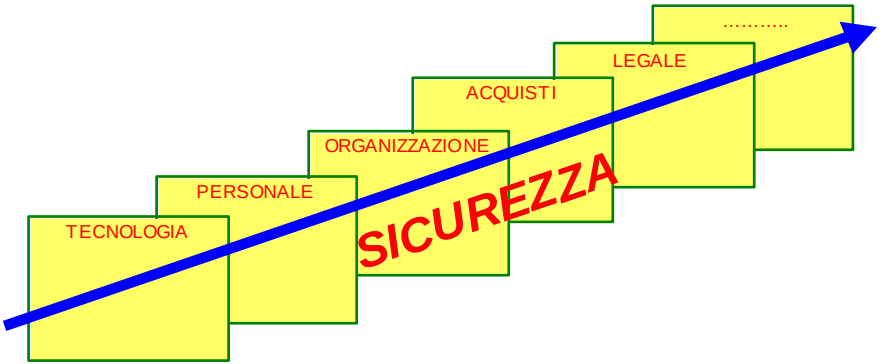
### CAPO I
### MISURE DI SICUREZZA

### 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.

Da insieme di sistemi, strumenti, meccanismi di natura tecnologica…

… a **P**rocesso aziendale continuativo e trasversale

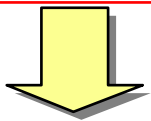


- Adozione dello standard BS7799 come framework di riferimento per realizzare un Integrated Security Management System

- Attivazione dei meccanismi organizzativi per coinvolgere la Direzione e le funzioni aziendali (Comitato di Sicurezza, Security Forum)

- Attivazione del presidio specifico degli aspetti non operativi della sicurezza

L'esigenza di offrire alla clientela servizi di sicurezza, di avere una garanzia circa la bontà delle scelte in caso di contenzioso, di avere una forma di tutela circa le scelte di sicurezza di fronte agli obblighi di legge portano…



… alla necessità di una validazione formale della sicurezza aziendale attraverso un processo di certificazione ufficialmente riconosciuto

In considerazione della complessità della materia e del livello di esperienza interno, l'attività di Certificazione secondo lo standard BS779 della sicurezza aziendale è stata affrontata per step partendo dal contesto di Internet Banking (Novembre 2002)

Attualmente è in corso l'attività di preparazione del secondo step: la certificazione della Certification Authority interna a supporto dei servizi di Firma Elettronica (Febbraio 2004).

Più che verificare la validità tecnica degli strumenti e dei meccanismi di sicurezza, l'attività di certificazione è volta a verificare:

- La condivisione delle scelte
- Il corretto presidio organizzativo e documentale di tutti i fenomeni (con particolare riferimento alla gestione degli incidenti)
- La diffusione della conoscenza e la sensibilizzazione sui temi della sicurezza

# Come possiamo sintetizzare i ritorni dell'adozione dello standard BS7799 in azienda?

- *La nuova situazione non ha, di fatto ed in maniera diretta, incrementato il livello di sicurezza aziendale nei suoi aspetti tecnologici/operativi*
- *Al contrario, essa ha dato un volto nuovo alla sicurezza; un volto formalmente riconosciuto e, soprattutto, condiviso da tutte le funzioni attraverso le nuove strutture organizzative, le nuove attività ed il nuovo livello di sensibilità diffuso a tutta l'azienda*
- *Questa impostazione ha consentito di coinvolgere, in modo importante, l'Alta Direzione*
- *Inoltre sono stati creati validi presupposti utilizzabili per altri importanti contesti (es. Basilea 2, Nuovo Testo Unico sulla Privacy)*