



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Il Piano Nazionale per la Sicurezza ICT nella PA

Franco Guida

*Fondazione Ugo Bordononi*

*Seminario di formazione e sensibilizzazione*

*dei Dirigenti Generali della Pubblica Amministrazione in materia di sicurezza ICT*



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Comitato Tecnico Nazionale sulla sicurezza ICT nelle PA (1)

- Previsto dalla Direttiva del 16 gennaio 2002 sulla sicurezza ICT nella PA, emanata dal Ministro per l'Innovazione e le Tecnologie, di intesa con il Ministro delle Comunicazioni
- Istituito il 24 luglio 2002 con decreto dei due suddetti Ministri
- Composto inizialmente da cinque membri poi portati a sette
  - 3 membri (tra cui il Presidente) nominati dal Min. delle Comunicazioni
  - 4 membri nominati dal Ministro per l'Innovazione e le Tecnologie
- Membri: C. Manganelli (Presidente), L. Angelone, F. Berghella, D. Bruschi, F. Guida, C. Sarzana di S. Ippolito, G. Tonelli
- Scadenza mandato: fine legislatura



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Comitato Tecnico Nazionale sulla sicurezza ICT nelle PA (2)

## COMPITI

- Formula proposte strategiche ai fini dello sviluppo:
  - del Piano Nazionale di sicurezza ICT per la PA, del quale verifica annualmente lo stato di avanzamento e individua le azioni correttive
  - del Modello Organizzativo di sicurezza ICT per la PA, del quale verifica l'attivazione e l'applicazione
  - della certificazione della sicurezza ICT nella PA
  - della formazione dei dipendenti pubblici in tema di sicurezza ICT



# Comitato Tecnico Nazionale sulla sicurezza ICT nelle PA

## Documenti di riferimento predisposti dal Comitato

1. *“Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione”* – Marzo 2004
2. *“Linee guida per la certificazione di sicurezza ICT nella Pubblica Amministrazione”* – Gennaio 2006



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione

MARZO 2004

Ministro per l'Innovazione e le Tecnologie

Ministro delle Comunicazioni



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Gruppo di lavoro per lo sviluppo del PN e del MO



- Istituito su iniziativa del CNIPA
- Coordinatore: C. Sarzana di S. Ippolito
- Membri del Comitato Tecnico Nazionale sulla sicurezza ICT nelle PA: D. Bruschi, F. Guida, G. Tonelli (oltre al Coordinatore)
- Membri del CNIPA: G. Manca, G. Moxedano, G. Pontevolpe, M. Pucciarelli, G. Rellini Lerz, M. Terranova
- Membri del Dip. per l'Innovazione Tecnologica: V. Merola
- Membri del Ministero delle Comunicazioni: L. Franchina, G. L. Petrillo



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Piano Nazionale e Modello Organizzativo

## Piano Nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione

- Stabilisce le azioni necessarie per attuare la sicurezza informatica

## Modello Organizzativo Nazionale di sicurezza ICT per la pubblica amministrazione

- Definisce i processi e le strutture con cui le azioni previste nel Piano Nazionale possono essere attuate

I due documenti saranno entro breve pubblicati dal CNIPA



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Piano Nazionale: struttura (1)

1. Premessa
2. Sintesi del Piano Nazionale
3. Guida alla lettura
4. Strategia nazionale di sicurezza ICT
5. Iniziative in corso
6. Ulteriori interventi per la sicurezza ICT
7. L'attuazione del piano nazionale
8. Conclusioni



# Piano Nazionale: struttura (2)

## Appendici

- A. Linee guida per la valutazione dei rischi
- B. Situazione internazionale della certificazione di sicurezza per i sistemi e prodotti ICT
- C. I contratti relativi alla sicurezza informatica
- D. La *business continuity*
- E. Le verifiche secondo *best practices*
- F. Bibliografia normativa
- G. Glossario



# Piano Nazionale: contenuti (1)

## STRATEGIA NAZIONALE DI SICUREZZA ICT

- Approccio che non si limita a considerare un'analisi in termini di costi/benefici per la PA
- L'analisi deve essere anche applicata, in termini non solo economici (es: tutela dei diritti e delle libertà del cittadino), all'intero sistema paese



# Piano Nazionale: contenuti (2)

## INIZIATIVE IN CORSO

- Adeguamento alla direttiva sulla sicurezza informatica
- L'Organismo per la certificazione della sicurezza (OCSI presso ISCOM-Ministero Comunicaz.)
- L'Unità di gestione degli incidenti (GovCERT.it presso CNIPA)
- L'Unità di formazione (presso ISCOM-Min.Comunic.)
- Le iniziative internazionali (in particolare ENISA – Agenzia europea per la sicurezza ICT)



Organismo di Certificazione della Sicurezza Informatica



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Piano Nazionale: contenuti (3)

## ULTERIORI INTERVENTI PER LA SICUREZZA ICT

- La cultura della sicurezza
- La protezione delle informazioni gestite dalle amministrazioni
- L'utilizzo delle certificazioni di sicurezza nelle PA
- Le infrastrutture di connessione condivise
- Il coordinamento nazionale della sicurezza ICT



# Piano Nazionale: contenuti (4)

## L'ATTUAZIONE DEL PIANO NAZIONALE

- Tempi e priorità
- Il processo di monitoraggio e verifica
- Gli audit di sicurezza
- La gestione del Piano Nazionale



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Modello Organizzativo: struttura (1)

1. Scopo e struttura del documento
2. Riferimenti al piano nazionale della sicurezza ICT
3. Il coordinamento nazionale della sicurezza ICT
4. L'Organizzazione di sicurezza delle amministrazioni
5. Le strutture per la certificazione della sicurezza ICT in Italia



# Modello Organizzativo: struttura (2)

## Appendici

- A. Indicazioni per la gestione della sicurezza ICT
- B. Indicazioni per la gestione degli incidenti informatici
- C. Indicazioni per l'*outsourcing*
- D. Gli aspetti etici della sicurezza informatica
- E. Esempi di procedure per la gestione della sicurezza
- F. I codici deontologici di riferimento
- G. Bibliografia normativa
- H. Glossario



# Modello Organizzativo: contenuti (1)

## L'ORGANIZZAZIONE DI SICUREZZA DELLE AMMINISTRAZIONI

- Logiche organizzative
- Ruoli e responsabilità
- Principali ruoli
- Unità locale di sicurezza SPC
- Gestione del personale
- Strutture operative
- I CERT-AM
- Strutture per l'emergenza
- Struttura di auditing
- Gli uffici e le responsabilità per la sicurezza



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Contenuti di particolare interesse per i dirigenti PA (1)

- **Analisi dei rischi** per le attività di propria competenza
  - Ordinamento delle attività in base alla criticità in termini di
    - possibili danni economici per per la PA e per la collettività
      - indisponibilità di servizi
      - impossibilità di beneficiare delle economie consentite dall'automatizzazione di processi e servizi a causa di
        - » scarsa affidabilità in termini di sicurezza ICT
        - » scarsa fiducia da parte del cittadino (nel caso di servizi offerti in forma telematica)
    - rispetto di norme di legge (ad es: norme a tutela del cittadino quali quelle sulla *Privacy*), con possibili riflessi in termini di responsabilità individuali



# Contenuti di particolare interesse per i dirigenti PA (2)

- **Gestione dei rischi** per le attività di propria competenza
  - Utilizzazione di un sistema di gestione della sicurezza affidabile (preferibilmente certificato) che rispecchi le indicazioni del PN e del MO e che preveda tra l'altro
    - l'utilizzazione, per quanto possibile, di risorse umane interne all'amministrazione, soprattutto per i delicati ruoli di gestione della sicurezza  
⇒ Formazione
    - il ricorso oculato all'*outsourcing*, secondo le indicazioni fornite nel Piano Nazionale e nel Modello Organizzativo, con l'obiettivo di ridurre progressivamente tale ricorso man mano che la Formazione produce i suoi benefici
  - Acquisizione di sistemi ICT che offrano adeguate garanzie di sicurezza, preferibilmente nella forma di una vera e propria certificazione



# Contenuti di particolare interesse per i dirigenti PA (3)

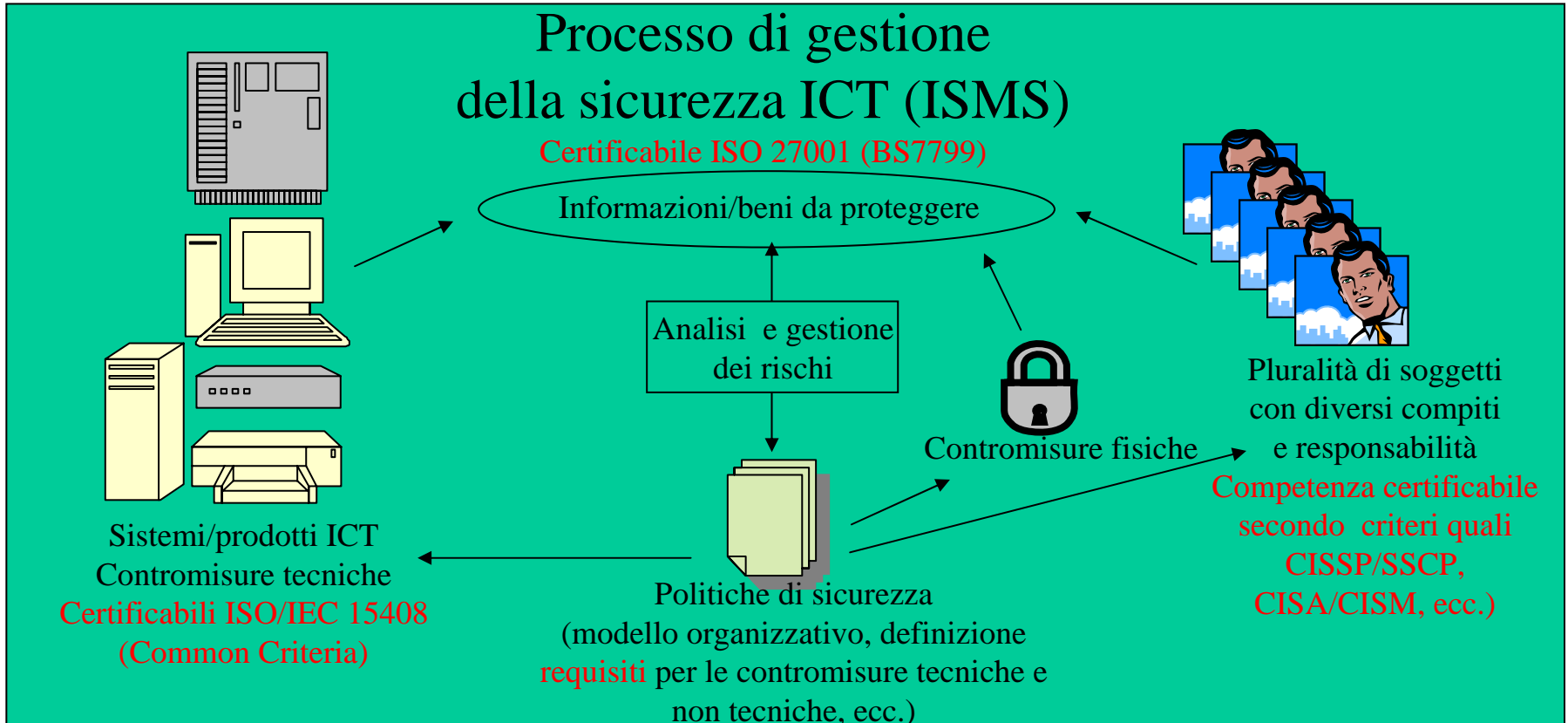
## ACQUISIZIONE DI SISTEMI ICT AFFIDABILI

- Individuazione ed esplicitazione dei requisiti di sicurezza, almeno in termini di obiettivi, se non di funzionalità di sicurezza richieste (in quest'ultimo caso, possibilmente secondo la forma di univoca interpretazione prevista dallo standard ISO 15408)
- Certificazione di sicurezza preferenziale o obbligatoria dipendentemente dalla criticità del sistema ICT da acquisire



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# La sicurezza ICT in un'Organizzazione





Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

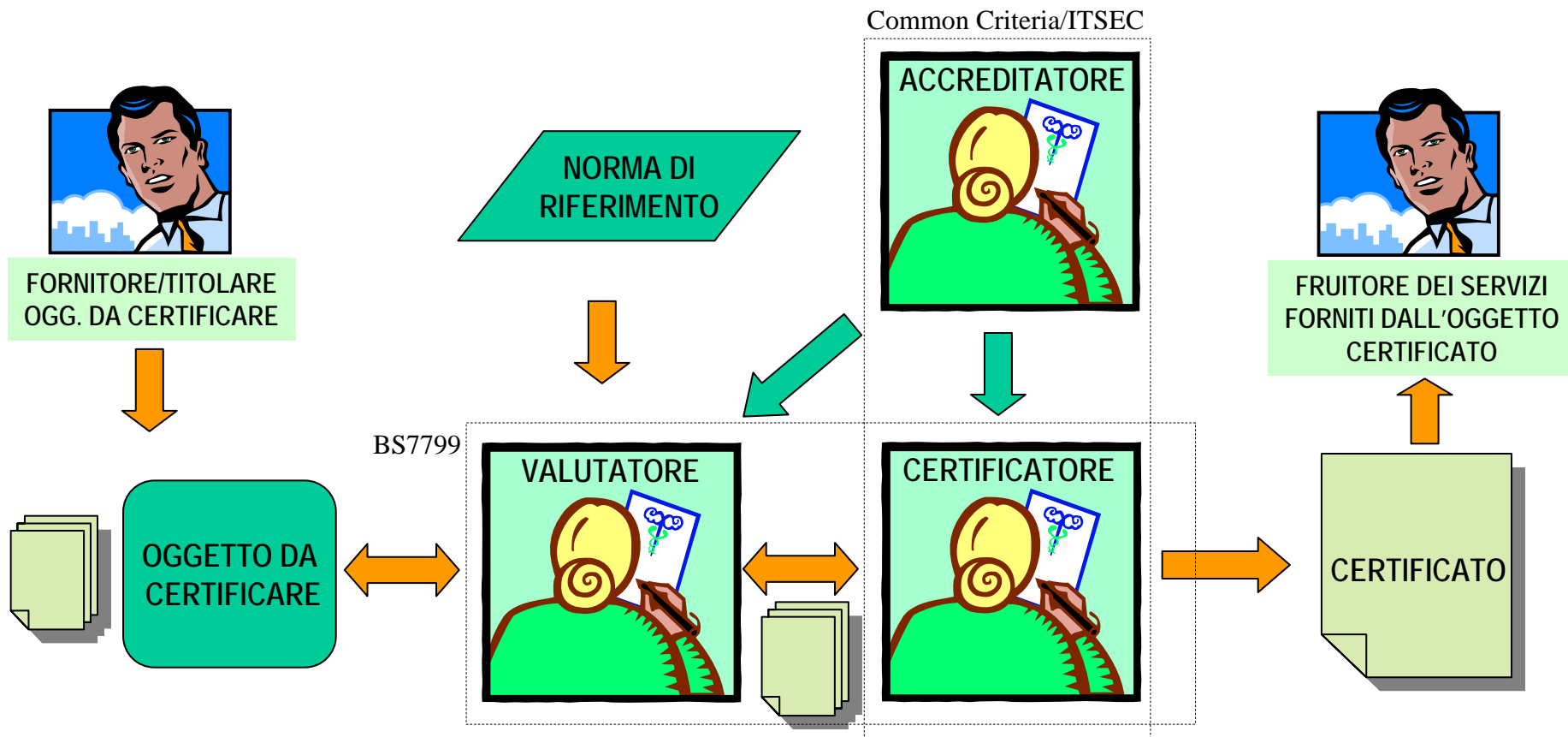
# Tipi di certificazione

Oggetto certificato	Norme di riferimento
Processo di gestione della sicurezza ICT (ISMS)	ISO/IEC IS 27001 (BS7799:2)
Sistema/prodotto ICT	<i>Common Criteria</i> (ISO/IEC IS15408) ITSEC
Competenza del personale	CISSP/SSCP, CISA/CISM, ecc.



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Le entità in gioco





# Le certificazioni in Italia regolate da DPCM

- Certificazione di prodotto/sistema ICT
  - Schema Nazionale del 1995 aggiornato nel 2002 (DPCM 11 aprile 2002 – GU n. 131 del 6 giugno 2002) applicabile nel contesto della sicurezza interna e esterna dello Stato
    - Ente di Certificazione/Accreditamento (EC): ANS/UCSi
      - Centri di Valutazione (Ce.Va.): 3 privati, 2 pubblici (tra cui ISCOM)
  - Schema Nazionale del 2003 (DPCM 30 ottobre 2003 – GU n. 98 del 27 aprile 2004) applicabile in tutti i contesti non coperti dal primo Schema
    - Organismo di Certificazione/Accreditamento (OCSI): ISCOM (Ministero Comunicazioni) che si avvale del supporto della Fondazione Ugo Bordoni
      - Laboratori di Valutazione (LVS) accreditati dall'OCSI



Comitato tecnico nazionale  
sulla sicurezza informatica e  
delle telecomunicazioni nelle  
pubbliche amministrazioni

# Certificazione della sicurezza di sistemi e prodotti ICT



Organismo di Certificazione della Sicurezza Informatica

[www.ocsi.gov.it](http://www.ocsi.gov.it)

- Può essere eseguita con costi e tempi contenuti se ci si attiene alle indicazioni fornite nel citato documento del Comitato e nel Piano Nazionale
- Ulteriori indicazioni che facilitano le certificazioni nella PA è previsto siano fornite da OCSI e CNIPA nell'ambito di una collaborazione che dovrebbe essere avviata entro breve



# Conclusioni

- E' fondamentale che i dirigenti della PA si convincano dell'assoluta necessità di proteggere informazioni e servizi in modo proporzionato alla loro criticità
- Con una gestione corretta della sicurezza gli investimenti fatti vengono ampiamente ripagati
  - dalla riduzione dei danni derivanti da incidenti informatici
  - dalla realizzazione di economie, di entità anche notevole, nell'ambito della PA e/o dell'intero paese
  - dall'adeguata tutela dei diritti del cittadino