

# **La sicurezza ICT nella pubblica amministrazione**

**Ing. Gianfranco Pontevolpe**  
**Responsabile Ufficio Tecnologie per la sicurezza**

Centro Nazionale per l'Informatica nella Pubblica Amministrazione



# Il questionario sulla sicurezza informatica

---

- Il CNIPA ha svolto un'indagine presso le amministrazioni centrali tramite un questionario formato da 53 quesiti sulla sicurezza dei CED
- Il questionario mirava a valorizzare i seguenti indicatori
  - Protezione logica
  - Sicurezza dell'infrastruttura
  - Sicurezza dei servizi
  - Organizzazione per la sicurezza



# I risultati

---

- Protezione logica (policy, certificazione, autenticazione ...) : **valori medio-bassi**
- Sicurezza delle infrastrutture (isolamento rete, firewall, IDS ...): **valori medi**
- Sicurezza dei servizi (mail server, web server, antivirus ...): **valori medio alti**
- Organizzazione per la sicurezza (definizione dei ruoli, outsourcing ...): **valori bassi**



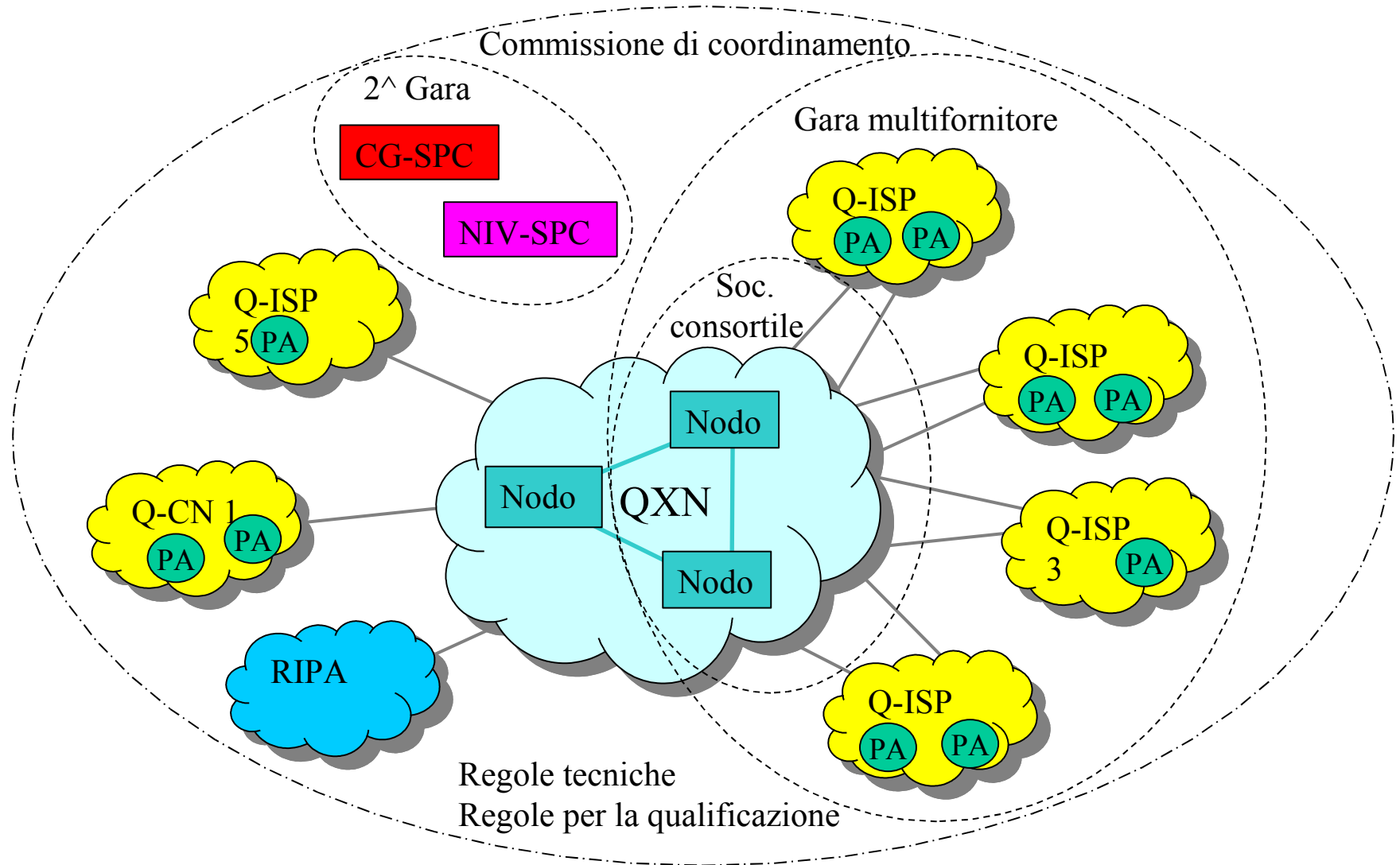
# Le iniziative

---

- Primi interventi promossi dal Comitato tecnico nazionale
  - Formazione
  - GovCert
- Sistema Pubblico di Connettività
- Centro di competenza sulla continuità operativa
- Piano nazionale e modello organizzativo



# Il Sistema Pubblico di Connettività





# I servizi di sicurezza SPC

---

- Gestione firewall
- Gestione antivirus & content filtering
- Network Intrusion Detection
- Event & log management
- Gestione VPN
- Hardening dei sistemi
- Gestione NAT
- Host Intrusion Detection System
- Vulnerability assessment;
- Manutenzione e assistenza (SOC, Call Center, fault man., conf & change man.; rendicontazione, supporto sistemistico, consulenza e formazione)



# Il quaderno n. 23 del CNIPA

---

- Linee guida per la sicurezza ICT delle pubbliche amministrazioni
  - Piano Nazionale della sicurezza delle tecnologie dell'informazione e comunicazione per la pubblica amministrazione
  - Modello organizzativo nazionale di sicurezza ICT per la PA
- Ai lavori hanno partecipato
  - Esperti del CNIPA
  - Componenti del Comitato Tecnico Nazionale
  - Esponenti del Ministero delle Comunicazioni



# I contenuti del Piano e del Modello

---

- Il **Piano Nazionale** indica le strategie e le iniziative di livello nazionale per la sicurezza delle informazioni
- Il **Modello Organizzativo** Delinea l'organizzazione con cui il comparto pubblico dovrà attuare il piano nazionale per la sicurezza



# Gli obiettivi del piano

---

- Tutelare i cittadini nei confronti di problemi che possono derivare da carenza di sicurezza nei processi istituzionali
- Abilitare lo sviluppo della società dell'informazione promuovendo o stimolando la fiducia nel mezzo informatico
- Migliorare l'efficienza del sistema paese, anche riducendo i costi derivanti da carenze nel campo della sicurezza informatica



# Documenti di riferimento per lo sviluppo del piano e del modello

---

- Direttiva 16/1/02 “sicurezza delle telecomunicazioni nelle pubbliche amministrazioni centrali”
- Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione del Comitato tecnico nazionale
- Risultati dei gruppi di lavoro per la realizzazione del Sistema Pubblico di Connettività



# Iniziative in corso

---

- Adeguamento alla direttiva sulla sicurezza informatica
- Diffusione degli strumenti di firma ed accesso ai servizi in rete (firma elettronica, CIE, CNS)
- Organismo per la certificazione della sicurezza
- Unità di gestione degli incidenti
- Unità di formazione



# Ulteriori iniziative: le protezioni

---

- Misure minime del DL 196/2003 per tutti i trattamenti di dati;
- Predisposizione delle applicazioni all'utilizzo di CIE e CNS;
- Classificazione dei dati
- Protezione messaggi scambiati via Internet



# Ulteriori iniziative: l'assetto organizzativo

---

- CERT-AM
- Sistema Pubblico di Connettività
- Misure organizzative
  - assegnazione dei compiti con modalità dipendenti dalla struttura e dimensione dell'ente;
  - figura referente per i problemi di sicurezza;
- Clausole per la sicurezza nei contratti di natura informatica



# Ulteriori iniziative: sensibilizzazione e coordinamento

---

- Sicurezza informatica nei percorsi educativi scolastici
- Campagne informative
- Centro nazionale di sicurezza ICT
  - coordinamento delle politiche di sicurezza delle amministrazioni
  - raccordo delle iniziative del settore pubblico e privato
  - raccolta delle segnalazioni
  - statistiche ed indicazioni sui profili e livelli di rischio



# Le priorità

---

1. Rete per lo scambio delle informazioni sulla sicurezza ICT
2. Avvio del processo di adeguamento delle organizzazioni
3. Sicurezza nei contratti
4. Predisposizione dei servizi all'uso della CIE e della CNS



# Il Modello organizzativo

---

- Compiti e responsabilità per il coordinamento nazionale
- Criteri per adeguare l'organizzazione delle amministrazioni
- Processi organizzativi che dovranno essere messi in atto



# Criteri seguiti nella definizione del modello

---

- Continuità con le organizzazioni e le iniziative esistenti
- Organizzazione della sicurezza di tipo federato
- Modularità e scalabilità delle soluzioni organizzative
- Esempi e modelli come best practices



# I ruoli nel coordinamento nazionale della sicurezza

---

- **ISCOM** ⇒ sicurezza delle comunicazioni e certificazione
- **Commissione di Coordinamento del SPC** ⇒ strategie di sicurezza delle amministrazioni centrali e locali
- **CNIPA** ⇒ verifica ed indirizzo dei progetti ICT delle amministrazioni centrali
- **CNSI** ⇒ coordinamento, monitoraggio, prevenzione, collaborazione internazionale



# La cooperazione tra organizzazioni centrali e locali

---

- Basata sul modello organizzativo del SPC (approvato dal tavolo tecnico permanente della Conferenza Unificata Stato Regioni, Città e Autonomie locali)
- Sicurezza dei processi trasversali attraverso l'organizzazione in domini di cooperazione



# Organizzazione della sicurezza nelle amministrazioni

	ammin. complesse presenti su più sedi su territorio nazionale	grosse ammin.. presenti su più sedi in una stessa città	grosse ammin.. presenti in una sola sede	ammin. di media complessità	piccole ammin.
Ministro, Direttore, Sindaco ...	✓	✓	✓	✓	✓
Consigliere tecnico per la sic. ICT	✓			✓	
Comitato per la sicurezza ICT	✓	✓	✓	✓	
Responsabile della sicurezza ICT	✓	✓	✓		✓
Comitato tecnico	✓	✓			
Ufficio di sicurezza centrale	✓		✓	✓	
Referente locale della sicurezza	✓	✓			
Gruppi di lavoro specifici	✓	✓	✓		
Strutture per l'emergenza	✓	✓	✓	✓	



# Temi trattati nelle appendici

---

- Valutazione dei rischi
- Stato della certificazione di sicurezza in altre nazioni
- Sicurezza ICT nei contratti
- Business continuity
- Verifiche secondo best practice



## ... temi trattati nelle appendici

---

- Modello operativo per la gestione della sicurezza informatica
- La gestione degli incidenti informatici
- *Outsourcing* dei servizi di sicurezza ICT
- Aspetti etici
- Esempi di procedure
- Codici deontologici di riferimento



---

Per maggiori informazioni

**[www.cnipa.gov.it](http://www.cnipa.gov.it)**