DigitPA

Stato dell'arte della sicurezza SPC

Mario Terranova
Responsabile Ufficio Sicurezza delle infrastrutture e dei centri di servizio
Area Infrastrutture e centri di servizio
DigitPA
terranova@digitpa.gov.it

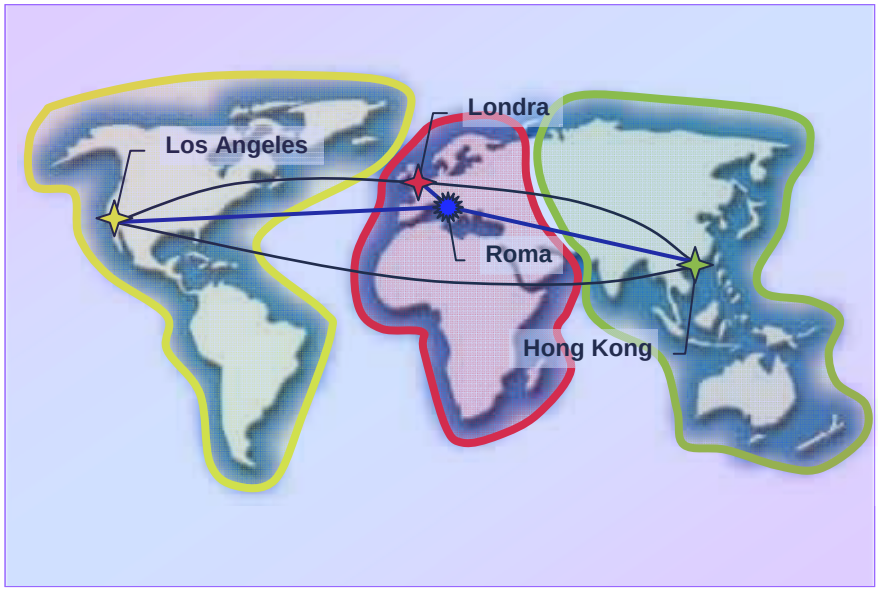
DigitPA

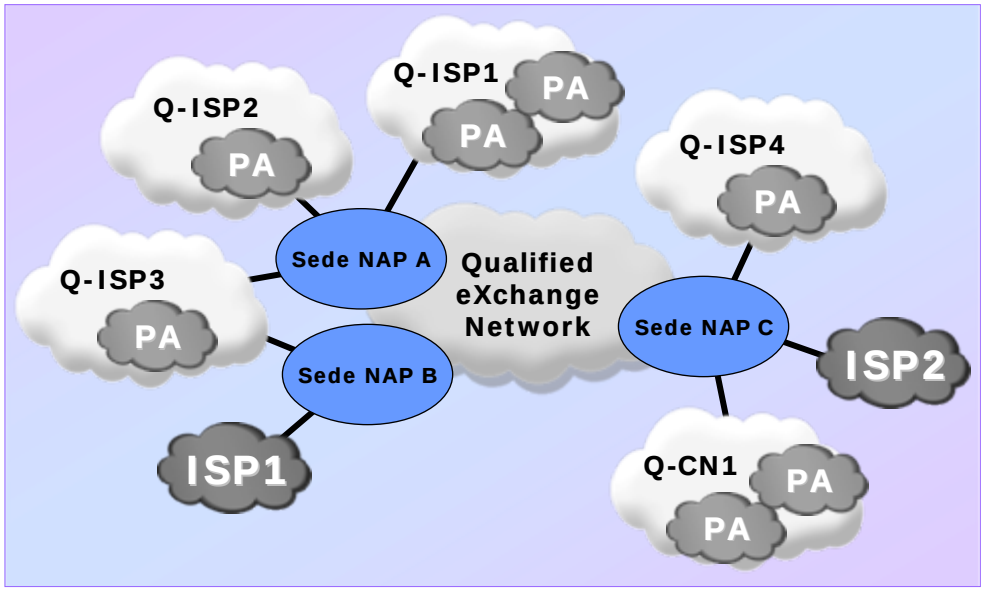
Sommario

- Il Sistema Pubblico di Connettività
- Organizzazione per la sicurezza
- Il modello di sicurezza SPC
- Compliance SPC

Le reti della PA

Reti progettate per garantire qualità di servizio e sicurezza, in grado di accomodare comunicazioni di sempre maggiore criticità.

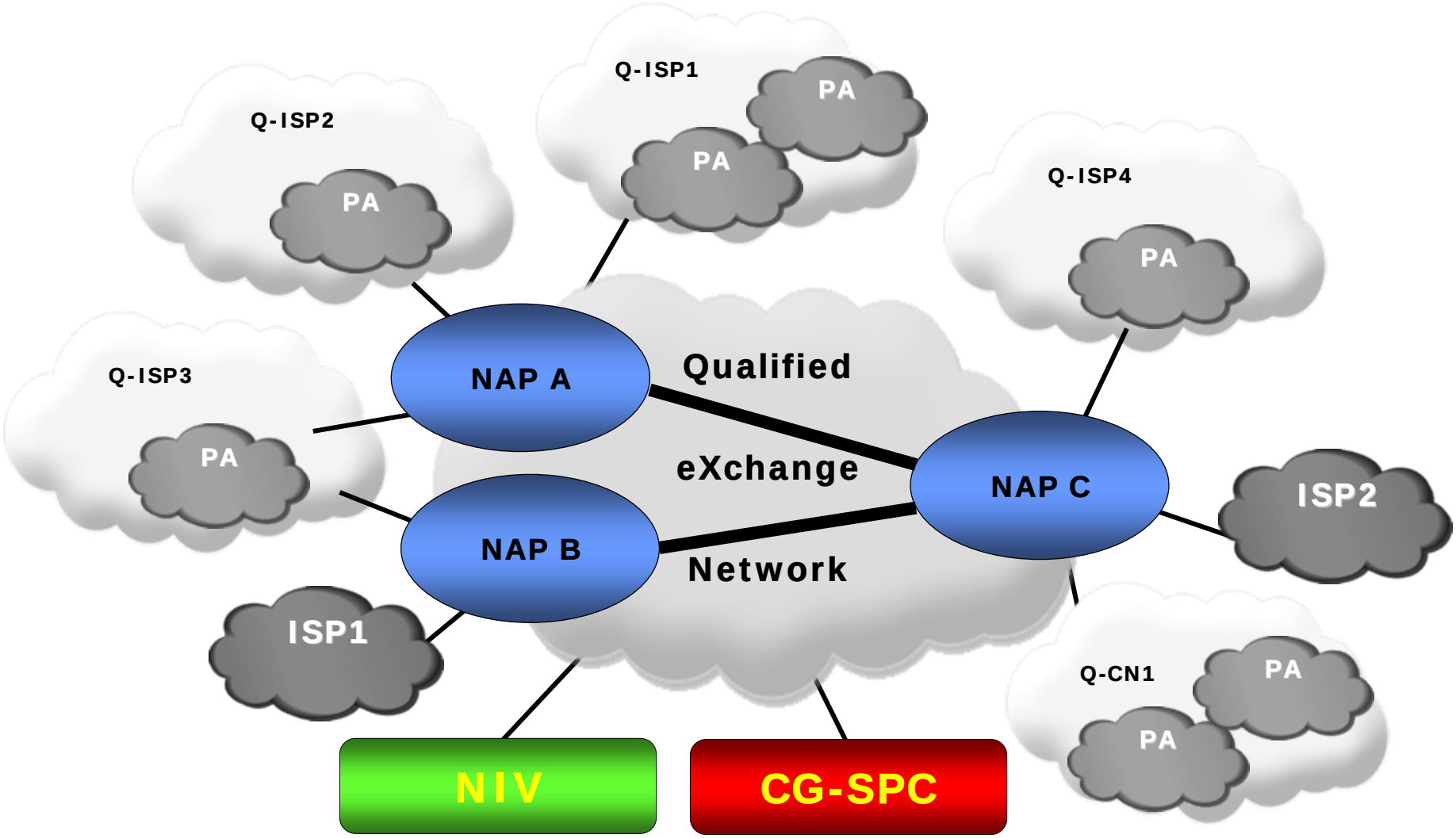




RIPA **SPC**

DigitPA

SPC = Trusted Internet



DigitPA

Servizi sicuri

- Requisiti di sicurezza di base
  - Locali
  - AAA amministratori
  - Backup
  - Analisi sistematica del rischio e delle vulnerabilità
- Opzioni di sicurezza
  - IPSec e SSL
  - Antivirus e antispam

DigitPA

Servizi di sicurezza

- Gestione VPN
- Gestione firewall e NAT
- Gestione filtraggio dei contenuti
- Gestione sistemi antintrusione
- Monitoraggio eventi
- Hardening sistemi
- Verifica vulnerabilità
- Manutenzione ed assistenza

DigitPA

Compiti del CG-SPC

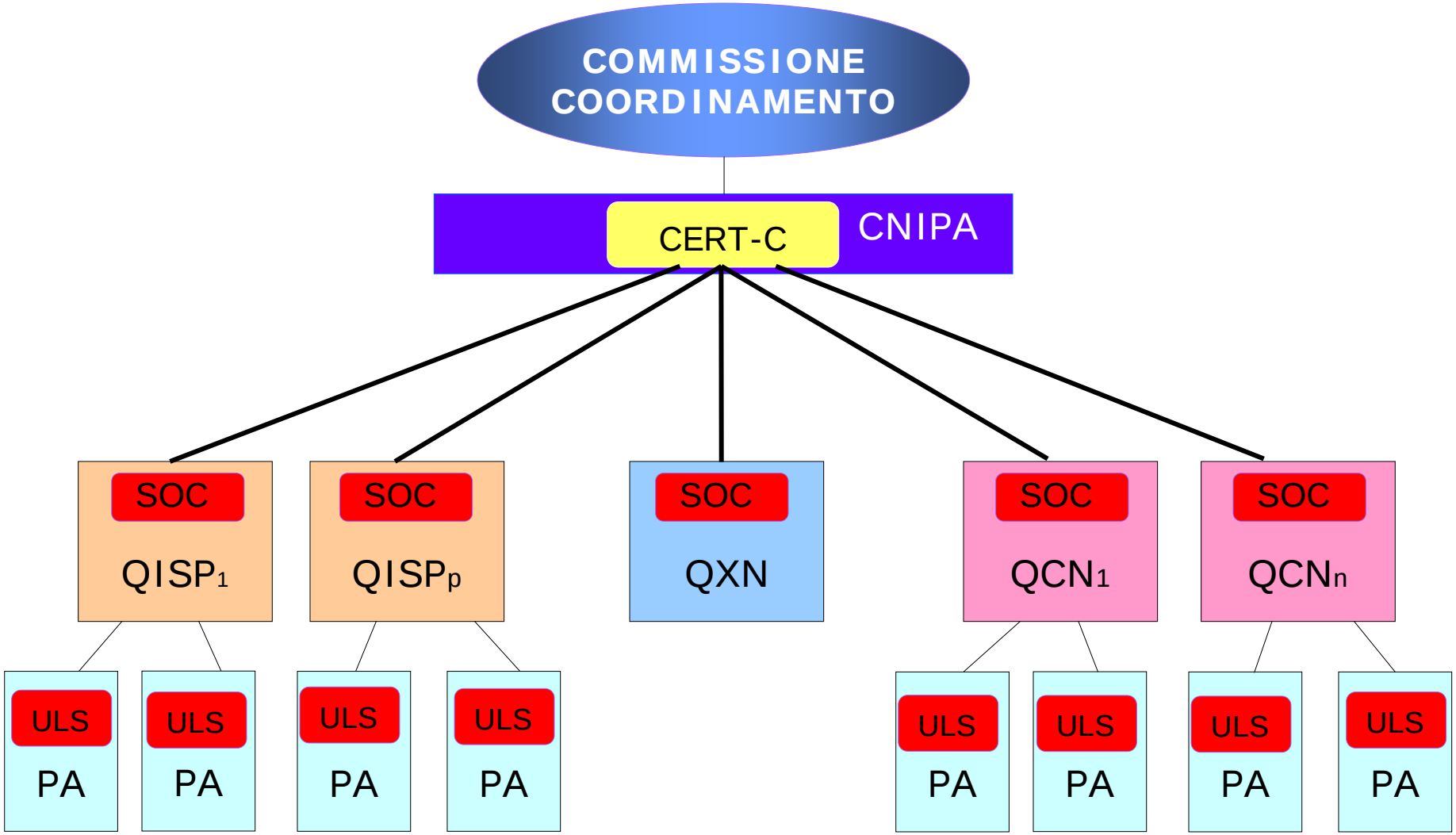
- Misure indirette: ricalcolo degli SLA a partire dai dati elementari provenienti dai soggetti monitorati.
- Misure dirette della qualità dei servizi erogati dai soggetti monitorati.
- Sicurezza: coordinamento operativo dei soggetti monitorati nella risposta alle minacce e gestione della PKI-SPC
- Formazione su temi legati al SPC.

DigitPA

Sommario

- Il Sistema Pubblico di Connettività
- Organizzazione per la sicurezza
- Il modello di sicurezza SPC
- Compliance SPC

Organizzazione sicurezza SPC



DigitPA

Funzioni delle ULS

- Sono responsabili della sicurezza della struttura di appartenenza.
- Garantiscono il mantenimento del livello minimo di sicurezza della rete.
- Gestiscono i flussi informativi da e verso le altre strutture del sistema di sicurezza.
- Gestiscono gli eventi di sicurezza in sinergia con le altre strutture.

Funzioni del CNIPA

CODICE DELL'AMMINISTRAZIONE DIGITALE ART. 81

Il CNIPA, nel rispetto delle decisioni e degli indirizzi forniti dalla Commissione, anche avvalendosi di soggetti terzi, gestisce le risorse condivise del SPC e le strutture operative preposte al controllo e supervisione delle stesse, per tutte le pubbliche amministrazioni di cui all'articolo 2, comma 2. Il CNIPA, anche avvalendosi di soggetti terzi, cura la progettazione, la realizzazione, la gestione e l'evoluzione del SPC per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39.

Il CERT-SPC-C

Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività

CERT-SPC-C (Computer Emergency Response Team del Sistema Pubblico di Connettività Centrale), la struttura collocata presso il CNIPA che è referente centrale per la prevenzione, il monitoraggio, la gestione, la raccolta dati e l'analisi degli incidenti di sicurezza, assicurando l'applicazione di metodologie per la gestione degli incidenti coerenti ed uniformi in tutto il sistema da essa controllato per la gestione degli incidenti.

DigitPA

Sommario

- Il Sistema Pubblico di Connettività
- Organizzazione per la sicurezza
- Il modello di sicurezza SPC
- Compliance SPC

Modello sicurezza SPC

DigitPA

Sommario

- Il Sistema Pubblico di Connettività
- Organizzazione per la sicurezza
- Il modello di sicurezza SPC
- Compliance SPC

Nessuna catena è più forte…

- SOC operativo H24x7
- MSS certificati
- Responsabilità nei confronti del sistema

Servizi obbligatori

- Porta rete insicura (Internet)
  - ELM
  - FW
  - NIS
- Porta rete sicura (Infranet)
  - ELM

Il modello CED centrico

- Concentra in un unico PAS gli ambiti infranet ed internet
- Corrisponde alla struttura tipica delle PA
- Semplifica la gestione riducendo i costi
- In caso di necessità consente di filtrare anche il traffico Infranet.

DigitPA

Misure minime

- Protocolli
- Server
- PdL
- Informazioni
- Amministratori di sistema
- Personale ULS

DigitPA

Conclusioni

- Robustezza complessiva
- Efficacia del modello SOC centrico
- Stimolo per le ULS
- Resistenza delle amministrazioni più evolute
- Necessità di riduzione dei costi attraverso economie di scala