ItaliaSicur@

Consiglio Nazionale degli Ingegneri

FUB Fondazione Ugo Bordoni Ricerca e Innovazione

DigitPA

Governo italiano

Presidenza del Consiglio dei Ministri

Ministro per la pubblica amministrazione e l'innovazione

Il modello di sicurezza SPC proiettato verso gli enti locali

Tavolo tecnico ItaliaSicur@

Magg. Gabriele Cicognani

22 marzo 2011

Camera dei Deputati

Riferimenti normativi

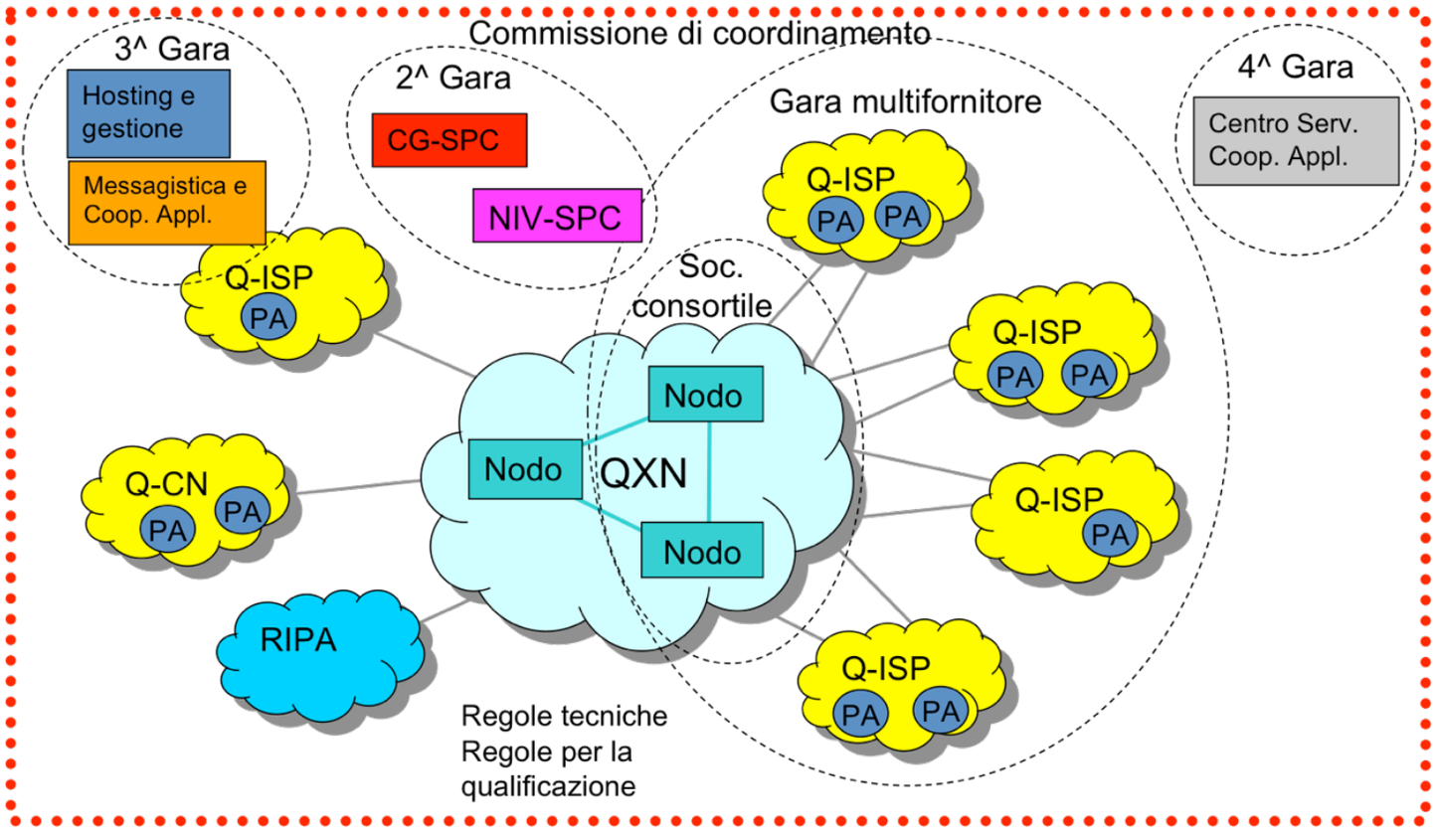
1. Codice dell'Amministrazione Digitale (CAD)
2. Regole tecniche e di sicurezza per la realizzazione ed il funzionamento del Sistema Pubblico di Connettività (DPCM 01.04.2008)
3. Codice della Privacy (Dlgs 196/2003)
4. Direttiva Stanca DM 16.01.2002
5. Contratti Quadro SPC
6. Documenti ufficiali SPC
   - 6.1.tassonomia degli incidenti
   - 6.2.processo di prevenzione degli incidenti
   - 6.3.processo di gestione degli incidenti

Linee guida e quaderni CNIPA

7. Quaderno n°5 – Sistema pubblico di connettività e cooperazione
8. Quaderno n°23 – Linee guida per la sicurezza ICT nelle PA.

Il Sistema Pubblico di Connettività

Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, **garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.**



Il Sistema Pubblico di Connettività

Il Sistema Pubblico di Connettività è definito come un insieme d'infrastrutture e regole condivise ed è stato disegnato come "***rete trusted***", cioè un dominio logico con una politica di sicurezza nota all'esterno e verificabile con processi di qualificazione o di monitoraggio.

Gli enti aderenti al SPC sono considerati degni di fiducia giacché accettano, condividono e assicurano l'attuazione di una serie di norme e prescrizioni, finalizzate a garantire la sicurezza e la stabilità dell'intero sistema, costituito da una federazione di domini affidabili basata su mutue relazioni organizzative e tecnologiche di tipo fiduciario.

L'insieme dei contenuti, delle prescrizioni e degli obblighi di sicurezza sono oggi distribuiti nell'intero quadro dispositivo di riferimento e vincolano tutti gli attori di SPC nella misura in cui sono necessari a mantenere affidabile il sistema rappresentato da infrastrutture condivise e da una rete che interconnette tutti i partecipanti. La *governance* della sicurezza di SPC non dispone delle scelte attuate all'intero dei singoli domini.

Il Sistema Pubblico di Connettività

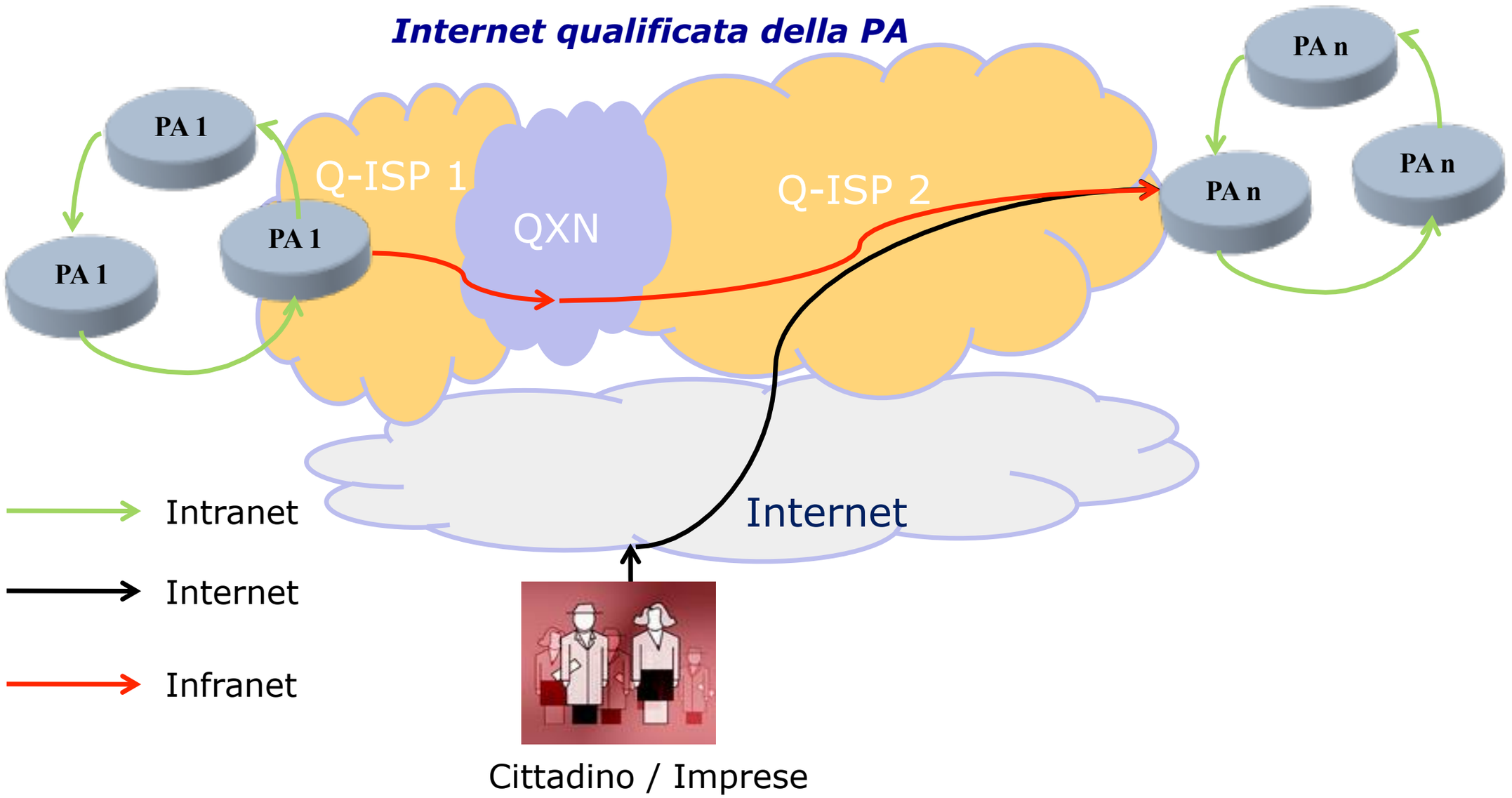
SPC è un sistema:

1. **federato:** costituito da una federazione di domini di sicurezza, all'interno del quale la salvaguardia della integrità, disponibilità e riservatezza delle informazioni veicolate o gestite avviene nel rispetto dell'autonomia del patrimonio informativo delle singole Amministrazioni;

2. **policentrico:** sono individuate le responsabilità e degli ambiti di competenza di ciascun soggetto che partecipa all'erogazione di un servizio composto in ambito SPC;

3. **non gerarchico**: tutte le amministrazioni condividono i medesimi Contratti Quadro e sono rappresentate nella Commissione di Coordinamento e in cui diversi soggetti si impegnano reciprocamente ad adottare le misure minime definite nell'ambito dell'SPC, atte a garantire i livelli di sicurezza necessari all'intero sistema

Il Sistema Pubblico di Connettività



Il Sistema Pubblico di Connettività

Il *framework* di sicurezza che è stato definito per SPC richiama alcuni dei domini di sicurezza descritti dallo standard internazionale ISO 27000, prevedendo l'adozione di determinate misure di sicurezza per la mitigazione del rischio; l'impianto regolamentare ed architetturale del Sistema Pubblico di Connettività, è stato definito in modo da realizzare un sistema strutturato per la gestione della sicurezza, che però salvaguardasse l'autonomia decisionale e gestionale delle singole amministrazioni.

Governance	
Threat mitigation	**Transaction and data integrity**
Identity and access management	**Application security**
Physical security	**Personel security**

Il Sistema Pubblico di Connettività

Threat Mitigation

Protezione del perimetro	Gestione delle vulnerabilità
Gestione degli incidenti	Controllo dei contenuti

E' previsto

1. Collezione log degli incidenti
2. PAT management: occultamento porte attive
3. NAT
4. Monitoraggio rete e gestione apparati
5. La PdR è definita come elemento logico con funzionalità di FW, IDS, VPN, IPSec,NAT
6. Filtraggio traffico nei punti di accesso
7. FW mangement
8. Separazione dei collegamenti tra i nodi QxN e nodi *untrusted*
9. Proxy applicativi per http (RIPA)
10. Funzionalità di firewalling (RIPA)
11. SOC dei fornitori conforme a normative vigenti in tema di sicurezza (RIPA)
12. VPN management erogato dal fornitore
13. IPSec con certificati X.509v3 emessi da una CA di rete in territorio nazionale
14. Tunnel cifrati per collegamenti VoiP tra sedi
15. Servizi di NIDS e HIDS forniti erogati dal fornitore assegnatario
16. NIDS per la QxN
17. Sensori di NIDS distribuiti per raccolta ed analisi dati su attacchi (RIPA)
18. Sezionamento dei collegamenti in SC-Qxn
19. Tunnel cifrati per collegamenti VoiP tra sedi
20. Intervento e distribuzione patch
21. Monitoraggio e verifica ad opera del fornitore assegnatario
22. vulerability assessment con cadenza non superiore a 2 volte nell'arco contrattuale
23. test di efficacia delle misure ed analisi delle vulnerabilità
24. URL filtering management
25. procedure di incident management definite tra SOC, CERT-SPC e ULS

Il modello di sicurezza per la PA

Con l'approvazione del **decreto legislativo del 30 dicembre 2010, n. 235** ("Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82), **è stata aggiornata la disciplina dei rapporti tra Stato, Enti locali, cittadini ed imprese che utilizzino le nuove tecnologie** quale modalità di interazione reciproca, con l'obiettivo di migliorare l'efficienza e l'efficacia dell'azione amministrativa delle singole PA e della macchina dello Stato nel suo complesso.

In questo contesto, gli aspetti di sicurezza sono stati ribaditi e rinforzati nella consapevolezza del ruolo trasversale rispetto ai Capi e Sezioni che compongono l'articolato del Codice.

Nello specifico, è previsto (art.12) - tra l'altro - che *"**Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza**, secondo le regole tecniche di cui all'articolo 71"*

E che **le regole tecniche (da adottarsi ai sensi dell'articolo 71) individueranno "*le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture* "** (art.51)

Il modello di sicurezza per la PA

Il Progetto Italia Sicur@ si propone di realizzare uno specifico programma di formazione sulla sicurezza informatica cui destinare gli ingegneri iscritti al CNI, al fine di qualificarne e specializzarne le professionalità sulle tematiche di sicurezza di maggiore emergenza, per un successivo intervento sulla Pubblica Amministrazione locale (PAL)

L'iniziativa avviata da CNI e FUB con il patrocinio del Ministero della Pubblica Amministrazione e con la partecipazione di DigitPA quale organo tecnico per conto del DIT, produrrà i suoi risultati a beneficio degli enti locali, con particolare riferimento a quelle realtà meno "all'avanguardia" sotto il profilo dell'innovazione tecnologica, al fine di facilitarne la crescita nell'impiego delle nuove tecnologie accompagnata dalla consapevolezza nell'adozione di misure e politiche di sicurezza ICT, coerenti con il modello di sicurezza adottato nel Sistema Pubblico di Connettività.

L'obiettivo è quello di facilitare ciascun ente, nell'ambito delle rispettive responsabilità, nella comprensione delle tematiche della sicurezza sviluppando quella consapevolezza necessaria per la riduzione della vulnerabilità, per garantire integrità e affidabilità dell'informazione pubblica, ma anche quale fattore abilitante al fine di perseguire standard elevati di efficacia ed efficienza della propria azione amministrativa

La definizione di un modello di sicurezza di riferimento, ispirato alle caratteristiche ed alle specifiche previste per SPC ed arricchito con i dati ottenuti dall'azione di monitoraggio svolta sul campo dagli ingegneri:

1. consentirà di uniformare il livello di sicurezza ICT di tutta la Pubblica Amministrazione, centrale e locale;
2. potrà adattarsi alle politiche di ampliamento delle autonomie locali e di federalismo;
3. risulterà coerente con i dettami del Codice dell'Amministrazione Digitale, anche in riferimento a tutte le indicazioni concernenti la continuità operativa.

Il modello di sicurezza per la PA

CAD

Regole Tecniche di sicurezza SPC (DM01.04.08)

CAD 2011

Tavolo tecnico ItaliaSicur@

Monitoraggio

Rapporto sulla sicurezza

Regole Tecniche ex art. 51 del Dlgs 235, del 30.12.10 (CAD)

(CAD)

Il modello di sicurezza per la PA

1. Sicurezza organizzativa
2. sicurezza delle reti
    - 2.1. Amm.ne SPC
    - 2.2. Amm.ne non SPC
3. sicurezza dei dati
4. sicurezza delle applicazioni
5. sicurezza dei servizi
6. politiche di sicurezza per il personale
7. gestione degli incidenti
8. outsourcing

1	Sicurezza organizzativa
1.1	*Analisi e gestione del rischio*
	E' stata definita ed approvata una metodologia ed una politica di gestione del rischio? E' stata effettuata l'analisi del rischio per il dominio/ambito di competenza? Ogni quanto tempo i risultati vengono verificati? Esiste la figura del Risk manager? I risultati costituiscono il presupposto per il DPS previsto dal Dlgs 196/03?
1.2	*Politiche di sicurezza*
	Sono state approvate delle politiche di sicurezza ICT valide per tutta l'amministrazione?
	Esiste una definizione di ruoli e responsabilità?
	Da chi dipende il responsabile della sicurezza?
	E' già stato identificato il Dirigente responsabile della sicurezza dell'Ente, previsto dall'art. 17 del CAD?
	Esiste un piano di formazione sulla sicurezza per il personale impegnato nel settore?
	Esiste un piano di sensibilizzazione di tutto il personale sui rischi e le minacce alla sicurezza?
	E' stata istituita l'Unità Locale di Sicurezza prevista dall'art. 21 del DPCM 01.04.2008?
	Se no, è presente un team di risposta agli incidenti?
	Esiste una previsione di spesa dedicata specificatamente alla sicurezza ?
	Se esiste una previsione di spesa dedicata alla sicurezza quale è la percentuale sul budget IT complessivo ?
	Ci sono servizi di sicurezza affidati a gestori esterni (outsourcer)?
	Se si, vengono effettuati controlli sul suo operato?
	Esiste un piano di business continuità e disaster recovery? Ogni quanto viene aggiornato?
	Esistono delle politiche per la gestione dei portatili e dei media removibili? Sono state previste ed adottate politiche di *change management* ?
	Sono state redatti documenti relativi alle procedure interne di gestione della sicurezza delle informazioni? Se si, esiste un registro su ci vengono annotate le modifiche?

2	**Sicurezza delle applicazioni**	
2.1	*Acquisizione e sviluppo applicativo*	
	Nel caso di acquisizione di prodotti o servizi, vengono considerate certificazioni di sicurezza ?	
	Nel caso vengano considerate certificazioni di sicurezza nell'acquisizione di prodotti o servizi, quali certificazioni sono considerate ?	
	Common criteria; ISO 27000 Certificazioni professionali Altro	☐ ☐ ☐ ☐
	Nella realizzazione dei capitolati, sono previste clausole di riferimento a processi di SDLC per garantire la sicurezza in tutte la fasi dello sviluppo e rilascio del software (es. SAMM)?	
	Sono previsti in fase di collaudo test di verifica del software rispetto alle principali vulnerabilità applicative note?	
2.2	*Mantenimento delle applicazioni*	
	E’ prevista la pianificazione di *vulnerability assessment* periodici sulle applicazioni in produzione?	
	Esiste una procedura di monitoraggio, controllo ed adattamento dell’utilizzo delle applicazioni?	
	E’ prevista una procedura di acquisizione ed installazione degli aggiornamenti di sicurezza?	

3	**Sicurezza di rete**	
	Connettività	
31	Quali tecnologie di *firewalling* sono utilizzate a difesa del dominio di competenza?	
	Statefull Xml applicativo	☐ ☐ ☐
	L'ente implementa VPN per la sicurezza delle connessioni verso l'esterno?	
	Sono installati servizi di IDS/IPS?	
	E' presente un servizio di Event Log Momitoring per l'analisi delle registrazioni degli apparati di frontiera	
	I servizi citati sono gestiti da risorse interne, affidati in *outsourcing* o con una soluzione intermedia?	
	E' prevista operatività H24 del personale impegnato nella gestione degli appariti di frontiera?	
	Se l'operatività H24 è affidata in esterno, è prevista la reperibilità del personale interno impegnato nella gestione degli appariti di frontiera?	
3.2	*Protezione della rete interna*	
	Sono impiegate separazioni logiche tra reti interne (es. per necessità di sapere)?	
	E' consentito l'accesso alla rete interna da Internet?	
	Se si, quali strumenti di sicurezza sono impiegati?	
	User-id e pwd Strong authentication https VPN	☐ ☐ ☐ ☐
	E' consentito ai fornitori l'accesso alla rete interna?	
	E' consentito ai fornitori l'accesso alla rete interna dall'esterno?	
	Se è presente una rete Wi-Fi, che tipo di tecnologia di autenticazione è implementata?	
	Wep Wpa Wpa2 Radius 802.1x	☐ ☐ ☐ ☐ ☐
	E' possibile l'accesso dall'esterno per lo svolgimento di servizi di Mgt?	
	Se si, come è protetto?	
	VPN https strong authentication	☐ ☐ ☐

Grazie per l'attenzione

cicognani@digitpa.gov.it

ItaliaSicur@