Il Centro di Gestione della Sicurezza di SPC e il processo di gestione degli incidenti di sicurezza

Roma, 27 Maggio 2008

Giovanni Abbadessa

CG-SPC: Il centro di Gestione del Sistema Pubblico di Connettività

Il CG-SPC svolge per conto del CNIPA il ruolo di terza parte nel Sistema Pubblico di Connettività

Servizi di Misura:

Il CG-SPC, attraverso i Servizi di Misura, Raccolta e Distribuzione dei dati, verifica le performance e la qualità del servizio degli operatori SPC (Q-ISP)

Funzioni centralizzate di Sicurezza:

Il CG-SPC svolge un ruolo di coordinamento nell'ambito della Sicurezza del Sistema Pubblico di Connettività

Svolge il ruolo di monitoraggio della Sicurezza del sistema SPC

Il CG-SPC svolge il ruolo di Incident Response Team di 2° livello rispetto ai SOC degli operatori SPC (Q-ISP)

Il CG-SPC coadiuva il CERT del CNIPA nel monitoraggio e miglioramento dei livelli di Sicurezza del sistema SPC

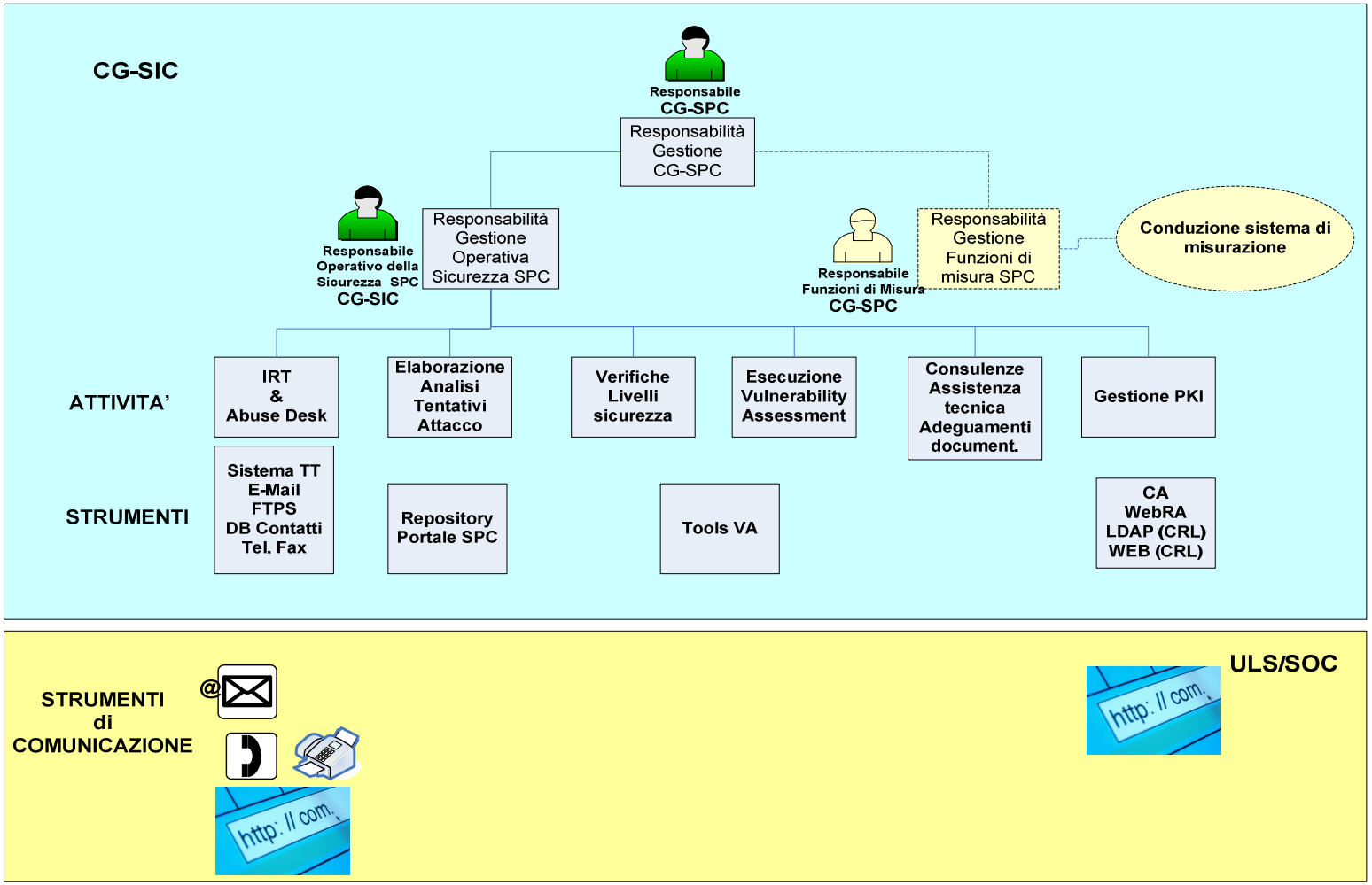
Funzioni Centralizzate di Sicurezza del CG-SPC

Il CG-SPC esercita funzioni centralizzate di sicurezza per il monitoraggio dei livelli di sicurezza di SPC e il coordinamento dei Q-ISP e delle ULS nella gestione degli incidenti con l'obiettivo di assicurare la sicurezza complessiva del SPC.

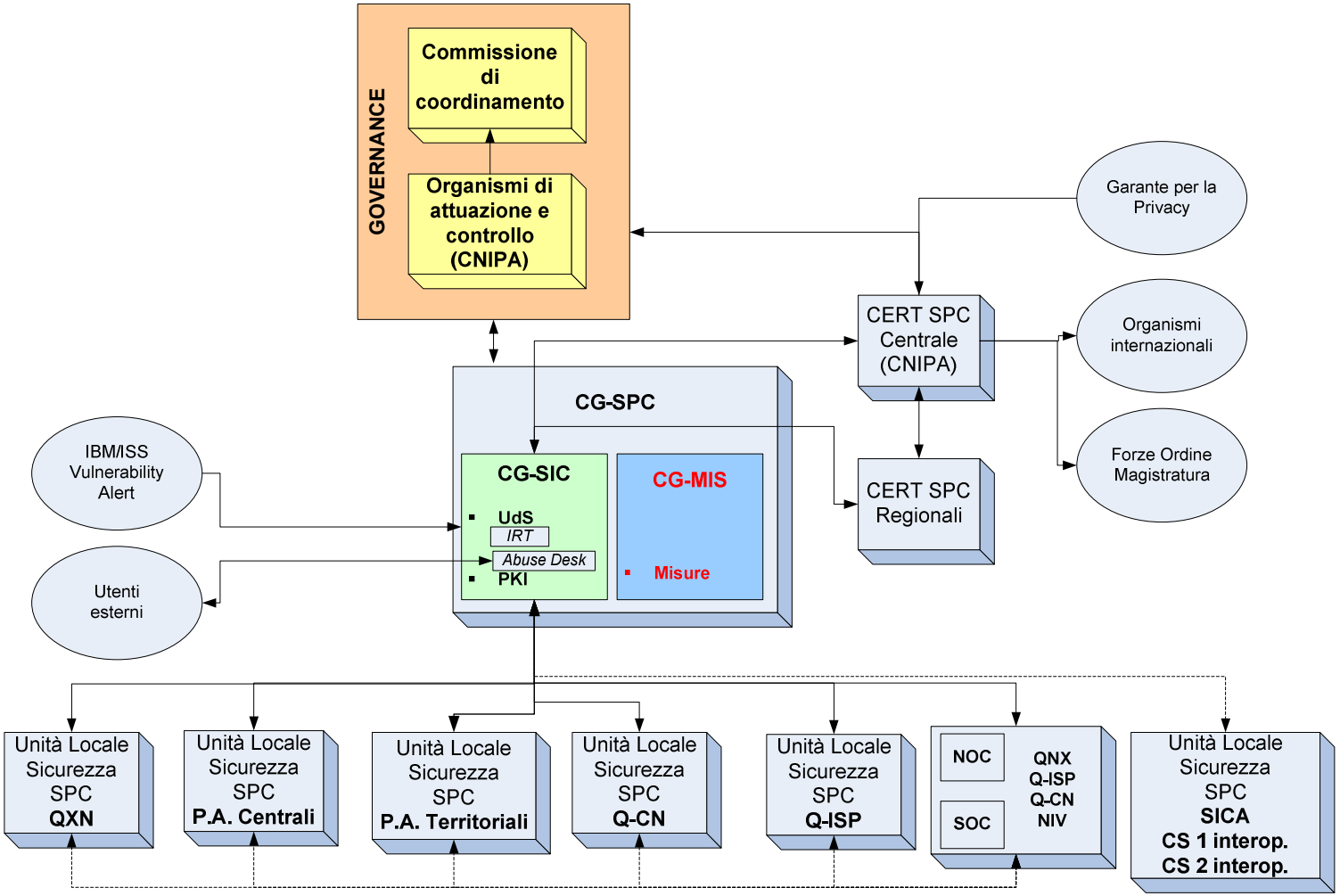
La componente del CG-SPC che assicura le funzioni sopra descritte è denominata **Centro di Gestione della Sicurezza del SPC (CG-SIC)** ed esegue le attività di:

- Supporto al CNIPA nella definizione delle politiche di sicurezza all'interno del SPC e nel monitoraggio della loro applicazione;
- Coordinamento delle attività di sicurezza svolte dalle ULS del SPC per la prevenzione e la risposta ad attacchi od altri eventi di sicurezza; **Incident Response Team, Abuse Desk**
- Gestione della **Public Key Infrastructure** (PKI) per l'emissione e la gestione di certificati per il funzionamento del sistema SPC.

Le attività e gli strumenti del CG-SIC



L’organizzazione del CG-SIC e l’interazione con i soggetti del SPC



La community della sicurezza SPC

- Il SPC è un sistema dove la connettività è fornita da vari fornitori
- Il SPC è un sistema “trusted” che permette l’utilizzo di tutti protocolli
- RUPA era un sistema con un unico fornitore di connettività
- RUPA era un sistema “untrusted” che permetteva solo l’utilizzo di determinati protocolli
- Il CG-SIC collabora con il CNIPA e il CERT-GOV-C, per contribuire a creare “La Community di Sicurezza del SPC”, coinvolgendo i Q-ISP e le ULS delle singole Amministrazioni.
- Scopo della Community di Sicurezza del SPC è quello di migliorare costantemente il livello di sicurezza del SPC
- Per “fare sistema” è necessario utilizzare lessico, metriche e procedure comuni

Obiettivi del processo di gestione degli incidenti

Gestire gli incidenti di sicurezza al fine di:

- Contenere e minimizzare l’impatto
- Ridurre disservizi e danni (diretti ed indiretti)
- Ripristinare il normale funzionamento in tempi rapidi

Raccogliere ed analizzare i dati per costituire una base di conoscenza utile per l’individuazione di:

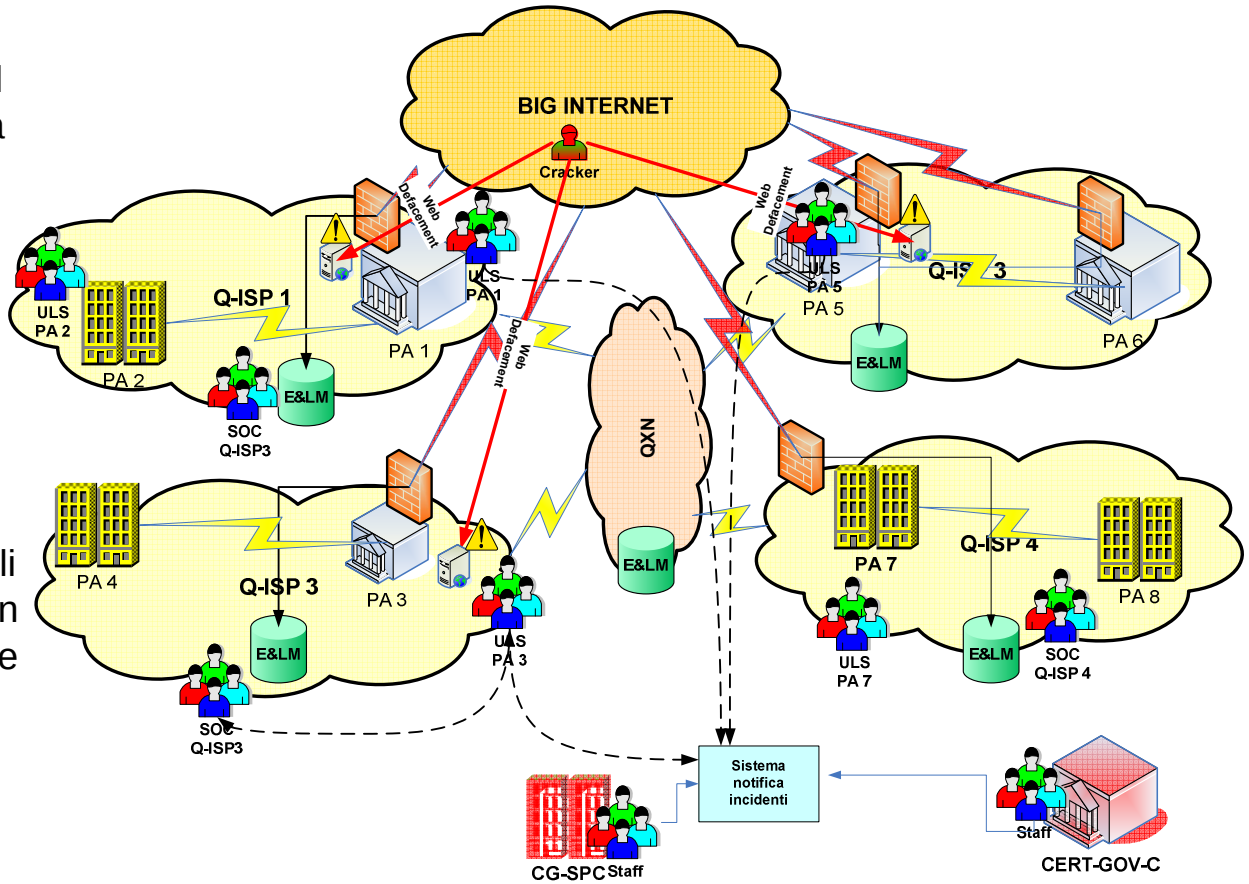
- eventi precursori di attacco
- azioni correttive
- nonché per finalità statistiche

Gestione degli incidenti SPC - Esempio 1-

L'incidente Response Team (IRT) del CG-SPC coordina la gestione della risposta agli incidenti di sicurezza informatica che colpiscono il SPC coinvolgendo le risorse in grado di risolvere l'incidente minimizzando i danni.

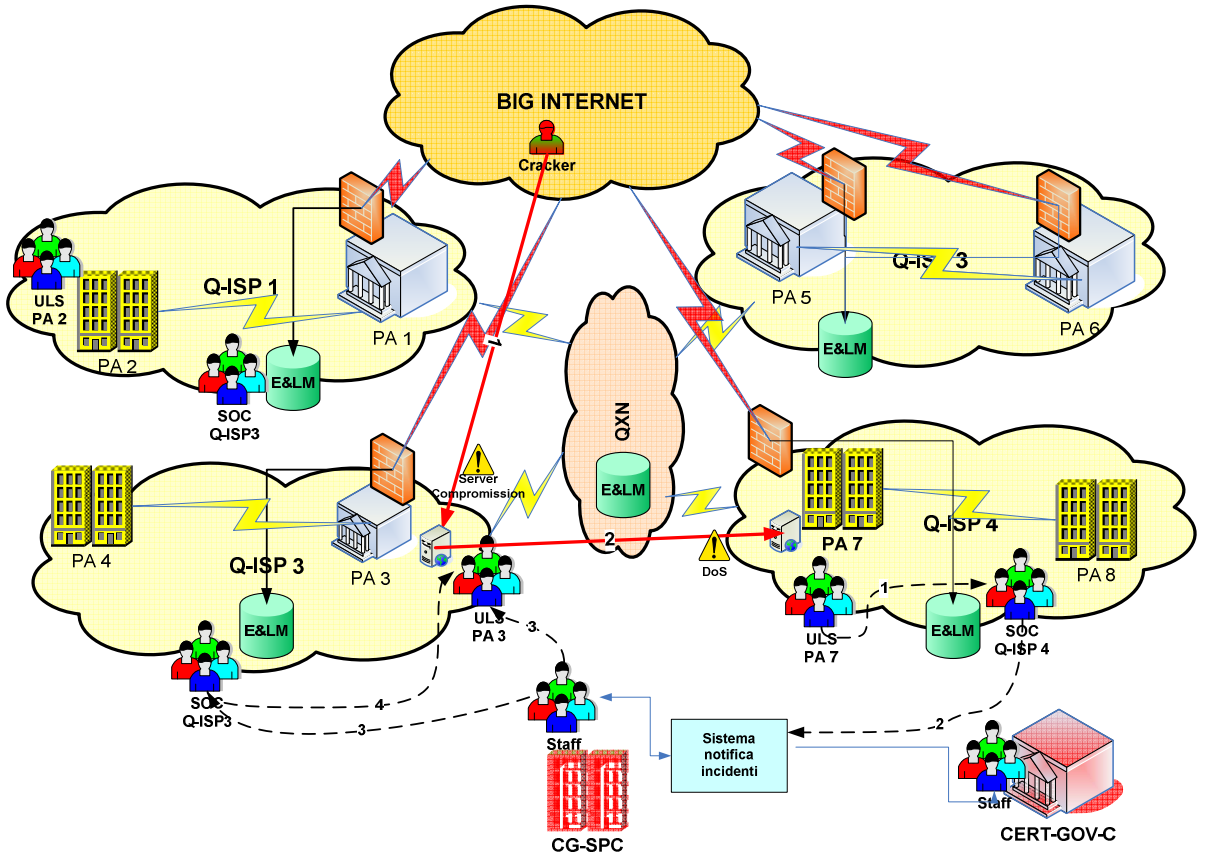
Es. attacco coordinato verso tre PA

Il CG-SPC ha una vista "globale" degli incidenti che stanno avvenendo e in base a ciò può decidere di emettere dei warning



Gestione degli incidenti SPC - Esempio 2 -

- L'ULS della PA7 si accorge di un attacco
- Contatta il SOC del suo Q-ISP
- Nella notifica di incidente, fatta dal SOC Q-ISP 4 al GS-SIC, è riportato l'indirizzo IP attaccante
- Il CG-SIC avvisa il SOC A-ISP3 e l'ULS PA3 che un attacco proviene da un server di pertinenza, probabilmente compromesso
- L'ULS PA3 risolve il problema sul proprio server

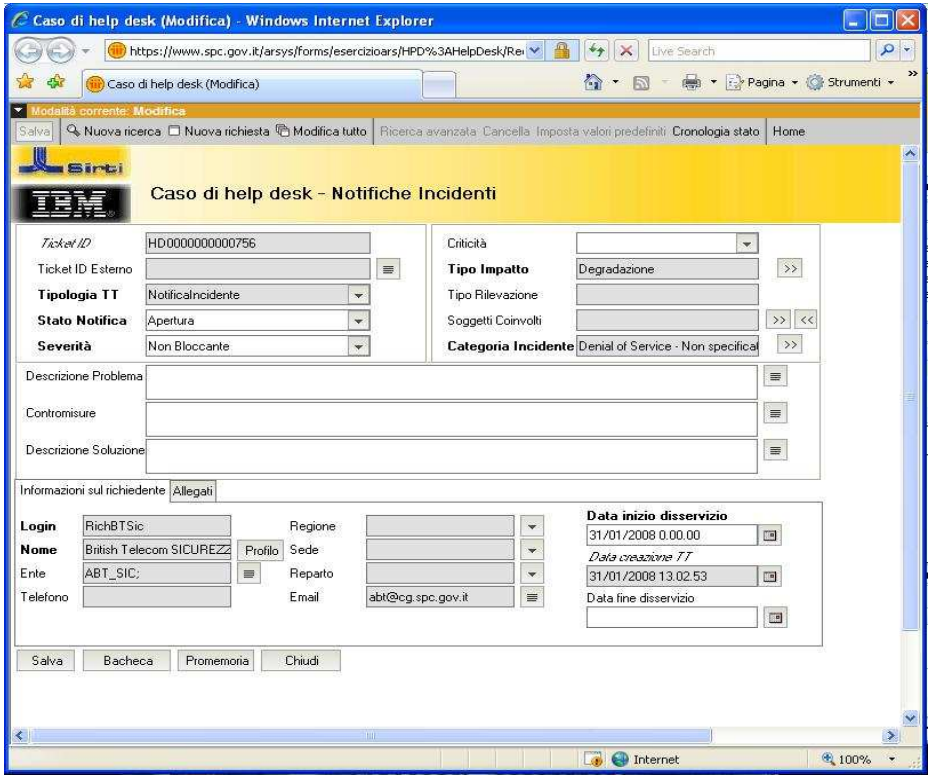


Gli strumenti del CG-SIC per la gestione degli incidenti di sicurezza: Il portale per la notifica degli incidenti

Il CG-SIC ha sviluppato un sistema per la notifica degli incidenti di sicurezza via web che viene utilizzato dai SPC dei Q-IPS e dalle ULS delle Amministrazioni

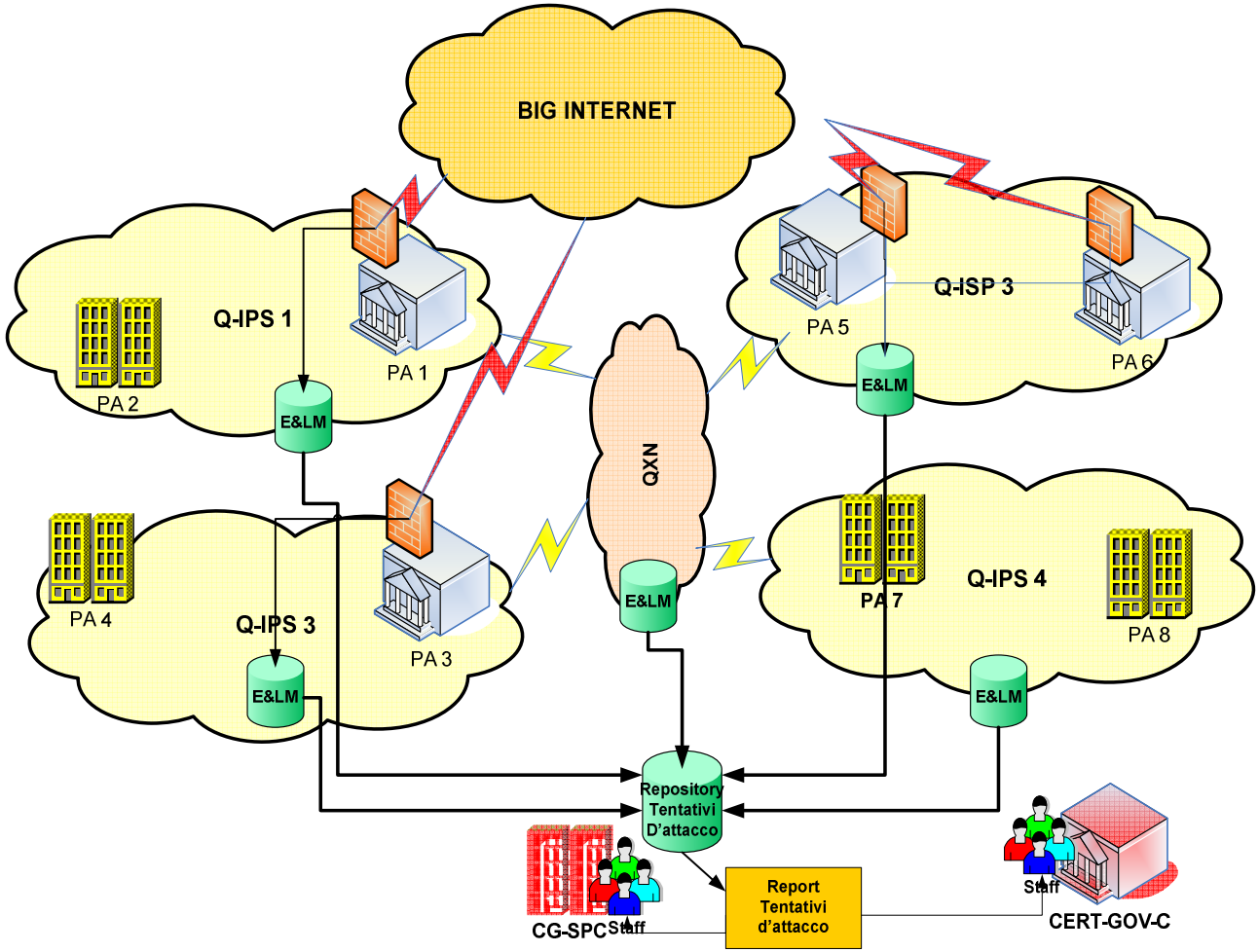
Mediante il portale il personale delle ULS può notificare che è in corso un incidente di sicurezza e richiedere all'IRT del CG-SIC supporto nella gestione di un incidente

Questo tool è disponibile sul portale del CG-SPC https://www.spc.gov.it agli appartenenti alle ULS registrati previa autenticazione



Gli strumenti del CG-SIC per la gestione della sicurezza: La raccolta dei dati relativi ai tentativi d'attacco (1 di 2)

- I dati raccolti dai FW e IDS delle Amministrazioni vengono raccolti dai sistemi di correlazione ed analisi dei Q-IPS.
- Questi dati vengono aggregati ed inviati al CG-SPC che li immagazzina nel proprio repository e li analizza per avere un'indicazione sullo stato globale dei tentativi d'attacco di tutto il SPC.



Gli strumenti del CG-SIC per la gestione della sicurezza: La raccolta dei dati relativi ai tentativi d'attacco (2 di 2)

I dati relativi ai tentativi d'attacco vengono immagazzinati nel repository del CG-SPC.

Si eseguono analisi di tipo statistico allo scopo di evidenziare eventuali anomalie

Tali anomalie possono essere ulteriormente investigate per scoprire eventi precursori d'attacco

Documenti di riferimento per la gestione degli incidenti SPC

I seguenti documenti, a disposizione delle ULS, sono essenziali per potere gestire correttamente un incidente di sicurezza ITC che colpisce il SPC:

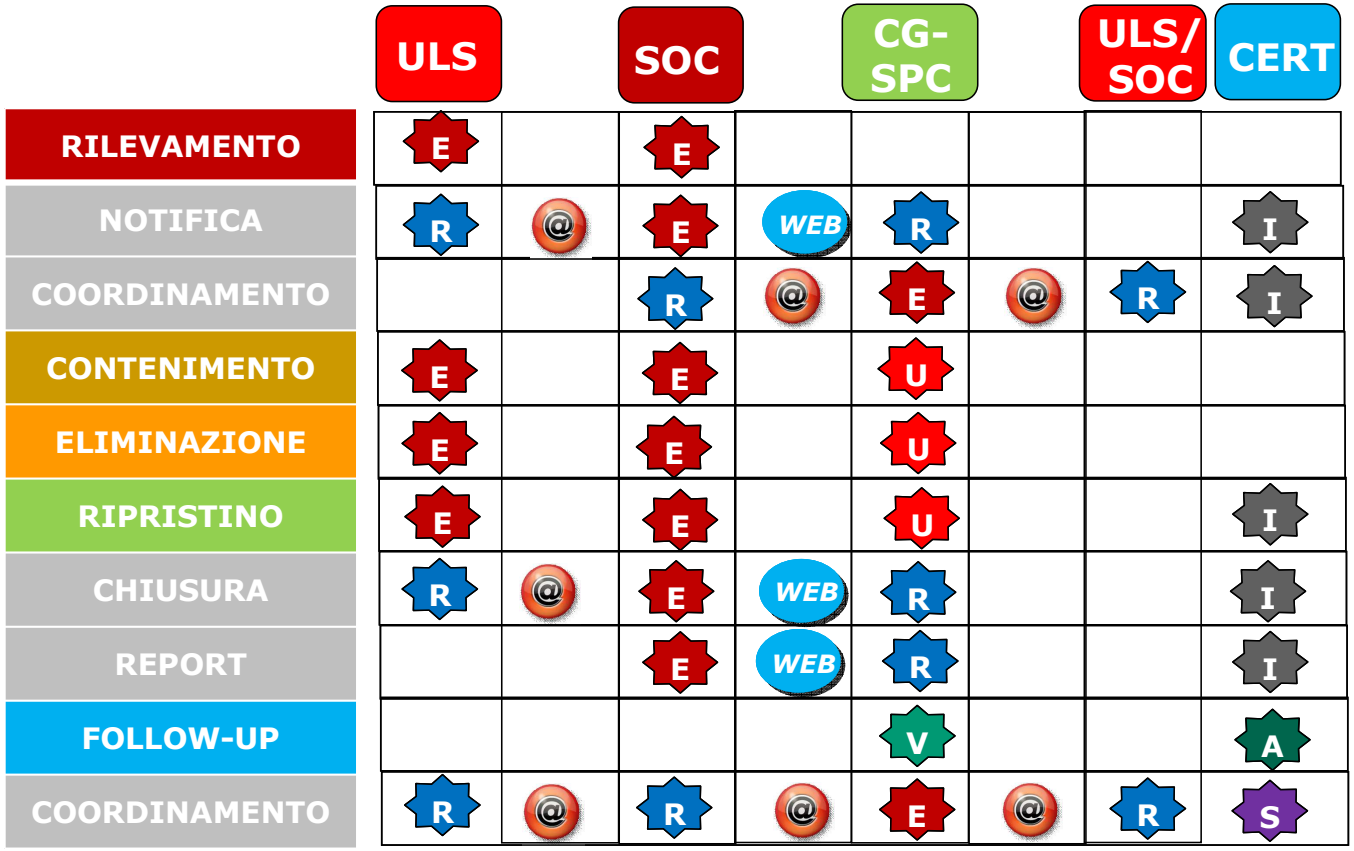
- Il Processo di gestione degli incidenti di sicurezza nel Sistema Pubblico di Connettività (emesso dal CNIPA)

- La Classificazione degli Incidenti Informatici nel Sistema Pubblico di Connettività (SPC) (emesso dal CNIPA)

- Manuale operativo per la comunicazione degli incidenti di sicurezza di SPC da parte delle ULS (emesso dal CG-SPC)

BACK-UP

Caso tipico d'incidente



Analizza	Effettua	Informato	Riceve	Supervisiona	Supporta	Verifica
A	E	I	R	S	U	V

Source:

G.Moxedano

Responsabile Prog. GovCert