

# Dal GovCERT al CERT-SPC-C

SPC e la Sicurezza nella PA  
Italiana

Roma, 27 maggio 2008

*Gianluigi Moxedano – GovCERT-CNIPA*

# Mission del GoVCERT

Il CERT governativo deve:

1. Fornire informazioni tempestive e supporto per gli eventi che possono recare danno alle infrastrutture, ai servizi ed agli utenti della PAC.
2. Fornire appropriate informazioni e supporto competente alla PAC nella gestione degli incidenti e delle emergenze relative alla sicurezza ICT.
3. Predisporre linee guida tecniche ed organizzative per favorire l'efficacia dei servizi erogati ed accrescere la cultura della sicurezza.
4. Raccogliere dati per finalità statistiche e valutazione delle tendenze.
5. Cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori ed autorità coinvolti alla sicurezza ICT e promuovere la loro interazione.

**Early warning**

**Incident response support  
and coordination**

**Guidelines and rules**

**Information gathering**

**Information sharing and  
cooperation**

# Linee di azione prioritarie

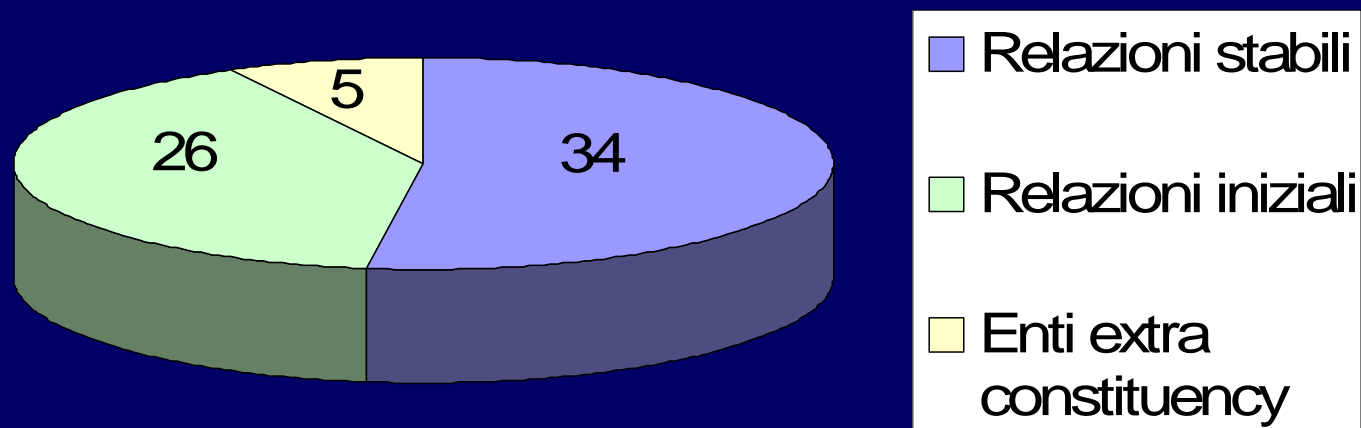
**Creazione e stabilizzazione delle relazioni con la  
Constituency**

**Progettazione, sviluppo ed erogazione dei servizi  
di maggiore utilità, efficacia ed economicità di  
sistema**

**Definizione di accordi di collaborazione con altri  
Organi dello Stato, con istituzioni analoghe anche  
internazionali, con fornitori di prodotti e servizi**

# Constituency

## Numeri attuali e distribuzione



Extra constituency: Garante protezione dati personali  
CERT Regione Friuli Venezia Giulia  
Agenzia del demanio  
SOGEI  
GARR

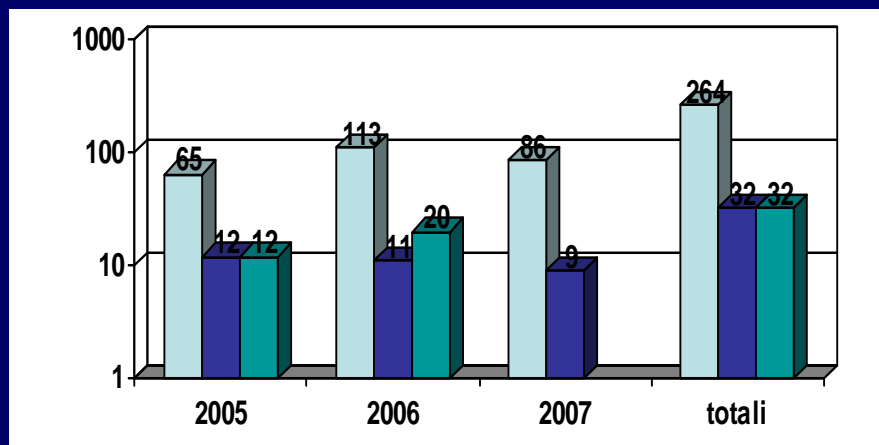
# Early Warning

**COSTITUITA RETE  
 INFORMATIVA**

**REALIZZATE LE  
 APPLICAZIONI**

**FORMALIZZATI  
 CRITERI, METRICHE E  
 PROCEDURE**

-3 FONTI  
 SPECIALISTICHE  
 -40 FONTI APERTE  
 ( SU 260 CENSITE)  
 -FONTI SUL  
 TERRITORIO



**METRICHE E  
 NOMENCLATURE  
 STANDARD**

**INFORMAZIONI  
 UTILI ANCHE  
 SUL SITO WEB**

**OLTRE 7000  
 TECNOLOGIE IN  
 OSSERVAZIONE**

**FORMATI  
 PREDEFINITI E  
 FIRMATI  
 DIGITALMENTE**

# Diffusione informazioni



GovCERT.it - GovCERT - Mozilla Firefox

http://www.govcert.it/

GOV CERT IT  
Computer Emergency Readiness Team

CNIPA

GovCERT.it

Constituency

Servizi

Alert e Warning

Documentazione

Eventi

Relazioni

Link

Archivio news

Il GovCERT è una unità del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), istituita per fornire supporto alle pubbliche amministrazioni centrali (ex d.lgs 39/93) nella prevenzione e gestione degli incidenti informatici. L'organismo svolge le funzioni di Computer Emergency Readiness Team governativo con il ruolo di struttura di coordinamento e di riferimento per i CERT-AM (le unità per la prevenzione e la gestione degli incidenti informatici interne a ciascuna amministrazione previste dalla Direttiva sulla sicurezza ICT del 16 gennaio 2002).

News

- 2007-05-16**  
Numerose fonti segnalano la crescente diffusione di un messaggio di posta elettronica ingannevole proveniente da un fittizio account della Polizia di Stato: [Prisco Mazzi] pris\_maz@poliziadistato.it. Tale messaggio di posta elettronica veicola in allegato un file .zip contenente un malware di tipo trojan downloader (Trojan.Zlobmi.B - nomenclatura Symantec) correntemente rilevato da tutti i prodotti e servizi antivirus aggiornati.
- 2007-05-15**  
Microsoft ha confermato l'anomalo impiego di risorse di sistema del servizio SVCHOST, segnalato da alcuni utenti, quando viene installato il software correttivo rilasciato in data 8 Maggio. Per ulteriori segnalazioni vedere la sezione Alert & Warning.
- 2007-04-13**  
Microsoft ha rilasciato un Advisory (935964) per segnalare una vulnerabilità di sicurezza di tipo "zero day" riguardante l'interfaccia Remote Procedure Call (RPC) del servizio DNS Server di Windows.

Contatti

Copyright Responsabilità

Il sito web [www.govcert.it](http://www.govcert.it) è online dal 10 luglio 2006

# Incident support and coordination

**REALIZZATE LE  
INFRASTRUTTURE E LE  
APPLICAZIONI**

**FORMALIZZATE LE  
PROCEDURE**



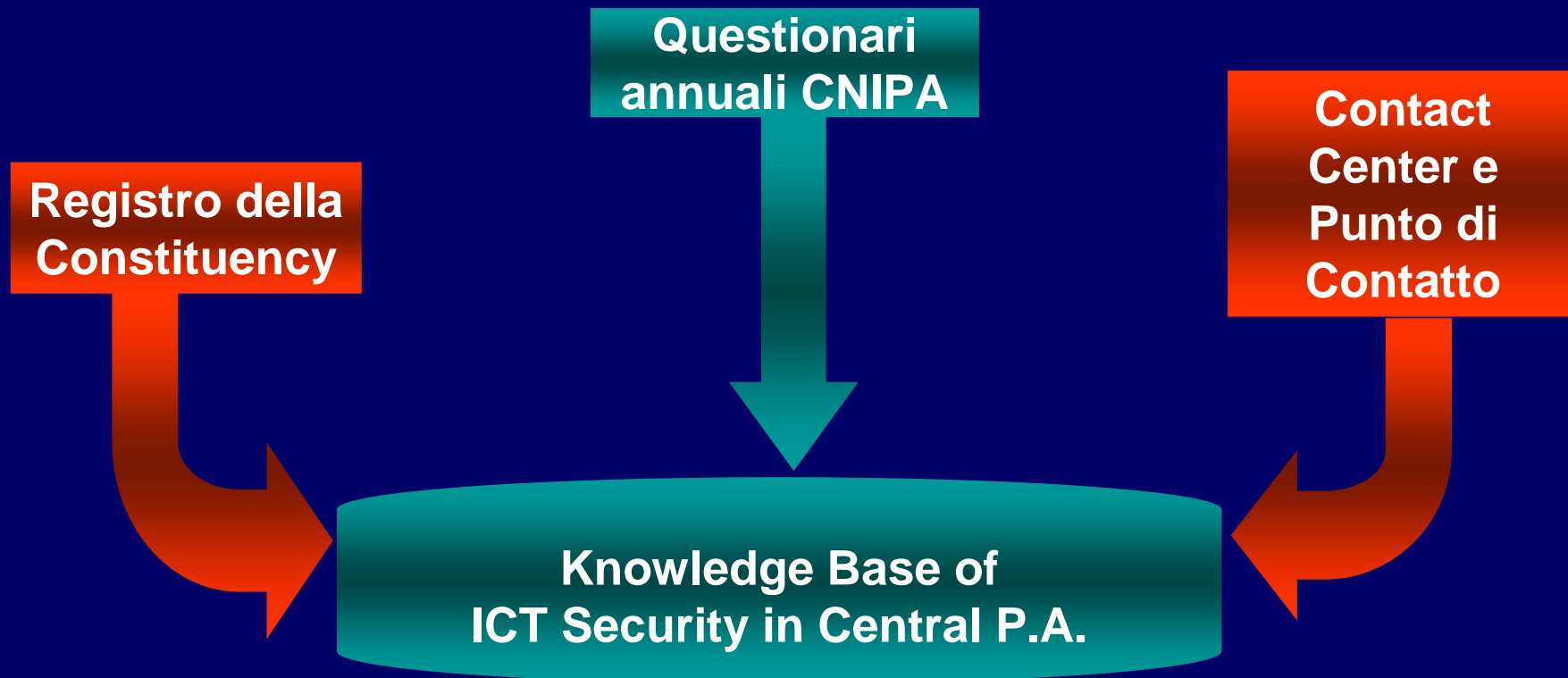
**IL CONTACT CENTER SUPPORTA LA  
CONSTITUENCY TRAMITE:**

- INVIO DOCUMENTAZIONE TECNICA SPECIFICA
- INFORMAZIONI TECNICHE
- INDICAZIONI FINALIZZATE AL CONTENIMENTO DELL'INCIDENTE
- INDICAZIONI DI CARATTERE LEGALE/GIURIDICO
  
- GESTITI 6 INCIDENTI

**CONTACT CENTER UFFICIALMENTE  
ATTIVO DAL 20 LUGLIO 2006.  
PROCEDURA DI CONTATTO INVIATA  
ALLA CONSTITUENCY.  
ALTRE INFORMAZIONI SUL WEB  
[WWW.GOVCERT.IT](http://WWW.GOVCERT.IT)**

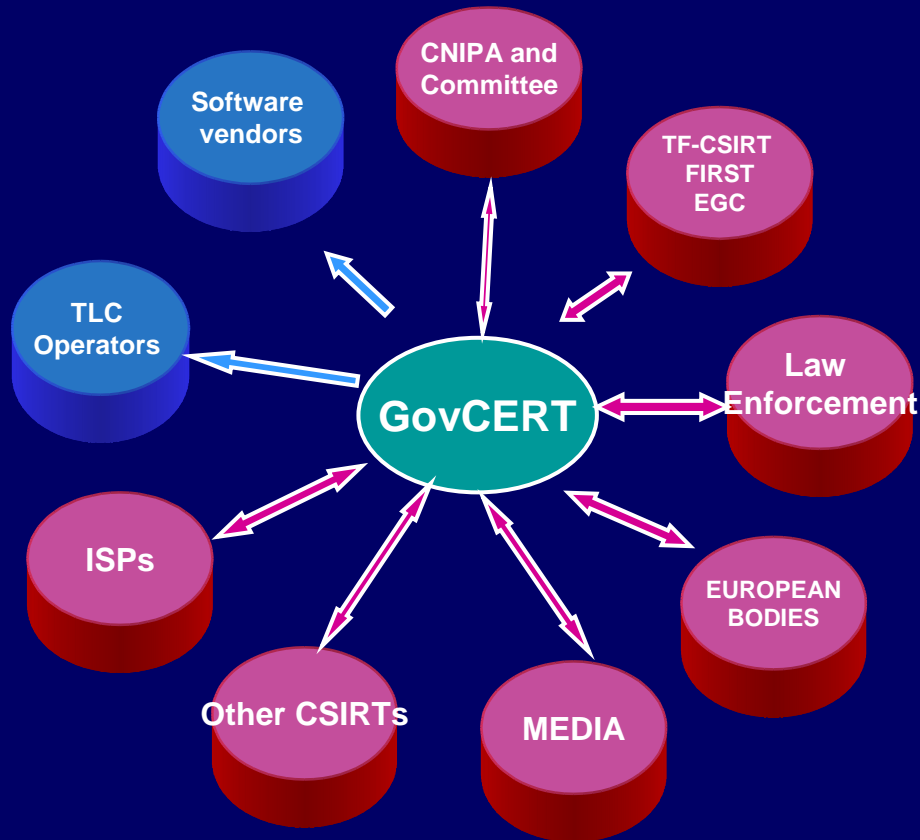
**RILEVAZIONE WEB DEFACEMENT  
SUI SITI WEB DELLA CONSTITUENCY,  
DELLE REGIONI, DELLE PROVINCE DI  
MAGGIORE IMPORTANZA.  
32 WEB DEFACEMENT  
RILEVATI E COMUNICATI**

# Information gathering





# Information sharing and cooperation



- Firmato Protocollo d'intesa con **CISCO** Italia
- Firmato P.I. con ABILab/CIPA
- P.I. con **Microsoft** alla firma
- Altri P.I. in corso di definizione con fornitori, operatori telco, autorità di polizia
- Agreement con CERT/RFVG e GARR
- Partecipazione al WG **ENISA** "CERTs cooperation" ed al **WG ENISA** "CERT Services"

# CERT governativi in EUROPA



# IL CERT-SPC-C

# Mission del CERT-SPC-C (art. 21, comma 5, lett. a - R.T.)

il CERT-SPC-C e i CERT-SPC-R, di concerto con gli Organismi di attuazione e controllo, **definiscono le metodologie per la prevenzione, il monitoraggio, la gestione e l'analisi degli incidenti di sicurezza, assicurando la coerenza e l'uniformità in tutto il sistema.**

**Il CERT-SPC (CERT-SPC-C e CERT-SPC-R) svolge i seguenti compiti:**

- **attività di prevenzione degli incidenti informatici ...;**
- **analisi degli incidenti di sicurezza ... al fine di proporre eventuali azioni correttive ...;**
- **collaborazione con le analoghe strutture presenti a livello nazionale ed internazionale, nonché con le autorità di polizia competenti;**

# Metodologie - Documenti prodotti

- **Prevenzione**
  - Revisione Early Warning (GovCERT - ULS CONSIP/MEF)
  - Specifiche tecniche per raccolta ed elaborazione dei tentativi di attacco (CNIPA - CG-SPC - SOC/QISP)
  - Acceptable Use Policy (CNIPA - CG-SPC)
- **Gestione Incidenti**
  - Definizione Processo Gestione (CNIPA - CG-SPC - SOC)
  - Definizione Classificazione (CNIPA - CG-SPC - SOC)
  - Manuale operativo utilizzo applicazioni CG-SPC

# Prevenzione - Early Warning

**BOLLETTINI  
MIRATI**

**NOTIZIARI  
GIORNALIERI**

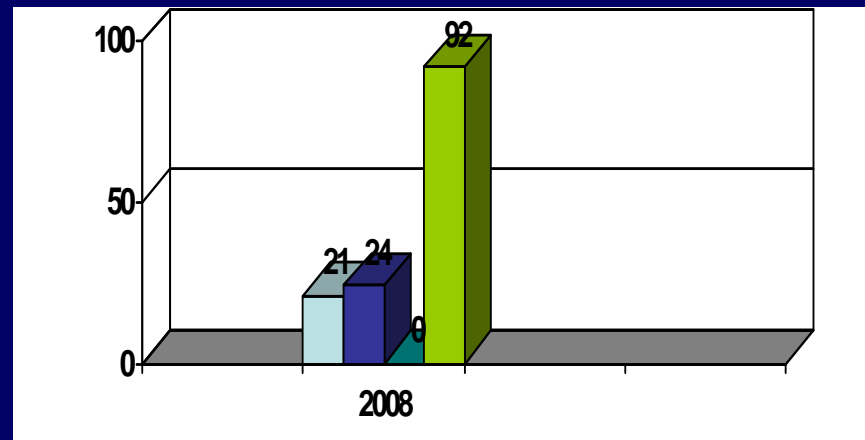
**CONTRIBUTO  
ULS**

**STANDARD  
CVE-CVSS -  
CME**

**INFORMATIVE  
FIRMATE**

- 3 FONTI  
SPECIALISTICHE  
- 40 FONTI  
APERTE (SU 260  
CENSITE)

**SITO WEB  
GovCERT -  
PORTALE CG-  
SPC**



■ Segnalazioni vulnerabilità 
 ■ Annunci Flash  
■ Avisi malware 
 ■ Notiziari giornalieri

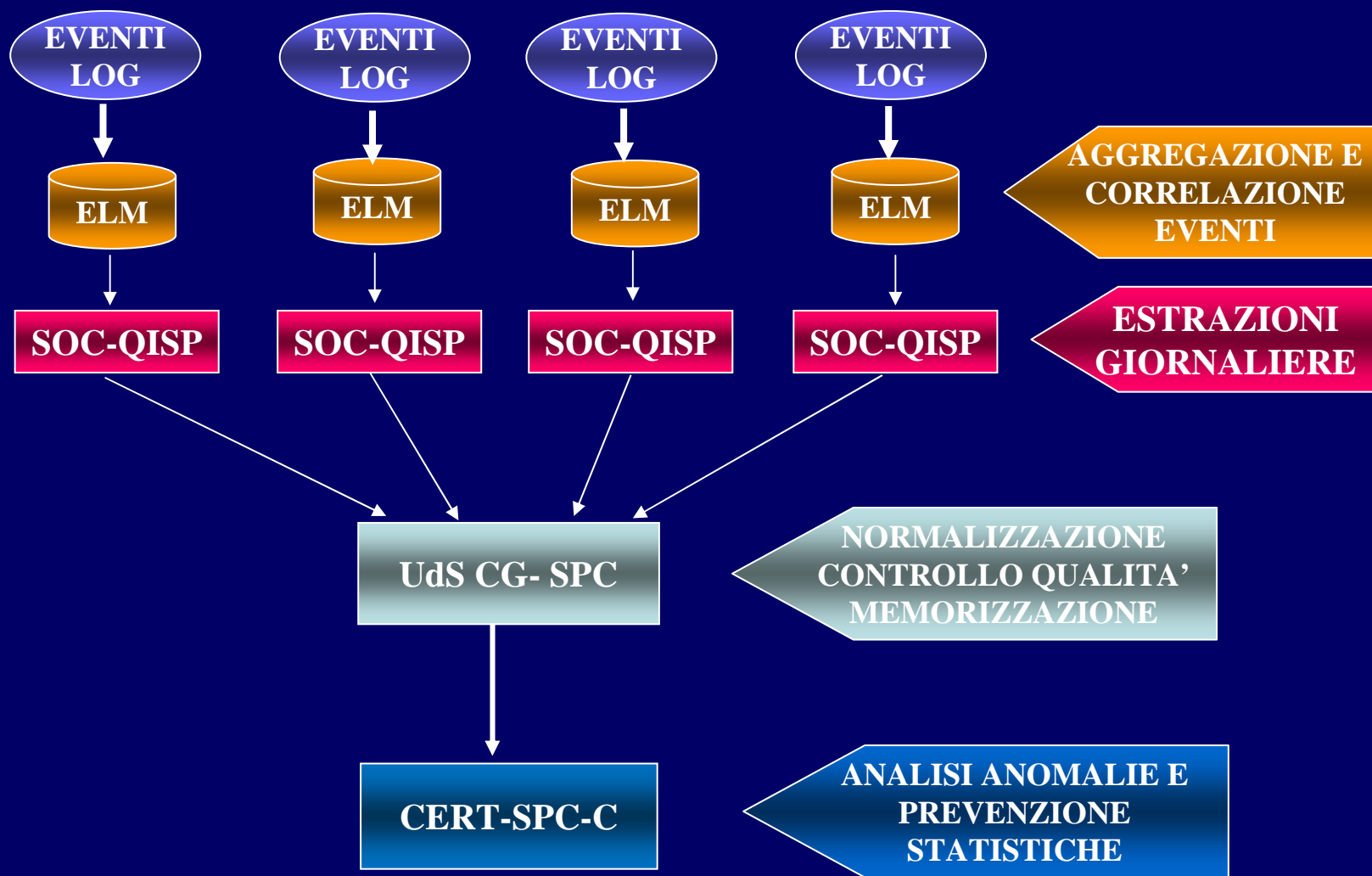
**STD FUTURI  
CWE - CAPEC -  
CEE**

**P.I. CON  
ISTITUZIONI  
ANALOGHE,  
FF.OO.**

**500 FAMIGLIE  
TECNOLOGICHE  
IN  
OSSERVAZIONE**

**P.I. CON  
VENDOR,  
TELCO**

# Prevenzione – Analisi tentativi



# Gestione ed Analisi incidenti

- Controllo incidenti segnalati al CG-SPC
- Esame report di chiusura degli incidenti
- Gli incidenti di carattere non prettamente informatico (ad es. violazione di policy/leggi o incidenti segnalati dall'esterno di SPC) vanno segnalati tempestivamente al solo CERT-SPC-C
- Analisi post-mortem: entro fine anno predisposizione un laboratorio e relativi strumenti hw/sw e procedure

*IN PREPARAZIONE PRIMA ESERCITAZIONE SPC-IH01*



# Servizi ed attività CERT-SPC e CG-SIC

## Reattivi

Early warning **CERT**

### Gestione Incidenti

Analisi **CG**  
Supporto alla risposta  
Coordinamento della risposta

### Gestione Vulnerabilità

Analisi **CG**  
Supporto alla risposta  
Coordinamento della risposta

### Gestione Codici pericolosi

Analisi **CERT/CG**  
Supporto alla risposta  
Coordinamento della risposta

## Proattivi

Annunci **CERT**

Verifiche **CG/CERT**

Disseminazione  
Informazioni **CERT/CG**

Raccolta e  
condivisione  
informazioni **CG/CERT**

## Qualità e sicurezza

Analisi dei rischi **CG**

Sensibilizzazione **CERT**

Formazione **CG**

# Operare e cooperare

CERT-SPC, CG-SIC, SOC QISP, QXN, ULS  
(strutture esterne: ad es. altri CERT)

Per poter operare efficacemente tutte le  
strutture SPC devono "fare sistema"

Per "fare sistema" è necessario utilizzare  
lessico, metriche e procedure comuni

Per "fare sistema" è necessario non solo  
collaborare sulla base di procedure condivise  
ma condividere l'obiettivo

**Grazie dell'attenzione**

[moxedano@cnipa.it](mailto:moxedano@cnipa.it)

[Spc.cert@cnipa.it](mailto:Spc.cert@cnipa.it)

[cert.prevenzione@cnipa.it](mailto:cert.prevenzione@cnipa.it)