Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Dal GovCERT al CERT-SPC-C

SPC e la Sicurezza nella PA Italiana

Roma, 27 maggio 2008

Gianluigi Moxedano – GovCERT-CNIPA

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - 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

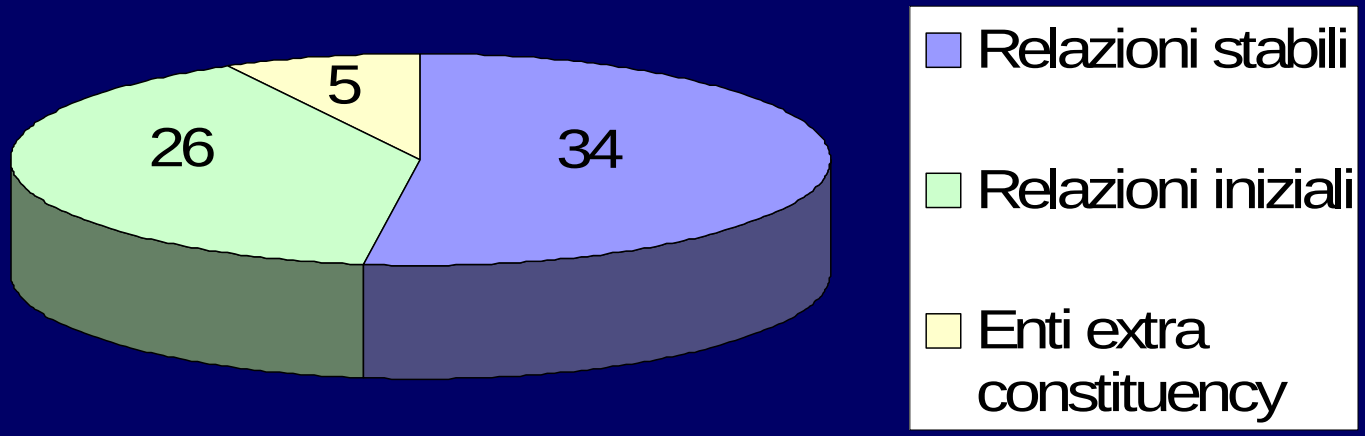
Creazione e stabilizzazione delle relazioni con la Constituency

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

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

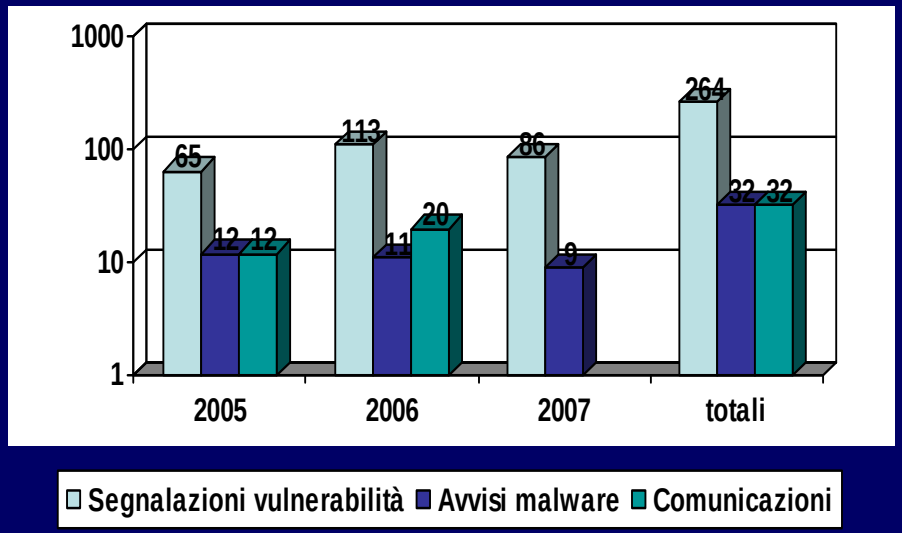
Early Warning

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

Il sito web www.govcert.it è online dal 10 luglio 2006

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

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

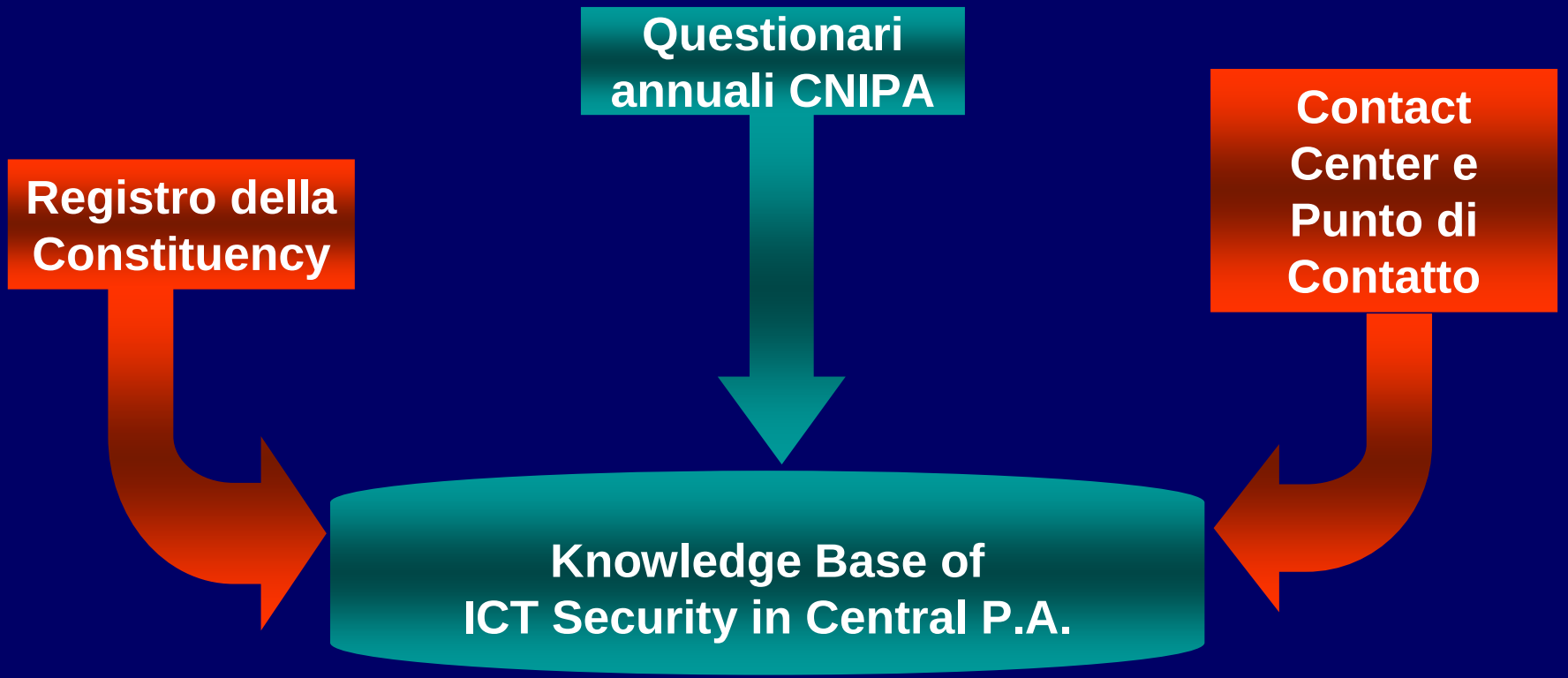
RILEVAZIONE WEB DEFACEMENT SUI SITI WEB DELLA CONSTITUENCY, DELLE REGIONI, DELLE PROVINCE DI MAGGIORE IMPORTANZA.

32 WEB DEFACEMENT RILEVATI E COMUNICATI

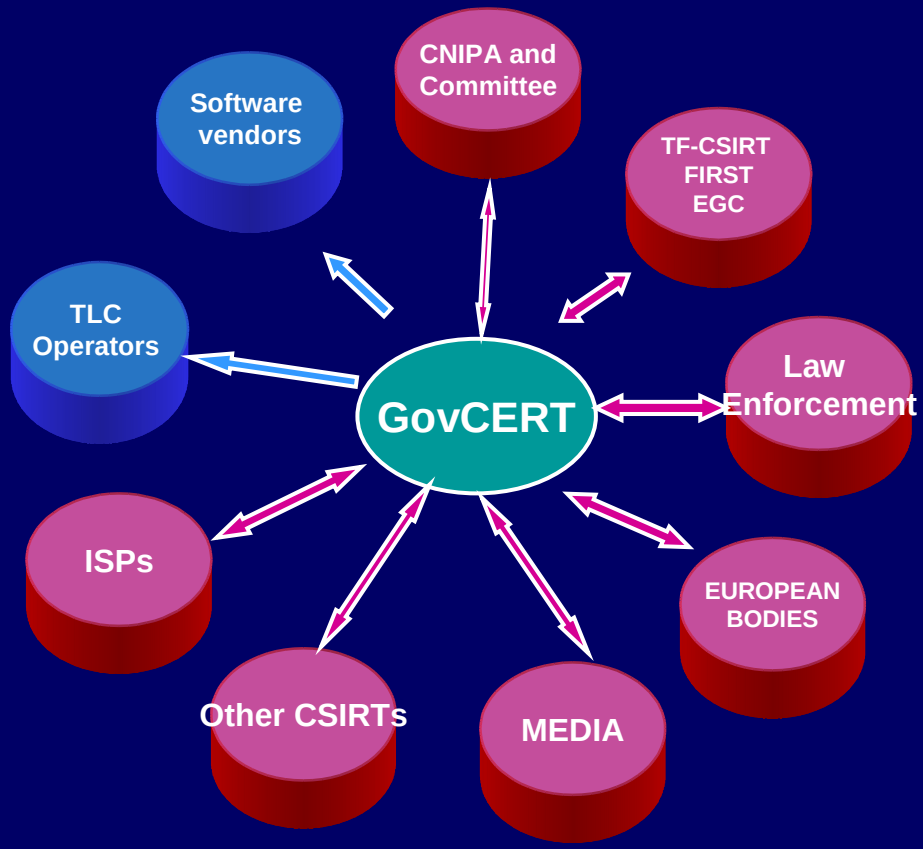
CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

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

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

Prevenzione - Early Warning

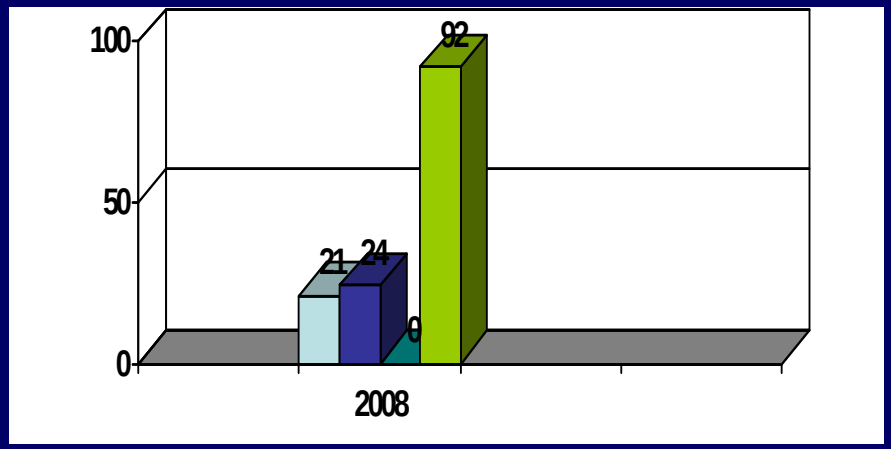
BOLLETTINI MIRATI

NOTIZIARI GIORNALIERI

CONTRIBUTO ULS

STANDARD CVE-CVSS - CME

INFORMATIVE FIRMATE



STD FUTURI CWE –CAPEC-CEE

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

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

SITO WEB GovCERT – PORTALE CG-SPC

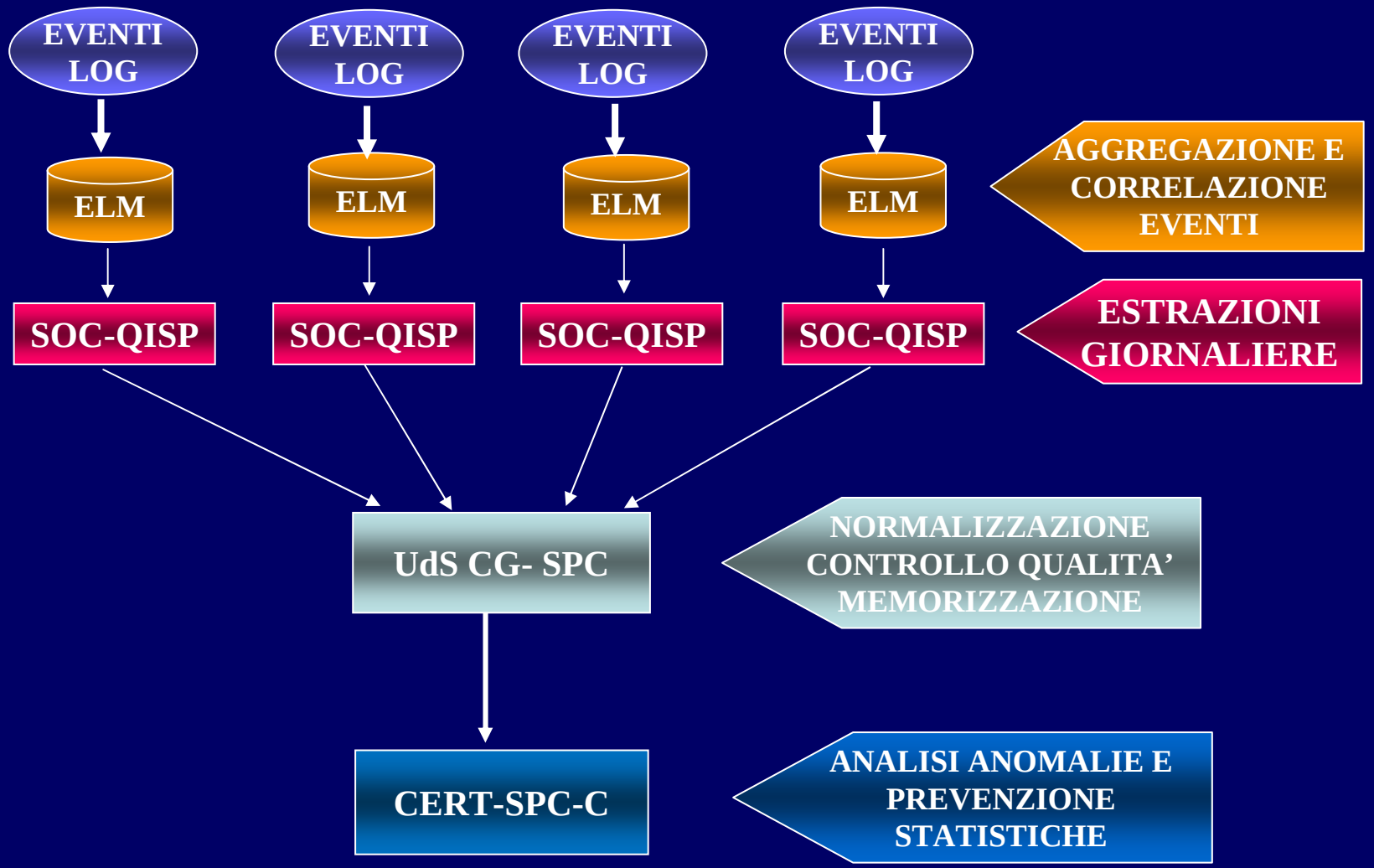
500 FAMIGLIE TECNOLOGICHE IN OSSERVAZIONE

P.I. CON VENDOR, TELCO

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

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

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

Servizi ed attività CERT-SPC e CG-SIC

Reattivi

- **Early warning** — CERT
- **Gestione Incidenti** — CG
  - Analisi
  - Supporto alla risposta
  - Coordinamento della risposta
- **Gestione Vulnerabilità** — CG
  - Analisi
  - Supporto alla risposta
  - Coordinamento della risposta
- **Gestione Codici pericolosi** — CERT/CG
  - Analisi
  - 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

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

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

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Computer Emergency Responce Team
CERT-SPC
Sistema Pubblico di Connettività - CNIPA

Grazie dell'attenzione

moxedano@cnipa.it

Spc.cert@cnipa.it

cert.prevenzione@cnipa.it