



Il ruolo dello CSIRT Italia nella strategia nazionale di Cyber Security

Aldo di Somma
Vice Capo Divisione CSIRT Italia - ACN

Torino - 11 Dicembre 2025

L'inquadramento dello CSIRT Italia





Servizio operazioni e gestione delle crisi cyber

Preparazione, prevenzione, gestione e
risposta a eventi cibernetici



CSIRT Italia



Gestione rischio nazionale,
governance e capacità cyber



Gestione rapporti con
AG. P.G. P.N.A.A.



Stato della minaccia,
gestione delle crisi ed
esercitazioni

Assicura il **funzionamento dello CSIRT Italia** in base ai compiti di legge:

- monitoraggio e l'analisi dei rischi e delle minacce cyber a livello nazionale
- pubblicazione di early warning e alert
- divulgazione di informazioni agli operatori interessati
- ricezione di notifiche obbligatorie e volontarie di incidenti cyber
- l'analisi degli incidenti
- definizione di modalità di intervento e risposta

Cura lo sviluppo e il mantenimento delle **capacità nazionali** di prevenzione, monitoraggio, rilevamento, analisi e risposta

Coordina e partecipa a **esercitazioni** nazionali e internazionali

Supporta il **Nucleo per la cybersicurezza** nella programmazione e pianificazione operativa della risposta a situazioni di crisi

Valuta e promuove procedure di **condivisione delle informazioni** per la diffusione di allarmi relativi ad eventi cibernetici

Lo CSIRT Italia – I Desk

Sviluppo & Nuove Soluzioni



Sviluppo di soluzioni e applicazioni IT per i desk del CSIRT Italia

Operazioni correnti



Front End – Ricezione segnalazioni e triage



Back End – Elaborazione segnalazioni e attivazione Risposta



Constituency monitoring – Raccolta e distribuzione info su minacce ed eventi + **Scansione** proattiva dei sistemi accessibili al pubblico



Outreach – Pubblicazione di alert, e annunci riguardo vulnerabilità e rischi

Fusion Center



Collaborazione tecnica nazionale (rete CSIRT regionali) ed internazionale (CSIRT Network)

Operazioni di prevenzione della minaccia



HUMINT - Gestione raccolta di informazioni da fonti OSINT ed altro

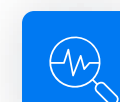


Cyber Threat Intelligence - raccolta, analisi e divulgazione di dati su minacce potenziali o esistenti



CVD & Red Team – identificazione di punti deboli e vulnerabilità – moderazione e coordinamento della disclosure di vulnerabilità

Operazioni di risposta



Malware Analysis – analisi dei comportamenti e delle minacce in artefatti malevoli



IR – pianificazione ed esecuzione della risposta agli incidenti



Digital Forensics – analisi tracce digitali

Il processo di notifica allo CSIRT Italia



Definizioni (art. 6 Direttiva NIS2)

Ulteriormente specificato nella Determinazione 164179



INCIDENTE

Evento che **compromette** la disponibilità, l'autenticità, l'integrità o la riservatezza di dati [...]

È **significativo** se:

- ha causato o è in grado di causare grave perturbazione operativa dei servizi o perdite finanziarie
- Ha/può avere impatto su altre fisiche o giuridiche con perdite materiali o immateriali



NEAR-MISS

Evento che **avrebbe potuto compromettere** la disponibilità, l'autenticità, l'integrità o la riservatezza di dati, ma che è stato **efficacemente evitato** o non si è verificato



MINACCIA INFORMATICA

Circostanza, evento o azione che **potrebbe** avere un impatto sulla rete e sui sistemi informativi, sugli utenti e altre persone

È **significativa** se, in base alle sue caratteristiche tecniche, **può avere un impatto grave** con perdite materiali o immateriali considerevoli

Il processo di notifica

- NIS2
 - Amplia il campo di applicazione degli obblighi di notifica
 - Prescrive dei requisiti di segnalazione più stringenti
 - Definisce la modalità di valutazione degli incidenti

TIPOLOGIA DI NOTIFICA

OBBLIGATORIA

VOLONTARIA

COSA NOTIFICARE



Incidente con impatto significativo



Incidente



Minaccia informatica



Near miss

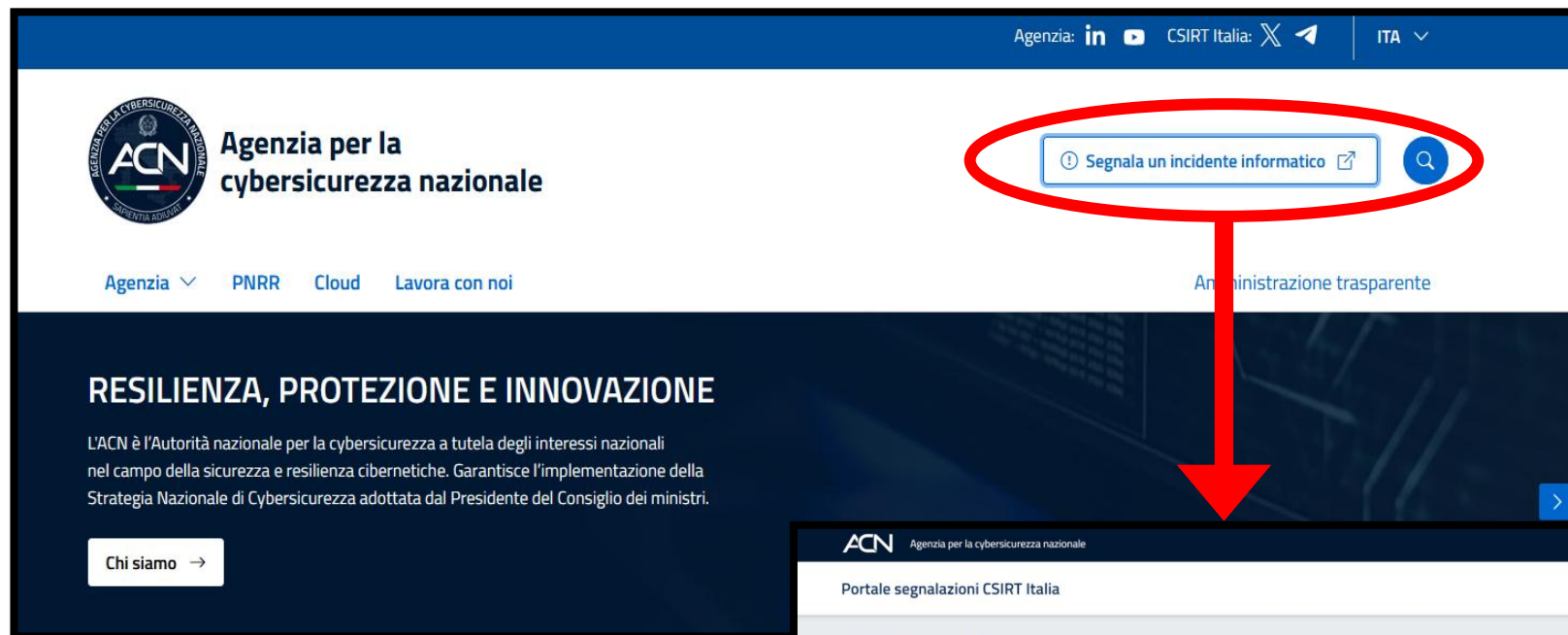
QUANDO NOTIFICARE

Entro le **24 ore**

Entro **le 72 ore** – integrazione alla precedente

Nessun limite temporale

Come segnalare (oggi)



ACN Agenzia per la cybersicurezza nazionale

Portale segnalazioni CSIRT Italia

Notifica incidente

Il presente servizio può essere utilizzato per inviare informazioni di dettaglio in merito agli incidenti di sicurezza e non al fine di avviare procedimenti amministrativi di alcun tipo.

Eventuali segnalazioni non attinenti incidenti di sicurezza saranno scartate.

La notizia non costituisce denuncia, querela o esposto, per la cui presentazione si rinvia agli organi di Polizia competenti o Autorità giudiziaria.

Identificazione soggetto segnalante

☒ Ulteriori soggetti	☐ NIS/Telco Soggetti OSE/FSD/TELCO (d.l.n° 65/2018 e d.l.n° 259/2003)	☐ Perimetro Soggetti inclusi nel perimetro sicurezza nazionale (d.l. n° 105/2019)	☐ Legge 28 giugno 2024, n. 90 Soggetti sottoposti alle disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (Legge n° 90/2024)
---	--	--	--

Nome* Cognome* Email personale*

Come segnalare (dal 9 gennaio 2026)

Home / Servizio CSIRT / Apri Segnalazione / Segnalazione incidente NIS

Segnalazione incidente NIS

DL n.138/2024 NIS2

[Guida alla notifica degli incidenti al CSIRT Italia](#)

Stai creando una nuova segnalazione

I campi contrassegnati con asterisco (*) sono obbligatori

Riferimento normativo*

☐ Obbligatoria

art. 25 D.lgs 138/2024 [Scopri di più](#)

☒ Volontaria

art. 26 D.lgs 138/2024 [Scopri di più](#)

i La tipologia di notifica (ENISA) è obbligatoria per gli incidenti volontari - Art. 18 D.lgs 138/2024

Tipologia di notifica (ENISA)*

☐ Segnalazione di test

Si tratta di una modalità di compilazione finalizzata alla verifica delle funzionalità e delle voci previste nel form, che non genera notifiche al centro indicato né comporta l'adempimento di obblighi normativi.

☐ Minaccia Cyber

Si intende qualsiasi circostanza, evento o azione potenziale che **potrebbe** danneggiare, interrompere o comunque influire negativamente sui sistemi di rete e informativi, sugli utenti di tali sistemi e su altre persone.

☐ Quasi incidente

Si intende un evento che **avrebbe potuto** compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati memorizzati, trasmessi o trattati o dei servizi offerti da sistemi di rete e informativi o accessibili tramite essi, ma che è stato efficacemente impedito o che non si è verificato

☐ Incidente

Si intende un evento che **compromette** la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o dei servizi offerti da sistemi di rete e informativi o accessibili tramite essi.

Stato della notifica*

[Scopri di più](#)

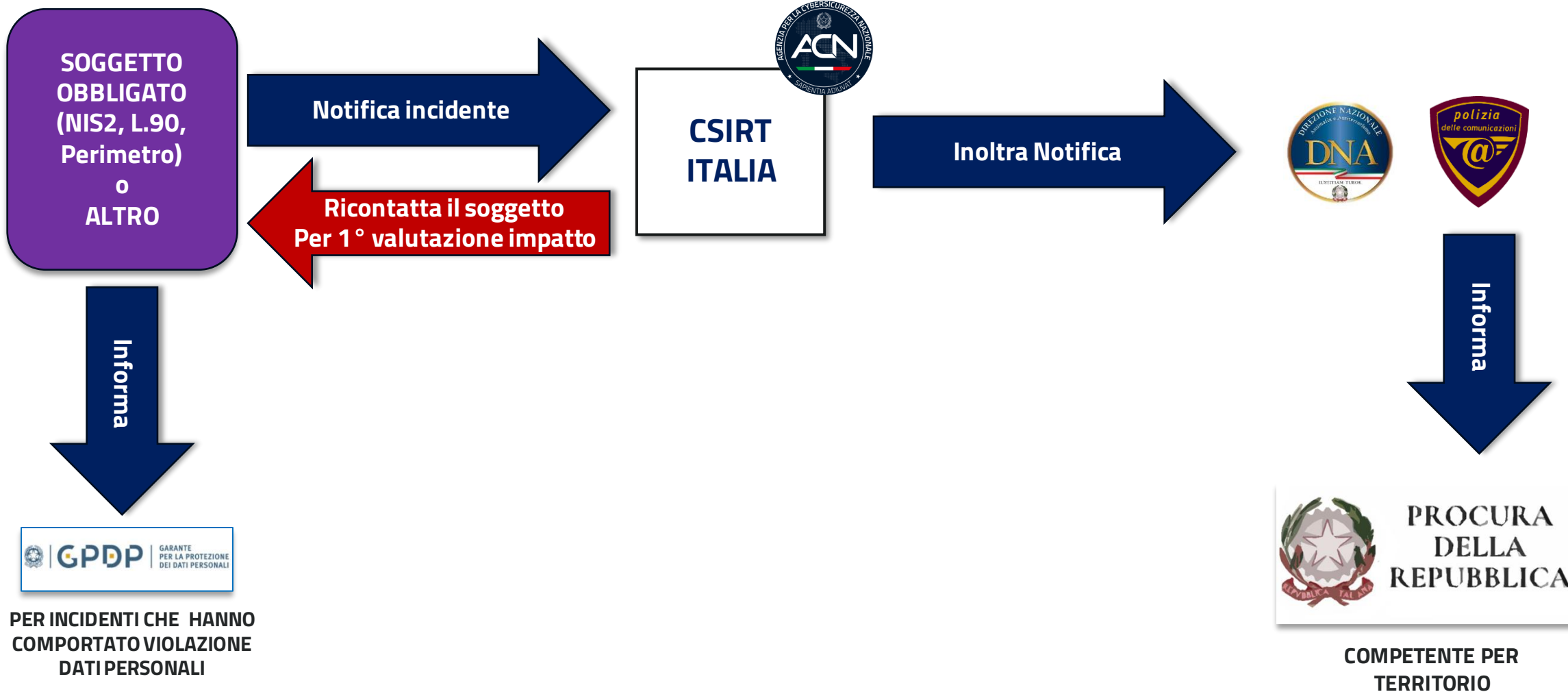
☒ Segnalazione di test

Prova di invio segnalazione, non sarà presa in considerazione dai sistemi CSIRT

☐ Pre notifica

Allerta di incidente, si invia nelle prime **24 ore** dal rilevamento

Flusso segnalazione



Procedure in caso di intervento



GRAZIE

