Il ruolo dello CSIRT Italia nella strategia nazionale di Cyber Security

Aldo di Somma
Vice Capo Divisione CSIRT Italia - ACN

Milano, 03/12/2025

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 persone 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

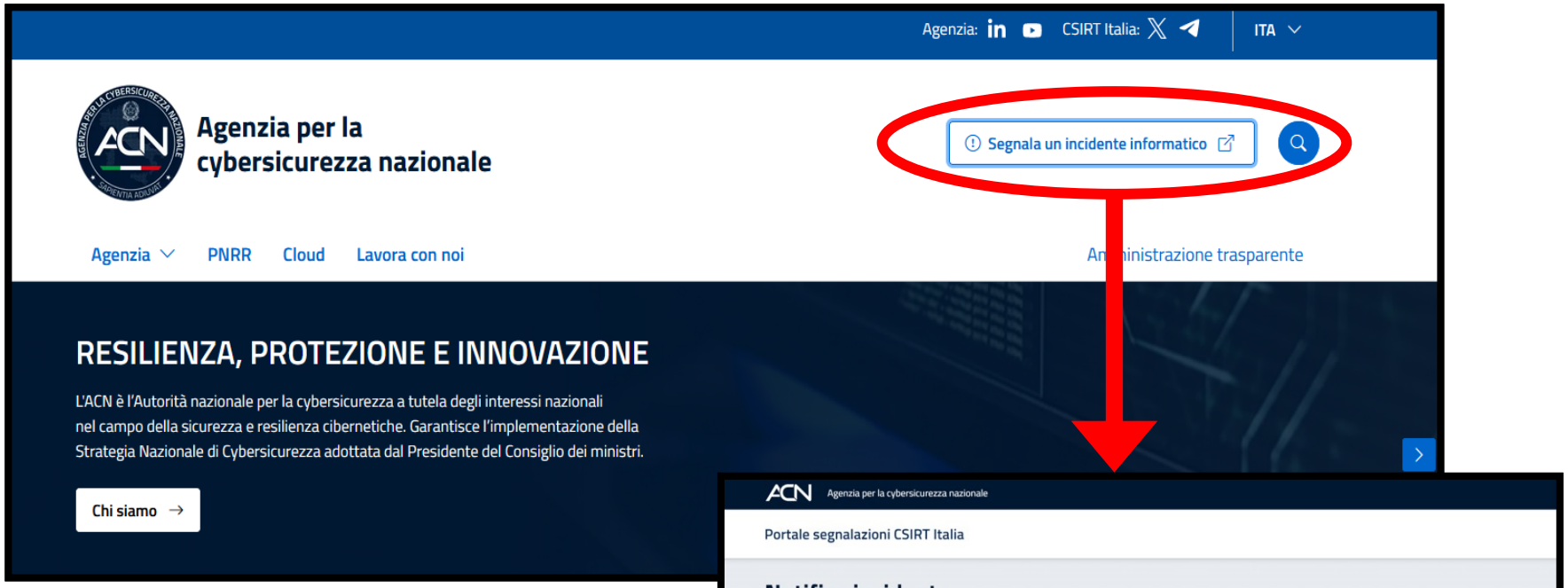
Circostanza, evento o azione che **potrebbe** avere un impatto sulla rete e sui sistemi informativi, sugli utenti e altre persone
È **significativa** se, in base alle sue caratteristiche tecniche, **può avere un impatto grave** con perdite materiali o immateriali considerevoli

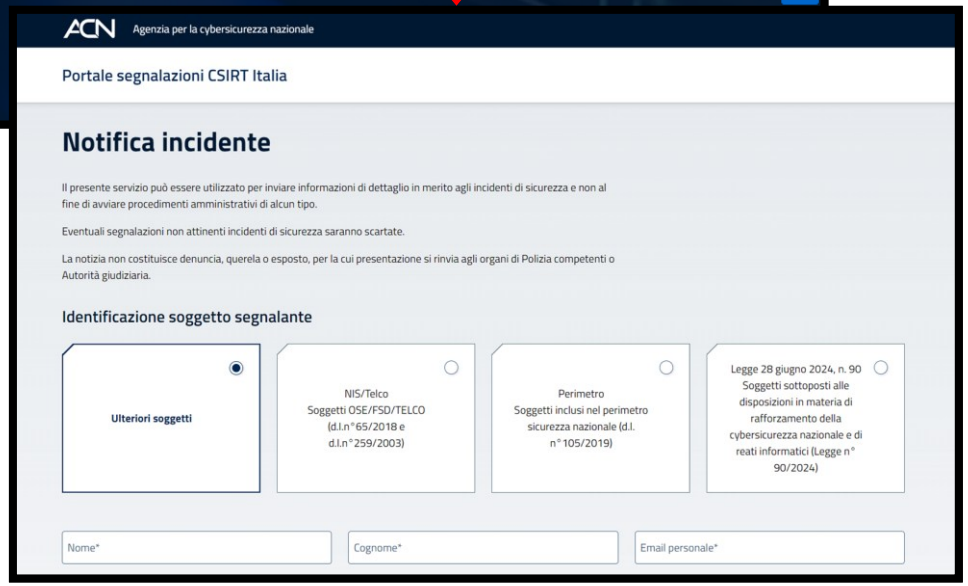
Il processo di notifica

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

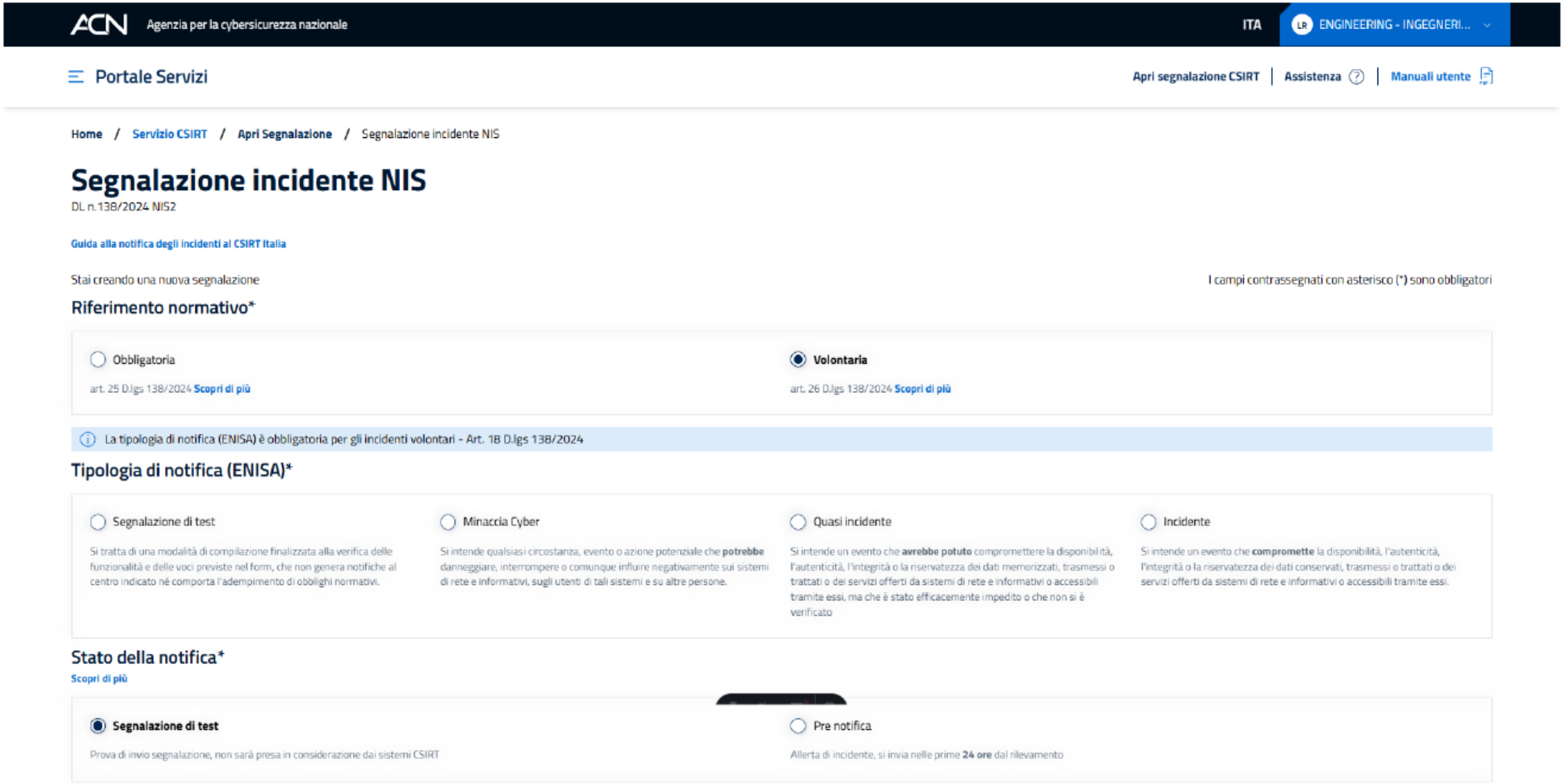
TIPOLOGIA DI NOTIFICA	COSA NOTIFICARE	QUANDO NOTIFICARE
OBBLIGATORIA	**Incidente con impatto significativo**	Entro le **24 ore** Entro **le 72 ore** – integrazione alla precedente
VOLONTARIA	**Incidente**	**Nessun limite temporale**
	Minaccia informatica	
	Near miss	

Come segnalare (oggi)

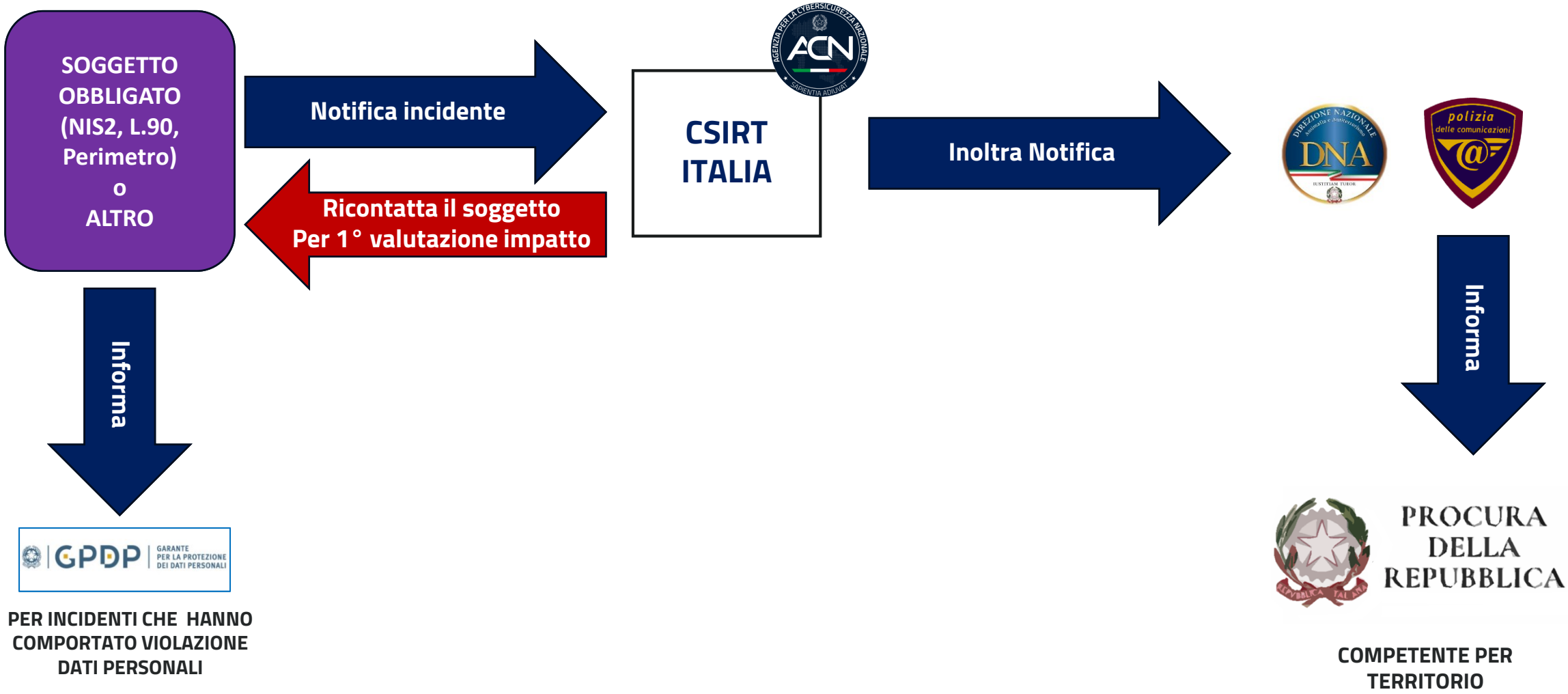




Come segnalare (dal 9 gennaio 2026)



Flusso segnalazione



PER INCIDENTI CHE HANNO COMPORTATO VIOLAZIONE DATI PERSONALI

COMPETENTE PER TERRITORIO

Procedure in caso di intervento

CSIRT ITALIA

Attiva sul posto/in remoto

CSIRT ITALIA
TEAM IR

Acquisisce con il soggetto gli elementi per definire il piano d'azione

ANALISI

CONTENIMENTO

RIPRISTINO

SOGGETTO IMPATTATO

polizia delle comunicazioni

COLLABORAZIONE FATTIVA
Flusso informativo costante
Report finale (DFIR Report)

ELEMENTI ACQUISITI

ROADMAP EVOLUTIVA

AWARENESS

INTEGRAZIONE DENUNCIA

INDIVIDUAZIONE RESPONSABILITÀ

GRAZIE


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT