NIS NEWS

# Le linee guida ACN sulla gestione degli incidenti di sicurezza informatica

Studio Previti
ASSOCIAZIONE PROFESSIONALE

# 1) PREPARAZIONE

**Politiche di sicurezza informatica**

1) **Monitoraggio eventi di sicurezza.**

2) **Risposta agli incidenti e ripristino** con almeno:

- Previsione di strumenti di rilevazione tempestiva degli incidenti
- Definizione dei livelli di servizio attesi (SL) diversi dagli SLA
- Definizione modelli di comunicazione delle minacce significative a:

a) Destinatari dei servizi che possono subire ripercussioni significative sulla fornitura dei servizi a seguito degli incidenti che comprenda eventuali misure correttive o di mitigazione da adottare

b) Pubblico sugli incidenti occorsi

3) **Continuità operativa, disaster recovery e gestione crisi**.

- Per i soggetti essenziali richiesti adempimenti più gravosi.
- Riesame annuale e aggiornamento in caso di evoluzioni normative o incidenti significativi.

# Ruoli e responsabilità

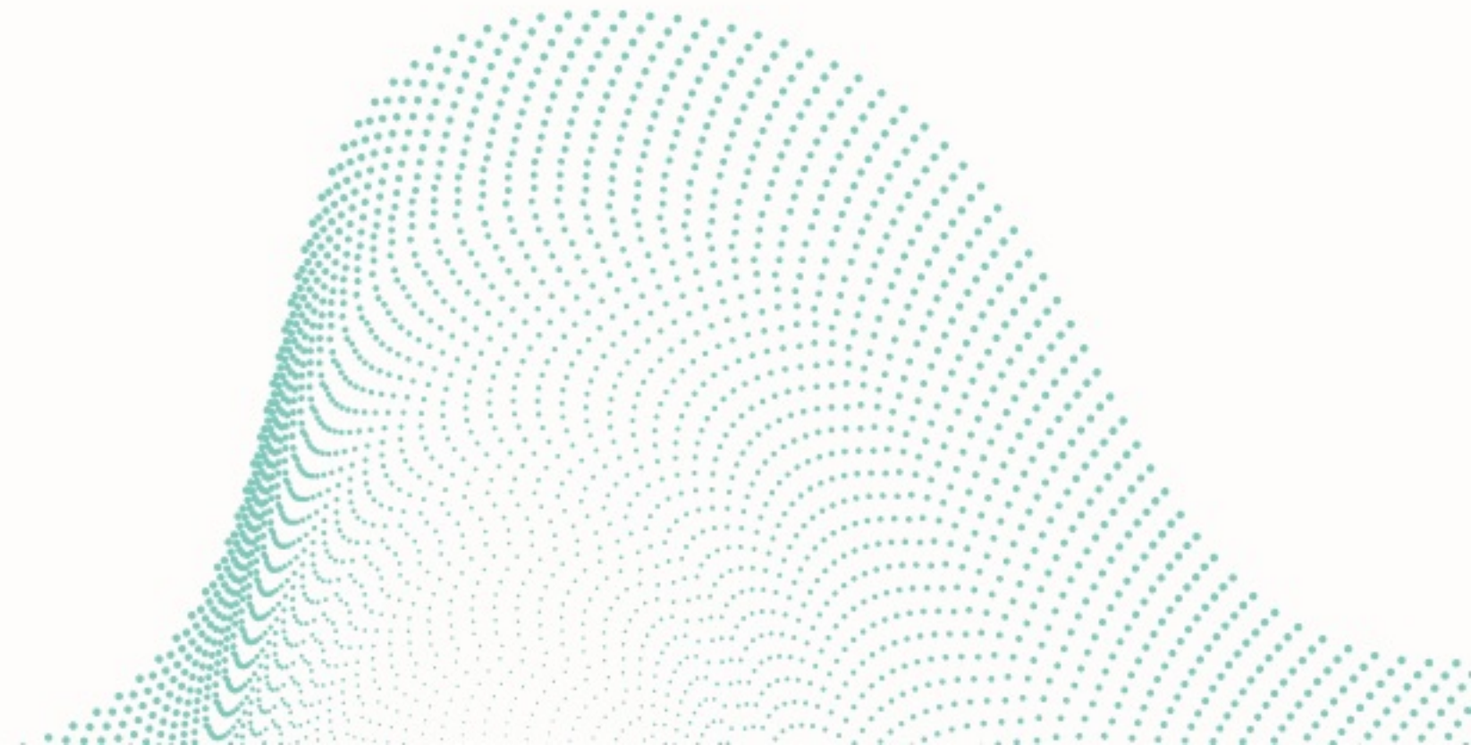
Mappatura terze parti e ruoli e responsabilità in materia di sicurezza informatica

# Inventario e identificazione

- Inventario aggiornato dei sistemi informativi e di rete (hardware, software, flussi di rete e servizi cloud). → IDENTIFICAZIONE sistemi da proteggere e determinare le priorità per le attività di risposta e ripristino.
- Identificazione vulnerabilità (*vulnerability assessment e/o penetration test* per almeno i sistemi informativi e di rete rilevanti per soggetti essenziali).

**Misure di protezione:** per ridurre probabilità incidente e/o limitarne l'impatto.

- **Tecnologiche:** pianificazione backup periodici (con copie offline) almeno per i sistemi informativi e di rete rilevanti con test di ripristino per verificare utilizzabilità dei dati di backup, acquisizione log per monitoraggio eventi di sicurezza, in particolare relativi agli accessi da remoto e/o effettuati da utenze con privilegi amministrativi, controllo accessi, firewall, previsione di sistemi di comunicazione di emergenza protetti (soggetti essenziali).



- **Organizzative**: •procedure sulle attività connesse al processo di gestione degli incidenti (a titolo esemplificativo procedure operative almeno per le politiche di backup e conservazione copie di backup, acquisizione e conservazione dei log, aggiornamento e configurazione dei sistemi perimetrali e di rilevamento degli incidenti significativi, procedure per le comunicazioni interne/esterne, ripristino. (per gli essenziali procedure ulteriori riguardo la protezione e la riutilizzabilità di backup, uso di strumenti per analisi e filtraggio sul flusso di traffico in ingresso ecc).
- Piano di formazione del personale

# 2) RILEVAMENTO

**Rilevamento:** individuare e analizzare gli eventi di sicurezza informatica rilevanti per rilevare tempestivamente gli incidenti e limitarli per impatto ed estensione.

- Esempi di eventi rilevanti (molteplici tentativi di autenticazione su diverse utenze provenienti da stesso indirizzo IP; picco di traffico da molteplici indirizzi IP, autenticazioni di hostname o indirizzi IP identificati come Indicatore di Compromissione IOC ..)

- PREVEDERE ATTIVITÀ DI MONITORAGGIO CONTINUATIVO con supporto di strumenti di tecnologie automatizzate come SIEM, SOAR o EDR;

- Definizione e documentare livelli di servizio attesi delle attività soggetto NIS (SL).

# 3) Risposta

**Costituita da diverse sottofasi** (non tutte sempre necessarie) **che non seguono un ordine lineare/cronologico.**

- **Segnalazione il cui termine decorre dal momento in cui si ha avuto EVIDENZA dell'incidente e cioè dal momento in cui il soggetto NIS dispone degli elementi oggettivi dai quali si evince che si sia verificato un incidente di sicurezza informatica** (ad esempio dall'evidenza emersa dall'analisi di una segnalazione proveniente da soggetti interni/esterni o dal sistema tecnologico di monitoraggio)

→ Obblighi di notifiche obbligatorie al CSIRT Italia tramite portale presente sul sito ACN (entro 24h pre-notifica, entro 72h notifica completa, relazioni intermedie eventuali e relazione finale dopo un mese) per gli incidenti significativi. Per la segnalazione non rileva la conoscenza della causa dell'incidente;

- **<u>Comunicazione</u>** a stakeholder e pubblico (questo su intimazione dell'ACN);

- **<u>•Investigazione:</u>** analisi forense, ricostruzione dinamica dell'incidente, individuazione della causa dell'incidente e della categoria di compromissione, della gravità e dell'impatto, valutazione supporto terze parti per gestione, acquisizione log, definizione attività risposta e ripristino.

- **<u>Contenimento</u> per limitare impatto incidente:** isolamento sistemi, blocco accessi, tracciamento attività. Queste attività devono essere tracciate.

- **<u>Eradicazione:</u>** rimozione artefatti malevoli, bonifica credenziali, patch vulnerabilità.

**NB.** Soggetto che dialoga direttamente con CSIRT Italia è il referente CSIRT, tuttavia nell'ambito di alcune decisioni potrebbe non essere competente. Per questo è importante definire ruoli e responsabilità.
Nei casi più rilevanti, le decisioni devono essere prese dagli organi di amministrazione e direttivi.

# 4) Ripristino

**Definizione di:**

- Procedure per riportare i sistemi allo stato sicuro (business continuity e disaster recovery, tracciamento dei sistemi impattati, raggiungimento degli obiettivi dell'attività di ripristino definiti nella fase di risposta, documentazione delle motivazioni delle attività di ripristino individuate.
- Mappatura parti coinvolte nelle attività di ripristino
- Monitoraggio sistemi per verificare efficacia operazioni
- Comunicazione alle parti interne interessate

# 5) Miglioramento

Nell’ottica di miglioramento continuo, prevedere Riunioni di “*lesson learned*” da cui scaturiscono:

- Esigenze di aggiornamento di politiche e procedure, implementazione di nuove logiche di rilevamento e gestione.
- Piani di continuità operativa, disaster recovery e gestione crisi.
- Valutazione periodica dell’efficacia delle misure (KPI come MTTD, MTTR).

# Studio Previti

ASSOCIAZIONE PROFESSIONALE


contatti@previti.it
www.previti.it

06.3234623
02.795587

Via Cicerone, 60 00193 Roma
Via Stradivari, 4 20131 Milano