



**DATA CONSEC**

DATA PROTECTION - CONSULTING - SECURITY

***NIS 2***  
***Prossime scadenze e***  
***adempimenti***

**Webinar, 11 febbraio 2026**

# Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- Q&A

# Agenda

## ➤ **Recepimento e attuazione e prossime scadenze**

- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- Q&A

# Recepimento e attuazione

1/2



Febbraio 23 -  
metà ottobre 24

## Recepimento

- Avvio informale di alcuni tavoli settoriali
- Adozione definitiva in CDM (7 agosto)
- Pubblicazione in Gazzetta Ufficiale (1° ottobre)
- Entrata in vigore (16 ottobre)

Metà ottobre 24 -  
metà aprile 25

## Prima fase attuativa

- [ACN e Autorità di settore] Avvio formale di tutti i tavoli settoriali
- [Soggetti] Censimento e registrazione dei soggetti (entro febbraio 2025)
- [ACN e Autorità di settore] Adozione dell'elenco dei soggetti NIS e notifica (aprile 2025)
- [ACN] Elaborazione e adozione degli obblighi di base (aprile 2025)

Metà aprile 25 -  
metà ottobre 26

## Seconda fase attuativa

- [Soggetti] Aggiornamento annuale (termine 07/2025)
- [Soggetti] Implementazione obblighi di base (termine per notifiche di incidente 01/2026)
- [ACN] Monitoraggio e supporto dell'implementazione obblighi di base
- [ACN] Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi (aprile 2026)
- [ACN] Elaborazione e adozione degli obblighi a lungo termine

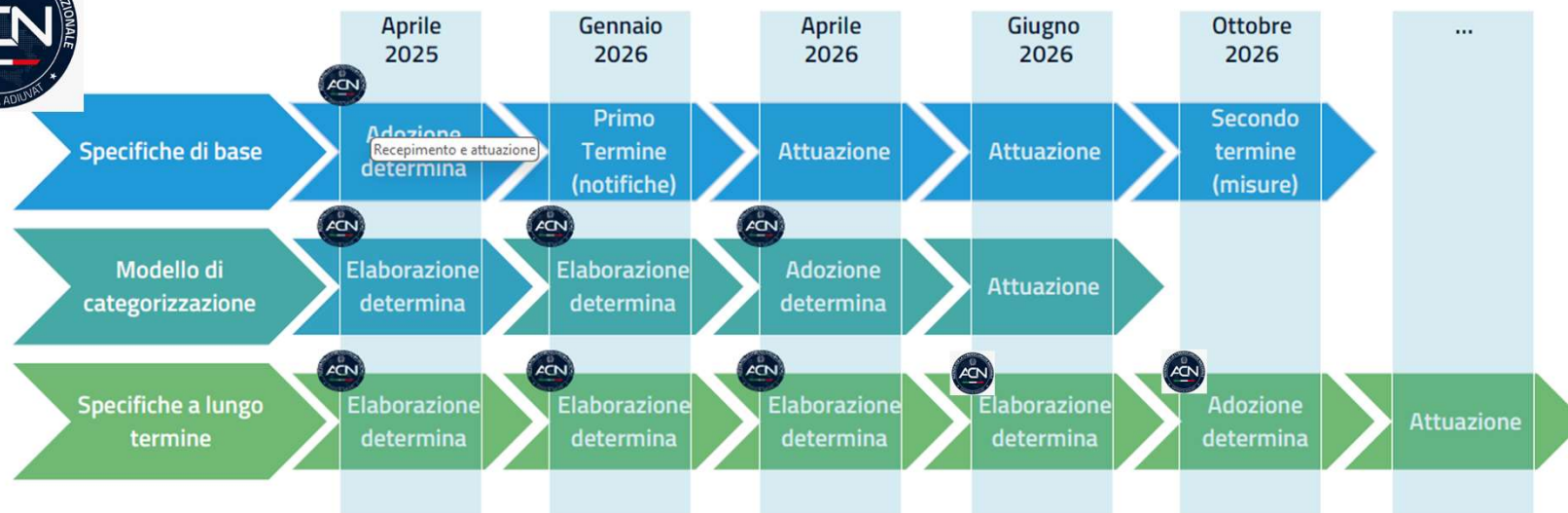
Da metà aprile 26

## Terza fase attuativa

- [Soggetti] Completamento dell'implementazione obblighi di base (termine per misure di sicurezza 10/2026)
- [Soggetti] Categorizzazione delle attività e dei servizi
- [Soggetti] Implementazione degli obblighi a lungo termine

# Recepimento e attuazione

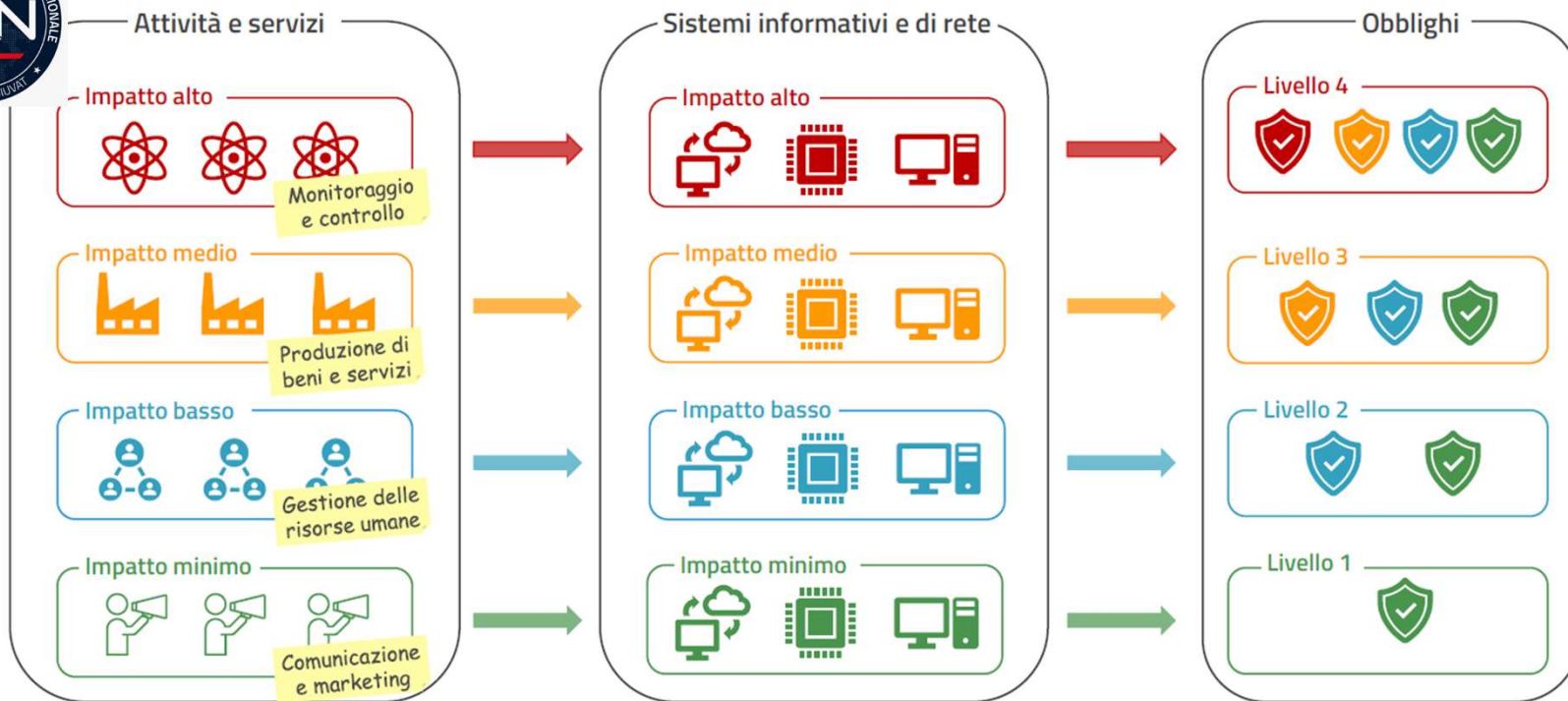
2/2



**Specifiche di base**  
Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

**Specifiche a lungo termine**  
Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine.

# Recepimento e attuazione – Proporzionalità degli obblighi



# Prossime scadenze



# Agenda

- Recepimento e attuazione e prossime scadenze
- **Applicazione della normativa – Le specifiche di base e alcuni approfondimenti**
- ☐ Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- ☐ Simulazione di una notifica di incidente di sicurezza
- ☐ Q&A

# Le misure di sicurezza di base per i soggetti essenziali e importanti

1/3

**D. Lgs. 138/2024 (Decreto NIS)**

**Art. 23**  
Organi di amministrazione e direttivi

**Art. 24**  
Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

**Art. 26**  
Obblighi in materia di notifica di incidente



**Determinazione ACN 379907 del 18 dicembre 2025**

**Allegato 1**  
Misure di sicurezza di base – soggetti importanti

**Allegato 2**  
Misure di sicurezza di base – soggetti essenziali

**Allegato 3**  
Incidenti significativi di base – soggetti importanti

**Allegato 4**  
Incidenti significativi di base – soggetti essenziali

# Le responsabilità degli organi amministrativi e direttivi

Con la locuzione “**organi di amministrazione**” e “**organi direttivi**” ci si riferisce a quegli organi che detengono il **potere di direzione del Soggetto NIS**, incluso, ove presente, il Consiglio di amministrazione (art. 1, lett. e), Determinazione ACN del 10 aprile 2025, n. 136117).

## Art. 23 Decreto NIS



**Approvano** le modalità di **implementazione** delle **misure di gestione dei rischi** per la sicurezza informatica, adottate dal Soggetto NIS



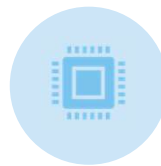
**Sovrintendono** all'**implementazione** degli **obblighi in materia di gestione del rischio** per la sicurezza informatica e di **notifica degli incidenti**, oltre che di **comunicazione di informazioni specifiche** all'Autorità competente NIS (ACN)



Sono **responsabili delle violazioni del Decreto NIS** (es: mancata osservanza degli obblighi in materia di gestione del rischio di sicurezza informativa; mancate registrazioni o comunicazioni; inottemperanza alle disposizioni della Autorità competente o mancata collaborazione con Autorità e CSIRT; ecc.)



Sono tenuti a **seguire una formazione** in materia di sicurezza informatica



**Promuovono** l'offerta periodica di una **formazione in materia di sicurezza informatica** ai dipendenti



Sono **informati** su base periodica o, se opportuno, tempestivamente **degli incidenti e delle notifiche effettuate**

# Le misure di sicurezza

## Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, Decreto NIS)

Politiche di analisi dei rischi e di sicurezza dei sistemi informativi

Gestione degli incidenti

Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi

Sicurezza catena approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con fornitori e fornitori di servizi

Sicurezza catena approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con fornitori e fornitori di servizi

Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

Pratiche di igiene informatica di base e formazione in materia di cybersicurezza

Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura

Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti

Uso di soluzione di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti

# Le misure di sicurezza di base (Det. ACN 379907/2025)



## Struttura misura

Codice

Descrizione

Requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNCS versione 2025.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

### Misure di sicurezza

- 37 per soggetti importanti ed essenziali.
- 6 per i soli soggetti essenziali.

### Requisiti

- 87 per soggetti importanti ed essenziali.
- 29 per i soli soggetti essenziali.

PR.DS-11

**I backup dei dati sono creati, protetti, mantenuti e verificati.**

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

Linee Guida NIS – Specifiche di base – Guida alla lettura (settembre 2025) [<https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base>]

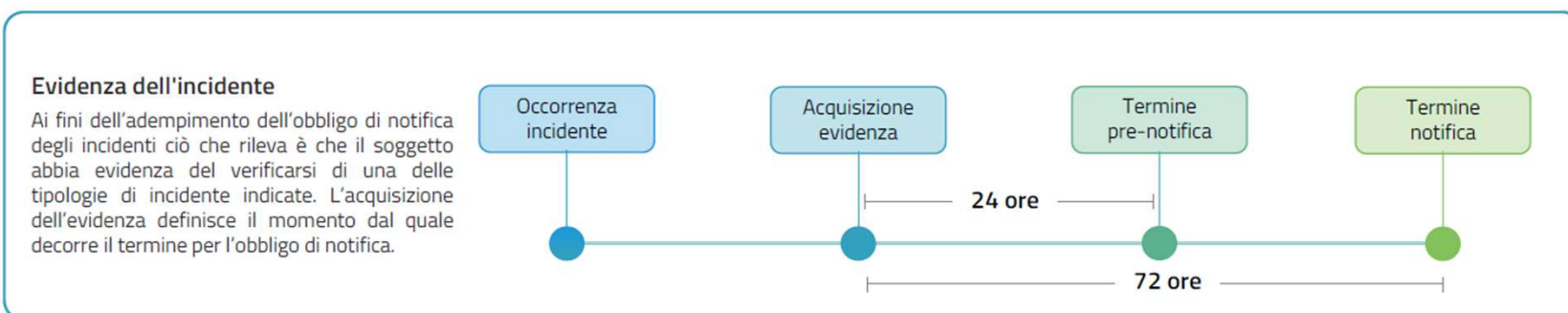
# Incidenti significativi di base



IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base di parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

■ Soggetti importanti ed essenziali

■ Solo soggetti essenziali



Linee Guida NIS – Specifiche di base – Guida alla lettura (settembre 2025) [<https://www.acn.gov.it/portale/documents/d/guest/definizione-del-processo-di-gestione-degli-incidenti-di-sicurezza-informatica>]

# Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- **Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche**
- ❑ Simulazione di una notifica di incidente di sicurezza
- ❑ Q&A

# Gestione e segnalazione degli incidenti – Cos'è un incidente di *sicurezza informatica significativo*?

## Incidente

Un evento che **compromette** la **disponibilità**, l'**autenticità**, l'**integrità** o la **riservatezza** di **dati** conservati, trasmessi o elaborati o dei **servizi offerti dai sistemi informativi e di rete** o accessibili attraverso di essi

## Quasi-incidente (*near-miss*)

Un evento che **avrebbe potuto configurare un incidente** senza che quest'ultimo si sia verificato, ivi incluso il caso in cui un incidente sia stato **efficacemente evitato**.

## Incidente di sicurezza su vasta scala

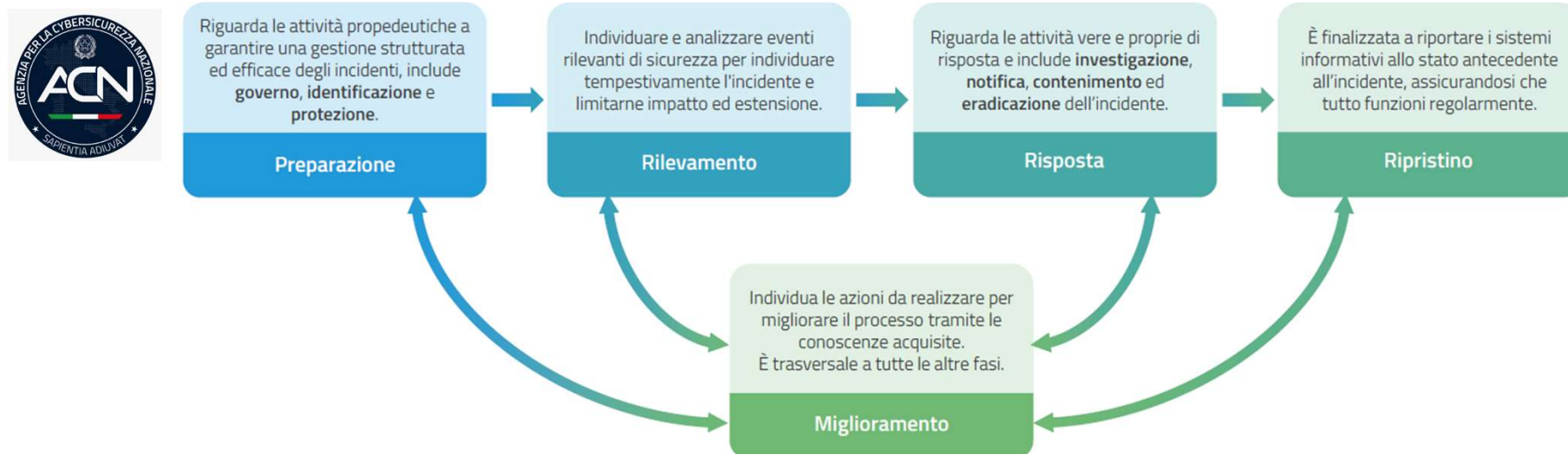
Un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di risponderci o che ha un **impatto significativo su almeno due Stati membri**.

I soggetti essenziali e importanti notificano, senza ingiustificato ritardo al **CSIRT Italia** ogni **incidente** che ha un **impatto significativo** sulla fornitura dei loro servizi, secondo modalità e tempistiche precise.

Un incidente è considerato **significativo** se:

- ha causato o è in grado di causare una **grave perturbazione operativa dei servizi** o **perdite finanziarie** per il soggetto interessato;
- ha avuto ripercussioni o è idoneo a provocare **ripercussioni su altre persone fisiche o giuridiche** causando **perdite materiali e immateriali** considerevoli.

# Modello del processo di gestione degli incidenti



# Gestione degli incidenti – Preparazione-Governo



In questa sotto-fase, il soggetto definisce il quadro strategico e organizzativo per la gestione degli incidenti, provvedendo, in particolare, all'elaborazione delle **politiche di sicurezza informatica** e all'assegnazione dei **ruoli e delle responsabilità** per le attività del processo di gestione degli incidenti.

## Misure di sicurezza

- ✓ **GV.PO-01:** La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.
- ✓ **GV.PO-02:** La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.
- ✓ **GV.RR-02:** I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.
- ✓ **GV.SC-02:** I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.

# Gestione degli incidenti – Preparazione-Identificazione



In questa sotto-fase è acquisita una conoscenza del contesto operativo al fine di pianificare in modo efficace la risposta agli incidenti. Le attività di *identificazione* riguardano, ad esempio, l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità.

## Misure di sicurezza

- ✓ **ID.AM-01:** Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione..
- ✓ **ID.AM-02:** Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione..
- ✓ **ID.AM-03:** Sono mantenute le rappresentazioni delle comunicazioni di rete e dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.
- ✓ **ID.AM-04:** È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi cloud.

# Gestione degli incidenti – Preparazione-Protezione



In questa sotto-fase sono stabilite le misure di protezione volte a ridurre la probabilità e limitare l'impatto degli incidenti. Ridurre la probabilità, e dunque il numero, di incidenti consente di dedicare maggiori risorse alla risposta degli incidenti più critici e complessi, mentre limitare l'impatto dell'incidente rende generalmente meno complesse le attività di contenimento ed eradicazione, oltre a mitigare le conseguenze dell'attacco, in termini non solo di sistemi informativi e di rete compromessi, ma anche operativi, economici e reputazionali.

## Misure di sicurezza

- ✓ **PR.DS-11:** I backup dei dati sono creati, protetti, mantenuti e verificati.
- ✓ **PR.PS-04:** I registri di log sono generati e resi disponibili per il monitoraggio continuo..
- ✓ **PR.IR-01:** Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.
- ✓ **PR-IR-03:** Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.
- ✓ **PR.AT-01:** Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.
- ✓ **PR-AT-02:** Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.

# Gestione degli incidenti – Rilevamento



La fase di rilevamento è finalizzata a individuare e analizzare gli **eventi rilevanti per la sicurezza informatica** con l'obiettivo di individuare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione.

Gli *eventi rilevanti per la sicurezza informatica* sono eventi di natura intenzionale o accidentale che compromettono o potrebbero compromettere la sicurezza dei sistemi informativi e di rete e che necessitano pertanto di un'analisi (triage) al fine di verificare se si tratta di un incidente.

Nel caso in cui l'analisi di un evento rilevante per la sicurezza informatica abbia effettivamente determinato che è relativo a un incidente, viene dichiarato l'incidente e si passa alla successiva fase di risposta.

## Misure di sicurezza

- ✓ **DE.CM-01:** Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.
- ✓ **DE.CM-09:** L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

# Gestione degli incidenti – Risposta



La fase di risposta inizia nel momento in cui è stato dichiarato l'incidente e rappresenta la fase centrale del processo di gestione degli incidenti ed è costituita dalla seguenti sotto-fasi:

- **segnalazione:** si procede a notificare l'incidente alle autorità competenti e a comunicarlo alle parti, interne ed esterne, interessate;
- **investigazione:** viene esaminato in modo approfondito l'incidente con l'obiettivo di ricostruire possibilmente l'intera sequenza degli eventi occorsi (cosiddetta cyber kill chain), individuare la causa dell'incidente e valutare l'estensione della compromissione.
- **contenimento:** viene circoscritto il perimetro dell'attacco in modo da limitare l'impatto dell'incidente ed evitarne l'estensione ad altri sistemi informativi e di rete;
- **eradicazione:** viene rimossa ogni capacità di controllo e persistenza nella rete da parte dell'attaccante.

## Misure di sicurezza

- ✓ **RS.MA-01:** Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

# Gestione degli incidenti – Ripristino



La fase di ripristino è finalizzata a riportare i sistemi informativi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente e riguarda, ad esempio, la creazione di golden/clean image, la reinstallazione dei sistemi a partire dalle golden/clean image, il ricollegamento in rete dei sistemi informativi e di rete bonificati, il monitoraggio dei sistemi per verificare l'efficacia delle attività.

## Misure di sicurezza

- ✓ **RC.RP-01:** La parte del piano di risposta agli incidenti relativa al ripristino viene eseguita una volta avviata dal processo di risposta agli incidenti.
- ✓ **RC.CO-03:** Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.

# Gestione degli incidenti – Miglioramento



La fase di miglioramento si estende per l'intero ciclo di vita del processo ed è finalizzata a potenziare la capacità di gestione degli incidenti e riguarda principalmente attività come l'analisi post-incidente al fine di individuare eventuali carenze e valutare l'efficacia della risposta.

A tal fine sono organizzate le cosiddette riunioni di lesson learned in cui si ha l'opportunità di trarre insegnamenti, alla luce di quanto emerso durante la gestione dell'incidente, dalle azioni intraprese e dalla loro efficacia e di individuare gli interventi correttivi e di potenziamento

## Misure di sicurezza

- ✓ **ID.IM-01:** Sono identificati miglioramenti in esito alle valutazioni.
- ✓ **ID-IM-04:** I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

# Gestione e segnalazione degli incidenti – Esempio di piano di gestione degli incidenti informatici

- 1 Fasi e procedure di gestione degli incidenti:**
  - a) **segnalazione/rilevazione** dell'evento e relativa tracciatura (data e ora dell'evento e della segnalazione; elenco degli asset coinvolti; servizi impattati; descrizione del problema);
  - b) **analisi e classificazione** dell'evento a seconda del livello di rilevanza, secondo metriche definite;
  - c) identificazione e adozione delle **strategie di contenimento ritenute più efficaci**, finalizzate a minimizzare ogni ulteriore conseguenza e ad evitare un peggioramento della situazione;
  - d) **ripristino**, in particolare con riguardo al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti dall'incidente di sicurezza;
  - e) **lesson learned** e valutazione dell'eventuale revisione di politiche, procedure, processi, strumenti, modalità, compresa l'analisi del rischio
- 2** Fasi e procedure per la **notifica dell'incidente alle autorità** competenti e per la **predisposizione e trasmissione delle correlate relazioni**, secondo le modalità e le tempistiche individuate dalle normative vigenti, in particolare il Decreto NIS
- 3** **Ruoli e responsabilità nella gestione degli incidenti**, comprese quelle degli organi di amministrazione e gestione della Società (CdA)
- 4** **Informazioni di contatto** per la segnalazione degli incidenti, interne e, ove necessario, esterne
- 5** Modalità previste per la **comunicazione interna** relativamente agli incidenti, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi
- 6** Procedure per **comunicare senza ingiustificato ritardo**, anche quando intimato dall'autorità competente:
  - a) ai **destinatari dei servizi**, gli **incidenti significativi** che possono ripercuotersi negativamente sulla fornitura degli stessi;
  - b) ai **destinatari dei servizi** potenzialmente interessati da una **minaccia informatica significativa**, le misure o azioni correttive o di mitigazione che questi possono adottare in risposta a detta minaccia;
  - c) al pubblico, gli incidenti occorsi
- 7** **Reportistica** da utilizzare per la **documentazione dell'incidente**, tenuto anche conto dei modelli eventualmente messi a disposizione dall'autorità competente.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Tempistiche e caratteristiche

**a** senza ingiustificato ritardo, e comunque **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di **atti illegittimi o malevoli** o può avere un **impatto transfrontaliero**

**b** senza ingiustificato ritardo, e comunque **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **notifica dell'incidente** che, ove possibile, **aggiorni le informazioni** di cui alla lettera a) e indichi una **valutazione iniziale** dell'incidente significativo, comprensiva della sua **gravità** e del suo **impatto**, nonché, ove disponibili, gli **indicatori di compromissione**

**c** su **richiesta del CSIRT Italia**, una **relazione intermedia** sui pertinenti aggiornamenti della situazione

una **relazione finale entro un mese** dalla trasmissione della notifica di cui alla lettera b), che comprenda:

- d**
- una **descrizione dettagliata** dell'incidente, inclusi la sua gravità e il suo impatto;
  - il **tipo di minaccia** o la causa originale (**root cause**) che ha probabilmente innescato l'incidente;
  - le **misure di attenuazione** adottate e in corso;
  - ove noto, l'**impatto transfrontaliero** dell'incidente.

**e** in caso di **incidente in corso** al momento della trasmissione della relazione finale di cui alla lettera d), una **relazione mensile sui progressi** e una **relazione finale entro un mese dalla conclusione** della gestione dell'incidente.

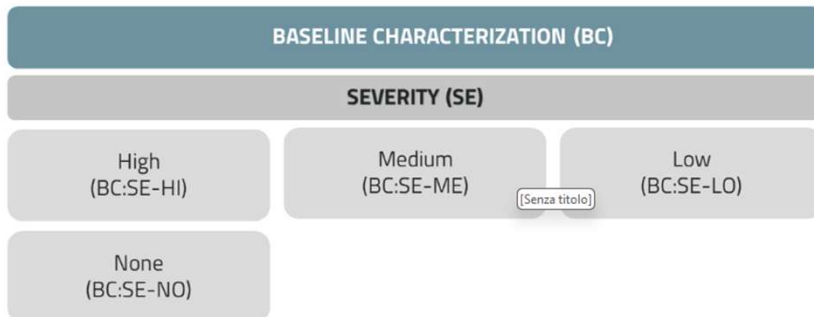
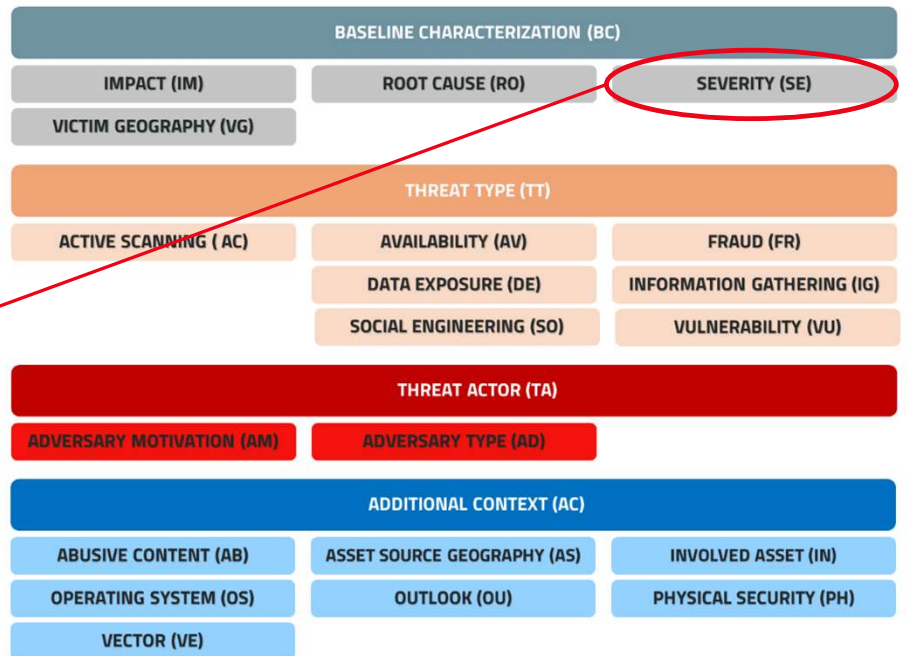
In aggiunta all'obbligo di notifica degli incidenti significativi, possono essere trasmesse, **su base volontaria**, notifiche **al CSIRT Italia** da parte dei:

- a) soggetti essenziali e soggetti importanti, per quanto riguarda gli **incidenti diversi da quelli significativi**, le **minacce informatiche** e i **quasi-incidenti**;
- b) soggetti **diversi, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del Decreto NIS**, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.

# Focus – Analisi e classificazione degli eventi



[https://www.acn.gov.it/portale/documents/20119/552690/ACN\\_Tassonomia\\_Cyber\\_CLEAR.pdf/9595cc35-1c0b-4007-07b2-8f0468e5b82e?t=1731598519616](https://www.acn.gov.it/portale/documents/20119/552690/ACN_Tassonomia_Cyber_CLEAR.pdf/9595cc35-1c0b-4007-07b2-8f0468e5b82e?t=1731598519616)



# Le modalità di intervento del CSIRT Italia in caso di notifica di incidenti di sicurezza informatica

## Riscontri, consulenza e supporto tecnico

Senza ingiustificato ritardo e ove possibile **entro 24 ore dal ricevimento della pre-notifica**, il CSIRT Italia fornisce una **risposta al soggetto notificante**, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, **orientamenti** o **consulenza** sull'attuazione di **possibili misure tecniche di mitigazione**. Su richiesta del soggetto notificante, il CSIRT Italia fornisce **ulteriore supporto tecnico**.

## Orientamenti su segnalazioni alle istituzioni

Qualora si sospetti che l'incidente significativo abbia **carattere criminale**, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla **segnalazione dell'incidente significativo**, all'organo centrale del **Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione** (Autorità di contrasto).

## Indicazioni su ulteriori comunicazioni

Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i **soggetti essenziali** e i **soggetti importanti comunicano**, senza ingiustificato ritardo, **ai destinatari dei loro servizi** gli **incidenti significativi** che possono **ripercuotersi negativamente sulla fornitura di tali servizi**.

I **soggetti essenziali** e i **soggetti importanti**, se ritenuto opportuno e **qualora possibile**, sentito il CSIRT Italia, **comunicano** senza ingiustificato ritardo, ai **destinatari dei loro servizi** che sono potenzialmente **interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione** che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari **anche la natura di tale minaccia** informatica significativa.

## Gestione delle segnalazioni volontarie

Il CSIRT Italia:

- tratta le notifiche volontarie applicando la **procedura ordinaria**;
- tratta le **notifiche di incidenti significativi prioritariamente** rispetto alle notifiche volontarie;
- tratta le **notifiche volontarie** soltanto qualora ciò **non costituisca un onere sproporzionato o eccessivo**.

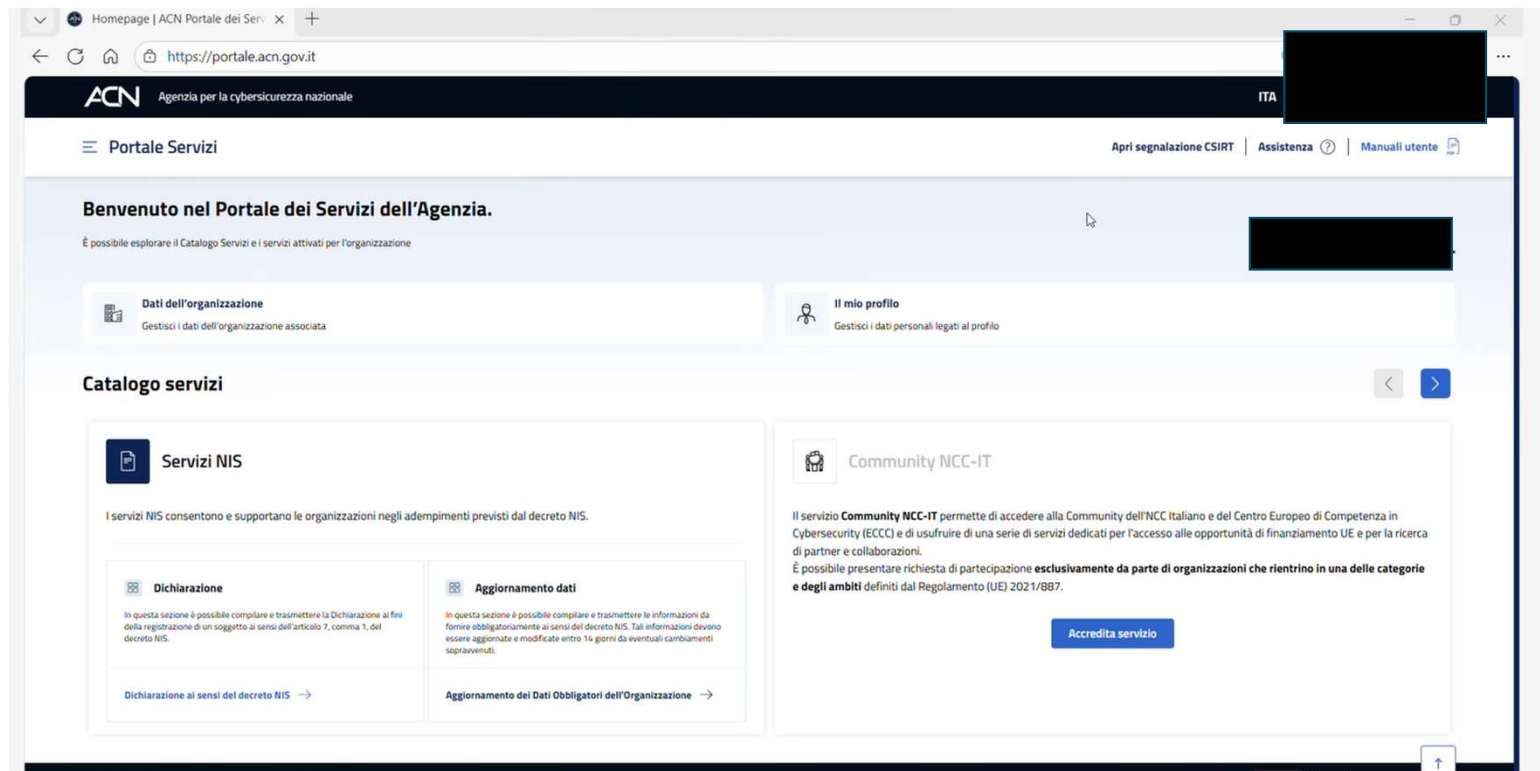
# Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- **Simulazione di una notifica di incidente di sicurezza**

☐ Q&A

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

1/37



The screenshot displays the ACN (Agenzia per la cybersicurezza nazionale) Portale dei Servizi. The page is in Italian and shows the following elements:

- Header:** ACN logo, "Agenzia per la cybersicurezza nazionale", and language selector "ITA".
- Navigation:** "Portale Servizi" menu, "Apri segnalazione CSIRT", "Assistenza", and "Manuali utente".
- Welcome Message:** "Benvenuto nel Portale dei Servizi dell'Agenzia." with a sub-message: "È possibile esplorare il Catalogo Servizi e i servizi attivati per l'organizzazione".
- User Management:** "Dati dell'organizzazione" (Gestisci i dati dell'organizzazione associata) and "Il mio profilo" (Gestisci i dati personali legati al profilo).
- Catalogo servizi:** A section with navigation arrows containing:
  - Servizi NIS:** A section for NIS services. It states: "I servizi NIS consentono e supportano le organizzazioni negli adempimenti previsti dal decreto NIS." It contains two sub-sections:
    - Dichiarazione:** "In questa sezione è possibile compilare e trasmettere la Dichiarazione ai fini della registrazione di un soggetto ai sensi dell'articolo 7, comma 1, del decreto NIS." with a link "Dichiarazione ai sensi del decreto NIS →".
    - Aggiornamento dati:** "In questa sezione è possibile compilare e trasmettere le informazioni da fornire obbligatoriamente ai sensi del decreto NIS. Tali informazioni devono essere aggiornate e modificate entro 14 giorni da eventuali cambiamenti sopravvenuti." with a link "Aggiornamento dei Dati Obbligatorie dell'Organizzazione →".
  - Community NCC-IT:** A section for the NCC-IT community. It states: "Il servizio **Community NCC-IT** permette di accedere alla Community dell'NCC Italiano e del Centro Europeo di Competenza in Cybersecurity (ECCC) e di usufruire di una serie di servizi dedicati per l'accesso alle opportunità di finanziamento UE e per la ricerca di partner e collaborazioni. È possibile presentare richiesta di partecipazione **esclusivamente da parte di organizzazioni che rientrano in una delle categorie e degli ambiti** definiti dal Regolamento (UE) 2021/887." with an "Accredita servizio" button.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 2/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Home / Servizio CSIRT / Apri Segnalazione

### Apri Segnalazione

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

Il presente servizio può essere utilizzato per inviare informazioni di dettaglio in merito agli eventi di sicurezza e non al fine di avviare procedimenti amministrativi di alcun tipo.  
Eventuali segnalazioni non attinenti le finalità del Portale CSIRT 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

Pubblica amministrazione / impresa / Cittadino

NIS  
di. n° 138/2024

Perimetro Soggetti inclusi nel perimetro sicurezza nazionale (d.l. n° 105/2019)

**i** Ai sensi del [Decreto Legge 138/2024](#), i soggetti NIS - medie e grandi imprese, in alcuni casi anche le piccole e microimprese, e le Pubbliche amministrazioni a cui si applica la nuova normativa - sono tenuti a notificare al CSIRT Italia gli incidenti significativi di base stabiliti.

**Invia**

Il trattamento dei dati personali per le finalità del servizio verrà effettuato nel rispetto della vigente normativa in materia di protezione dei dati personali secondo l'informativa consultabile al [presente link](#).

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 3/37

The screenshot shows a web browser window with the URL <https://portale.acn.gov.it/csirt/report/nis>. The page header includes the ACN logo (Agenzia per la cybersicurezza nazionale) and the language 'ITA'. The main navigation bar contains 'Portale Servizi' and links for 'Apri segnalazione CSIRT', 'Assistenza', and 'Manuali utente'. The breadcrumb trail is 'Home / Servizio CSIRT / Apri Segnalazione / Segnalazione incidente NIS'. The main heading is 'Segnalazione incidente NIS' with the reference 'DL n.138/2024 NIS2'. Below this is a link to the 'Guida alla notifica degli incidenti al CSIRT Italia'. A note states: 'I campi contrassegnati con asterisco (\*) sono obbligatori'. A prompt asks: 'Scegli se vuoi creare una nuova segnalazione o integrare una precedente\*'. There are two radio buttons: the first is selected and labeled 'Nuova segnalazione', and the second is labeled 'Modifica una bozza oppure integra una segnalazione già inviata'. At the bottom left is an 'Annulla segnalazione' button, and at the bottom right is a blue 'Procedi' button.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 4/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Home / Servizio CSIRT / Apri Segnalazione / Segnalazione incidente NIS

### Segnalazione incidente NIS

DL n.138/2024 NIS2

Guida alla notifica degli incidenti al CSIRT Italia

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](#)

**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

La notifica è valida ai fini previsti dalla Legge 28 giugno 2024, n. 90.

La notifica è originata da una comunicazione del CSIRT Italia?

Se si specificare quale

Es. CSIRT-ITA #CXXXXX

# Notifiche a CSIRT degli incidenti di sicurezza informatica

## – Una simulazione

5/37

The screenshot shows the ACN (Agenzia per la cybersicurezza nazionale) portal. The main content is a modal window titled "Notifica obbligatoria ai sensi art. 25 D.lgs 138/2024". The text within the modal is as follows:

**Art.25 - Obblighi in materia di notifica di incidente**

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.
2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente.
3. La notifica non espone il soggetto che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.
4. Un incidente è considerato significativo se:
  - ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
  - ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.
5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:
  - senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
  - senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
  - su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
  - una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:
    - una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
    - il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
    - le misure di attenuazione adottate e in corso;
    - ove noto, l'impatto transfrontaliero dell'incidente;
  - in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.
6. In deroga a quanto previsto dal comma 5, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.
7. In deroga a quanto previsto dall'articolo 15, comma 4, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera a), il CSIRT Italia fornisce una risposta al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, ove opportuno, orientamenti o consulenze sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico.
8. In caso di incidente significativo che abbia carattere criminale, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla segnalazione dell'incidente significativo, all'organo centrale del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto).
9. Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

Seleziona una delle opzioni seguenti.

La notifica è originata da una comunicazione del CSIRT Italia?

Se si, specificare quale

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 6/37

The screenshot shows a web browser at the URL <https://portale.acn.gov.it/csirt/report/nis>. The page header includes the ACN logo (Agenzia per la cybersicurezza nazionale) and the language 'ITA'. The main navigation bar contains 'Portale Servizi', 'Apri segnalazione CSIRT', 'Assistenza', and 'Manuali utente'. The breadcrumb trail is 'Home / Servizio CSIRT / Apri Segnalazione / Segnalazione incidente NIS'. The main heading is 'Segnalazione incidente NIS' with the reference 'DL n.138/2024 NIS2' and a link to the 'Guida alla notifica degli incidenti al CSIRT Italia'. A note states 'I campi contrassegnati con asterisco (\*) sono obbligatori'. The 'Riferimento normativo\*' section has two radio buttons: 'Obbligatoria' (selected) with reference 'art. 25 D.lgs 138/2024' and 'Volontaria' with reference 'art. 26 D.lgs 138/2024'. The 'Stato della notifica\*' section has a radio button for 'Pre notifica' (selected) with the description 'Allerta di incidente, si invia nelle prime 24 ore dal rilevamento'. Below this are two checkboxes: 'La notifica è valida ai fini previsti dalla Legge 28 giugno 2024, n. 90.' and 'La notifica è originata da una comunicazione del CSIRT Italia?'. A text input field is labeled 'Se si specificare quale' with an example 'Es. CSIRT-ITA #CXXXXX'.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

7/37

https://portale.acn.gov.it/csirt/report/nis

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT Assistenza Manuali utente

La notifica è originata da una comunicazione del CSIRT Italia? Se si specificare quale  
Es. CSIRT-ITA #CXXXXX

**Sezione A** Dati dell'organizzazione

**Generalità dell'organizzazione**

**Denominazione Sociale\*** [REDACTED] **Tipologia di soggetto\*** [REDACTED]  
Identificazione Essenziale o Importante ai sensi del decreto NIS2

**Settori di competenza\*** [REDACTED] **Codice fiscale\*** [REDACTED]  
1 elemento selezionato  
Identificazione del settore di competenza ai sensi del decreto NIS2  
Almeno un campo tra Piva e Codice Fiscale deve essere valorizzato

**Partita IVA** [REDACTED] **Codice IPA** [REDACTED]  
Almeno un campo tra Piva e Codice Fiscale deve essere valorizzato  
Identificativo Ufficio Pubblica Amministrazione

**Codice identificativo unico (NIS)\*** [REDACTED] **Domicilio digitale\*** [REDACTED]  
Identificativo ENISA ai sensi dell'individuazione del soggetto NIS2  
Indirizzo PEC rappresentativo della tua organizzazione così come definito in IPA o INAD

Presente solo una organizzazione associata all'utenza.

**Sezione B** - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione B** Dati del segnalante e referente CSIRT

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 8/37

https://portale.acn.gov.it/csirt/report/nis

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT Assistenza Manuali utente

Sezione B - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione B** Dati del segnalante e referente CSIRT

**Fornire le generalità del segnalante**

Nome e cognome\* [redacted] Ruolo e funzione rivestiti\* [redacted]

Email PEC/PEO\* [redacted] Recapito telefonico\* [redacted]

Indirizzo di posta elettronica ordinaria oppure certificata

[redacted] +39 Recapito telefonico alternativo

**Dati del Referente CSIRT**  
I dati di contatto del Referente CSIRT sono quelli comunicati tramite adempimenti NIS.

Nome e cognome [redacted] Codice fiscale [redacted]

Email PEC/PEO [redacted]

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

9/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Email PEC/PEO

Sezione C - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione C Descrizione dell'incidente

Fornire le informazioni dell'incidente

Stato dell'incidente all'atto della notifica\*  
Stato di gestione dell'incidente

Codice identificativo interno o nome dell'incidente

Data del rilevamento\*  
Ora del rilevamento\*

Data in cui si è verificato l'incidente/evento  
Ora in cui si è verificato l'incidente/evento

Descrizione\*  
0 / 1000

Se noto lo sfruttamento di una vulnerabilità specificare quale

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 10/37

The screenshot displays the ACN (Agenzia per la cybersicurezza nazionale) reporting portal. The browser address bar shows the URL <https://portale.acn.gov.it/csirt/report/nis>. The page header includes the ACN logo and the text "Agenzia per la cybersicurezza nazionale". The main navigation bar contains "Portale Servizi" and links for "Apri segnalazione CSIRT", "Assistenza", and "Manuali utente".

The form is titled "Sezione C - Presenti campi obbligatori da riempire oppure il formato non è corretto." and is labeled "Sezione C Descrizione dell'incidente". It contains the following fields:

- Email PEC/PEO:** art.lleshi@gea.com
- Stato dell'incidente all'atto della notifica\*:** A dropdown menu with options: "In corso non gestito" (selected), "In corso di gestione", and "Concluso".
- Codice identificativo interno o nome dell'incidente:** An empty text input field.
- Orta del rilevamento\*:** A date and time picker.
- Orta in cui si è verificato l'incidente/evento:** A date and time picker.
- Descrizione\*:** A large text area for describing the incident.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 11/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuall utente

Il campo è obbligatorio. 0 / 1000

Se noto lo sfruttamento di una vulnerabilità specificare quale

0 / 1000

È stata identificata la causa dell'incidente

Descrizione delle cause

0 / 1000

Com'è stato rilevato l'incidente/evento?\*

I

0 / 1000

Si è supportati da un supporto specialistico da parte di un fornitore esterno?

Specificare il nome dell'azienda

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 12/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT Assistenza Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione D** Tipologia di incidente

**Fornire le informazioni sulla tipologia dell'incidente**

Classificazione dell'incidente\*

Tassonomia NIS\*

Tassonomia NIS: Scopri di più

Seleziona una o più Tassonomie ACN\*

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise**  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise**  
Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.
- Impact - Availability**  
Eventi nei quali le attività malevole condotte da un attaccante hanno causato effetti sulla disponibilità del sistema o servizio erogato. Specificare anche il predicato Availability.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 13/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT | Assistenza | Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione D Tipologia di incidente

Fornire le informazioni sulla tipologia dell'incidente  
Classificazione dell'incidente\*

Seleziona una voce

- Cybersquatting
- Danno fisico
- Defacement
- Diffusione malware tramite email
- Distribuzione di malware
- DoS/DDoS

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.
- Impact - Availability  
Eventi nei quali le attività malevole condotte da un attaccante hanno causato effetti sulla disponibilità del sistema o servizio erogato. Specificare anche il predicato Availability.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

14/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione D Tipologia di incidente

Fornire le informazioni sulla tipologia dell'incidente

Classificazione dell'incidente\*

Seleziona una voce

- DoS/DDoS
- Esfiltrazione
- Esposizione dati
- Flusso crittografico
- Furto di identità

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.
- Impact - Availability

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 15/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione D Tipologia di incidente

Fornire le informazioni sulla tipologia dell'incidente

Classificazione dell'incidente\*

Seleziona una voce

- Guasto
- Hacking
- Intrusione tramite credenziali valide
- Malfunzionamento HW
- Malfunzionamento SW

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise

Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

16/37

ACN Agenzia per la cybersicurezza nazionaleITA

☰ Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente 📄

🔔 Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione D** Tipologia di incidente ^

**Fornire le informazioni sulla tipologia dell'incidente**

Classificazione dell'incidente\*

Seleziona una voce ^

- Man-in-the-middle
- Misconfiguration
- Perdita o furto di materiale
- Phishing
- Ransomware

Cerca una parola chiave della tipologia di evento cyber 🔍

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 17/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT Assistenza ? Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione D Tipologia di incidente

**Fornire le informazioni sulla tipologia dell'incidente**  
Classificazione dell'incidente\*

Seleziona una voce

- SCADA/ICS attack
- Scansione attiva su credenziali
- Scansioni attive sul perimetro di rete
- Sfruttamento di vulnerabilità note o di vulnerabilità in componenti, servizi e/o applicazioni
- Sfruttamento vulnerabilità

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 18/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione D Tipologia di incidente

Fornire le informazioni sulla tipologia dell'incidente

Classificazione dell'incidente\*

Seleziona una voce

- Smishing
- Spam e scam
- Spear phishing
- Supply chain
- Typosquatting

Cerca una parola chiave della tipologia di evento cyber

Elementi presenti: 219 Selezionati: 0

- Impact - Account Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.
- Impact - Application Compromise  
Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

19/37

ACN Agenzia per la cybersicurezza nazionaleITA

☰ Portale ServiziApri segnalazione CSIRT | Assistenza ? | Manuali utente 📄

ⓘ Sezione D - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione D** Tipologia di incidente ^

**Fornire le informazioni sulla tipologia dell'incidente**

Classificazione dell'incidente\* v

\* il campo è obbligatorio.

**Tassonomia NIS\***

Seleziona una voce ^

- IS-1 - Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale
- IS-2 - Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale
- IS-3 - Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01
- IS-4 - Il soggetto NIS ha evidenza, anche sulla base dei parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale

Elementi presenti: 219 Selezionati: 0

Impact - Account Compromise

Eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset.

Impact - Application Compromise

Eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 20/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Sezione E - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione E** Descrizione Impatto

Fornire le informazioni sui servizi impattati

Indicazione della tipologia di impatto\* Il servizio ha mantenuto operatività anche durante l'interruzione?\*

Scopri di più

Servizi coinvolti\*

Cerca una parola chiave della tassonomia dei servizi ACN

Elementi presenti: 56 Selezionati: 0

- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Servizi di connettività interna
- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Servizi di connettività ad internet
- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Rete di accesso
- Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi Data Center on premise
- Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi di Hosting e Housing

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

21/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Sezione E - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione E** Descrizione Impatto

Fornire le informazioni sui servizi impattati

Indicazione della tipologia di impatto\*

Seleziona una voce

- Economico-finanziario
- Operativo
- Reputazionale
- Proprietà intellettuale
- Salute e sicurezza delle persone
- [...]

Il servizio ha mantenuto operatività anche durante l'interruzione?\*

Il servizio ha mantenuto operatività anche durante l'interruzione?\*

Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Servizi di connettività ad internet

Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Rete di accesso

Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi Data Center on premise

Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi di Hosting e Housing

# Notifiche a CSIRT degli incidenti di sicurezza informatica - Una simulazione

22/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Sezione E - Presenti campi obbligatori da riempire oppure il formato non è corretto.

Sezione E Descrizione Impatto

Fornire le informazioni sui servizi impattati

Indicazione della tipologia di impatto\*

Il campo è obbligatorio.  
Scopri di più

Servizi coinvolti\*

Cerca una parola chiave della tassonomia dei servizi ACN

Elementi presenti: 56 Selezionati: 0

- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Servizi di connettività interna
- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Servizi di connettività ad internet
- Servizi Infrastrutturali - Servizi di trasmissione e distribuzione dati - Rete di accesso
- Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi Data Center on premise
- Servizi Infrastrutturali - Servizi Cloud e Data Center - Servizi di Hosting e Housing

Il servizio ha mantenuto operatività anche durante l'interruzione?\*

Seleziona una voce

- Sì, tutte le funzionalità erano disponibili
- Sì, ma alcune funzionalità non erano disponibili
- Sì, ma molte funzionalità non erano disponibili
- No
- L'incidente non ha causato interruzione del servizio

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 23/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Indicazione della tipologia di impatto\* Il servizio ha mantenuto operatività anche durante l'interruzione?\*

Scopri di più

Servizi coinvolti\*

Cerca una parola chiave della tassonomia dei servizi ACN

Elementi presenti: 56 Selezionati: 0

- Servizi Applicativi - Applicazioni di gestione dati - Gestione di dati non strutturati
- Servizi Applicativi - Applicazioni di gestione dati - Sistemi di business intelligence
- Servizi Applicativi - Applicazioni di gestione dati - Altro
- Servizi Applicativi - Applicazioni di gestione e supporto - Applicazioni di Gestione Documentale
- Servizi Applicativi - Applicazioni di gestione e supporto - Applicazioni di Gestione Accessi

Altri servizi impattati non presenti nella selezione

Presenti impatti transfrontalieri

0 / 1000

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 24/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Tipologie di Servizi impattati  Descrivere servizi e funzioni coinvolti

IP Privato  FQDN

L'incidente ha avuto un impatto significativo sulla continuità dei servizi da questi erogati?  
 L'interruzione per la tipologia di servizio indicato è ancora in corso?

Se sì, descrivere quali  
Descrivere i servizi che hanno avuto impatto

Data di inizio interruzione  Ora di inizio interruzione

Data fine interruzione  Ora fine interruzione

Durata del disservizio (min)

L'incidente ha comportato danni materiali?  
Descrivere i danni materiali

Se sì, descrivere quali

# Notifiche a CSIRT degli incidenti di sicurezza informatica

## - Una simulazione

25/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Data di inizio interruzione

Ora di inizio interruzione

Data fine interruzione

Ora fine interruzione

Durata del disservizio (min)

L'incidente ha comportato danni materiali?

Se sì, descrivere quali

Descrivere i danni materiali

Vi sono altri operatori/fornitori, nazionali o comunitari, che utilizzano i servizi compromessi dall'incidente?

Se sì, descrivere quali

Descrivere gli operatori/fornitori nazionali o comunitari impattati

Descrivere le azioni già intraprese per mitigare l'impatto dell'incidente

0 / 1000

Descrivere eventuali ulteriori azioni che si intende intraprendere

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

26/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Descrivere gli operatori/fornitori nazionali o comunitari impattati

Descrivere le azioni già intraprese per mitigare l'impatto dell'incidente 0 / 1000

Descrivere eventuali ulteriori azioni che si intende intraprendere 0 / 1000

Numero di utenti impattati\* Percentuale di utenti impattati\*

In via diretta o in quanto dipendenti dal servizio colpito per l'erogazione di propri servizi Percentuale degli utenti colpiti rispetto al totale degli utenti nazionale del servizio interessato

Indicare quanto l'incidente impatti sulla continuità e sull'efficienza del servizio Impatto sulle interconnessioni a livello nazionale

L'incidente ha causato una violazione dei dati personali? Descrivere la violazione dei dati personali avvenuta

(Data breach)

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

27/37

ACN Agenzia per la cybersicurezza nazionaleITA

☰ Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente

L'incidente ha causato una violazione dei dati personali? Descrivere la violazione dei dati personali avvenuta  
(Data breach)

❗ Sezione F - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione F** Azioni di contenimento ^

**Fornire le informazioni dell'incidente**

Attivazione della risposta di continuità operativa (business continuity response)*	Descrizione (se disponibile)
Azioni di follow-up*	Descrizione (se disponibile)
Misure di recupero*	Descrizione (se disponibile)
Minacce e tecniche usate dal threat actor*	Descrizione (se disponibile)

❗ Sezione G Diffusione transfrontaliera - Non disponibile se non presenti impatti transfrontalieri.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

28/37

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

29/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

L'incidente ha causato una violazione dei dati personali?

Descrivere la violazione dei dati personali avvenuta  
(Data breach)

Sezione F - Presenti campi obbligatori da riempire oppure il formato non è corretto.

**Sezione F** Azioni di contenimento

Fornire le informazioni dell'incidente

Attivazione della risposta di continuità operativa (business continuity response)\*

Descrizione (se disponibile)

Azioni di follow-up\*

Descrizione (se disponibile)

Misure di recupero\*

Seleziona una voce

- No
- Non noto
- Si

Descrizione (se disponibile)

Descrizione (se disponibile)

Sezione G Diffusione transfrontaliera - Non disponibile se non presenti impatti transfrontalieri.

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

30/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

Il campo è obbligatorio.

Minacce e tecniche usate dal threat actor\*

Descrizione (se disponibile)

Il campo è obbligatorio.

Sezione G Diffusione transfrontaliera - Non disponibile se non presenti impatti transfrontalieri.

Sezione H Eventuali notifiche

Eventuali altre notifiche già inviate

Forze di Polizia

Se sì, descrivere quali

Carabinieri, Polizia di Stato, Polizia Penitenziaria, Guardia di Finanza

Garante della privacy

Se sì, descrivere quali

Garante della privacy, altre autorità civili a tutela del cittadino

Eventuali CERT nazionali o esteri

Se sì, descrivere quali

CSIRT Regionali, altri CERT nazionali o esteri da coinvolgere

Altro

0 / 1000

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 31/37

ACN Agenzia per la cybersicurezza nazionale ITA

Portale Servizi Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Non noto v Descrizione (se disponibile)

Minacce e tecniche usate dal threat actor\*

Non noto v Descrizione (se disponibile)

Sezione G Diffusione Geografica: Transfrontaliera ^

Compilare questa sezione se l'incidente ha impattato utenti in due o più Stati dell'Unione Europea

L'operatore opera in due o più Stati europei? Se sì, descrivere quali v  
Descrizione degli stati in cui si opera

L'incidente ha avuto un impatto significativo sui servizi di altri Stati membri UE? Se sì, descrivere quali v  
Descrizione degli stati impattati

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

32/37

ACN Agenzia per la cybersicurezza nazionaleITA

CSIRT Regionali, altri CERT nazionali o esteri da coinvolgere

Altro

0 / 1000

**Sezione I** Tipologia di attacco - MITRE ATT&CK ^

**Fornire una descrizione di attacco seguendo quanto descritto nel framework del MITRE**

Descrizione

0 / 1000


Inserire solamente l'id del MITRE  
[Scopri di più](#)

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

33/37

Sezione L Indicatori di attacco o compromissione

Fornire eventuali indicatori di compromissione o attacco noti (uno per ogni campo) + Aggiungi IOC

TIPO	TIPOLOGIA	VALORE
 Non sono presenti elementi da visualizzare		

*Sezione N Relazione finale - E' possibile compilare questa sezione quando si è in chiusura e invio della relazione finale.*

*Presenti campi obbligatori da riempire oppure il formato non è corretto.*

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

## 34/37

The screenshot shows the ACN (Agenzia per la cybersicurezza nazionale) portal for reporting incidents. The main page has a navigation bar with 'Portale Servizi' and 'Apri segnalazione CSIRT'. Below the navigation bar, there are two radio buttons: 'Segnalazione di test' and 'Pre notifica'. The 'Pre notifica' option is selected. Below this, there are three checkboxes: 'La notifica è valida ai fini previsti dalla Legge 28 giugno 2024, n. 90.', 'La notifica è originata da una comunicazione del CSIRT Italia?', and 'La notifica è originata da una comunicazione del CSIRT Italia?'. The main content area is divided into sections: 'Sezione A - Dati dell'organizzazione', 'Generalità dell'organizzazione', 'Settori di competenza\*', 'Codice IVA', 'Codice IPA', and 'Identificativo ufficio Pubblica Amministrazione'. A modal window titled 'Aggiungi IoC/IoA' is open, showing a dropdown menu for 'Tipo di indicatore' with options 'IoC', 'IoC', and 'IoA'. The 'Caricamento singolo' option is selected. The modal also has a 'Tipologia\*' dropdown and 'Annulla' and 'Conferma' buttons.

# Notifiche a CSIRT degli incidenti di sicurezza informatica

## - Una simulazione

35/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza | Manuali utente

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

Pre notifica  
Alerta di incidente, si invia nelle prime 24 ore dal rilevamento

La notifica è valida ai fini previsti dalla Legge 28 giugno 2024, n. 90.

La notifica è originata da una comunicazione del CSIRT Italia?

### Aggiungi IoC/IoA

\* Campi obbligatori

Caricamento singolo  Caricamento da file CSV  Caricamento massivo

Tipo di indicatore: IoC

Tipologia\*:  
Seleziona una voce  
regkey  
regkey\value  
AS  
filename  
vulnerability

Valore\*

Sezione A Dati dell'organizzazione

Generalità dell'organizzazione

Denominazione Sociale\*  
GEA PROCOMAC S.P.A.

Settori di competenza\*  
1 elemento selezionato

Identificazione del settore di competenza ai sensi del decreto NIS2

Partita IVA  
02220940346

Codice IPA

Domicilio digitale\*


# Notifiche a CSIRT degli incidenti di sicurezza informatica

## - Una simulazione

36/37

**ACN** Agenzia per la cybersicurezza nazionaleITA

☰ Portale ServiziApri segnalazione CSIRT | Assistenza ⌚ | Manuali utente 📄

TIPO	TIPOLOGIA	VALORE
 <p>Non sono presenti elementi da visualizzare</p>		

**Relazione finale** Report finale di chiusura incidente ⤴

**Fornire le informazioni richieste per chiudere l'incidente.**

Identificazione e perimentrazione

Descrivere le fasi che hanno permesso la scoperta dell'evento/incidente, senza tralasciare indicazioni temporali ed ulteriori dettagli utili. Individuare inoltre i sistemi compromessi.

0 / 1000

Analisi

Descrivere le azioni intraprese per valutare e classificare l'evento/incidente. Includere ogni elemento di analisi che può far emergere eventuali tecniche utilizzate da potenziali attaccanti.

0 / 1000

# Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione

37/37

ACN Agenzia per la cybersicurezza nazionale

ITA

Portale Servizi

Apri segnalazione CSIRT | Assistenza ? | Manuali utente

Indicare in questa sezione le azioni intraprese per il contenimento dell'incidente (se verificato) prima delle azioni di rimozione di eventuali artefatti malevoli, la completa pulizia e ripristino dei sistemi. A titolo di esempio, vanno indicate in questa parte le azioni come il blocco di traffico telematico mediante apposite regole nei dispositivi di rete, blocco di utenze o / sospette... 0 / 1000

Eradicazione e ripristino

Descrivere in questa sezione tutte le attività poste in essere per rimuovere artefatti malevoli dai sistemi ed eventuali azioni di ripristino adottate, per rendere nuovamente funzionali i sistemi a supporto del core business dell'organizzazione. 0 / 1000

Attività post incidente

Indicare le scelte adottate dall'organizzazione relative alla nuova postura cyber, in conseguenza dell'evento, al fine di limitare le probabilità che lo stesso possa presentarsi nuovamente in futuro. 0 / 1000

Timeline

Elencare le principali fasi dell'evento/incidente in ordine sequenziale. 0 / 1000

Presenti campi obbligatori da riempire oppure il formato non è corretto.

Annulla segnalazione Ricomincia Annulla inserimento Salva la bozza Invia segnalazione

# Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- **Q&A**

# Q&A

**Grazie per l'attenzione!**

# DATA CONSEC

DATA PROTECTION - CONSULTING - SECURITY



V.le Fratti, 56 Parma - Italia  
Tel. e Fax: +39 0521 77 12 98  
e-mail: [info@dataconsec.com](mailto:info@dataconsec.com)  
[amministrazione@pec.dataconsec.com](mailto:amministrazione@pec.dataconsec.com)  
web: [www.dataconsec.com](http://www.dataconsec.com)