GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, anche attuando il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza, promuovendone azioni comuni.

L'Agenzia è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. In tale veste ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico del Paese promuovendo la realizzazione di azioni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese. A tal fine sviluppa anche capacità necessarie per proteggere dalle minacce informatiche reti, sistemi informativi e servizi informatici delle Pubbliche Amministrazioni e degli operatori di infrastrutture critiche nazionali, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Siti web: **Agenzia per la Cybersicurezza Nazionale** **CSIRT Italia**

Contatti: **info@acn.gov.it**

Seguici sui nostri canali social:

Esclusione di responsabilità

Il presente documento fornisce, a titolo esemplificativo e non esaustivo, indicazioni di mero ausilio alle attività di sicurezza dell'Organizzazione e non solleva la stessa dall'onere di porre in essere, nel rispetto della normativa vigente in materia di cybersicurezza, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici.

SOMMARIO

INDICE DELLE FIGURE

1 INTRODUZIONE

L'obiettivo della presente Linea Guida è illustrare ad ogni soggetto le informazioni necessarie per effettuare la **notifica** di incidente al CSIRT (Computer Security Incident Response Team) Italia, sia che il soggetto abbia un **obbligo normativo di notifica**, come i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), gli Operatori di Servizi Essenziali (OSE), i Fornitori di Servizi Digitali (FSD), i Telco e i soggetti sottoposti alle disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici[1] (di seguito per brevità "*Soggetti Legge n. 90/2024*"), sia che esso **non operi in settori critici e non abbia vincoli** in tal senso, come Piccole e Medie Imprese e cittadini.

Il documento è organizzato in **sezioni chiave**, che, per ciascuna tipologia di soggetto segnalante, forniscono informazioni sul contesto normativo di riferimento, sulle eventuali e specifiche tempistiche da rispettare e relative sanzioni per il mancato adempimento nonché una descrizione delle fasi in cui si articola il flusso di processo. Tale organizzazione mira a offrire chiarezza e praticità per una corretta adozione del protocollo di comunicazione in funzione del soggetto che effettua la notifica, facilitando la comprensione e l'implementazione del processo.

[1] Legge 28 giugno 2024, n. 90 "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", art.1, comma 1.

2 IL CSIRT ITALIA

Il **CSIRT Italia** è il centro operativo all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN) incaricato delle azioni di preparazione, prevenzione, gestione e risposta a eventi ed incidenti cibernetici.

Il CSIRT è stato istituito con **D.Lgs. 18 maggio 2018, n. 65**, attuativo della "*Direttiva 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea*" (cosiddetta Direttiva NIS), che ne ha anche dettagliato compiti e funzioni, nonché individuato gli OSE e i FSD quali soggetti con obblighi di notifica degli incidenti al CSIRT Italia.

Successivamente, il **Decreto del Presidente del Consiglio dei ministri 8 agosto 2019**, "*Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano*" ha definito la costituzione, l'organizzazione ed il funzionamento del CSIRT italiano presso il Dipartimento delle informazioni per la sicurezza (DIS) ora - a seguito delle modifiche introdotte dal **D.L. 14 giugno 2021, n. 82** - presso l'ACN, assumendo la denominazione di **CSIRT Italia**. In tale quadro, i soggetti pubblici e privati, in caso di incidente cibernetico e/o di notifica di evento, hanno **quale nuovo ed unico interlocutore** il CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli OSE e dei FSD, ai sensi del D.Lgs. n. 65/2018.

A fronte di tale quadro normativo, il CSIRT Italia assume il ruolo di:

- struttura tecnica di **prevenzione, coordinamento e risposta agli eventi e incidenti informatici** con impatto, effettivo o potenziale, sul territorio nazionale;
- punto di riferimento per le **notifiche degli incidenti** occorsi in danno di tutte le infrastrutture digitali della pubblica amministrazione e private, con particolare riferimento alle **notifiche previste ai sensi di legge**, ad opera dei soggetti inclusi nel PSNC, degli OSE e dei FSD individuati dalla Direttiva NIS e per i soggetti sottoposti ad obbligo di notifica ai sensi del Codice delle comunicazioni elettroniche e della Legge n. 90/2024;

- membro della rete composta dai CSIRT europei (CSIRT Network) avente quale finalità quella di contribuire a sviluppare la fiducia tra gli Stati membri dell'UE e promuovere la **cooperazione operativa in ambito internazionale**.

3 LA NOTIFICA DEGLI INCIDENTI

Il modello presentato di seguito fornisce uno **schema di base** per il processo di **notifica** degli incidenti informatici. Questo schema nelle sezioni a seguire sarà personalizzato per ciascuna categoria di soggetti, adattandosi alle specifiche esigenze e ai relativi obblighi normativi.

Solo nei casi previsti, la fase di notifica è preceduta dalla tempestiva segnalazione dell'incidente.

Il **flusso di notifica** degli incidenti al CSIRT Italia è articolato in **quattro fasi:**

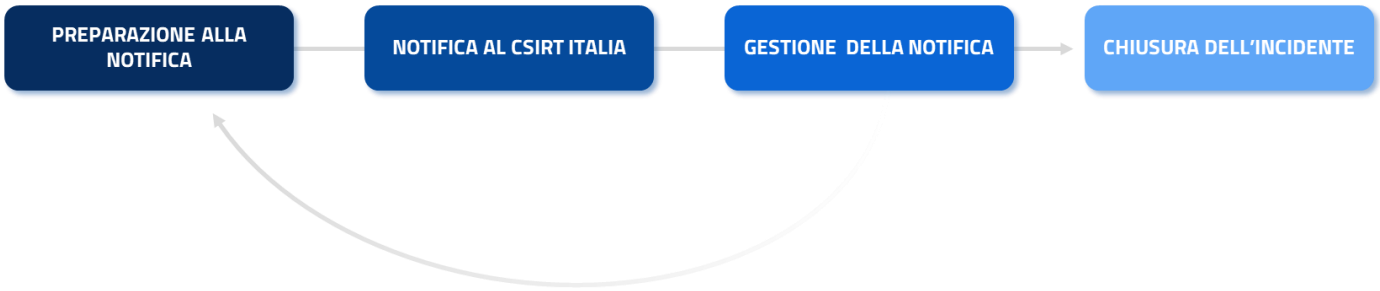

Figura 1: Flusso di notifica - modello di base

Ogni fase include un insieme di attività che possono essere effettuate dal soggetto segnalante:

1. PREPARAZIONE ALLA NOTIFICA

A seguito della rilevazione di un incidente, il soggetto segnalante avvia una fase preparatoria alla **notifica** con l'obiettivo di raccogliere le informazioni minime per garantire che la comunicazione permetta al CSIRT Italia un'attivazione proporzionata alla potenziale criticità ed ai potenziali impatti di natura sistemica derivanti dall'incidente stesso. Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

2. NOTIFICA AL CSIRT ITALIA

Una volta raccolte le informazioni necessarie ad effettuare la **segnalazione**, ove prevista, e/o la **notifica**, si potrà procedere alla compilazione di un **modulo online** disponibile sul sito internet del CSIRT Italia: https://www.csirt.gov.it/segnalazione.

3. GESTIONE DELLA NOTIFICA

Dopo aver ricevuto la **segnalazione**, ove prevista, e/o la **notifica**, sulla base del livello di servizio previsto per la specifica categoria di soggetto segnalante, il CSIRT Italia, compatibilmente con le risorse a disposizione e la criticità del soggetto segnalante, valuterà l'opportunità di fornire **supporto** nelle operazioni di incident handling, da remoto o *in loco*. Durante questa fase, in base alla tipologia del soggetto segnalante e alla normativa vigente, su richiesta del CSIRT Italia potranno essere effettuate ulteriori attività anche a seguito della risoluzione dell'incidente.

4. CHIUSURA DELL'INCIDENTE

Una volta terminate le attività di gestione dell'incidente da parte del soggetto segnalante ed eventualmente pianificate le attività di rientro dell'incidente, il CSIRT Italia procederà alla **chiusura dell'incidente**.

GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

SOGGETTI PSNC

CHI SONO I SOGGETTI INCLUSI NEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

Il D.L. n. 105 del 2019 ha istituito il **Perimetro di Sicurezza Nazionale Cibernetica (PSNC)** al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività fondamentali per l'interesse dello Stato.

I soggetti inclusi nel PSNC sono individuati, in accordo ai criteri di cui all'articolo 1, comma 2 del D.L. n. 105/2019, secondo le modalità disciplinate dal DPCM n. 131/2020, sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici (art.1, co. 2, lett. a), n. 2-*bis*, D.L. n. 105/2019). Nello specifico sono individuati:

- i soggetti che esercitano una **funzione essenziale dello Stato** e il cui esercizio dipende da reti, sistemi informativi e servizi informatici (art. 1, co. 2, lett. a), n. 1 e n. 2, D.L. n. 105/2019);
- i soggetti che assicurano un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per lo Stato e il cui esercizio dipende da reti, sistemi informativi e servizi informatici (art. 1, co. 2, lett. a), n. 1 e n. 2, D.L. n. 105/2019).

L'**elenco dei soggetti inclusi nel PSNC**, aggiornato secondo le predette modalità, è contenuto in un atto amministrativo – adottato dal Presidente del Consiglio dei Ministri, su proposta del CIC – non soggetto a pubblicazione e per il quale è escluso il diritto di accesso (art.1, co. 2-*bis*, D.L. n. 105/2019). Dell'avvenuta iscrizione nel cennato elenco è data, separatamente, comunicazione a ciascun soggetto.

PERCHÉ NOTIFICARE GLI INCIDENTI AL CSIRT ITALIA

La notifica obbligatoria o volontaria degli incidenti al CSIRT Italia da parte dei soggetti inclusi nel PSNC (c.d. notifica) discende dal combinato disposto dell'art. 1 commi 3 e 3-bis del D.L. n. 105/2019, dal DPCM n. 81/2021 e dalla DETERMINA ACN del 3 gennaio 2023.

COSA NOTIFICARE AL CSIRT ITALIA

Per i soggetti inclusi nel PSNC sono previste due modalità di notifica di un incidente: obbligatoria e volontaria (artt. 3 e 4 DPCM n. 81/2021).

La notifica è **obbligatoria** quando viene rilevato un incidente appartenente alla tassonomia di cui all'**allegato A del DPCM n. 81/2021**, avente impatto su:

- un **bene ICT** di pertinenza;
- un sistema informativo o un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'art. 7, comma 2, del DPCM n. 131/2020, condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione (cd. **beni contigui**).

La notifica è **obbligatoria**, altresì, quando viene rilevato un incidente appartenente alla tassonomia di cui all'**allegato A della Determina ACN del 3 gennaio 2023**, avente impatto su **reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai precedenti**. In questo caso è, inoltre, necessario, prima della notifica, procedere senza ritardo alla **segnalazione**.

La notifica è **volontaria** per gli incidenti:

- che occorrono a carico di un **bene ICT** e che non sono riconducibili a una delle tipologie della tassonomia di cui all'**allegato A del DPCM n. 81/2021**;
- che occorrono a carico di **reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai beni ICT e dai beni contigui** e che sono riconducibili ad una delle tipologie della tassonomia di cui all'**allegato A del DPCM n. 81/2021**[2].

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

Il soggetto PSNC che ha subito un incidente e che rientra nei casi previsti per la notifica obbligatoria o volontaria verso il CSIRT Italia deve procedere a suddetta notifica nei tempi previsti dalla normativa vigente, **attraverso la compilazione e l'invio di un apposito modulo *online* disponibile sul sito internet del CSIRT Italia** (https://www.csirt.gov.it/segnalazione).

[2] Si ricorda che la notifica è obbligatoria per le selezionate fattispecie della tassonomia dell'allegato A del DPCM 81/2021 inserite nell'allegato A della Determina ACN del 3 gennaio 2023**.**

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

In relazione alla normativa PSNC, si definisce **incidente** "*ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*" (**art. 1, comma 1, lett. *h*) del DPCM n. 81/2021**).

Tuttavia, per regolamentare e prioritizzare le varie tipologie di incidente che devono essere oggetto di notifica al CSIRT Italia, il legislatore ha definito una **tassonomia degli incidenti** che ne permette la categorizzazione.

Tale tassonomia classifica gli incidenti in categorie, strutturate come segue:

- la tabella con gli identificativi "**ICP-A**" indica le tipologie degli incidenti aventi impatto sui **beni ICT o sui beni contigui** da notificare entro 6 ore (definita nell'**allegato A del DPCM n. 81/2021**);
- la tabella con gli identificativi "**ICP-B**" indica le tipologie degli incidenti aventi impatto sui **beni ICT o sui beni contigui** da notificare entro 1 ora (definita nell'**allegato A del DPCM n. 81/2021**);
- la tabella con gli identificativi "**ICP-C**" indica le tipologie degli incidenti con impatto su **reti, sistemi informativi e servizi informatici diversi dai beni ICT** (definita nell'**allegato A** della **Determina ACN del 3 gennaio 2023**).

QUALI SONO I TEMPI DA RISPETTARE PER LA NOTIFICA DI UN INCIDENTE

Il soggetto PSNC è tenuto a rispettare le tempistiche di notifica dell'incidente al CSIRT Italia secondo quanto previsto dalla normativa vigente. Tali tempistiche dipendono dalla tipologia di incidente da segnalare (indicate nelle tre tabelle di cui è composta la tassonomia degli incidenti) e dal fatto che l'incidente abbia impatto sul bene ICT, su beni contigui o su reti, sistemi informativi e servizi informatici di pertinenza diversi dai precedenti.

Le tempistiche decorrono dal momento in cui si è venuti a conoscenza di un incidente, a seguito delle evidenze ottenute, anche mediante le attività di monitoraggio, test e controllo previste dalla normativa PSNC (art. 1, co. 3, lett. b), n. 6, del D.L. n. 105/2019).

Nel dettaglio, per le **notifiche obbligatorie** sono definite le tempistiche a seguire.

Per gli incidenti ai sensi dell'art. 1, co. 3, lett. a) del D.L. n. 105/2019, così come disciplinato dall'art. 3 del DPCM 81/2021:

- 1 ora per gli incidenti di cui alla Tabella 2 dell'allegato A del DPCM 81/2021 (incidenti ICP-B);
- 6 ore per gli incidenti di cui alla Tabella 1 dell'allegato A del DPCM 81/2021 (incidenti ICP-A).

Per gli incidenti con impatti su **reti, sistemi informativi e servizi informatici diversi dai beni ICT** (art. 1, co. 3-bis del D.L. n. 105/2019):

- **Segnalazione** entro 24 ore e relativa **notifica** completa entro 72 ore (incidenti ICP-C).

Non sono definite tempistiche per le **notifiche volontarie**.

TIPOLOGIA DI EVENTO	IDENTIFICAZIONE DELL'ASSET	CLASSE IDENTIFICATIVA INCIDENTE	TIPO DI NOTIFICA	TEMPISTICHE
Incidente che rientra nelle classificazioni della tassonomia	BENE ICT O CONTIGUO	ICP-B	OBBLIGATORIA	**ENTRO 1 ORA** dal rilevamento dell'incidente
Incidente che rientra nelle classificazioni della tassonomia	BENE ICT O CONTIGUO	ICP-A	OBBLIGATORIA	**ENTRO 6 ORE** dal rilevamento dell'incidente
Incidente che rientra nelle classificazioni della tassonomia	DIVERSO DA BENE ICT	ICP-C	OBBLIGATORIA	**Segnalazione: ENTRO 24 ORE** **Notifica: ENTRO 72 ORE** dal rilevamento dell'incidente
Incidente che rientra nelle classificazioni della tassonomia	DIVERSO DA BENE ICT E DA BENE CONTIGUO	ICP-A/B	VOLONTARIA	**NESSUNA TEMPISTICA**
Incidente che **non** rientra nelle classificazioni della tassonomia	BENE ICT	-	VOLONTARIA	**NESSUNA TEMPISTICA**

Figura 2: PSNC - tempistiche notifica

NOTIFICA PERIMETRO PER I SOGGETTI GIÀ OSE, FSD E/O RICOMPRESI NEL CODICE DELLE COMUNICAZIONI ELETTRONICHE E/O NELLA LEGGE N. 90/2024

Qualora il soggetto PSNC fosse già stato individuato quale OSE o FSD (artt. 12 e 14 D.Lgs. 18 maggio 2018, n°65) e/o ricompreso nel Codice delle comunicazioni elettroniche (art. 16-ter, comma 2 del D.Lgs. n. 259/2003) la notifica obbligatoria effettuata ai sensi dell'art. 1, co. 3, let.

a) del D.L. n. 105/2019 costituisce anche adempimento per gli obblighi di notifica ai sensi dei predetti decreti legislativi.

SANZIONI PER IL MANCATO ADEMPIMENTO DELL'OBBLIGO DI NOTIFICA

Fatto salvo il caso in cui il fatto costituisca reato, per i soggetti PSNC il mancato adempimento dell'obbligo di notifica di cui all'art. 1, co. 3, let. a) del D.L. n. 105/2019 nei termini prescritti, comporta una sanzione amministrativa pecuniaria nei termini previsti dalla normativa vigente da euro 250.000 fino a euro 1.150.000 (art. 1, co. 9, lett. b), D.L. n. 105/2019).

Nei casi di reiterata inosservanza degli obblighi di notifica di cui all'articolo 1, comma 3-bis del D.L. 105/2019, si applica la sanzione amministrativa pecuniaria da euro 25.000 fino a euro 125.000.

FLUSSO DI NOTIFICA PER I SOGGETTI PSNC

Per i soggetti PSNC, le quattro fasi del flusso di notifica, proposto nel capitolo 3, includono le seguenti specifiche attività:

Fase 1 – Preparazione alla notifica

- Attività necessarie:
  - **identificazione** delle reti, dei sistemi informativi e servizi informatici impattati dall'incidente;
  - **identificazione della tipologia di incidente** da segnalare in accordo alla tassonomia degli incidenti di cui all'Allegato A del DPCM n. 81/2021 e di quella di cui all'Allegato A alla DETERMINA ACN del 3 gennaio 2023.
- Attività a supporto:
  - **raccolta** delle evidenze (es. IOC, evidenze, azioni di ripristino) relative all'incidente stesso;
  - **autovalutazione** dell'impatto sui sistemi e sull'erogazione dei servizi di business;
  - **definizione e pianificazione** di un piano di rientro.

Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

*Una volta terminate le "**attività necessarie**", il soggetto PSNC sarà a conoscenza della tipologia di incidente in corso, e avrà, dunque, le informazioni minime necessarie a **rispettare le tempistiche per l'obbligo di notifica** per i casi previsti dalla normativa vigente.*

Fase 2 – Notifica al CSIRT Italia

Il soggetto segnalante dovrà, secondo i tempi previsti dalla normativa vigente, compilare l'apposito modulo disponibile *online* sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) e fornire le seguenti informazioni:

- tipologia di impatto, distinta tra:
  - **impatto su bene ICT** (notifica art.3, comma 1 DPCM n. 81/2021);
  - **impatto su bene contiguo** (notifica art.3, comma 3 DPCM n. 81/2021);
  - **impatto su altri beni** (notifica art.1, comma 3-bis D.L. n.105/2019);
  - **impatto per cui non sussiste un obbligo di notifica** (art.4 DPCM n. 81/2021).
- date e ora di rilevamento dell'incidente;
- ulteriori dettagli dell'incidente, come ad esempio altri sistemi impattati o informazioni rilevanti;

- lista degli IOC (Indicator Of Compromise) raccolti fino al momento della notifica;
- evidenze rilevate (es. sample di malware, ransom note).

Solo nel caso di incidente con classe identificativa ICP-C (ai sensi dell'art. 1, comma 3-bis del D.L. n. 105/2019), è necessario procedere ad una **segnalazione** (entro 24 ore) e alla **successiva relativa notifica** (entro 72 ore).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "infectedacn".

Fase 3 - Gestione della notifica

Dopo aver ricevuto la segnalazione, ove prevista e/o la notifica da parte del soggetto segnalante, il CSIRT Italia compatibilmente con le risorse a disposizione e la criticità dell'incidente offrirà supporto, se del caso *in loco*, nelle operazioni di incident handling.

Nel caso in cui l'incidente coinvolga un bene ICT o un bene contiguo, il soggetto PSNC che ha proceduto alla notifica, **su richiesta del CSIRT Italia**, provvederà, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa, **entro sei ore** dalla richiesta (art. 3, co. 7 del DPCM n. 81/2021) a **integrare** la notifica con le nuove informazioni emerse durante le attività di analisi e riposta all'incidente tramite l'apposito modulo *online* sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione).

Fase 4 - Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, il soggetto PSNC ne dà tempestiva comunicazione al CSIRT Italia (art.3, co. 8 DPCM n. 81/2021), che ha la facoltà di richiedere al soggetto stesso **una relazione tecnica dell'incidente** riguardante gli aspetti significativi dell'incidente, quali:

- una valutazione delle conseguenze dell'impatto sui beni ICT;
- la descrizione delle azioni di recupero e ripristino **intraprese.**

A seguito della richiesta, il soggetto PSNC è tenuto a rispondere al CSIRT Italia, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa, **entro trenta giorni**, ai sensi dell'art. 3, co. 8, del DPCM n. 81/2021.

PREPARAZIONE ALLA NOTIFICA

Procedere con:

- Identificazione dell'insieme minimo di informazioni per categorizzare l'incidente:
  - tipo di Bene ICT impattato;
  - **tipologia di incidente** in accordo alla tassonomia definita da ACN (ICP-A, ICP-B, ICP-C).
- Raccolta delle evidenze relative all'incidente.
- Autovalutazione dell'impatto sui sistemi e sull'erogazione dei servizi di business.
- Pianificazione di un piano di ripristino.

Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

NOTIFICA AL CSIRT ITALIA

Fornire le seguenti informazioni:

- **Tipologia di impatto**, distinta tra:
  - impatto su bene ICT (notifica art.3, comma 1 DPCM n. 81/2021);
  - impatto su reti/sistemi contigui (notifica art.3, comma 3 DPCM n .81/2021);
  - impatto su altri beni (notifica art.1, comma 3-bis d.l. n.105/2019);
  - impatto per cui non sussiste un obbligo di segnalazione;
  - date e ora di rilevamento dell'incidente;
  - ulteriori dettagli dell'incidente;
  - lista degli IOC (Indicator Of Compromise);
  - evidenze rilevate (logs, sample, etc...).

GESTIONE DELLA NOTIFICA

A seguito della segnalazione, ove prevista, e/o della notifica sarà aperto un canale di comunicazione diretto tramite il quale il CSIRT Italia offrirà supporto alle attività di incident handling, ed eventualmente potrà richiedere ulteriori informazioni ad integrazione della notifica.

CHIUSURA DELL'INCIDENTE

Una volta definite ed avviate le attività di ripristino dei beni ICT impattati, il soggetto PSNC ne dà tempestiva comunicazione al CSIRT Italia, che, a questo punto, avrà la facoltà di richiedere al soggetto stesso una relazione tecnica dell'incidente riguardante gli aspetti significativi.

Figura 3: PSNC - flusso notifica

GUIDA ALLA NOTIFICA INCIDENTI AL CSIRT ITALIA

PSNC

SOGGETTI PSNC

Soggetti operanti nei settori critici e che sono individuati ai sensi dell'articolo 1, comma 2 del D.L. n° 105 del 2019.

PERCHÈ NOTIFICARE AL CSIRT ITALIA

L'obbligo di notifica degli incidenti al CSIRT Italia per i soggetti inclusi del PSNC è previsto dai seguenti articoli: Art. 1 co. 3, co. 3bis, co. 8 D.L. n. 105/2019; Art 2, 3, 4 DPCM n. 81/2021;Art. 2 Determina 3 gennaio 2023.

COSA NOTIFICARE AL CSIRT ITALIA

La notifica **obbligatoria** è prevista in caso di:

- incidenti con impatto sui beni ICT o contigui (ICP–B, ICP–A);
- incidenti con impatto sui beni diversi dai beni ICT (ICP–C).

La notifica **volontaria** è prevista in caso di:

- incidenti con impatto su beni ICT e non categorizzabili nella tassonomia degli incidenti;
- incidenti con impatto su beni diversi da beni ICT e da beni contigui (ICP–B, ICP-A).

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

Il legislatore ha definito la tassonomia degli incidenti che devono essere oggetto di notifica obbligatoria al CSIRT Italia, categorizzandoli in tre classi di identificativi:

- ICP–A per gli incidenti con impatto sui beni ICT o CONTIGUI;
- ICP–B per gli incidenti con impatto sui beni ICT o CONTIGUI;
- ICP–C per gli incidenti con impatto sui beni diversi da beni ICT.

CON QUALI TEMPISTICHE

La notifica obbligatoria ha delle tempistiche specifiche relativamente alla gravità dell'incidente e anche alla tipologia dei beni informatici impattati, divisi tra beni ICT o contigui e beni diversi da beni ICT.
La notifica volontaria non ha tempistiche specifiche.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della notifica sarà aperto un canale di comunicazione diretto tramite il quale il CSIRT Italia offrirà supporto alle attività di incident handling, ed eventualmente potrà richiedere ulteriori informazioni e una relazione tecnica complessiva dell'incidente.

GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

OSE E FSD

CHI SONO OSE E FSD

Il **D.Lgs. 18 maggio 2018, n. 65** "*Attuazione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" recepisce a livello nazionale la c.d. **Direttiva NIS**.

La stessa Direttiva stabilisce misure per incrementare la sicurezza e la resilienza delle reti e dei sistemi informativi degli **Operatori di Servizi Essenziali (OSE)** e dei **Fornitori dei Servizi Digitali (FSD)**. Nel dettaglio, gli **Operatori di Servizi Essenziali (OSE),** individuati secondo le modalità definite nell'articolo 4 del D.lgs. n. 65/2018, includono soggetti pubblici o privati che operano nei seguenti settori (cfr. Allegato II, D.lgs. n. 65/2018):

- energia;
- trasporti;
- bancario;
- infrastrutture dei mercati finanziari;
- sanitario;
- fornitura e distribuzione di acqua potabile;
- infrastrutture digitali.

I **Fornitori di Servizi Digitali (FSD)** includono ogni persona giuridica che fornisce un servizio digitale appartenente ad una delle seguenti tipologie (Allegato III, D.lgs. n. 65/2018):

- **Mercato online**: un servizio digitale che consente ai consumatori ovvero ai professionisti di concludere contratti di vendita o di servizi *online* con i professionisti sia sul sito web del mercato *online* sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato *online*.
- **Motore di ricerca online**: un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto.
- **Servizi di cloud computing**: un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

L'**elenco nazionale degli operatori di servizi essenziali** viene aggiornato almeno ogni due anni a

cura dell'ACN, quale Autorità nazionale competente NIS[3], che valuta le proposte di variazione delle Autorità di settore.

PERCHÉ NOTIFICARE GLI INCIDENTI AL CSIRT ITALIA

La notifica degli incidenti al CSIRT Italia è obbligatoria per **OSE** e **FSD** in base agli articoli 12 e 14 del D.Lgs. n. 65/2018.

COSA NOTIFICARE AL CSIRT ITALIA

Per gli **OSE**, è sancito l'obbligo di notifica per gli **incidenti aventi un *impatto rilevante sulla continuità dei servizi essenziali forniti,*** come stabilito dall'art. 12, co. 5, del D.lgs. n. 65/2018. La rilevanza dell'impatto di un incidente è determinata, tenuto conto dei parametri di cui all'art. 12, co. 8, del D.lgs. n. 65/2018, ***dal superamento delle soglie che determinano la gravità dell'incidente stesso***, definite nelle apposite linee guida emanate dall'Autorità nazionale competente NIS e comunicate direttamente agli OSE.

Per i **FSD**, è sancito l'obbligo di notifica per ***gli incidenti aventi un impatto rilevante sulla fornitura del servizio digitale che essi offrono sul territorio nazionale e all'interno dell'Unione Europea***, come stabilito dall'art. 14, co. 4, del D.lgs. n. 65/2018, ***per quei casi in cui siano superate le soglie che determinano la gravità dell'incidente stesso***.

Le notifiche devono avvenire **senza ingiustificato ritardo**.

Ai sensi dell'articolo 18 del D.Lgs. n.65/2018, i **soggetti che non sono stati identificati come OSE e i FSD** possono notificare al CSIRT Italia, su **base volontaria**, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

[3] Il D.L. n. 82/2021 ha designato l'Agenzia per la Cybersicurezza Nazionale quale Autorità nazionale competente NIS, in luogo del MIMIT (già MISE), del MIT, del MEF, del Ministero della salute, del MASE (già Ministero dell'ambiente e della tutela del territorio e del mare) e delle Regioni e delle Province autonome, precedentemente designati quali Autorità nazionali competenti NIS per i settori di rispettiva competenza.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

OSE e FSD che hanno subito un incidente che rientra nei casi previsti per la notifica obbligatoria verso il CSIRT Italia, procederanno a suddetta notifica attraverso la compilazione e l'invio di un apposito modulo *online* disponibile sul sito internet del CSIRT Italia https://www.csirt.gov.it/segnalazione.

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

Gli **OSE** notificano al CSIRT Italia gli **incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.** Le soglie e le modalità per valutare l'impatto di un incidente sono definite da linee guida emanate dall'Autorità nazionale competente NIS e **direttamente comunicate agli operatori interessati**.

I **FSD** notificano al CSIRT Italia **gli incidenti aventi un impatto rilevante sulla fornitura di un servizio offerto all'interno dell'Unione Europea**. I criteri per la valutazione della rilevanza di un impatto sono dettati dall'articolo 4 del Regolamento di esecuzione 2018/151 adottato dalla Commissione Europea il 30 gennaio 2018. Nello specifico, un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni:

- il servizio fornito da un FSD **non è stato disponibile per oltre 5.000.000 di ore utente**, dove per ore utente si intende il numero di utenti interessati nell'Unione Europea per una durata di sessanta minuti;
- l'incidente ha **provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo** del FSD che ha interessato oltre **100.000 utenti nell'Unione Europea**;
- l'incidente ha generato un **rischio per la sicurezza pubblica**, **l'incolumità pubblica** o in termini di **perdite di vite umane**;
- **l'incidente ha provocato danni materiali superiori a 1.000.000 di euro** per almeno un utente nell'Unione Europea.

QUALI SONO I TEMPI DA RISPETTARE PER LA NOTIFICA DI UN INCIDENTE

Per la **notifica obbligatoria**, OSE e FSD devono procedere alla notifica verso CSIRT Italia **senza ingiustificato ritardo**.

Figura 4: OSE & FSD - tempistiche notifica

SANZIONI PER IL MANCATO ADEMPIMENTO DELL'OBBLIGO DI NOTIFICA

Salvo che il fatto costituisca reato, il mancato adempimento dell'obbligo di notifica per i soggetti NIS (OSE e FSD) nei termini prescritti, comporta una sanzione amministrativa pecuniaria nei termini previsti dalla normativa vigente, come a seguire:

- l'**OSE** che non notifica al CSIRT Italia gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti, ai sensi dell'articolo 12, comma 5, è soggetto ad una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 (art. 21, co. 3, D.lgs. n. 65/2018);
- il **FSD** che non notifica al CSIRT Italia gli incidenti aventi un impatto rilevante sulla fornitura di un servizio fornito, ai sensi dell'articolo 14, comma 4, è soggetto ad una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 (art. 21, co. 6, D.lgs. n. 65/2018).

FLUSSO DI NOTIFICA PER OSE E FSD

Per OSE e FSD, le fasi del flusso di notifica di cui al capitolo 3 includono le seguenti attività:

Fase 1 - Preparazione alla notifica

OSE e **FSD**, che devono procedere alla notifica obbligatoria per i casi previsti, dovranno:

- individuare il numero di utenti impattati dall'incidente;
- definire la durata dell'incidente, delimitato dal periodo tra il momento in cui si è verificata la prima interruzione completa o parziale del servizio e il momento del ripristino;

- determinare la diffusione geografica dell'incidente prendendo in considerazione la localizzazione degli utenti, delle persone fisiche e delle persone giuridiche interessate dall'incidente.

In aggiunta alle suddette attività, i **soli FSD** dovranno, inoltre, ai sensi dell'art. 3 del citato Regolamento di esecuzione 2018/151:

- **misurare** la portata della perturbazione del funzionamento del servizio per una o più delle seguenti caratteristiche compromesse dall'incidente: disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi correlati;
- **dedurre**, sulla base di indicazioni quali la natura delle sue relazioni contrattuali con i clienti o, se del caso, il numero potenziale di utenti interessati, se l'incidente ha causato importanti perdite materiali o immateriali per gli utenti, ad esempio in relazione alla salute e alla sicurezza o danni materiali.

Fase 2 - Notifica al CSIRT Italia

OSE e FSD effettuano la notifica tramite modulo disponibile online sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) fornendo le seguenti informazioni:

- numero di utenti impattati;
- durata dell'incidente;
- diffusione geografica;
- date e ora di rilevamento dell'incidente;
- asset impattati;
- ulteriori dettagli dell'incidente (es. IOC);
- evidenze rilevate (es. sample di malware, ransom note).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "*infectedacn*".

Fase 3 - Gestione della notifica

OSE e FSD, se del caso, ricevono supporto dal CSIRT Italia nelle operazioni di incident handling e collaborano nel fornire ogni dettaglio richiesto ai fini di una tempestiva risoluzione della situazione.

Fase 4 - Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, si procederà alla chiusura dell'incidente.

PREPARAZIONE ALLA NOTIFICA

Per entrambi i soggetti *NIS*, **OSE** e **FSD**, si procede con:

- identificazione del **numero di utenti impattati** dall'incidente, **durata** e **diffusione geografica** dell'incidente.

In aggiunta, i soli soggetti **FSD** devono, inoltre, misurare:

- **portata della perturbazione** del funzionamento del servizio;
- numero potenziale di **utenti interessati**, **perdite materiali** o **immateriali** per gli utenti.

NOTIFICA AL CSIRT ITALIA

Fornire le seguenti informazioni:

- **Durata** dell'incidente.
- Diffusione **geografica**.
- **Data e ora** di rilevamento dell'incidente.
- **Asset** impattati.
- Ulteriori dettagli dell'incidente (es. IOC).
- Evidenze rilevati (es. sample di malware, ransom note).

GESTIONE DELLA NOTIFICA

A seguito della notifica, CSIRT Italia offre:

- **supporto diretto** nelle operazioni di *incident handling*;
- se necessario, **assistenza operativa** e fornitura di informazioni utili.

CHIUSURA DELL'INCIDENTE

Una volta definite ed avviate le attività di ripristino, viene effettuata la **chiusura dell'incidente**.

Figura 5: OSE & FSD - flusso notifica

GUIDA ALLA NOTIFICA INCIDENTI AL CSIRT ITALIA

OSE

SOGGETTI OSE

Operatori di Servizi Essenziali operanti nei settori critici e individuati ai sensi dell'articolo 4 del D. lgs. n.65/2018.

PERCHÈ NOTIFICARE AL CSIRT ITALIA

L'obbligo di notifica degli incidenti al CSIRT Italia per i soggetti individuati come OSE è prevista dall'articolo 12 del D. lgs. n.65/2018.

COSA NOTIFICARE AL CSIRT ITALIA

La notifica obbligatoria va effettuata per gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti, secondo i parametri definiti dalla regolamentazione vigente.

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

I parametri per valutare la rilevanza dell'impatto di un incidente informatico sono definiti nelle apposite linee guida emanate dalle Autorità competenti NIS e comunicate direttamente ai soggetti OSE.

CON QUALI TEMPISTICHE

La notifica obbligatoria dovrà essere effettuata senza ingiustificato ritardo.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della notifica sarà aperto un canale di comunicazione diretto, tramite il quale il CSIRT Italia offrirà al soggetto che effettua la notifica un supporto diretto alle attività di incident handling.

GUIDA ALLA NOTIFICA INCIDENTI AL CSIRT ITALIA

FSD

SOGGETTI FSD

Fornitore di servizio digitale è qualsiasi persona giuridica che fornisce un servizio di una tipologia tra mercato online, motore di ricerca online, servizi di cloud computing così come definito dell'art. 3, com. 1, lett. i), del D. lgs. n. 65/2018.

PERCHÈ NOTIFICARE AL CSIRT ITALIA

L'obbligo di notifica al CSIRT Italia per i soggetti inclusi nel FSD è previsto dall'articolo 14 del D. lgs. n. 65/2018.

COSA NOTIFICARE AL CSIRT ITALIA

La notifica obbligatoria va effettuata per gli incidenti aventi un impatto rilevante sulla fornitura di un servizio che essi offrono all'interno dell'UE, secondo i parametri definiti dalla regolamentazione vigente.

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

I parametri per stabilire la rilevanza di un impatto di un incidente sono definiti dal Regolamento di esecuzione 2018/151 adottato dalla Commissione europea il 30 gennaio 2018.

CON QUALI TEMPISTICHE

La notifica obbligatoria dovrà essere effettuata senza ingiustificato ritardo.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della notifica sarà aperto un canale di comunicazione diretto, tramite il quale il CSIRT Italia offrirà al soggetto che effettua la notifica un supporto diretto alle attività di incident handling.

GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

OPERATORI TELCO

CHI SONO I SOGGETTI INDIVIDUATI COME OPERATORI DI TELECOMUNICAZIONE (TELCO)

Gli operatori di telecomunicazioni (TELCO) sono le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi del D.Lgs. 1° agosto 2003 n. 259 "*Codice delle comunicazioni elettroniche*".

Al fine di individuare i soggetti TELCO per cui è prevista la **notifica obbligatoria** dell'incidente al CSIRT Italia, in attuazione e regolamentazione dell'articolo 40 del D.Lgs. n. 259/2003, il MIMIT (già Ministero dello sviluppo economico) ha emanato il **decreto ministeriale del 12 dicembre 2018** "*Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi*" (c.d. D.M. TELCO) nel quale i soggetti TELCO sono definiti (art. 3, co. 2, del citato D.M.) nelle seguenti due categorie:

- **fornitori di reti e servizi di comunicazione elettronica che servono un numero di utenti effettivo pari o superiore all'1% della base di utenti nazionale per ciascun servizio erogato** calcolato sulla base dei dati pubblicati dall'Osservatorio trimestrale delle comunicazioni a cura dell'Autorità per le garanzie nelle comunicazioni (AGCOM[4]);
- **fornitori di reti e servizi di comunicazione elettronica che servono un numero di utenti effettivo pari o superiore ad un milione.**

PERCHÉ NOTIFICARE GLI INCIDENTI AL CSIRT ITALIA

L'articolo 40, comma 3, lettera *b,* del D.lgs. n. 259/2003, stabilisce l'**obbligo di notifica** per i soggetti TELCO al fine di garantire un adeguato livello di sicurezza e una maggiore resilienza delle reti e dei sistemi nazionali.

COSA NOTIFICARE AL CSIRT ITALIA

La normativa vigente prevede l'obbligo di notifica degli incidenti significativi, come stabilito dall'articolo 40, comma 3, lettera b) del D.lgs. n. 259/2003.

[4] https://www.agcom.it/pubblicazioni/osservatori.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

Il soggetto TELCO impattato da un incidente, che rientra nei casi previsti per la notifica obbligatoria verso il CSIRT Italia, deve procedere alla notifica mediante la compilazione e l'invio di un apposito modulo *online*, disponibile sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione).

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

Per i soggetti TELCO, un **incidente di sicurezza** è "*un evento con un reale effetto pregiudizievole per la sicurezza delle reti o dei servizi di comunicazione elettronica*" (**art. 2, comma 1, lett. *u*, del D.lgs. n. 259/2003**).

In accordo all'articolo 5, comma 2 del D.M. TELCO un incidente, considerato significativo, **deve essere notificato obbligatoriamente al CSIRT Italia se ha**:

- **durata superiore ad un'ora** e **percentuale degli utenti colpiti superiore al quindici per cento** del totale degli utenti nazionali del servizio interessato;
- **durata superiore a due ore** e percentuale degli **utenti colpiti superiore al dieci per cento** del totale degli utenti nazionali del servizio interessato;
- **durata superiore a quattro ore** e percentuale degli **utenti colpiti superiore al cinque per cento** del totale degli utenti nazionali del servizio interessato;
- **durata superiore a sei ore** e percentuale degli **utenti colpiti superiore al due per cento** del totale degli utenti nazionali del servizio interessato;
- **durata superiore ad otto ore** e percentuale **degli utenti colpiti superiore all'uno per cento** del totale degli utenti nazionali del servizio interessato.

Un soggetto TELCO dovrà provvedere alla notifica **se viene superata anche solo una delle soglie suddette**.

QUALI SONO I TEMPI DA RISPETTARE PER LA NOTIFICA DI UN INCIDENTE

Il tempo massimo per effettuare la notifica è di 24 ore dall'avvenuta rilevazione dell'incidente (art. 5, co. 3, D.lgs. n. 259/2003).

DURATA DEL DISSERVIZIO	PERCENTUALE DI UTENTI COLPITI	TIPO DI NOTIFICA	TEMPISTICHE
SUPERIORE A **1 ORA**	**> 15%**	**OBBLIGATORIA**	**ENTRO 24 ORE dal rilevamento dell'incidente**
SUPERIORE A **2 ORE**	**> 10%**		
SUPERIORE A **4 ORE**	**> 5%**		
SUPERIORE A **6 ORE**	**> 2%**		
SUPERIORE A **8 ORE**	**> 1%**		

Figura 6: TELCO - tempistiche notifica

SANZIONI PER IL MANCATO ADEMPIMENTO DELL'OBBLIGO DI NOTIFICA

Salvo che il fatto non costituisca reato, il mancato adempimento dell'obbligo di notifica nei termini prescritti per i soggetti TELCO comporta una sanzione amministrativa pecuniaria nei termini previsti dalla normativa vigente: da euro 300.000 ad euro 1.800.000 per la mancata comunicazione di ogni incidente significativo (art. 30, co. 26, lett. b, D.Lgs. n. 259/2003).

FLUSSO DI NOTIFICA PER GLI OPERATORI TELCO

Per i soggetti TELCO le fasi del flusso di notifica proposto nel capitolo 3 includono le seguenti attività.

Fase 1 - Preparazione alla notifica

- **Determinare** il numero di utenti impattati dall'incidente;
- **determinare** la **durata dell'incidente**, delimitata dal periodo tra la prima interruzione completa o parziale del servizio e il momento del ripristino, oppure, nel caso in cui l'incidente e la sua gestione sia ancora in corso, al momento stimato per il ripristino;

- **determinare** la **diffusione geografica** dell'incidente prendendo in considerazione la localizzazione degli utenti, delle persone fisiche e delle persone giuridiche interessate dall'incidente;
- **misurare** l'impatto stimato sull'utenza del servizio interessato in termini percentuali rispetto alla base di utenti nazionale per il medesimo servizio;
- **valutare**, sulla base di indicazioni quali la natura delle sue relazioni contrattuali con i clienti, il **numero potenziale di utenti interessati**, se l'incidente ha causato importanti **perdite materiali o immateriali** per gli utenti, ad esempio in relazione alla salute e alla sicurezza o danni materiali.

Fase 2 - Notifica al CSIRT Italia

Il soggetto segnalante dovrà, entro **ventiquattro (24) ore dall'avvenuta rilevazione dell'incidente**, compilare l'apposito modulo disponibile *online* sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) e fornire le seguenti informazioni:

- date e ora di rilevamento dell'incidente;
- asset impattati;
- vettori d'attacco;
- misure di rientro intraprese e pianificate;
- IOC;
- autovalutazione dell'impatto sul business;
- evidenze rilevanti (es. sample di malware, ransom note).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "infectedacn".

Fase 3 - Gestione della notifica

Dopo aver ricevuto la notifica da parte del soggetto segnalante, il CSIRT Italia offre supporto diretto nelle operazioni di incident handling. Inoltre, **entro cinque giorni** dalla notifica di sicurezza, i soggetti TELCO trasmettono al CSIRT Italia un **rapporto tecnico** dell'incidente in cui sono riportati:

- una descrizione formale dell'incidente;
- la causa dell'incidente;

- le conseguenze dell'incidente sul servizio fornito;
- il dettaglio delle infrastrutture e dei sistemi colpiti;
- l'impatto sulle interconnessioni a livello nazionale;
- le azioni di risposta intraprese per mitigare l'impatto dell'incidente;
- le azioni messe in atto per ridurre la probabilità del ripetersi dell'incidente o di incidenti simili.

Eventuali informazioni rilevanti, emerse successivamente all'invio del suddetto rapporto, saranno oggetto di un'ulteriore integrazione **trasmessa con la massima tempestività** al CSIRT Italia.

Fase 4 - Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, si procederà alla chiusura dell'incidente.

PREPARAZIONE ALLA NOTIFICA

Valutare e determinare:

- il **numero di utenti** impattati dall'incidente;
- la **durata dell'incidente** chiuso o stima del tempo per la relativa chiusura, in caso di incidente in corso;
- la **diffusione geografica** dell'incidente;
- l'**impatto stimato sull'utenza** del servizio interessato;
- eventuali importanti **perdite materiali** o **immateriali** per gli utenti (es.: salute, sicurezza o danni).

NOTIFICA AL CSIRT ITALIA

Fornire le seguenti informazioni:

- **date e ora** di rilevamento dell'incidente;
- **asset impattati**;
- **vettori d'attacco**;
- **misure di rientro** intraprese e pianificate;
- **IOC**;
- **autovalutazione** dell'impatto sul business;
- **evidenze rilevanti** (es. sample di malware, ransom note, ecc.).

GESTIONE DELLA NOTIFICA

A seguito della notifica, CSIRT Italia offre **supporto diretto** nelle operazioni di *incident handling*.
Entro 5 giorni dalla notifica, deve essere trasmesso al CSIRT Italia un **rapporto tecnico** dell'incidente.

CHIUSURA DELL'INCIDENTE

Una volta definite ed avviate le attività di ripristino, viene effettuata la **chiusura dell'incidente**.

Figura 7: TELCO - flusso notifica

GUIDA ALLA NOTIFICA INCIDENTI AL CSIRT ITALIA

OPERATORI TELCO

SOGGETTI TELCO

Fornitori di reti e servizi di comunicazione elettronica che: servono un numero di utenti effettivo pari o superiore all'1% della base di utenti nazionale per ciascun servizio erogato, calcolato sulla base dei dati pubblicati dall'Osservatorio trimestrale delle comunicazioni a cura dell'Autorità per le garanzie nelle comunicazioni (AGCOM); servono un numero di utenti effettivo pari o superiore ad un milione.

PERCHÈ NOTIFICARE AL CSIRT ITALIA

L'obbligo di notifica degli incidenti per i soggetti TELCO è previsto dall'art. 40 del D.lgs. n. 259/2003 e regolamentato dal D.M. del 12 dicembre 2018 (DM TELCO).

COSA NOTIFICARE AL CSIRT ITALIA

La notifica obbligatoria va effettuata per gli incidenti significativi, come stabilito dall'articolo 40, comma 3 del D.lgs. n. 259/2003 e successive modificazioni.

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

I parametri di significatività dell'Incidente sono stabiliti dal DM TELCO.

CON QUALI TEMPISTICHE

La notifica è obbligatoria entro le 24 ore dall'avvenuta rilevazione dell'incidente (Art. 5 co. 3 DM TELCO).

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della notifica, sarà aperto un canale di comunicazione diretto tramite il quale il CSIRT Italia offrirà supporto alle attività di incident handling al soggetto che effettua la notifica.

GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

SOGGETTI LEGGE N. 90/2024

CHI SONO I SOGGETTI INCLUSI NELLA LEGGE N. 90/2024

L'articolo 1 della **legge n. 90/2024** "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", impone obblighi di notifica ai soggetti individuati al comma 1 del medesimo articolo, che comprendono:

- pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
- regioni;
- province autonome di Trento e di Bolzano;
- città metropolitane;
- comuni con popolazione superiore a 100.000 abitanti;
- comuni capoluoghi di regione;
- società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- aziende sanitarie locali.

Tra i medesimi soggetti ricadono le società in house dei soggetti precedentemente elencati che forniscono i seguenti servizi:

- servizi informatici;
- servizi di trasporto di cui al precedente elenco;
- servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991;
- servizi di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

Per le altre amministrazioni, non identificate nella predetta Legge n. 90/2024 e non soggette ad alcun vincolo normativo di notifica, si applica quanto riportato nella sezione ULTERIORI SOGGETTI.

PERCHÉ SEGNALARE E NOTIFICARE GLI INCIDENTI AL CSIRT ITALIA

L'articolo 1, co. 2 della Legge n. 90/2024, stabilisce che i soggetti indicati devono **segnalare entro ventiquattro ore** gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del D.L. n. 105/2019, convertito con modificazioni dalla citata legge, e **notificare entro settantadue ore** tutti gli elementi informativi disponibili.

COSA SEGNALARE E NOTIFICARE AL CSIRT ITALIA

L'articolo 1, co. 2, della Legge n. 90/2024, stabilisce che i soggetti devono **segnalare** e **notificare** al CSIRT Italia qualunque incidente riconducibile ad una delle tipologie individuate nella tassonomia di cui all'articolo 1, comma 3-bis, del D.L. n. 105/2019, ossia gli **incidenti riconducibili agli ICP-C** di cui alla sezione SOGGETTI PSNC.

Al di fuori di quanto sopra esposto, i soggetti Legge n. 90/2024, possono effettuare **notifiche volontarie** al CSIRT Italia, secondo quanto prescritto dall'articolo 18, commi 3, 4, 5 del D.Lgs. n. 65/2018.

COME EFFETTUARE UNA SEGNALAZIONE E SUCCESSIVA NOTIFICA AL CSIRT ITALIA

I soggetti Legge n. 90/2024 coinvolti in un incidente, devono inviare una segnalazione e successivamente una notifica completa tramite la compilazione e l'invio di un apposito modulo online disponibile sul sito web del CSIRT Italia (https://www.csirt.gov.it/segnalazione).

COME RICONOSCERE UN INCIDENTE DA SEGNALARE E NOTIFICARE

Si rinvia a quanto riportato nella sezione SOGGETTI PSNC, con riferimento agli **incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT** e **riconducibili alla tassonomia ICP-C**.

QUALI SONO I TEMPI DA RISPETTARE PER LA SEGNALAZIONE E LA NOTIFICA DI UN INCIDENTE

Secondo quanto stabilito dall'art.1, comma 2 della Legge n. 90/2024:

- La **segnalazione** deve essere effettuata senza ritardo e comunque **entro 24 ore** dal momento in cui si viene a conoscenza dell'incidente a seguito delle evidenze comunque ottenute, necessaria a informare tempestivamente e avviare le procedure di gestione, senza attendere ulteriori dettagli o conferme.
- La **notifica**, relazionata alla precedente segnalazione, deve essere effettuata **entro 72 ore** a decorrere dal medesimo momento e rappresenta una comunicazione completa di tutti gli elementi informativi disponibili.

Figura 8: Soggetti Legge n. 90/2024 - tempistiche notifica

SANZIONI PER IL MANCATO ADEMPIMENTO DELL'OBBLIGO DI SEGNALAZIONE E NOTIFICA

Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica è prevista una sanzione amministrativa pecuniaria **da euro 25.000 a euro 125.000** a carico dei soggetti. La violazione delle disposizioni del comma 1 del suddetto articolo può costituire causa di **responsabilità disciplinare e amministrativo-contabile** per i funzionari e i dirigenti responsabili (art.1, co. 6, Legge n. 90/2024).

FLUSSO DI SEGNALAZIONE E NOTIFICA PER I SOGGETTI INCLUSI NELLA LEGGE N. 90/2024

Dopo aver effettuato la **segnalazione** di incidente attraverso il modulo online dedicato, disponibile sul sito del CSIRT Italia (https://www.csirt.gov.it/segnalazione), la **successiva relativa notifica** segue le fasi del flusso descritte nel capitolo 3 e include le seguenti attività.

Fase 1 – Preparazione alla notifica

Le attività consigliate da effettuare durante questa fase sono le seguenti:

- raccolta delle evidenze (es. IOC, evidenze, azioni di ripristino) relative all'incidente stesso;
- identificazione dei sistemi impattati;
- autovalutazione dell'impatto sui sistemi e sull'erogazione dei servizi di business;

- definizione e pianificazione di un piano di rientro.

Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

Fase 2 - Notifica al CSIRT Italia

Il soggetto segnalante dovrà compilare l'apposito modulo disponibile online sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) e fornire le seguenti informazioni:

- data e ora di rilevamento dell'incidente;
- asset impattati;
- vettori d'attacco;
- misure di rientro intraprese e pianificate;
- IOC;
- evidenze rilevanti (es. sample di malware, ransom note).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "infectedacn".

Fase 3 - Gestione della notifica

Dopo aver ricevuto la segnalazione e la notifica da parte del soggetto segnalante, il CSIRT Italia compatibilmente con le risorse a disposizione e la criticità del soggetto segnalante offrirà supporto, se del caso *in loco*, nelle operazioni di incident handling.

I soggetti segnalanti sono chiamati a garantire il pieno supporto al personale del CSIRT Italia durante le suddette operazioni, compreso l'accesso a locali e sistemi informativi delle amministrazioni coinvolte, come da **Direttiva del Presidente del Consiglio dei ministri del 6 luglio 2023**, in cui si enfatizza l'importanza di una collaborazione completa per acquisire una conoscenza dettagliata della situazione, necessaria per la prevenzione e la gestione degli incidenti di cybersicurezza.

Fase 4 - Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, si procederà alla chiusura dell'incidente.

PREPARAZIONE ALLA NOTIFICA

Le attività consigliate da effettuare sono le seguenti:

- **raccolta** delle evidenze (es. IOC, evidenze, azioni di ripristino) relative all'incidente stesso;
- **identificazione** dei sistemi impattati;
- **autovalutazione** dell'impatto sui sistemi e sull'erogazione dei servizi di business;
- definizione e pianificazione di un **piano di rientro**.

Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

NOTIFICA AL CSIRT ITALIA

Fornire le seguenti informazioni:

- **data e ora** di rilevamento dell'incidente;
- **asset impattati;**
- **vettori d'attacco**;
- **misure di rientro** intraprese e pianificate;
- **IOC**;
- **evidenze** rilevanti (es. sample di malware, ransom note).

GESTIONE DELLA NOTIFICA

Dopo aver ricevuto la notifica da parte del soggetto segnalante, CSIRT Italia compatibilmente con le risorse a disposizione e la criticità del soggetto segnalante offrirà supporto, se del caso in loco, nelle operazioni di incident handling.

CHIUSURA DELL'INCIDENTE

Una volta definite ed avviate le attività di ripristino, si procederà alla **chiusura dell'incidente**.

Figura 9: Soggetti Legge n. 90/2024 - flusso notifica

GUIDA ALLA SEGNALAZIONE E NOTIFICA INCIDENTI AL CSIRT ITALIA

SOGGETTI LEGGE N. 90/2024

SOGGETTI LEGGE N. 90/2024

Soggetti individuati dall'art.1, comma 1 della Legge n. 90/2024 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

PERCHÈ SEGNALARE E NOTIFICARE AL CSIRT ITALIA

L'obbligo di segnalazione e successiva notifica è previsto dall'art.1, comma 2 della Legge n. 90/2024 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

COSA SEGNALARE E NOTIFICARE AL CSIRT ITALIA

Qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1, come stabilito dall'art.1, comma 2 della Legge n. 90/2024 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

COME RICONOSCERE UN INCIDENTE DA SEGNALARE E NOTIFICARE

Un incidente è da definirsi tale quando incide sulla protezione, disponibilità, accessibilità, integrità e riservatezza dei dati e sulla continuità operativa dei sistemi e delle infrastrutture.

CON QUALI TEMPISTICHE

La segnalazione e notifica sono obbligatorie:

- Segnalazione entro 24 ore;
- Notifica successiva entro 72 ore.

COME EFFETTUARE UNA SEGNALAZIONE E SUCCESSIVA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una segnalazione e successiva notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della segnalazione sarà aperto un canale di comunicazione diretto, relazionato alla successiva notifica, tramite il quale il CSIRT Italia offrirà al soggetto supporto alle attività di incident handling.

GUIDA ALLA NOTIFICA DEGLI INCIDENTI AL CSIRT ITALIA

ULTERIORI SOGGETTI

CHI SONO GLI ULTERIORI SOGGETTI

Pubbliche Amministrazioni non ricomprese nella Legge n. 90/2024, Piccole e Medie Imprese, privati cittadini che non operano in settori critici e non sono vincolati da obbligo normativo di notifica incidente cyber.

PERCHÉ NOTIFICARE GLI INCIDENTI AL CSIRT ITALIA

La notifica al CSIRT Italia permette al soggetto di aprire gli opportuni canali di comunicazione tecnica con il personale specializzato del CSIRT Italia e, nel contempo, contribuisce alla raccolta di dati relativi alle minacce che insistono sul cyberspazio nazionale. Nello specifico favorisce, quindi, la più ampia diffusione possibile di una consapevole cultura nel campo della cybersecurity e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.

COSA NOTIFICARE AL CSIRT ITALIA

Al di fuori degli obblighi derivanti dalla normativa di riferimento, gli ulteriori soggetti possono notificare in **forma volontaria** gli incidenti di sicurezza, nonché qualsiasi evento cyber con potenziale impatto su almeno un soggetto nazionale.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

Il soggetto segnalante impattato da un incidente, che ha intenzione di comunicarlo al CSIRT Italia, può procedere in tal senso attraverso la compilazione e l'invio di un apposito modulo *online*, disponibile sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione).

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

Un incidente che abbia causato la perdita di riservatezza, disponibilità o integrità del bene informatico impattato.

QUALI SONO I TEMPI DA RISPETTARE PER LA NOTIFICA DI UN INCIDENTE

Per tali soggetti segnalanti, non essendo presente un quadro normativo di riferimento, non sono previste tempistiche da rispettare per la notifica di un incidente al CSIRT Italia. Tuttavia, è consigliabile procedere con la notifica nel più breve tempo possibile.

FLUSSO DI NOTIFICA PER GLI ULTERIORI SOGGETTI

Per gli ulteriori soggetti, le fasi del flusso di notifica cui al capitolo 3 includono le seguenti attività.

Fase 1 - Preparazione alla notifica

Gli **ulteriori soggetti** che hanno intenzione di effettuare **volontariamente** la notifica al CSIRT Italia è bene che raccolgano **tutte le informazioni pertinenti** per descrivere in modo dettagliato l'incidente. Questo aiuterà a fornire al CSIRT Italia una visione chiara e concisa dell'incidente in corso di gestione, facilitando così un supporto più efficace.

Fase 2 - Notifica al CSIRT Italia

Il soggetto segnalante dovrà compilare l'apposito modulo disponibile online sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) e fornire le seguenti informazioni:

- data e ora di rilevamento dell'incidente;
- asset impattati;
- vettori d'attacco;
- misure di rientro intraprese e pianificate;
- IOC;
- evidenze rilevanti (es. sample di malware, ransom note).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "infectedacn".

Fase 3 - Gestione della notifica

Dopo aver ricevuto la notifica da parte del soggetto segnalante, il CSIRT Italia, compatibilmente con le risorse a disposizione e la criticità del soggetto segnalante, offrirà supporto, se del caso in loco, nelle operazioni di incident handling.

Fase 4 - Chiusura dell'incidente

Una volta definite ed avviate le attività di ripristino, si procederà alla chiusura dell'incidente.

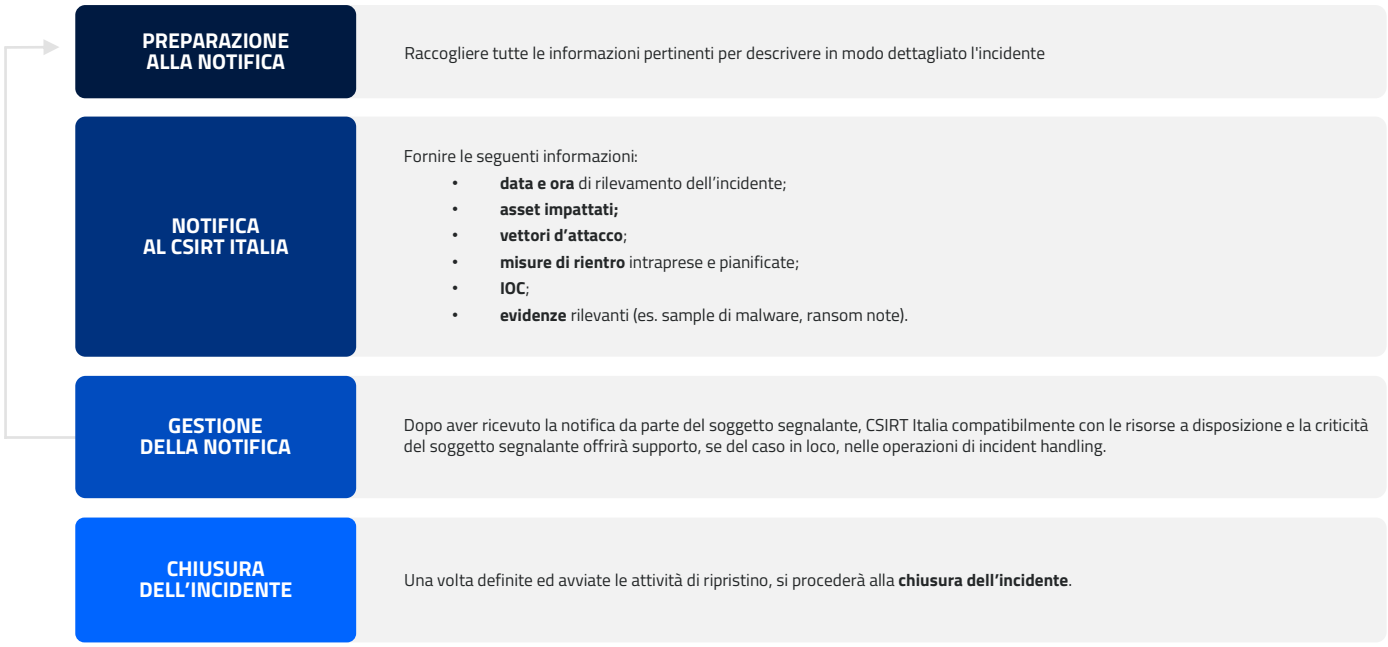

Figura 10: Ulteriori soggetti - flusso notifica

GUIDA ALLA NOTIFICA INCIDENTI AL CSIRT ITALIA

ULTERIORI SOGGETTI

ULTERIORI SOGGETTI

Pubbliche Amministrazioni escluse dalla Legge n. 90/2024, Piccole e Medie Imprese, privati cittadini che non operano in settori critici e non sono vincolati da obbligo normativo di notifica incidente cyber e non rientrano tra i soggetti per cui sussiste un riferimento normativo che li definisce.

PERCHÈ NOTIFICARE AL CSIRT ITALIA

Per contribuire alla raccolta di dati relativi alle minacce che insistono sul cyberspazio nazionale.

COSA NOTIFICARE AL CSIRT ITALIA

Notifica volontaria degli incidenti ed eventi cyber che rilevanti in termini di impatto sui beni informatici dei soggetti segnalanti.

COME RICONOSCERE UN INCIDENTE DA NOTIFICARE

Un incidente informatico che abbia causato la perdita di riservatezza, disponibilità o integrità del bene informatico impattato.

CON QUALI TEMPISTICHE

La notifica è volontaria:
nessuna tempistica defnita.

COME EFFETTUARE UNA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della notifica sarà aperto un canale di comunicazione diretto tramite il quale il CSIRT Italia offrirà al soggetto che effettua la notifica supporto in base alla criticità dell'incidente segnalato.

4 CONSIDERAZIONI FINALI

La corretta adozione della procedura di notifica degli incidenti cibernetici al CSIRT Italia costituisce un elemento cruciale per garantire la sicurezza e resilienza delle risorse digitali.

A tal fine sul sito internet del CSIRT Italia (https://www.csirt.gov.it/segnalazione) ACN mette a disposizione dei diversi soggetti segnalanti l'apposito modulo per effettuare tale adempimento.

Le informazioni da raccogliere mediante la compilazione del predetto modulo e i termini da rispettare per l'assolvimento dell'obbligo di notifica sono stabiliti, per i diversi soggetti, dalla normativa cyber.

Per i **soggetti che operano in settori critici**, vincolati a specifiche regolamentazioni, si rende indispensabile la conformità ai vincoli di legge nel corso del processo di notifica. Tale conformità non solo si traduce nella risposta a obblighi normativi, ma costituisce altresì una premessa essenziale per garantire una risposta appropriata e tempestiva da parte del CSIRT Italia.

Per i **soggetti non vincolati da obblighi normativi** specifici, la fase di notifica mantiene comunque una rilevanza cruciale nella gestione degli incidenti. In tutti i casi, la prontezza e la precisione delle informazioni fornite durante il processo di notifica rivestono un ruolo fondamentale in quanto consentono al CSIRT Italia di acquisire una sempre più completa ed esaustiva conoscenza dell'incidente occorso e conseguentemente di fornire ai soggetti impattati il supporto necessario all'individuazione ed implementazione delle azioni da attuare nell'immediato per il contenimento dell'incidente, nonché di quelle volte al ripristino di una più efficiente erogazione dei servizi.

La presente linea guida sarà oggetto di revisione, soprattutto in considerazione dell'implementazione a livello nazionale della direttiva europea NIS2 o di eventuali ulteriori emendamenti alle legislazioni citate nel documento.

ACRONIMI

Termini	Definizioni
ACN	Agenzia per la Cybersicurezza Nazionale
CCE	Codice delle Comunicazioni Elettroniche
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
D. Lgs.	Decreto Legislativo
D.L.	Decreto-Legge
DPCM	Decreto del Presidente del Consiglio dei ministri
FSD	Fornitori di Servizi Digitali
ICP	Incidente con Impatto
NIS	Network and Information Systems
OSE	Operatori di Servizi Essenziali
PSNC	Perimetro di Sicurezza Nazionale Cibernetica
UE	Unione Europea

Tabella 1: Acronimi

RIFERIMENTI NORMATIVI

Riferimento	Link
Decreto legislativo 30 luglio 1999, n. 300 *Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59.*	Link online
Decreto legislativo 30 marzo 2001, n. 165 *Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.*	Link online
Decreto legislativo 1° agosto 2003, n. 259 *Codice delle comunicazioni elettroniche (CEE).*	Link online
Decreto legislativo 7 marzo 2005, n. 82 *Codice dell'amministrazione digitale.*	Link online
Decreto legislativo 19 agosto 2016, n. 175 *Testo unico in materia di società a partecipazione pubblica.*	Link online
AgID – Circolare 18 aprile 2017, n. 2 *Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».*	Link online
Regolamento di esecuzione (UE) 2018/151 della commissione del 30 gennaio 2018 *recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.*	Link online
Decreto legislativo 18 maggio 2018, n.65 *Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6*	Link online

luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.	
Decreto Ministeriale TELCO del 12 dicembre 2018 *Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi.*	Link online
Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 *Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano.*	Link online
Decreto-legge 21 settembre 2019, n. 105 *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.*	Link online
Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 *Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.*	Link online
Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81 *Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.*	Link online
Decreto-legge 14 giugno 2021, n. 82 *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.*	Link online
Legge 4 agosto 2021, n. 109 *Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.*	Link online
Decreto legislativo 8 novembre 2021, n. 207 *Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione).*	Link online
Determina dell'Agenzia per la Cybersicurezza Nazionale del 3 gennaio 2023 *Tassonomia degli incidenti che debbono essere oggetto di notifica.*	Link online
Direttiva del Presidente del Consiglio dei ministri del 6 luglio 2023	Link online

Indirizzi di coordinamento e organizzazione volti a promuovere la gestione adeguata e coordinata delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica.	
Legge 28 giugno 2024, n. 90 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.*	Link online

Tabella 2: Riferimenti normativi