Dalla NIS1 alla NIS2, per approdare alla Legge 90/2024

Guida pratica alla notifica degli incidenti

Introduzione

Ormai da anni la comunità Europea si sta ritagliando sempre più un ruolo di rilievo nello scenario globale in materia di sicurezza dei dati e delle informazioni, definendo i confini geografici e normativi nei rapporti con tutti i paesi terzi per l'erogazione dei servizi destinati all' Europa ed ai suoi interessati, ed erogati dagli operatori interni. Ma non solo, l'Europa sta lavorando molto anche per innalzare il livello generale della sicurezza informatica dei paesi membri, sia dei soggetti pubblici che privati. Dopo il Regolamento UE 2016/679 Regolamento Privacy ed è stata la volta della Direttiva NIS1 Dir. 2016/1148 e da lì in poi un'escalation di atti e pubblicazioni, come il Regolamento Cybersecurity Act, per approdare alla Direttiva NIS2 Dir. 2022/2555.

L'approccio generale definito è quello di una regia di coordinamento europea (CSIRT Network) per la gestione degli incidenti di cybersicurezza relativi ai servizi essenziali e non essenziali, che si verificano all'interno dei paesi membri.

L'Italia in questo ha recepito tali direttive istituendo il CSIRT e ponendo questo team all'interno dell'ACN.

Nel corso degli anni fino alla prossima pubblicazione del decreto di recepimento della NIS2, sono stati emanati una serie di DPCM e DL per definire ruoli, tempi, modalità, e le definizioni per l'applicazione della Direttiva NIS1 ed il Cybersecurity ACT, già orientati alla NIS2.

La nuova NIS2 porta con sé in dote l'obbligo e la volontarietà della notifica degli incidenti al CSIRT, in questa guida ci preoccupiamo proprio di questo aspetto e di fare un focus esteso sulle modalità di notifica cercando di dare con i giusti modi le informazioni necessarie per comprendere la classificazione dei soggetti destinatari della NIS2 e quindi alla notifica, un cenno al quadro normativo e la sponda agli standard normativi che predispongono i soggetti pubblici e privati all'erogazione dei servizi oggetto delle misure di cybersicurezza della NIS2, necessari per l'erogazione di tali servizi agli operatori pubblici e privati ed agli utilizzatori finali.

In tutto ciò è opportuno ricordare che la NIS2 si applica oltre che alle organizzazioni classificate come "Soggetti essenziali", anche alla catena di approvvigionamento come definito all'art. 21/2 lett. d) della Direttiva NIS2.

Glossario e definizioni

ACN, Agenzia per la cybersicurezza nazionale;
CSIRT, Computer Security Incident Response Team, Istituito con D.Lgs 65/2018 in attuazione alla Direttiva 2016/1148 Direttiva NIS1;
PSNC, Perimetro di Sicurezza Nazionale Cibernetica
OSE, Operatori di servizi Essenziali
FSD, Fornitori di servizi Digitali
TELCO, Operatori di servizi di telecomunicazione

Schema normativo

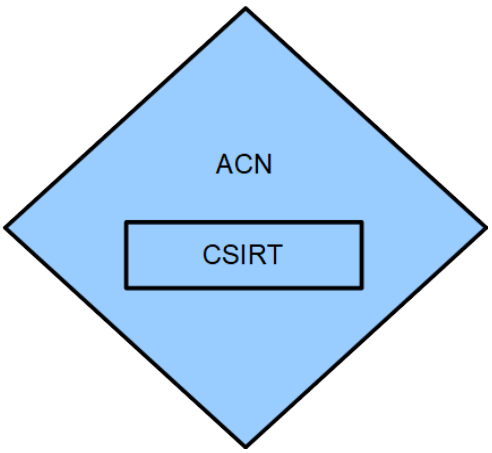
Nello schema che segue viene riportata l'evoluzione del quadro normativo dalla pubblicazione delle Direttive europee al quadro normativo italiano.

Direttive Europee	Italia	Estensioni
Dir. NIS1 Dir. 2016/1148	Decreto recepimento NIS1 L. 65/2018 Istituzione CSIRT	
Regolamento di esecuzione 2018/151		DM TELCO 12 dicembre 2017
		D.L. 105/2019 PSCN
		DPCM 131/2020 Soggetti
		DPCM 81/2021 Notifica degli incidenti
		DL 82/2021 Istituzione ACN
		DPCM 15.06.21 Beni, servizi e sistemi ICT per il PSCN
Reg. UE 881/19 Cyber Security ACT	Decreto di recepimento 123/22 Cyber Security ACT	
		Determina ACN 3.1.2023 Classificazione degli incidenti
Dir. NIS2 Dir. 2022/2555	L. 90/2024	

Ruolo del CSIRT

Nel contesto italiano il servizio del CSIRT è stato inglobato all'interno dell'ACN e di fatti chi volesse oggi avviare una segnalazione relativa ad un incidente informatico, potrà notare raggiungendo il sito https://www.csirt.gov.it/ a presenza del logo di ACN presente anche nella sezione dedicata alle segnalazioni https://www.csirt.gov.it/segnalazione

Al CSIRT sono delegate le funzioni previste dalla Direttiva NIS1:
- Prevenzione, coordinamento e risposta ad eventi ed incidenti informatici;
- Punto di riferimento per le notifiche degli incidenti per PA, OSE e FSD ed obbligati definiti nella L. 90/2024;
- Cooperazione internazionale in Europa con i CSIRT europei nel CSIRT Network.



Notifica di un incidente

Fatta chiarezza su ruoli, sigle, nomi degli attori e del contesto, possiamo passare all'oggetto di questa guida pratica, le modalità con cui avviare una segnalazione obbligatoria e/o volontaria al CSIRT, le modalità con cui inviarle ed i tempi da rispettare per non incorrere in sanzioni.

Le quattro fasi della notifica di un incidente:
Per tutti gli operatori, e per tutti i tipi di segnalazioni, obbligatorie e volontarie, le fasi di notifica sono sempre quattro: *preparazione, notifica, gestione della notifica e chiusura dell'incidente*, ogni attore sarà obbligato al rispetto di queste quattro fasi con modalità e tempi diversi in funzione del proprio ruolo e del tipo di incidente.

Preparazione
Fase di preparazione della comunicazione che prevede la raccolta delle informazioni utili e necessarie al CSIRT per valutare la potenziale criticità dell'incidente.

Notifica
Compilazione del modulo di segnalazione disponibile al sito: https://www.csirt.gov.it/segnalazione.

Gestione della notifica
In base al tipo di incidente segnalato ed in funzione della criticità e del soggetto segnalante il CSIRT decide ed avvia il supporto da remoto od in loco e le eventuali misure successive alla risoluzione dell'incidente.

Chiusura dell'incidente
Terminate le attività di gestione dell'incidente da parte del segnalante, il CSIRT chiude l'incidente.

Vediamo adesso nello specifico quali sono le attività da compiere per queste quattro fasi per ognuno dei ruoli che classificano gli attori obbligati e non ad inviare una notifica al CSIRT.

Notifica dei soggetti PSCN

I PSNC sono amministrazioni ed enti pubblici dai quali dipende l'esercizio di una funzione o di un servizio essenziale dello Stato. Il loro elenco è riservato. La segnalazione da parte di queste figure può essere obbligatoria o volontaria in base alla corrispondenza dei tipi di incidenti classificati secondo la definizione dell' Allegato A DPCM 81/2021.

La notifica viene effettuata tramite il sito https://www.csirt.gov.it/segnalazione

Gli incidenti da notificare sono classificabili come eventi di natura accidentale od intenzionale, che determinano il malfunzionamento, l'interruzione o l'utilizzo improprio di rete, sistemi informativi o dei servizi informatici, secondo la classificazione delle categorie ICP-A, ICP-B definite all'Allegato A DPCM 81/2021, e ICP-C definite con Determina ACN 3 gennaio 2023.

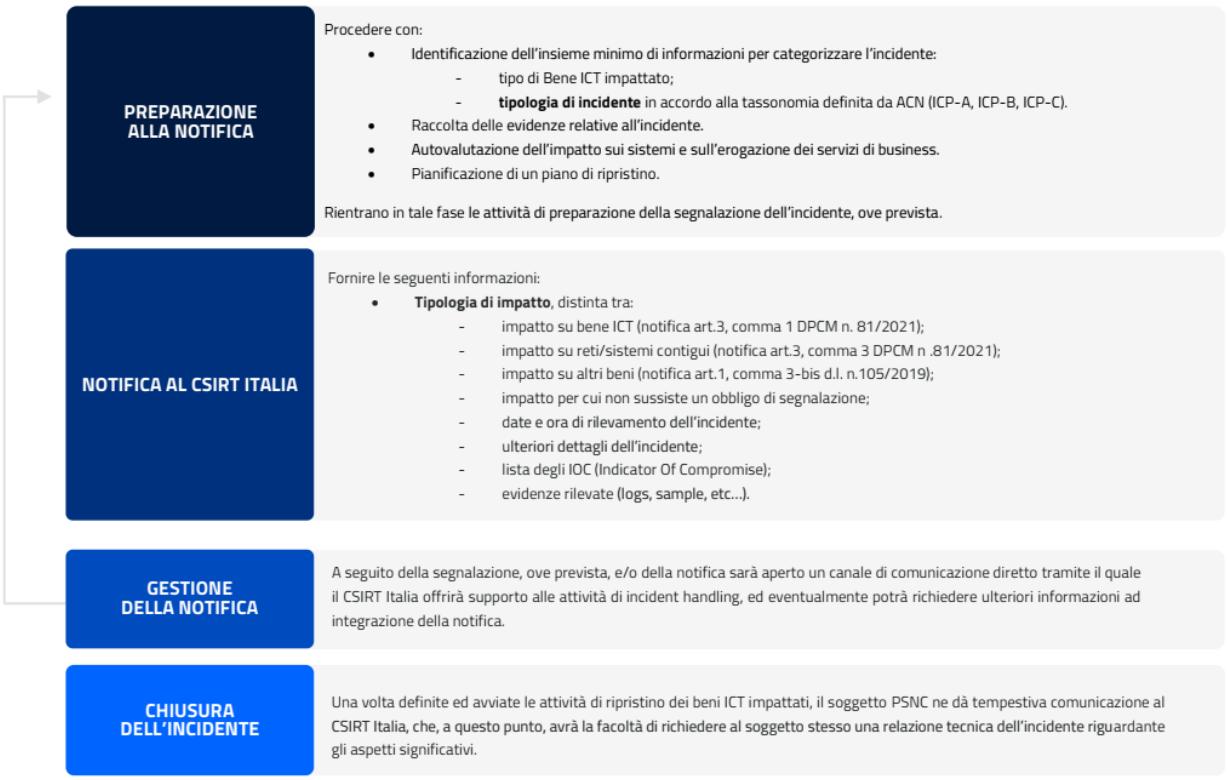
Dal momento in cui si è venuti a conoscenza dell'incidente, per le notifiche obbligatorie, la stessa deve essere formulata entro 1 ora per gli incidenti classificati di tipo ICP-B, entro 6 ore per gli incidenti classificati di tipo ICP-A, 24 ore per gli incidenti classificati di tipo ICP-C.

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**

Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

La mancanza della notifica obbligatoria, comporta una sanzione amministrativa da euro 250k a 1.150k per gli incidenti con obbligo di notifica di cui all'art. 1 co. 3 let. A DL 105/2019 e da euro 25k a 125k per gli incidenti di cui all'art. 1 co. 3-bis DL 105/2019.

Il sistema di notifica a quattro fasi è quello già descritto; di seguito un dettaglio del caso specifico per i soggetti PSNC.



Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

NIS2 vs ISO27001

L' approfondimento di questi due articoli porta ad una sintesi che definisce negli elenchi di seguito riportati gli aspetti fondamentali da prendere in considerazione e di cui tener conto, per una corretta valutazione del livello di sicurezza da applicare per questi due attori.

Elementi di controllo per la sicurezza delle reti e dei sistemi informativi:
a) la sicurezza dei sistemi e degli impianti;
b) trattamento degli incidenti;
c) gestione della continuità operativa;
d) monitoraggio, audit e test;
e) conformità con le norme internazionali

Paramentri di rilevanza per l'impatto di un incidente:
a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi;
b) la durata dell'incidente;
c) la diffusione geografica relativamente all'area interessata dall'incidente;
d) la portata della perturbazione del funzionamento del servizio;
e) la portata dell'impatto sulle attività economiche e sociali.

Per richiamare modelli e standard di riferimento e per permettere il giusto orientamento per le organizzazioni che dovranno adeguarsi ed aderire alla Direttiva NIS2, possiamo sicuramene affermare che una applicazione rigorosa della norma ISO27001:2022 ed in affiancamento ad essa, lanorma ISO31000:2018, possono soddisfare a pieno le indicazioni della Direttiva NIS2.

Notifica dei soggetti OSE e FSD

La definizione dei soggetti OSE e FSD è frutto del D. Lgs 65/2018 in attuazione della Direttiva UE 2016/1148 (direttiva NIS1).

Operatori dei servizi essenziali OSE
Rientrano in questa definizione gli operatori dei seguenti settori: Energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione acqua potabile, infrastrutture digitali.

Fornitori dei servizi digitali FSD
Rientrano in questa definizione le figure che forniscono servizi digitali appartenenti alle seguenti tipologie: mercato online, motori di ricerca, servizi di cloud computing.

Gli elenchi di questi due tipi di soggetti sono aggiornati almeno ogni due anni.

La notifica relativa agli incidenti in questo caso è obbligatoria per tutti gli incidenti che possono determinare un impatto rilavante sulla continuità deli servizi essenziali forniti per gli OSE e sulla continuità dei servizi digitali forniti dagli operatori FSD.

Per entrambe questi soggetti sono definite le soglie che classificano la gravità degli incidenti, rispettivamente per gli operatori OSE nell'art. 12 D. Lgs 65/2018 e per gli operatori FSD nell'art. 14 D. Lgs 65/2018.

La comunicazione di questi incidenti è di natura volontaria, e va fatta sempre attraverso il sito: https://www.csirt.gov.it/segnalazione

Le notifiche obbligatorie di questi due attori devono essere fatte verso il CSIRT senza ingiustificato ritardo, ed anche in questo caso la mancata notifica espone questi due attori a sanzioni amministrative, che in applicazione dell'art. 12 comma 5 e dell'art 21 comma 3 D.Lgs 65/2018, prevede una sanzione da minimo 25.000 euro fino a 125.000 euro.

Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

Il flusso e le fasi di notifica per questi due attori sono quelli già descritti nel paragrafo "Notifica di un incidente"; fatta salva la necessità per OSE e FSD di comunicare nella fase 1 di preparazione della notifica alcune informazioni aggiuntive, ecco un riepilogo:

OSE e FSD:
- numero di utenti impattati nell'incidente
- durata dell'incidente
- diffusione geografica

solo per gli FSD, l' impatto dell'incidente per le caratteristiche di:

- Disponibilità
- Autenticità
- Integrità o riservatezza

relativi ai dati o ai servizi correlati.

Ecco lo schema di riepilogo per le notifiche di OSE e FSD:

Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

NIS2 vs ISO27001

Volendo fare un altro parallelismo fra NIS2 e ISO27001, noteremo come la misura dell'impatto su Riservatezza, Integrità e Disponibilità del dato, sia la medesima definita nel SGSI della ISO27001, ma non solo, anche nell' art. 32 del UE 2016/679 GDPR, si parla di alterazione del dato personale in relazione proprio alle violazioni di riservatezza, integrità e disponibilità del dato stesso.

L'approccio pertanto è il medesimo con una estensione per la notifica degli incidenti al CSIRT per gli OSE e gli FSD che dovranno notificare oltre all'impatto RID dei dati, anche quello per i servizi correlati.

Notifica degli operatori TELCO

Per Operatori TELCO si intendono così come definite dal D.Lgs 259/2003, tutte quelle figure che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico.

Per questi attori il DM TELCO del 12 dicembre 2018, ha definito i criteri per i quali è prevista la notifica obbligatoria, classificando l'obbligo per due categorie di operatori, quelli che erogano servizi che servono un numero di utenti superiore all' 1% della base degli utenti nazionali per ogni servizio erogato o che servono un numero complessivo di utenti superiore ad un milione per ogni servizio erogato.

L' art 40 comma 3 del D.Lgs 259/2003 definisce l'obbligo di notifica per questi operatori, per tutti gli incidenti classificabili come significativi.

Le modalità e le fasi di notifica sono quelle già definite nel paragrafo "Notifica di un incidente" da effettuare tramite il link https://www.csirt.gov.it/segnalazione.

Quello che cambia rispetto agli altri attori è l'obbligo di notifica per determinati tipi di incidenti in funzione del numero di utenti interessati in percentuale rispetto agli utenti nazionali del medesimo servizio.

Le notifiche dovranno essere effettuate entro le 24 ore dall'avvenuta rilevazione dell'incidente.

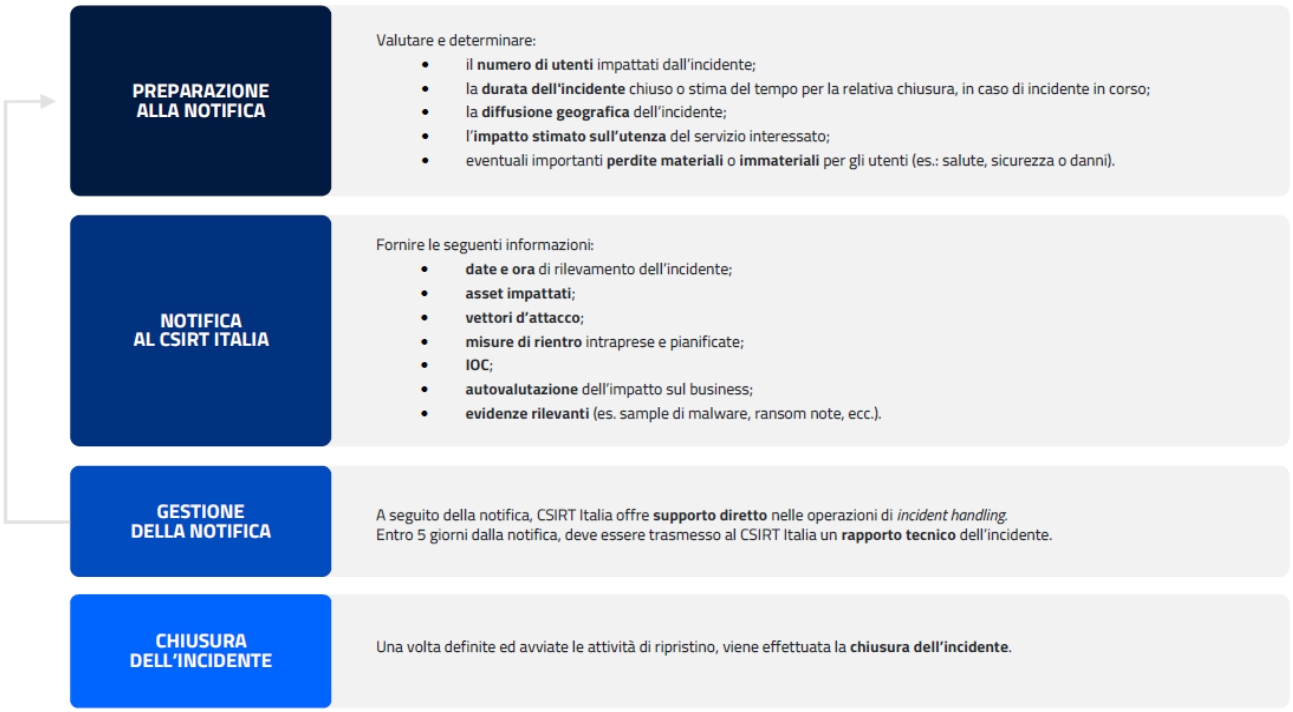
Anche per questi attori sono previste sanzioni per il mancato adempimento di notifica, definite dall'art. 30 del D.Lgs 259/2003, che vanno dal 300k euro a 1.800k euro, per la mancata comunicazione.

Ecco la tabella di riepilogo per la notifica:

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%		

Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

Anche per questi attori, la notifica a quattro fasi si articola con la raccolta di una serie di informazioni necessarie, ecco lo schema di riepilogo del flusso di notifica:



Fonte: Guida alla notifica degli incidenti al CSIRT Italia – ACN

Notifica dei soggetti Legge n.90/2024

Con l'obiettivo di estendere la cultura della cybersicurezza e di estendere l'obbligo di notifica degli incidenti informatici, il legislatore italiano con la Legge 90/2024 ha esteso ad una serie di figure e attori questo obbligo, ecco l'elenco delle figure:

- pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, Legge 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.

Questo elenco si estende per tutte le società in house dei soggetti precedenti che realizzano e forniscono servizi nei seguenti ambiti:

- 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.

L' obbligo si estende a tutti gli incidenti riconducibili a quelli della classificazione ICP-C come già visto per i soggetti PSNC.

Per tutti questi soggetti è fatto obbligo di segnalazione al CSIRT entro le 24 ore dall'avvenuta conoscenza di un incidente, se questo rientra in quelli classificati secondo la classificazione dell'art 1 comma 3-bis DL 105/2009, con obbligo di notifica di tutti gli elementi informativi entro le 72 ore.

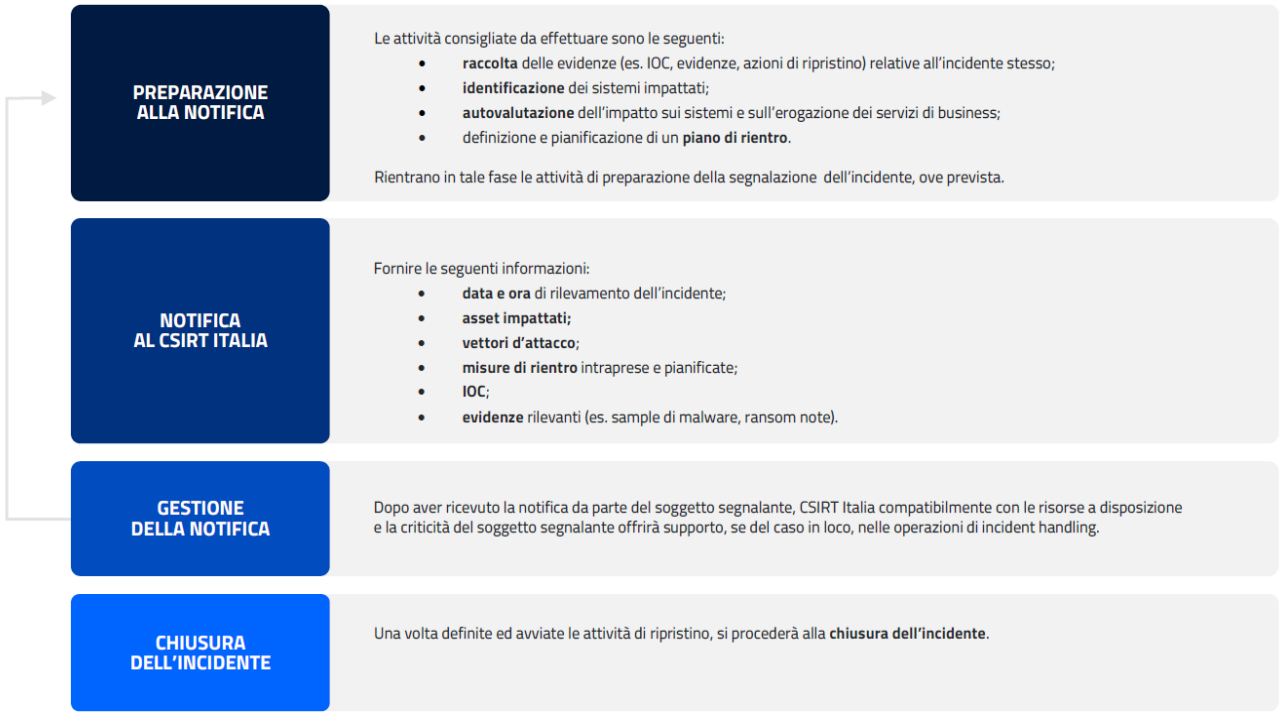
Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

Le modalità e le fasi della notifica sono le medesime di quelle già viste per i soggetti PSNC esclusivamente per gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT sempre riconducibili alla tassonomia ICP-C.

Come detto oltre alla segnalzione è fatto obbligo di notifica con le stesse modalità già viste per gli altri soggetti, tramite il link https://www.csirt.gov.it/segnalazione.

Anche per queste figure ed attori sono previste delle sanzioni per la mancata notifica, per la reiterata inosservanza di questo obbligo nell'arco di 5 anni. La sanzione va da un minimo di 25k euro ad un massimo di 125k euro, la violazione della notifica può anche costituire causa di responsabilità disciplinare e amministrativo-contabile.

Ecco un riepilogo del flusso di notifica:



Fonte: Guida alla notifica degli incidenti al CSIRT Italia - ACN

Notifica di ulteriori soggetti

Per tutti i soggetti non descritti nelle precedenti classificazioni e quindi pubbliche amministrazioni non comprese nella L. 90/2024, Piccole e Medie imprese e privati cittadini non sono previsti obblighi di notifica, bensì è previsto che possano effettuare notifiche in forma volontaria degli incidenti di sicurezza.

Gli incidenti da notificare sono quelli in cui è impattata la riservatezza, la disponibilità o l'integrità di un bene informatico.

Non sono previsti tempi obbligatori per la notifica o sanzioni amministrative, ma è consigliabile avviarla nel più breve tempo possibile.

Le modalità di notifica prevedono sempre le quattro fasi già descritte nel paragrafo "Notifica di un incidente" da avviare sempre tramite il medesimo link https://www.csirt.gov.it/segnalazione.

Ecco uno schema di riepilogo del flusso di notifica:

Fonte: Guida alla notifica degli incidenti al CSIRT Italia – ACN

Conclusioni

Con gli ulteriori soggetti e le segnalazioni volontarie si conlclute questa breve guida alla notifica delgi incidenti di cybersicurezza all' ACN ed in particolare al CSIRT Italia. Entro i primi di ottobre è attesa la pubblicazione del decreto legislativo di recepimento della Direttiva NIS2, che permetterà l'entrata in vigore della Direttiva con il suo quadro sanzionatorio, nell'attesa della sua pubblicazione,il consigli outile è quindi quello di iniziare a familiarizzare con questo nuovo approccio alla cybersicurezza, e ad iniziare a masticare questi nuovi termini ed a familiarizzare con le procedure. E' inoltre opportuno rimboccarsi le machine specie per quelle realtà che hanno sempre rinviato una attenta valutazione dei rischi legagi alla sibersicurezza della propria infrastruttura e die propri asset, con l'idea che „Tanto non può succedere proprio a me", il consigio è sempre quello di valutare quale impatto per il proprio business per i servizi resi alle comunità o ai propri utenti, oltre agli eventuali danni economici, potrebbe avere un cyberattacco che oltre a bloccare l'attività potrebbe portare anche alla perdina o ancora peggio alle esflintrazione e pubblicazione nel dark web die propri dati.

BUONA DIFESA A TUTTI

Settembre 2024