MODELLO DI NOTIFICA INCIDENTE

TIPOLOGIA DI NOTIFICA

- ◯ Obbligatoria
- ◯ Volontaria - ex art. 18 D.lgs. 65/2018

Sezione A: Soggetto che effettua la notifica

Nome e cognome

Ruolo e funzione rivestiti

Indirizzo PEC e/o e-mail

Recapito telefonico

Ulteriori informazioni utili

Sezione B: Dettagli dell'operatore/fornitore

Denominazione ente/azienda e ragione sociale

Indirizzo sede legale
(indicare anche il nominativo del rappresentante legale dell'azienda in Italia)

Tipologia del servizio fornito

Servizi digitali:

- ◯ motore di ricerca
- ◯ e-commerce
- ◯ cloud computing
- ◯ servizi digitali multipli

Se servizi digitali multipli, specificare quali:

Servizi essenziali:

- ◯ Energia
- ◯ Trasporti
- ◯ Settore bancario
- ◯ Infrastrutture dei mercati finanziari
- ◯ Settore sanitario
- ◯ Fornitura e distribuzione di acqua potabile
- ◯ Infrastrutture digitali

Notifiche volontarie ex art. 18 D.lgs. 65/2018
(specificare la tipologia del servizio fornito)

Sezione C: Tipologia dell'incidente

Data e ora rilevamento

Data e ora in cui si è verificato l'incidente
(se nota)

Durata dell'incidente

Tipologia

- ◯ cyber (compilare sezione G)
- ◯ non-cyber (compilare sezione H)
- ◯ entrambi (compilare sezioni G ed H)

Codice identificativo interno o nome dell'incidente
(se applicabile)

Descrizione

Sono state identificate le cause dell'incidente?

- ◯ NO
- ◯ SI

Se sì, descrivere le cause:

Come è stato rilevato l'incidente?

Stato dell'incidente all'atto della notifica

- ◯ in corso
- ◯ concluso
- ◯ in corso ma gestito

Reti, sistemi e funzioni incisi dall'incidente

Sezione D: Impatto dell'incidente

Numero di utenti interessati
(in via diretta o in quanto dipendenti dal servizio colpito per l'erogazione di propri servizi)

Diffusione geografica

- ◯ esclusivamente nazionale
- ◯ transfrontaliera (compilare sezione E)

Portata della perturbazione del funzionamento del servizio
(solo per i Fornitori di Servizi Digitali)

Impatto sulle attività economiche e sociali
(solo per i Fornitori di Servizi Digitali)

- ◯ impatto sulla sicurezza pubblica
- ◯ impatto sulla sicurezza dei cittadini
- ◯ allo stato non noto

Numero di ore di indisponibilità del servizio
(tempo intercorso dal momento in cui il servizio è risultato indisponibile e/o intaccato nella integrità, autenticità e riservatezza fino al momento del suo pieno ripristino)

L'incidente ha causato una violazione dei dati personali?
(data breach)

- ◯ NO
- ◯ Non noto al momento della notifica
- ◯ SI

Se sì, specificare:

L'incidente ha comportato danni materiali?

- ◯ NO
- ◯ SI

Se sì, specificare:

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

- ◯ NO
- ◯ SI

Se sì, quali operatori/fornitori?

L'incidente ha avuto un impatto significativo sulla continuità dei servizi da questi erogati?
(solo se si è risposto "Sì" alla domanda precedente)

- ◯ NO
- ◯ SI

Se sì, fornire la descrizione dell'impatto:

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

Descrivere eventuali ulteriori azioni che si intende intraprendere

Sezione E: Incidenti transfrontalieri

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

L'operatore/fornitore opera in due o più Stati europei?

- ◯ NO
- ◯ SI

Se sì, specificare quali:

L'incidente ha avuto un impatto significativo sui servizi di altri Stati membri?

- ◯ NO
- ◯ Non noto al momento della notifica
- ◯ SI

Se sì, descrivere l'impatto:

Sezione F: Eventuali notifiche

Completare questa sezione se l'incidente è stato notificato ad altre autorità/organizzazioni italiani

Forze di polizia

- ◯ NO
- ◯ SI

Se sì, quali:

Eventuali CERT

- ◯ NO
- ◯ SI

Se sì, quali:

Altro

Sezione G: Informazioni aggiuntive – Incidenti cyber

Classificazione dell'incidente

- ◯ Denial of Service (DoS)
- ◯ Distribuzione di malware
- ◯ Ransomware
- ◯ Trojans
- ◯ Man-in-the-Middle
- ◯ Furto di identità
- ◯ Hacking
- ◯ Sfruttamento di vulnerabilità note o di vulnerabilità in componenti, servizi e/o applicazioni
- ◯ Flusso crittografico
- ◯ Malfunzionamento SW
- ◯ Interferenza con HW
- ◯ Malfunzionamento HW
- ◯ Danno fisico
- ◯ Perdita o furto di materiale
- ◯ Altro

Se Altro, specificare

Nel caso di Distribuzione di malware, specificare come si è verificato l'incidente

- ◯ attraverso e-mail (includendo phishing)
- ◯ attraverso siti web
- ◯ attraverso dispositivi mobili e/o dispositivi USB
- ◯ attraverso infiltrazioni di rete
- ◯ attraverso altri vettori di infezione o vettori non noti

Se noto, specificare quale altro vettore

Nel caso di Furto di identità, specificare come si è verificato l'incidente

- ◯ Phishing
- ◯ Spoofing
- ◯ Pharming
- ◯ Altro

Se Altro, specificare

Nel caso di Hacking, specificare come si è verificato l'incidente

- ◯ Injection
- ◯ Errori di configurazione
- ◯ Broken authentication
- ◯ Altro

Se Altro, specificare

Nel caso di Sfruttamento di vulnerabilità note o di vulnerabilità in componenti, servizi e/o applicazioni, fornire ulteriori dettagli
(ad esempio il numero di CVE)

Sezione H: Informazioni aggiuntive – Incidenti non-cyber

Classificazione dell'incidente

- ☐ Allagamento
- ☐ Incendio
- ☐ Guasto agli impianti
- ☐ Mancanza di elettricità
- ☐ Errore umano
- ☐ Incidente riconducibile ad attività criminale
- ☐ Disastro naturale
- ☐ Altro

Se Disastro naturale, specificare

Se Altro, specificare

Sezione I: Ulteriori informazioni rilevanti

Riportare ogni altra informazione ritenuta utile ai fini dell'inquadramento dell'incidente e della sua rilevanza