Tabella delle revisioni

Data	*Descrizione*	*Verifica*	*Approvazione*
01.12.2018	Prima emissione		
30.06.2025	Seconda emissione		
19.01.2026	Adeguamento alla direttiva NIS2 nella definizione delle fasi previste per la gestione di un incidente. Aggiunta matrice RACI		

Sommario

1. Premessa

La presente Procedura per la Gestione degli Incidenti di Sicurezza è istituita per garantire la **continuità operativa** e la **resilienza** del Soggetto NIS, ed è pienamente **conforme ai requisiti minimi di sicurezza NIS2** (come dettagliato nella Determina ACN n. 164179/2025), agli **obblighi di notifica e di protezione dei dati personali previsti dal Regolamento Generale sulla Protezione dei Dati (GDPR - Reg. UE 2016/679), e ai principi di gestione della sicurezza delle informazioni definiti dalla norma ISO/IEC 27001.**

Scopo del documento è la definizione delle fasi di risposta ad un incidente di sicurezza. Particolare attenzione sarà data al piano di risposta ed ai ruoli coinvolti nella risposta.

Il piano deve essere testato regolarmente per assicurare la sua efficacia e la sua capacità di gestire gli incidenti di sicurezza.

Nelle varie fasi possono essere utilizzate specifiche istruzioni operative o procedure per la gestione dei sistemi.

2. Ambito di Applicazione

Applicabile a tutte le aree IT e operative dell'azienda.

3. Ruoli aziendali coinvolti

- Referente IT
- Responsabile sicurezza delle informazioni (CISO)
- CSIRT - Computer Security Incident Response Team (Gruppo di Intervento per la Sicurezza Informatica in caso di Incidente). Il CSIRT riporta direttamente al CISO.
- Incident Manager. Leader del team CSIRT.
- Punto di Contatto aziendale NIS2
- DPO (Data Protection Officer) /Referente Privacy
- Organi direttivi

Il principale motivo per separare i ruoli di CISO e Incident Manager risiede nella necessità di gestire la **differenza tra strategia e operatività**, specialmente durante una crisi. Il CISO ha un orientamento strategico (correlato alla visione d'insieme delle fasi di risposta all'incidente) mentre l'Incident Manager ha un ruolo più operativo e focalizzato sulla risoluzione tecnica dell'incidente.

4. Piano di risposta ad un incidente di sicurezza

Identificazione dell'incidente

Valutazione dell'incidente

Isolamento dell'incidente

Risposta all'incidente

Comunicazione dell'incidente

Documentazione dell'incidente

Analisi dell'incidente e delle cause

Ripristino del sistema

Implementazione di azioni correttive

Monitoraggio e valutazioni

Identificazione dell'incidente

La prima fase del piano consiste nell'identificazione dell'incidente. Questa fase può essere svolta attraverso l'uso di strumenti di monitoraggio dei sistemi e delle reti, di segnalazioni dei dipendenti o di altre fonti di informazione. L'obiettivo è rilevare tempestivamente gli incidenti e agire prontamente per minimizzare i danni. Tutte le segnalazioni devono convergere sull'**Incident Manager** che valuta se si tratta di un incidente reale o di un falso positivo (con il supporto del CSIRT). In caso di incidente reale, l'Incident Manager aggiorna il **registro degli incidenti.** Il registro degli incidenti può essere gestito tramite programma informatico o mediante specifico foglio di calcolo.

Personale coinvolto ⇒ operatori IT, personale che ha riportato l'incidente, Incident Manager.

Valutazione dell'incidente

Una volta che l'incidente è stato identificato, si procede alla sua valutazione per determinare la natura dell'incidente, l'entità dei danni causati e le possibili conseguenze.

L'Incident Manager è responsabile della valutazione di gravità ed impatto dell'incidente. In caso di incidente significativo (grave perturbazione operativa, perdite finanziarie, impatto su altri soggetti, perdita di riservatezza, integrità o disponibilità), l'Incident Manager attiva immediatamente il CISO ed il Punto di Contatto NIS2, informando che è necessario avviare la procedura di notifica ACN. In questa fase deve, inoltre, essere compreso se "L'incidente *coinvolge*, o si sospetta *possa coinvolgere*, dati personali (es. database clienti, file HR, credenziali)". In tal caso l'Incident manager deve coinvolgere il DPO.

Il CISO in questa fase ha il compito di gestire l'escalation verso gli organi direttivi.

Personale coinvolto ⇒ responsabili delle unità organizzative coinvolte nell'incidente, CISO/responsabile IT, Incident Manager, CSIRT, DPO (se necessario).

Il CISO deve verificare il corretto aggiornamento del registro degli incidenti.

Isolamento dell'incidente

La terza fase del piano consiste nell'isolare l'incidente al fine di prevenire la sua diffusione e limitare i danni causati. Questa fase può includere la disattivazione temporanea di alcuni servizi o l'isolamento di parti del sistema interessato dall'incidente.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT, responsabili delle unità organizzative coinvolte nell'incidente.

Risposta all'incidente

La quarta fase del piano consiste nella risposta all'incidente. In questa fase vengono attuate le misure necessarie per contenere l'incidente, ripristinare la normale operatività dei sistemi interessati e recuperare i dati eventualmente persi. Ciò può includere la disattivazione di account utente compromessi, la separazione dei sistemi compromessi dalla rete e la rimozione di malware. L'Incident Manager deve assicurarsi che il contenimento non causi più danni dell'incidente stesso.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT, responsabili delle unità organizzative coinvolte nell'incidente.

Comunicazione dell'incidente

La quinta fase del piano consiste nella comunicazione dell'incidente. In questa fase si dovrebbe informare il personale impattato dall'incidente, gli stakeholder rilevanti (p.e. clienti, fornitori o terze parti) e le autorità competenti (p.e. ACN/CSIRT Italia, garante privacy). Questa fase si svolge in parallelo alla fase precedente, ma è gestita dagli attori di compliance attivati dall'Incident Manager supervisionato dal Responsabile IT/CISO. Al CISO è inoltre demandata anche la trasmissione degli aggiornamenti sulla risoluzione dell'incidente (*status update*).

- **FLUSSO 1: Notifica GDPR (se attivato DPO)**
  - **Responsabile:** DPO.
  - Il DPO, sulla base delle informazioni tecniche ricevute dall'Incident Manager/CSIRT, valuta il rischio per i diritti e le libertà degli interessati.
  - **Scadenza:** Se la notifica è dovuta, il DPO la invia al **Garante Privacy entro 72 ORE** dalla *conoscenza della violazione*.
  - **Comunicazione:** Il DPO valuta anche se comunicare la violazione agli interessati (se il rischio è elevato).
- **FLUSSO 2: Notifica NIS 2 (se attivato Punto di Contatto NIS2)**
  - **Responsabile:** Punto di Contatto NIS 2.
  - Il Punto di contatto, sulla base delle informazioni ricevute dall'Incident Manager/CSIRT e con il supporto del CISO gestisce le notifiche al **CSIRT Italia (ACN)**.
  - **Scadenza 1 (Entro 24 ORE):** "Allarme Rapido" (Pre-notifica).
  - **Scadenza 2 (Entro 72 ORE):** "Notifica Incidente" (con dettagli e IoC - indicatori di compromissione).
  - **Comunicazione:** Se l'incidente impatta i servizi ai clienti, l'Incident Manager informa il CISO che coordina la comunicazione esterna ai destinatari.

Personale coinvolto ⇒ Punto di Contatto NIS2, CISO, DPO.

Documentazione dell'incidente

La sesta fase del piano si concentra sull'assicurare che tutte le informazioni relative all'incidente siano correttamente inserite nel registro degli incidenti.

La documentazione dell'incidente non consiste nella mera produzione di documenti cartacei, ma nell'aggiornamento continuo e dettagliato del Registro degli Incidenti, inteso come base informativa, perno centrale e unica fonte unica di verità (Single Source of Truth) del processo di gestione degli incidenti di sicurezza.

Non è un semplice archivio di documenti statici, ma un repository strutturato e dinamico progettato per raccogliere e conservare in modo continuo e tracciabile tutte le informazioni relative a un evento di sicurezza.

Le informazioni includono (elenco non esaustivo):

- La natura e la causa principale (root cause) dell'incidente.
- L'entità dei danni o l'impatto finale (economico, operativo, sociale).
- Le misure di contenimento adottate.
- Le azioni correttive o preventive intraprese per impedire futuri incidenti (lessons learned).

Il contenuto informativo varia a seconda del tipo di incidente ed è a discrezione dell'Incident Manager che ha la responsabilità di mantenere aggiornato il registro degli incidenti.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT, responsabili delle unità organizzative coinvolte nell'incidente.

Analisi dell'incidente e delle cause

Il CSIRT raccoglie e preserva le evidenze (log, IoC) e le fornisce all'Incident Manager.

In questa fase si cerca di identificare le cause dell'incidente, di valutare le misure di sicurezza adottate e di definire eventuali azioni correttive per prevenire il verificarsi di futuri incidenti.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT.

Ripristino del sistema

Solo dopo che l'incidente è stato risolto e la causa identificata, si può procedere al ripristino del sistema interessato. Eventualmente ricorrendo a procedure di restore dei sistemi/dati. Al termine della fase di ripristino si deve verificare che tutti i dati siano stati ripristinati correttamente e che i sistemi funzionino come previsto.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT.

Implementazione di azioni correttive

Il CSIRT con il supporto di altro personale tecnico (se necessario) deve aggiornare il registro degli incidenti con eventuali azioni correttive atte a prevenire incidenti simili in futuro.

Personale coinvolto ⇒ CSIRT e personale tecnico specializzato, CISO/Responsabile IT.

Monitoraggio e valutazione

Si deve valutare l'efficacia delle misure di sicurezza adottate e monitorare il sistema per rilevare eventuali nuovi incidenti e migliorare continuamente il piano di risposta agli incidenti di sicurezza.

Personale coinvolto ⇒ CISO/Responsabile IT, responsabili qualità (sistema gestione sicurezza delle informazioni).

Matrice RACI

Attività / Fase	Personale	Incident Manager	CSIRT	DPO (Privacy)	Punto di Contatto	CISO	Organi Direttivi
IDENTIFICAZIONE	R	A	C			I	
VALUTAZIONE		A/R	C	I	I	I	I
ISOLAMENTO		A	R	I	I	I	I
RISPOSTA		A	R	I	I	I	I
COMUNICAZIONE -GDPR-		C	C	A/R		C	I
COMUNICAZIONE -ACN-		C	C		A/R	C	I
DOCUMENTAZIONE		A	R	I	I	I	I
ANALISI		A	R	I	I	I	I
RIPRISTINO		A	R	C	C	C	I
AZIONI CORRETTIVE		A	R	C	C	C	I
MONITORAGGIO E VALUTAZIONE			C	I		A	I

Legenda:

- **R** = Responsible (Esegue l'attività)
- **A** = Accountable (Responsabile ultimo)
- **C** = Consulted (Deve essere consultato)
- **I** = Informed (Deve essere informato)

NOTA: La presente procedura si integra con eventuali **procedure operative interne** le quali possono contenere **ulteriori dettagli e specificazioni operative** in merito, restando inteso che i requisiti previsti dalla presente procedura rimangono inderogabili.