# Piano per la gestione degli incidenti di sicurezza informatica

Autore: DIREZIONE IT

Tipo Documento: Aziendale

| Versione | Data | Descrizione |
|---|---|---|
| 1.0 | 28 – 08- 2026 | Creazione documento |
| 1.1 | 30 – 08 – 2026 | Correzione dies a quo e termini di notifica; disciplina Referente CSIRT/Punto di contatto; raccordo incidenti-crisi-BC/DR e chiusura verso rischio/adeguamento |
| 1.2 | 30 – 08 – 2026 | Allineamento IS-3 ai livelli di servizio attesi (SL), uniformazione Referente CSIRT/sostituti e gestione della relazione intermedia |
| 1.3 | 30 – 08 – 2026 | Richiamo esplicito all'Allegato 3 della Determinazione ACN 379907/2025 e rimozione di un esempio non pertinente alla tassonomia di base dei soggetti importanti |

Ai fini della NIS2, il presente documento tiene in considerazione lo stato della conoscenza attuale dei sistemi rilevanti di Ateneo derivabili dalla documentazione relativa alla certificazione della ISO27001.

## EXECUTIVE SUMMARY

### Il contesto e la necessità di governo

L'art. 25 del D.Lgs. 138/2024 (Decreto NIS) e l'art. 33 del GDPR impongono all'Ateneo procedure tassative per rilevare, gestire e notificare gli attacchi o i disservizi informatici.

Questo documento stabilisce il flusso decisionale e operativo per gestire qualsiasi anomalia di sicurezza, definendo i criteri per distinguere i piccoli eventi interni dalle emergenze e fissando le responsabilità formali di notifica verso le Autorità nazionali (ACN/CSIRT Italia e Garante Privacy).

### Come funziona il modello di gestione

Il processo struttura l'intervento su quattro fasi operative:

- Rilevazione e Triage di I Livello: qualsiasi anomalia viene segnalata al Team Cybersecurity della Direzione IT via ticketing o canale dedicato (nis2@ateneo.univr.it) per una prima valutazione di fondatezza.
- Classificazione dell'Evento: il Referente CSIRT o, in sua assenza, un sostituto designato classifica la severità dell'evento in:
    - *Evento / Near Miss (Quasi-incidente):* anomalie o tentativi sventati senza impatto effettivo.
    - *Incidente Non Significativo:* disservizi minori gestiti con procedure ordinarie.
    - *Incidente Significativo / Di Base:* violazioni che integrano almeno una delle fattispecie di incidente significativo di base definite da ACN: perdita di riservatezza verso l'esterno, perdita di integrità con impatto verso l'esterno oppure violazione dei livelli di servizio attesi (SL) definiti ai sensi di DE.CM-01. Gli SL non coincidono necessariamente con gli SLA contrattuali.
    - *Data Breach:* compromissione di dati personali (con immediata attivazione dell'Ufficio Privacy e del DPO).
- Tempistiche Tassative di Notifica ad ACN/CSIRT Italia: In caso di incidente significativo scatta il canale istituzionale vincolante sul portale ACN:
    - Entro 24 ore dalla conoscenza dell'incidente significativo da parte dell'Ateneo: prenotifica a CSIRT Italia con le informazioni disponibili, inclusi, ove possibile, natura dell'incidente, eventuale origine malevola e possibile impatto transfrontaliero.
    - Entro 72 ore dalla medesima conoscenza dell'incidente significativo: notifica a CSIRT Italia che aggiorna, ove possibile, la prenotifica e contiene una valutazione iniziale di gravità e impatto e gli indicatori di compromissione disponibili.
    - Su richiesta di CSIRT Italia: relazione intermedia sullo stato e sulla gestione dell'incidente. Entro un mese dalla notifica: relazione finale. Se a tale scadenza l'incidente è ancora in corso, sono trasmesse relazioni mensili sullo stato di avanzamento e la relazione finale è inviata entro un mese dalla conclusione della gestione dell'incidente.
- Comunicazione Esterna agli Utenti: Qualora l'incidente impatti i servizi o sussista un'intimazione formale di ACN, l'Ateneo concorda con il CSIRT le modalità e i contenuti delle comunicazioni pubbliche e agli utenti.

**Implicazioni e decisioni cardine richieste al cda**

1. Approvazione Formale della Procedura: Adottare il documento per garantire la piena conformità ai requisiti di risposta e notifica NIS 2 e ACN.
2. Presa d'Atto delle Nomine Operative: Riconoscere il ruolo del *Referente CSIRT* insieme ai sostituti designati quali soggetti deputati alle interlocuzioni operative e alle notifiche verso CSIRT Italia, in raccordo con il Punto di contatto. In via eccezionale, in caso di indisponibilità del Referente CSIRT e di tutti i sostituti, il Punto di contatto può effettuare le notifiche nei casi previsti dalla disciplina ACN vigente.
3. Coinvolgimento nelle Crisi e Comunicazioni Istituzionali: Essere informati tempestivamente in caso di *incidenti significativi di base* e deliberare, di concerto con il Referente CSIRT, sulle comunicazioni esterne straordinarie e sugli impatti per l'Ateneo.
4. Monitoraggio e Riesame: Esaminare con cadenza almeno annuale le statistiche su eventi e incidenti informatici in sede di riesame direzionale e approvare l'aggiornamento della procedura almeno ogni due anni.

# 1 SCOPO

Il presente documento descrive la procedura da adottarsi qualora si verifichino eventi relativi alla sicurezza informatica e alla sicurezza delle informazioni in accordo a quanto previsto dall'articolo 25 del D.lgs. 138/2024 (Decreto NIS) e all'articolo 33 del Regolamento UE 2016/679 (GDPR).

In particolare, il presente documento ha lo scopo di definire procedure e responsabilità relative a:

- Segnalazione, valutazione e registrazione dell'evento;
- Comunicazioni con CSIRT;
- Relazione sull'incidente;
- Comunicazione alle parti interessate.

# 2 CAMPO DI APPLICAZIONE

La procedura si rivolge a tutto il personale dell'organizzazione e viene adottata ogniqualvolta si verifichi un evento che potrebbe costituire un incidente relativo alla sicurezza informatica e alla sicurezza delle informazioni.

# 3 RESPONSABILITÀ

| Ruolo | Responsabilità |
|---|---|
| **Organi di Ateneo** | Approva la procedura |
| **RSGSI** | Redige la procedura |
| **Referente CSIRT e sostituti** | Interloquiscono con CSIRT Italia e curano prenotifica, notifica, eventuale relazione intermedia, aggiornamenti e relazione finale. In via eccezionale, se Referente CSIRT e tutti i sostituti sono indisponibili, il Punto di contatto può effettuare le notifiche nei casi previsti dalla Determinazione ACN n. 127437/2026. |
| **Personale** | Implementano l'applicazione della procedura |
| **Responsabile del servizio impattato, come definito dalla PRO031 del SGSI** | Responsabile del servizio impattato (individuato nella BIA ALL009 o secondo la PRO031 del SGSI, coordinandosi con il Crisis Management Team per eventi di livello C2/C3) — Si occupa della comunicazione agli stakeholders secondo i canali autorizzati |

# 4 REQUISITI

La presente procedura viene adottata in conformità a:

- Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione europea (direttiva NIS 2);
- Decreto Legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555;

- Determinazione ACN 379907/2025, Allegato 1, in particolare: RS.MA-01: punti 1, 2 e 3; RS.CO-02: punti 1 e 2; Allegato 3 – Incidenti significativi di base per i soggetti importanti (IS-1, IS-2 e IS-3).

Determinazione ACN n. 127437 del 13 aprile 2026, con particolare riferimento alle modalità di accesso al Portale ACN, alla designazione del Referente CSIRT e dei sostituti e alla disciplina eccezionale di notifica da parte del Punto di contatto in caso di loro indisponibilità.

- Linee guida ACN.

Fonti autoritative interne: il documento «Organizzazione per la sicurezza informatica» e la Matrice RACI governano ruoli e responsabilità; la Valutazione del rischio e ALL004 governano metodologia e registro dei rischi; il Piano di trattamento del rischio e di gestione delle crisi governa l'escalation a crisi; il Piano di continuità operativa e di ripristino in caso di disastro governa continuità e recovery. Per SIR esterni al perimetro gestionale della Direzione IT operano il Responsabile SIR e il Gestore tecnico formalmente individuati, con raccordo di Direzione IT e RSGSI.

# 5 PROCEDURA

## 5.1 Rilevazione e Segnalazione dell'evento

### 5.1.1 Rilevazione e Comunicazione

L'evento negativo (di origine interna o esterna) deve essere tempestivamente comunicato al Team Cybersecurity di I livello della Direzione IT (utilizzando la mail nis2@ateneo.univr.it oppure il sistema ticketing), da chiunque rilevi un'anomalia rispetto alla normale attività istituzionale o riceva una segnalazione automatizzata. La prima rilevazione o segnalazione deve essere registrata con data e ora.

Ricevuta la comunicazione dell'evento, il Team Cybersecurity di I livello raccoglie tutte le informazioni riguardanti l'evento potenzialmente negativo e svolge una valutazione preliminare al fine di determinare se la segnalazione è fondata e necessita di essere portata all'attenzione del Referente CSIRT.

Nominativi, recapiti, ordine di sostituzione, deleghe e data di efficacia del Referente CSIRT e dei sostituti sono mantenuti nell'atto di designazione o in un registro nominativo a diffusione controllata, aggiornabile senza riapprovazione del presente Piano. Nel Piano è utilizzata esclusivamente la denominazione funzionale «Referente CSIRT e sostituti».

### 5.1.2 Segnalazione

La registrazione formale della segnalazione avviene ad opera del Gruppo di Cybersecurity di I Livello, tramite la compilazione della Sezione 1 "segnalazione dell'evento" del modulo MOD_001 – Gestione evento. Tale modulo deve essere trasmesso al Referente CSIRT nel più breve tempo possibile.

## 5.2 Classificazione e Registrazione dell'evento

### 5.2.1 Classificazione dell'evento

Il Referente CSIRT o un sostituto designato riceve il MOD_001 - Gestione evento con la Sezione 1 compilata e, senza attendere la completezza di ogni informazione tecnica, valuta gli elementi disponibili, compila la Sezione 2 «Classificazione evento» e registra preliminarmente l'evento nel Registro eventi, incidenti, data breach contenuto nel sistema di ticketing. Devono essere registrati separatamente almeno: data/ora della prima rilevazione o segnalazione; data/ora in cui l'Ateneo dispone di elementi sufficienti per essere consapevole della natura significativa dell'incidente; data/ora della prenotifica e della notifica. L'incompletezza delle informazioni non sospende l'escalation né i termini di legge.

| CATEGORIA | DEFINIZIONE | ESEMPIO | COSA DEVE FARE L'ORGANIZZAZIONE |
|---|---|---|---|
| **EVENTO** | Qualsiasi cambiamento significativo o anomalia rispetto alla normale attività aziendale che *potrebbe* indicare un possibile incidente di sicurezza. | Ricezione di un'e-mail di phishing; alert antivirus; rallentamento anomalo di un sistema. | Rilevare, registrare, analizzare e classificare l'evento. |
| **A) NEAR MISS (QUASI-INCIDENTE)** | Evento che *avrebbe potuto* configurare un incidente ma che non ha prodotto effetti negativi, perché evitato o per condizioni fortuite. Non si è verificato alcun impatto sulle informazioni o sui servizi. | Violazione di un server di test privo di dati. | Gestione interna discrezionale. |
| **B) INCIDENTE (DI SICUREZZA)** | Evento che impatta negativamente sulla sicurezza delle informazioni (riservatezza, integrità, disponibilità), senza però raggiungere le soglie di significatività previste dalla normativa. | Malware su una postazione isolata senza propagazione; breve indisponibilità di un servizio interno non critico. | Gestione interna. Discrezionale coinvolgimento del CSIRT. |
| **INCIDENTE SIGNIFICATIVO** | Incidente che:<br>a) ha causato o può causare una grave perturbazione operativa o perdite finanziarie; oppure<br>b) ha causato o può causare ripercussioni rilevanti su altre persone fisiche o giuridiche, con perdite materiali o immateriali considerevoli. [1] | Attacco ransomware con blocco di servizi critici; compromissione di sistemi condivisi con clienti/partner. | Gestione interna e valutazione qualificabilità come "incidente significativo di base". |
| **C) <u>INCIDENTE SIGNIFICATIVO DI BASE</u>** | Tipologia di incidente significativo, ricorre quando si integra almeno uno dei casi definiti da ACN: IS-1 – L'Organizzazione ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale. IS-2 - L'Organizzazione ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà | Esfiltrazione di dati aziendali; modifica non autorizzata di dati; violazione dei livelli di servizio attesi (SL). | Gestione interna e **<u>notifica obbligatoria al CSIRT</u>** (entro 24 e 72 ore come di seguito definito).<br><br>Possibilità di chiedere supporto al CSIRT per la gestione. |

[1] Ai sensi del D.lgs 138/2024 art. 25 comma 4

| | | | |
|---|---|---|---|
| | o sui quali esercita il controllo, anche parziale.<br>IS-3 - L'Organizzazione ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio attesi (SL) definiti e mantenuti ai sensi di DE.CM-01. La PRO_008, ove vigente per il perimetro DIT, costituisce una delle evidenze operative di riferimento, senza sostituire la definizione degli SL applicabili. | | |
| **D) DATA BREACH** | Incidente di sicurezza che comporta, accidentalmente o in modo illecito, distruzione, perdita, modifica, divulgazione non autorizzata o accesso a **dati personali**.<br>Può coincidere o meno con un incidente significativo. | Furto di database clienti; invio errato di dati personali; accesso non autorizzato a dati HR. | Coinvolgere l'ufficio privacy e, se necessario, il DPO; valutare l'impatto sui dati personali e l'eventuale notifica al Garante e agli interessati. |

## 5.3 Attivazione della procedura di risposta agli incidenti

Quando l'evento è qualificato come incidente significativo, il Referente CSIRT o il sostituto attiva senza ritardo le escalation previste, informa i ruoli di governo competenti e avvia gli adempimenti verso CSIRT Italia. Se gravità e impatto richiedono l'attivazione dei livelli C2/C3, si applica la catena di comando del Piano di trattamento del rischio e di gestione delle crisi; se sono minacciate continuità, RTO o RPO, viene attivato anche il Piano di continuità operativa e di ripristino in caso di disastro dal Responsabile SIR o dal ruolo competente per il perimetro interessato. Classificazione/notifiche, crisi e BC/DR restano così processi coordinati senza duplicazione della catena di comando.

Qualora si sospetti che l'incidente significativo abbia carattere criminale, l'Organizzazione seguirà gli orientamenti forniti da CSIRT Italia in merito alla segnalazione dell'incidente all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione.

## 5.4 Pre-notifica a CSIRT

**Senza ingiustificato ritardo e comunque entro 24 ore da quando l'Ateneo è venuto a conoscenza dell'incidente significativo, il Referente CSIRT o un sostituto designato effettua la prenotifica a CSIRT Italia tramite i servizi NIS del Portale ACN. Se alcune informazioni non sono ancora disponibili, la prenotifica contiene quanto noto in quel momento ed è successivamente integrata. Il tempo necessario al completamento del MOD_001 o alla ricostruzione tecnica non sospende né differisce il termine. Ove possibile, è indicato se l'incidente possa derivare da atti illegittimi o malevoli o possa avere un impatto transfrontaliero.**

Entro lo stesso termine il Referente può valutare di inoltrare a CSIRT una richiesta di orientamento o consulenza sull'attuazione di possibili misure tecniche di mitigazione.

## 5.5 Gestione dell'incidente

Il Referente CSIRT provvede alla compilazione della Sezione 3. "Gestione Incidente" del MOD_001 – Gestione evento.

Vi inserisce le attività di mitigazioni effettuate o in corso, in particolare dando evidenza delle attività di rimedio, intraprese per contenere i danni più immediati della violazione, e delle azioni correttive, volte ad un miglioramento sul lungo termine, pensate per intervenire sulle cause della violazione e per prevenirne il ripetersi.

Vi inserisce una valutazione della gravità dell'incidente e dell'impatto dello stesso con riferimento alla tipologia degli eventuali settori essenziali coinvolti, all'estensione nazionale e/o transfrontaliera dell'incidente, all'impatto operativo in riferimento alle interruzioni operative tanto subite quanto provocate, e alle perdite di riservatezza e integrità delle informazioni di proprietà dell'organizzazione o in suo possesso.

L'Organizzazione definisce la gravità dell'incidente secondo i seguenti criteri:

| | **Livello di gravità** | | |
|---|---|---|---|
| | **GRAVITÀ BASSA** | **GRAVITÀ MEDIA** | **GRAVITÀ ALTA** |
| **Perdita di riservatezza / integrità dei dati** | Riguarda esclusivamente informazioni pubbliche o comunque non riservate. | Riguarda informazioni non confidenziali dell'Organizzazione o dei quali essa ha il controllo. | Riguarda informazioni anche confidenziali dell'Organizzazione o dei quali essa ha il controllo. |
| **Interruzioni operative** | Limitate per numero di servizi o per durata e non coinvolgono servizi o sistemi rilevanti per l'Organizzazione e/o per i propri clienti. | Modeste per numero di servizi o per durata, ma possono coinvolgere servizi o sistemi rilevanti per l'Organizzazione e/o per i propri clienti. | Estese e/o prolungate; possono coinvolgere uno o più servizi o sistemi rilevanti per l'Organizzazione e/o per i propri clienti. |
| **Ripristino dei livelli di servizio** | Avviene quasi immediatamente, senza necessità di interventi straordinari o del coinvolgimento di terze parti. | Avviene con uno sforzo da parte dell'Organizzazione, gestibile tramite le normali procedure operative. | Il ripristino dei livelli di servizio attesi risulta complesso e richiede l'attivazione della procedura di gestione delle crisi. |
| **Perdite economiche / danni** | Non sono prospettabili perdite economiche dirette o indirette. | Possono essere registrate perdite economiche dirette o indirette. | Possono verificarsi perdite economiche considerevoli, sia dirette che indirette. |

| | | | |
|---|---|---|---|
| **Costi di ripristino** | Trascurabili. | Gestiti dall'Organizzazione senza necessità di allocare ulteriore budget, ma possono richiedere l'intervento di figure esterne. | Elevati e tali da richiedere un intervento sulla destinazione dei fondi dell'Organizzazione. |

Sulla base della valutazione di cui sopra, il Referente CSIRT ultima la registrazione dell'evento all'interno del Registro eventi, incidenti, data breach.

## 5.6 Notifica al CSIRT

**Entro 72 ore dalla medesima conoscenza dell'incidente significativo, il Referente CSIRT o un sostituto designato effettua la notifica a CSIRT Italia tramite i servizi NIS del Portale ACN.**

La notifica, ove possibile, aggiornerà le informazioni fornite con la Pre-notifica e indicherà una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione (IoC).

## 5.7 Relazione sull'incidente

**Su richiesta di CSIRT Italia, il Referente CSIRT o un sostituto designato trasmette una relazione intermedia recante gli aggiornamenti pertinenti sullo stato e sulla gestione dell'incidente. La richiesta, la data/ora di trasmissione e il relativo riferimento sono registrati nel MOD_001 e nel registro dell'incidente.**

**Entro un mese dalla notifica a CSIRT Italia, il Referente CSIRT o un sostituto designato trasmette la relazione finale prevista dall'art. 25 del D.lgs. 138/2024, utilizzando il MOD_001 - Gestione evento e gli eventuali allegati pertinenti.**

Se, alla scadenza prevista per la relazione finale, l'incidente è ancora in corso, sono trasmesse a CSIRT Italia relazioni mensili sullo stato di avanzamento della gestione, aggiornando il MOD_001 e le evidenze pertinenti.

**Entro un mese dalla conclusione della gestione dell'incidente, il Referente CSIRT o un sostituto designato trasmette a CSIRT Italia la relazione finale definitiva, con il MOD_001 interamente aggiornato e gli eventuali allegati pertinenti.**

## 5.8 Comunicazione alle parti interessate

### 5.8.1 Valutazione della Direzione

Il Referente CSIRT, coinvolgendo gli Organi di Ateneo, valuta l'opportunità di comunicare ai destinatari dei loro servizi:

- gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi
- la presenza di potenziali minacce informatiche significative e misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Eventualmente comunicando anche la natura di tale minaccia.

Di tale confronto viene lasciata un'evidenza scritta.

### 5.8.2 Consultazione del CSIRT

Se l'esito del confronto è positivo, il Referente CSIRT interpella CSIRT Italia e ne acquisisce il riscontro. Ottenuto il parere, l'Organizzazione provvede senza ritardo alla comunicazione secondo modalità definite con gli Organi di Ateneo competenti e nel rispetto delle attribuzioni del Punto di contatto e degli altri ruoli istituzionali.

### 5.8.3 Intimazione di ACN

ACN detiene il potere di informare il pubblico riguardo l'incidente significativo occorso con il fine di evitare ulteriori incidenti, di gestire un incidente in corso, oppure qualora la diffusione venga ritenuta nell'interesse pubblico.

In ogni caso, qualora intimata da ACN[2], l'Organizzazione deve:

g) comunicare senza ingiustificato ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi

h) comunicare senza ingiustificato ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia, nonché, se opportuno, la minaccia informatica significativa stessa

i) informare il pubblico sugli incidenti occorsi.

## 6 DOCUMENTAZIONE E ANALISI

L'Organizzazione conserva la documentazione e le evidenze attinenti all'evento.

La chiusura dell'incidente comprende una verifica post-incident e le lesson learned. Quando pertinenti, l'esito determina l'aggiornamento di ALL004, l'apertura o revisione di azioni nel Piano di trattamento, l'inserimento di gap strutturali nel Piano di adeguamento, l'aggiornamento della BIA/BC-DR e la successiva verifica mediante audit o riesame. Le evidenze sono collegate al medesimo evento e ai relativi ticket, evitando registri paralleli non riconciliati.

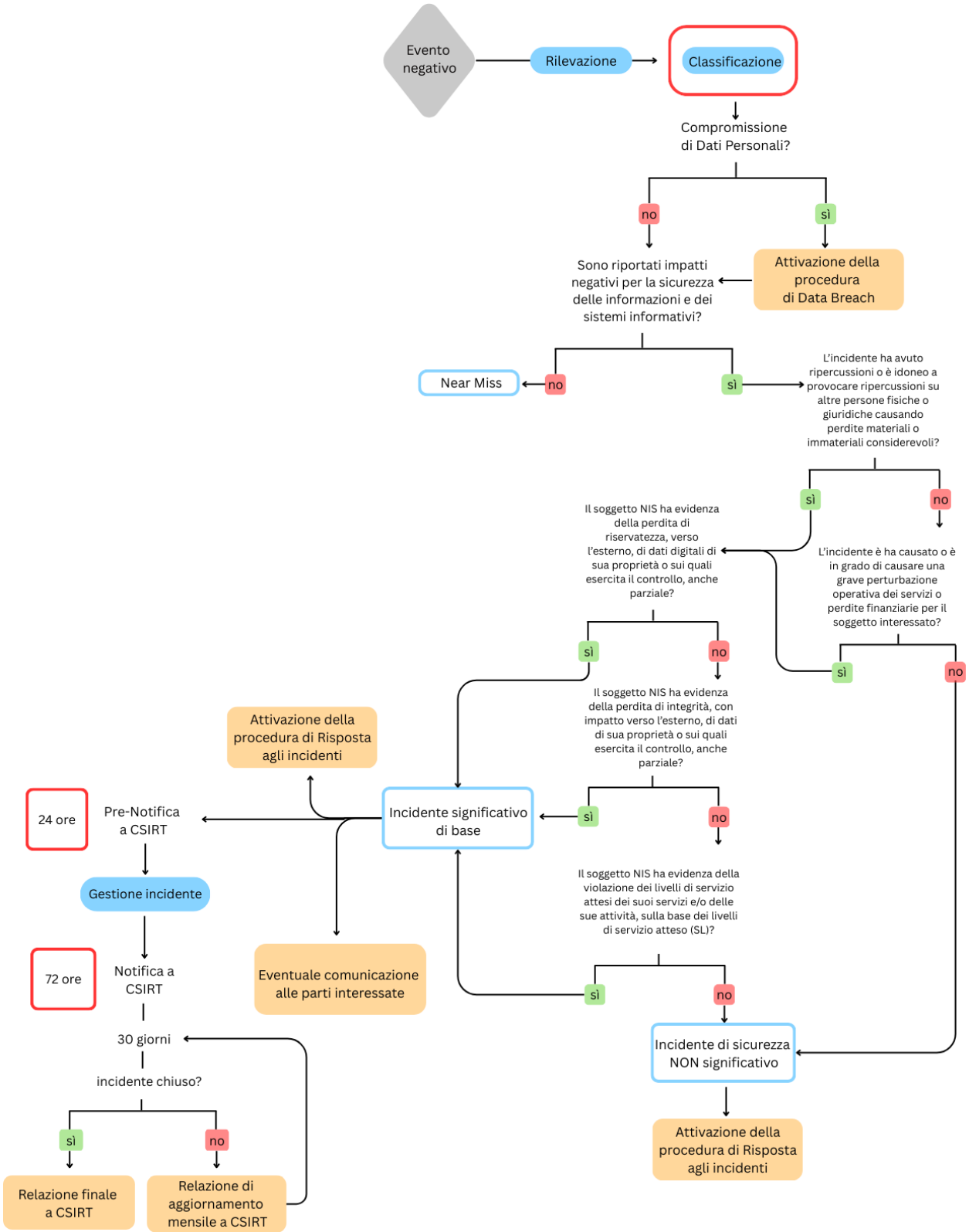
Almeno una volta all'anno sono analizzate, con il coinvolgimento degli Organi di Ateneo competenti, le statistiche relative agli eventi e agli incidenti che hanno coinvolto l'Organizzazione; dell'analisi è data evidenza nel Riesame della Direzione.

## 7 AGGIORNAMENTO

La presente procedura è riesaminata e aggiornata periodicamente, almeno ogni due anni, nonché qualora si verifichino incidenti significativi, integrando le lezioni apprese e/o i mutamenti dell'esposizione alle minacce e ai rischi.

[2] Ai sensi dell'articolo 37 comma 3 del Decreto NIS

# 8 SCHEMA DEGLI STEP DA INTRAPRENDERE



| | | |
|---|---|---|
| | **GESTIONE EVENTO** | **MOD001 – Ver. 1.2 del 30/08/2026**<br>Autore: Referente CSIRT<br>Approvato da: Direzione<br>Tipo Documento: Aziendale |
| Codice evento: Yyyy-mm-dd-n. progressivo | | |

| **Sezione 1. Descrizione evento** | | | |
|---|---|---|---|
| **Data dell'evento:** | | **Ora dell'evento:** | |
| **Data della prima rilevazione o segnalazione dell'evento:** | | **Ora della prima rilevazione o segnalazione:** | |
| **Data della conoscenza dell'incidente significativo ai fini dell'art. 25 D.lgs. 138/2024:** | | **Ora della conoscenza:** | |
| **Data della prenotifica a CSIRT Italia:** | | **Ora della prenotifica:** | |
| **Data della notifica a CSIRT Italia:** | | **Ora della notifica:** | |
| Data richiesta relazione intermedia da CSIRT Italia: | | Ora richiesta: | |
| Data trasmissione relazione intermedia a CSIRT Italia: | | Ora trasmissione: | |
| **Ragioni dell'eventuale ritardo della segnalazione:** | | | |
| **Modalità di rilevamento dell'evento** (come è stato rilevato l'incidente?): | | | |
| **Conclusione dell'evento** | ☐ Concluso in data: _____ ☐ In corso | | |
| **Dati del segnalante** | Nome: | | |
| | Cognome: | | |
| | Area e sede: | | |
| **Descrizione dell'evento** (includere descrizione documenti/dati coinvolti): | | | |
| **Tipo di violazione** (es. distruzione, perdita, modifica, divulgazione non autorizzata, accesso non autorizzato): | | | |
| **Origine dell'evento:** | ☐ Interna ☐ Esterna | | |
| **Causa della violazione** (azione intenzionale, azione accidentale, sconosciuta, altro): | | | |
| **Soggetti testimoni** | ☐ Nessuno<br>☐ Segnalante<br>☐ Altri: _____ | | |
| **L'evento ha coinvolto informazioni interne o confidenziali dell'azienda** | ☐ No<br>☐ Sì, indicare quali: _____ | | |
| **L'evento ha coinvolto dati personali** (data breach) | ☐ Sì ☐ No | | |
| **Soggetti, risorse e asset coinvolti** (inclusi sistemi IT) | | | |

| **Sezione 2. Classificazione evento (a cura del Referente CSIRT o di un sostituto designato; la valutazione avviene senza ritardo e non sospende i termini di notifica, che decorrono dalla conoscenza dell'incidente significativo)** | |
|---|---|
| **Data:** | |
| **Classificazione dell'evento:** | ☐ Evento che non costituisce incidente (near miss)<br>☐ Incidente significativo di base<br>☐ Incidente che impatta sulla sicurezza delle informazioni<br>☐ Data breach |
| **Motivazione della classificazione:** | |
| **Incidente significativo di base*** | ☐ Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.<br>☐ Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.<br>☐ Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL). |
| **Tipologia di incidente** | ☐ Cyber<br>☐ Non-Cyber<br>☐ Entrambi |
| **Evento cyber** | ☐ Denial of Service (DoS)<br>☐ Distribuzione di malware, attraverso:<br>☐ Ransomware<br>☐ Man-in-the-middle<br>☐ Furto di identità, attraverso:<br>☐ Hacking (injection, errori di configurazione, broken authentication, altro)<br>☐ Sfruttamento di vulnerabilità note o di vulnerabilità in componenti, servizi e/o applicazioni<br>☐ Flusso crittografico<br>☐ Malfunzionamento SW<br>☐ Danno fisico<br>☐ Perdita o furto di materiale<br>☐ altro: |

| | |
|---|---|
| **Evento non-cyber** | ☐ Allagamento<br>☐ Incendio<br>☐ Guasto agli impianti<br>☐ Mancanza di elettricità<br>☐ Errore umano<br>☐ Incidente riconducibile ad attività criminale<br>☐ Disastro naturale, quale:<br>☐ Altro |
| **Origine dell'evento** | ☐ Sospetto atti illegittimi o malevoli |
| **Diffusione dell'evento** | ☐ Esclusivamente nazionale<br>☐ Transfrontaliera |
| **Richiesta supporto CSIRT** | ☐ Sì ☐ No |

| Ruolo | Nome e Cognome | Data | Firma |
|---|---|---|---|
| Referente CSIRT / sostituto designato | | | |
| * Rappresentante legale/Altro rappresentante del Titolare se Incidente significativo di base | | | |
| Altri soggetti coinvolti | | | |

| **Sezione 3. Gestione incidente** (eventualmente da aggiornare mensilmente fino a chiusura dell'incidente) | | |
|---|---|---|
| **Data:** | | |
| **Reti, sistemi e funzioni incisi dall'incidente:** | | |
| **Numero utenti interessati** (direttamente o indirettamente): ___ | **Impatto sull'utenza** (percentuale degli utenti colpiti rispetto al totale degli utenti nazionali del servizio interessato): ____ | **Durata del disservizio:** ____ |
| **Portata della perturbazione del funzionamento del servizio:** | | |
| **Impatto sulle interconnessioni a livello nazionale:** | | |
| **Impatto sulle attività economiche e sociali** (solo per i fornitori di servizi digitali):<br>☐ Impatto sulla sicurezza pubblica<br>☐ Impatto sulla sicurezza dei cittadini<br>☐ Allo stato non noto | | |
| **Danni materiali** | ☐ No ☐ Sì, quali: | |
| **Operatori/fornitori, nazionali o comunitari, che utilizzano i servizi compromessi dall'incidente** | ☐ No ☐ Sì, quali: | |
| **Impatto significativo sulla continuità dei servizi erogati dagli operatori/fornitori** | ☐ No ☐ Sì, quali: | |
| **Attività intraprese immediatamente (Azioni di Rimedio) per limitare i danni della violazione:** | | |
| **Azioni intraprese successivamente (Azioni correttive) per prevenire il ripetersi di incidenti analoghi:** | | |

Codice evento: Yyyy-mm-dd-n. progressivo

| | | | |
|---|---|---|---|
| **Identificazione della Root Cause** (minaccia o causa originale che ha innescato l'incidente - system failures, fenomeno naturale, errore umano, azione malevola, third-party failures) | | | |
| **Indicatori di compromissione** (specificare gli elementi che indichino la presenza di attività malevole o intrusioni subite) | | | |
| ☐ **Incidente concluso in data:** | | ☐ **Incidente in corso:** | ☐ gestito - in miglioramento<br>☐ gestito - stabile<br>☐ gestito - in peggioramento<br>☐ non gestito |
| **Durata dell'incidente:** | | | |
| **Gravità dell'Incidente** | **Ragioni della valutazione:** | | |
| ☐ Bassa | | | |
| ☐ Media | | | |
| ☐ Alta | | | |
| **Costi sostenuti per la gestione:** | | | |
| **Perdite economiche subite** (dirette o indirette): | | | |
| **Allegati:** | | | |
| **Comunicazione alle parti interessate:** | ☐ **Sì**<br>Destinatari:<br>Modalità: | | |
| | ☐ **No**<br>Ragioni: | | |

Relazione intermedia CSIRT Italia

Riferimenti

Richiesta ricevuta

Data/ora: _____ Riferimento richiesta: _____

Trasmissione effettuata

Data/ora: _____ Riferimento/protocollo: _____ Referente CSIRT/sostituto: _____

| Ruolo | Nome e Cognome | Data | Firma |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Referente CSIRT / sostituto designato | | | |
| Rappresentante legale/Altro rappresentante del Titolare* | | | |
| Altri soggetti coinvolti | | | |

| **Sezione 4. Data Breach**** | |
|---|---|
| **Data:** | |
| **Categoria di Data Breach** | ☐ Confidentiality breach (accesso o divulgazione non autorizzato o accidentale)<br>☐ Availability breach (alterazione non autorizzata o accidentale della disponibilità)<br>☐ Integrity breach (modifica e/o integrità non autorizzata) |
| **Descrizione della violazione dei dati personali avvenuta:** | |
| **Categorie di dati personali coinvolti** (anagrafici, contatto, dati relativi alla salute, dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla vita sessuale o all'orientamento sessuale e dati giudiziari…): | |
| **Quantità di dati coinvolti** (se nota): | |
| **Categorie di interessati coinvolti** (se note): | |
| **Danni causati agli interessati** (se noti): | |
| **Si è valutata la probabilità che la violazione dei dati personali presenti un rischio per diritti e libertà delle persone fisiche?** (self-assesment svolto sul sito del Garante) | ☐ No, ragioni:<br>☐ Sì, esito: |
| **Possibili conseguenze per gli interessati** | **In caso di perdita di confidenzialità:**<br>☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento<br>☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati<br>☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito<br>☐ Altro (specificare)_____<br>**In caso di perdita di integrità:**<br>☐ I dati sono stati modificati e resi inconsistenti<br>☐ I dati sono stati modificati mantenendo la consistenza<br>☐ Altro (specificare) _____<br>**In caso di perdita di disponibilità:**<br>☐ Mancato accesso a servizi<br>☐ Malfunzionamento e difficoltà nell'utilizzo di servizi<br>☐ Altro (specificare) |

| | |
|---|---|
| **Possibili conseguenze per gli interessati (anche negative):** | |
| | |
| **Necessaria segnalazione al Garante** | ☐ No ☐ Sì, effettuata in data_____ |
| **Ragioni della mancata segnalazione** | |
| **Se gli interessati hanno ricevuto comunicazione, specificarne la modalità e sintetizzarne il contenuto** | |
| **Self-assessment sul sito del Garante** | ☐ No ☐ Sì, effettuata in data_____ |
| **Ragioni dell'eventuale ritardo** (se la notifica al Garante è avvenuta dopo le 72h dalla conoscenza della violazione o la comunicazione agli interessati non è avvenuta immediatamente): | |
| **Eventuali note:** | |

Nota sui termini NIS: l'eventuale incompletezza delle informazioni disponibili non sospende i termini dell'art. 25 del D.lgs. 138/2024. Prenotifica e notifica riportano le informazioni disponibili al momento dell'invio e sono integrate secondo le modalità vigenti. L'eventuale richiesta di relazione intermedia da parte di CSIRT Italia e la relativa trasmissione devono essere registrate con data, ora e riferimento.