Università di Genova

Politica - Risposta agli incidenti e ripristino

Documento: GV_PO-01f – Versione 2.0 – 10 settembre 2026

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e direttivi NIS2

3 – Gestione degli incidenti informatici

4 – Ruoli, segnalazione e coordinamento operativo

5 – Documentazione ed evidenze

6 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la corretta gestione degli incidenti di sicurezza informatica è essenziale per contenere gli impatti sui sistemi informativi e di rete e assicurare il tempestivo ripristino dei servizi. A tal fine, l'Ateneo definisce e applica modalità strutturate per la gestione, la notifica, la comunicazione e la documentazione degli incidenti, coordinandosi, ove necessario, con il CSIRT Italia, le autorità competenti e le terze parti interessate.

La presente politica costituisce attuazione del Regolamento di Ateneo per la cybersicurezza, e si coordina con la Procedura di gestione e notifica degli incidenti informatici approvata dal Consiglio di Amministrazione nel dicembre 2025. Essa si applica agli incidenti che interessano sistemi, reti, servizi e dati compresi nel perimetro di cybersicurezza dell'Ateneo, inclusi gli asset gestiti dalle strutture fondamentali e dai responsabili scientifici.

Criterio di proporzionalità - La gestione è graduata in funzione della natura, della gravità, dell'estensione e dell'impatto dell'evento, distinguendo gli incidenti ordinari dagli incidenti significativi. La classificazione tiene conto anche della criticità dei servizi, dei sistemi e dei dati risultante dal censimento degli asset, i cui criteri sono approvati dal Consigliop di Amministrazione.

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

Gli Organi di Amministrazione e Direttivi NIS2 adottano indirizzi strategici e misure organizzative finalizzate a supportare i seguenti obiettivi:

- assicurare la definizione, l'attuazione, l'aggiornamento e la documentazione di un Piano per la gestione degli incidenti di sicurezza informatica e per la notifica al CSIRT Italia;
- garantire che il Piano definisca le fasi e le procedure di gestione e notifica degli incidenti, i ruoli e le responsabilità, le informazioni di contatto, le modalità di comunicazione interna ed esterna, la reportistica e le procedure per la predisposizione e la trasmissione delle relazioni previste dalla normativa;
- approvare il piano per la gestione degli incidenti e assicurarne il riesame almeno ogni due anni, nonché a seguito di incidenti significativi o di mutamenti dell'esposizione alle minacce e ai relativi rischi, integrando le lezioni apprese;
- assicurare l'adozione di comunicazioni ai destinatari dei servizi sulle minacce e sugli incidenti di cybersicurezza significativi, nonché l'informazione al pubblico nei casi previsti dalla normativa vigente anche in coerenza a quanto previsto in materia di trattamento di dati personali (data breach).
- garantire l'adozione di procedure per il ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti negli incidenti.

3 – Gestione degli incidenti informatici

L'Ateneo definisce, attua, aggiorna e documenta un Piano per la gestione degli incidenti informatici e per la notifica al CSIRT Italia. Il piano disciplina le fasi di gestione e notifica, i ruoli e le responsabilità, le modalità di predisposizione e trasmissione delle relazioni previste dalla normativa, i contatti per la segnalazione, le comunicazioni interne ed esterne e la reportistica necessaria a documentare gli incidenti. L'Ateneo adotta inoltre procedure per comunicare, senza ingiustificato ritardo e nei casi previsti, gli incidenti significativi ai destinatari dei servizi, fornire indicazioni sulle misure applicabili in presenza di minacce informatiche significative, informare il pubblico su indicazione dell'Agenzia per la cybersicurezza nazionale e ripristinare il normale funzionamento dei sistemi informativi e di rete coinvolti.

Fasi minime: Il processo comprende almeno: rilevazione e segnalazione; registrazione e prima qualificazione; analisi tecnica e valutazione degli impatti; contenimento ed eventuale isolamento; mitigazione ed eliminazione della causa; ripristino sicuro e verifica del ritorno alla normale operatività; notifiche e comunicazioni dovute; chiusura, analisi delle cause e lezioni apprese. Le priorità di risposta e ripristino sono correlate alla criticità degli asset e dei servizi interessati e si raccordano, ove necessario, con i piani di continuità operativa, disaster recovery e gestione della crisi.

Notifica NIS2: Per gli incidenti significativi sono rispettati i termini e i contenuti delle notifiche previsti dall'art. 25 del D.lgs. 138/2024 e dalle determinazioni ACN applicabili. I Referenti CSIRT curano l'interlocuzione operativa e l'esecuzione materiale delle notifiche, sulla base delle indicazioni dell'Incident Response Team e in coordinamento con il Punto di Contatto NIS2.

Coordinamento privacy: Qualora l'incidente comporti o possa comportare una violazione di dati personali, l'Incident Response Team coinvolge tempestivamente il DPO e l'ufficio competente affinché siano svolte, in parallelo e senza reciproco ritardo, la valutazione del data breach e le eventuali notifiche o comunicazioni previste dal Regolamento (UE) 2016/679.

4 – Ruoli, segnalazione e coordinamento operativo

Segnalazione interna**:** Tutto il personale, le strutture fondamentali, gli Amministratori di Sistema, i responsabili scientifici e gli altri soggetti che gestiscono o utilizzano sistemi ICT segnalano con la massima tempestività ogni evento sospetto o incidente effettivo all'indirizzo incidenti.ict@unige.it o agli ulteriori recapiti ufficiali pubblicati dall'Ateneo, evitando iniziative autonome che possano alterare evidenze o aggravare l'incidente.

- il Punto di Contatto NIS2 coordina, per quanto di competenza, la gestione delle notifiche di incidente significativo e cura i rapporti istituzionali con ACN;
- l'Incident Response Team analizza e qualifica l'evento, coordina le attività di risposta e mitigazione e predispone gli elementi informativi necessari;
- i Referenti CSIRT interloquiscono operativamente con CSIRT Italia e con le altre autorità di settore ed effettuano le notifiche nei termini applicabili;

- l'Area ICT attua il contenimento e il ripristino per i sistemi di propria competenza e coordina il supporto tecnico alle altre strutture;
- le strutture fondamentali e i responsabili dei sistemi interessati cooperano immediatamente, preservano le evidenze e attuano le indicazioni ricevute dall'Incident Response Team;
- il DPO è consultato tempestivamente per gli incidenti che coinvolgono o possono coinvolgere dati personali; le comunicazioni istituzionali interne ed esterne sono effettuate dai soggetti competenti sulla base degli indirizzi degli Organi.

Terze parti e crisi: I fornitori e le terze parti coinvolte cooperano secondo gli obblighi normativi e contrattuali, assicurando tempestiva comunicazione, disponibilità delle informazioni, supporto al contenimento e al ripristino e conservazione delle evidenze. In presenza di una crisi informatica sono attivati i canali e i protocolli previsti dal Regolamento di Ateneo e dal relativo piano di gestione della crisi.

5 – Documentazione ed evidenze

Le attività di gestione, notifica, comunicazione e ripristino degli incidenti informatici sono supportate da adeguata documentazione ed evidenze, inclusa la reportistica utilizzata per registrare l'incidente e le azioni intraprese. Tale documentazione è conservata secondo le modalità definite dall'Ateneo, in modo da garantirne disponibilità, integrità, riservatezza e tracciabilità.

Per ciascun incidente sono registrati, in misura proporzionata: data e ora di rilevazione e segnalazione; sistemi, servizi e dati interessati; classificazione e impatti; decisioni assunte; soggetti coinvolti; azioni di contenimento, mitigazione e ripristino; notifiche e comunicazioni effettuate; evidenze tecniche, incluse quelle tratte dai log; esito, causa radice e azioni correttive. L'accesso è limitato ai soggetti autorizzati e il trattamento dei dati è circoscritto a quanto strettamente necessario.

6 – Revisione e approvazione

La presente politica è approvata dagli Organi di Amministrazione e direttivi NIS2 ed entra in vigore alla data di adozione. La revisione avviene con cadenza programmata, a seguito di cambiamenti organizzativi, tecnologici o normativi significativi, o in seguito a incidenti di sicurezza.