Università di Genova

Politica – Monitoraggio degli eventi di sicurezza

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

Sommario

1 – Principi generali
2 – Ruolo degli Organi di Amministrazione e direttivi NIS2
3 – Strumenti di monitoraggio, perimetro e livelli di servizio
4 – Protezione dei sistemi terminali e gestione degli eventi
5 – Sviluppo sicuro del software
6 – Documentazione, evidenze e riesame
7 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che il monitoraggio degli eventi di sicurezza costituisce una misura essenziale per individuare tempestivamente eventi potenzialmente avversi e incidenti significativi che interessano i sistemi informativi e di rete. A tal fine, l'organizzazione adotta misure coerenti con il rischio per assicurare la presenza, l'aggiornamento, la manutenzione e la configurazione adeguata degli strumenti tecnici di rilevamento e dei sistemi di protezione dei punti terminali, nonché la definizione dei livelli di servizio attesi dei servizi e delle attività.

La presente politica si coordina con il Regolamento di Ateneo per la sicurezza informatica, e si applica secondo criteri di adeguatezza, proporzionalità e gradualità rispetto al rischio. Il perimetro prioritario è costituito dalle reti e dai sistemi informativi rilevanti.

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 che, per almeno i sistemi informativi e di rete rilevanti, siano presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per censire gli eventi di sicurezza e per rilevare gli tempestivamente gli incidenti significativi;
- garantire che siano definiti e documentati i livelli di servizio attesi dei servizi e delle attività del soggetto NIS, anche ai fini di rilevare tempestivamente gli incidenti significativi;
- assicurare che, fatte salve motivate e documentate ragioni normative o tecniche, siano presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi di protezione degli asset per il rilevamento di minacce informatiche.

3 – Strumenti di monitoraggio, perimetro e livelli di servizio

Per almeno i sistemi informativi e di rete rilevanti, l'Ateneo assicura la presenza, l'aggiornamento, la manutenzione e la configurazione adeguata di strumenti tecnici per censire gli eventi di sicurezza e rilevare tempestivamente gli incidenti significativi in relazione ai livelli di servizi attesi.

L'Area ICT, ai sensi del Regolamento per la Cybersicurezza, coordina l'attuazione delle politiche di sicurezza, cura il monitoraggio degli eventi relativi alle infrastrutture di propria competenza e collabora con il Punto di Contatto NIS2, l'IRT e i Referenti CSIRT. Per i sistemi gestiti dalle strutture fondamentali, il monitoraggio è assicurato dai relativi Amministratori di Sistema e Responsabili scientifici delle attività di didattica o di ricerca o dei laboratori, in raccordo con l'Area ICT.

La definizione delle priorità, delle soglie di allerta, della profondità del monitoraggio e dei livelli di servizio tiene conto della classificazione degli asset, delle dipendenze ICT, dell'esposizione, della criticità dei dati e degli esiti dell'analisi del rischio prevista dal Regolamento di Ateneo per la Cybersicurezza.

4 – Protezione dei punti terminali e gestione degli eventi

Fatte salve motivate e documentate ragioni normative o tecniche, l'Ateneo assicura la presenza, l'aggiornamento, la manutenzione e la configurazione adeguata di sistemi di protezione dei punti terminali (endpoint) per il rilevamento preventivo, oltre che reattivo, delle minacce informatiche.

Tali sistemi sono adottati nell'ambito delle misure di monitoraggio degli eventi potenzialmente avversi che interessano hardware, software, e dati.

La raccolta, conservazione, protezione, consultazione e correlazione dei log avvengono secondo il Regolamento per la Cybersicurezza, nel rispetto dei principi di pertinenza, minimizzazione, integrità, tracciabilità degli accessi e protezione dei dati personali, definendo

- i periodi e le modalità di conservazione dei log, in base alla loro tipologia, in modo esplicito e motivato;
- le finalità legittimate per cui i log possono essere consultati nell'ambito degli audit, in coerenza con i succitati principi.

Le evidenze sono rese disponibili esclusivamente ai soggetti autorizzati e per finalità di sicurezza, gestione degli incidenti, audit e adempimento normativo, nel rispetto delle disposizioni previste nello Statuto dei lavoratori e dalla normativa in materia di trattamento dei dati personali.

Gli eventi che presentano indicatori di possibili incidenti sono gestiti secondo la Procedura di gestione e notifica degli incidenti approvata dal Consiglio di amministrazione il 22 dicembre 2025 e s.m.i.: le segnalazioni sono indirizzate tempestivamente all'IRT (Incident Response Team); l'analisi tecnica e il coordinamento della risposta competono all'IRT e alle strutture tecnico-gestionali; la notifica materiale all'ACN compete ai Referenti CSIRT. Gli Organi ricevono le informazioni necessarie all'esercizio delle funzioni di indirizzo e supervisione.

5 – Sviluppo sicuro del software

Nello sviluppo del software, l'Ateneo adotta e documenta pratiche di sviluppo sicuro del codice anche riferite a funzioni di monitoraggio che si integrino correttamente con i sistemi di rilevazione delle minacce gestiti dall'Ateneo.

Maggiori dettagli sullo sviluppo sicuro del software sono riportati nella Politica - Sviluppo e Manutenzione Sicura dei Sistemi - Documento: GV_PO-01m.

6 – Documentazione, evidenze e riesame

Le attività svolte ai fini del monitoraggio degli eventi di sicurezza sono supportate da adeguata documentazione ed evidenze. Tale documentazione è conservata secondo le modalità definite dall'organizzazione, in modo da garantirne disponibilità, integrità e tracciabilità.

Le strutture operative documentano, secondo le rispettive competenze, almeno il perimetro monitorato, le configurazioni essenziali, i livelli di servizio, le soglie di allerta, gli eventi rilevanti, le azioni intraprese e gli esiti delle verifiche. Le risultanze alimentano il riesame dell'analisi del rischio, la pianificazione delle misure correttive e il miglioramento continuo.

7 – 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, in seguito a incidenti di sicurezza o quando gli esiti del monitoraggio e dell'analisi del rischio evidenzino la necessità di adeguare le misure.