Università di Genova

Politica - Gestione delle vulnerabilità

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

Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e Direttivi NIS2
3 – Monitoraggio, identificazione e trattamento delle vulnerabilità
4 – Piano di gestione delle vulnerabilità
5 – Documentazione ed evidenze
6 – Revisione e approvazione

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che l'identificazione tempestiva, l'analisi e la gestione delle vulnerabilità che interessano i sistemi informativi e di rete costituiscono una misura essenziale per ridurre l'esposizione alle minacce informatiche e contenere il rischio di compromissione dei servizi e delle informazioni. A tal fine, l'organizzazione adotta un processo strutturato e documentato per monitorare le fonti informative rilevanti, identificare le vulnerabilità che possono interessare i propri asset, valutarne l'impatto e assicurare l'adozione delle opportune misure di risoluzione, mitigazione o accettazione del rischio.

La presente politica è attuata in coordinamento con il Regolamento di Ateneo per la cybersicurezza, che disciplina il processo di gestione delle vulnerabilità e il relativo assetto di responsabilità.

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 sia definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità, ai sensi dell'indicatore ID.RA-08 p. 4, previsto per i soggetti rientranti nel perimetro della cybersicurezza NIS2;
- garantire che siano monitorati i canali informativi rilevanti per l'acquisizione di informazioni su vulnerabilità e minacce emergenti, inclusi almeno i canali del CSIRT Italia e quelli di CERT e ISAC settoriali;
- promuovere l'identificazione tempestiva delle vulnerabilità che interessano i sistemi informativi e di rete dell'organizzazione;
- assicurare che le vulnerabilità identificate siano prontamente risolte mediante aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero gestite attraverso formale accettazione del rischio secondo i processi aziendali vigenti;
- garantire che il piano di gestione delle vulnerabilità sia approvato dagli Organi di Amministrazione e Direttivi e mantenuto coerente con l'evoluzione del contesto tecnologico e del rischio.

3 – Monitoraggio, identificazione e trattamento delle vulnerabilità

L'Ateneo monitora almeno i canali di comunicazione del CSIRT Italia e, ove opportuno, quelli di CERT e le fonti settoriali di informazione pertinenti ed autorevoli al fine di acquisire, analizzare e utilizzare le informazioni rilevanti sulle vulnerabilità che possono interessare i propri sistemi informativi e di rete.

Tali informazioni, unitamente alle evidenze interne disponibili, sono utilizzate per identificare tempestivamente le vulnerabilità, valutarne la rilevanza e gestirle in modo proporzionato al rischio, tenendo conto almeno della criticità degli asset coinvolti, dell'esposizione a minacce, della disponibilità di aggiornamenti di sicurezza o misure di mitigazione e del possibile impatto sull'operatività dell'organizzazione. Ove disponibili, gli aggiornamenti di sicurezza o le misure

di mitigazione sono applicati senza ingiustificato ritardo; ove ciò non sia possibile, il rischio residuo è valutato, documentato e gestito in coerenza con il piano di trattamento dei rischi adottato dall'organizzazione.

In coerenza col Regolamento per la Cybersicurezza, il processo comprende: i) raccolta da fonti qualificate; ii) prima valutazione e prioritizzazione con il coinvolgimento dell'Amministratore di Sistema e/o del Responsabile scientifico delle attività di didattica, ricerca o laboratorio; iii) valutazione e prioritizzazione delle vulnerabilità rilevanti da parte di ogni soggetto responsabile; iv) raccordo con la procedura di cui al GDPR laddove le vulnerabilità possano avere un impatto significativo sulla protezione dei dati personali; v) risoluzione mediante patching, misure di mitigazione o soluzioni temporanee e definitive; vi) rivalutazione attraverso nuove analisi volte a verificare l'efficacia delle azioni correttive.

In tale attività si forniscono i feedback richiesti alle autorità che abbiamo inoltrato comunicazione di specifica vulnerabilità riscontrata su asset dell'Ateneo.

Sulla base di un processo progressivo, anche a fronte del rafforzamento della struttura organizzativa per la gestione della cybersicurezza di cui alla politica GV_PO-01b_Policy_Ruoli_Responsabilità, l'Ateneo istituisce un sistema di gestione e divulgazione coordinata delle vulnerabilità, che preveda, tra gli altre, le seguenti prassi:

- canale pubblico e presidiato per le segnalazioni;
- regole di presa in carico, triage, riscontro e coordinamento;
- protezione del segnalante e gestione delle comunicazioni;
- eventuale pubblicazione di bollettini di sicurezza
- monitoraggio dei canali dei fornitori software critici;
- vulnerability assessment e penetration test periodici e prima dell'entrata in esercizio, secondo rischio.

4 – Piano di gestione delle vulnerabilità

L'Ateneo definisce, attua, aggiorna e documenta un piano di gestione delle vulnerabilità che comprenda almeno le modalità per l'identificazione delle vulnerabilità e la pianificazione delle relative attività, le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità, nonché le procedure, i ruoli e le responsabilità per lo svolgimento di tali attività. Il piano è approvato dagli Organi di Amministrazione e Direttivi e costituisce il riferimento operativo per la gestione coordinata e tracciabile delle vulnerabilità.

5 – Documentazione ed evidenze

Le attività svolte ai fini della gestione delle vulnerabilità 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.

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.