Università di Genova

Politica - Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete

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

Sommario

1 – Principi generali e ambito NIS2
2 – Responsabilità di governo e condizioni organizzative
3 – Gestione del software e aggiornamenti di sicurezza
4 – Ciclo di vita sicuro dello sviluppo software
5 – Supply chain e componenti di terze parti
6 – Documentazione, evidenze e verifiche
7 – Revisione e approvazione

Università di Genova

1 – Principi generali e ambito NIS2

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che lo sviluppo, la configurazione, la manutenzione e la dismissione dei sistemi informativi e di rete devono essere gestiti in modo controllato e coerente con il rischio al fine di preservarne la riservatezza, l'integrità e la disponibilità lungo l'intero ciclo di vita. A tal fine, l'organizzazione adotta misure organizzative e tecniche per assicurare che software, sistemi, componenti, configurazioni e registrazioni di sicurezza siano gestiti in modo sicuro, tracciabile e aggiornato.

La presente politica attua, in relazione alla prassi sopra descritta, quanto previsto espressamente dell'art. 24, comma 2, lett. e), del D.lgs. 4 settembre 2024, n. 138, relativo alla sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, incluse la gestione e la divulgazione delle vulnerabilità.

L'applicazione delle suddette misure è proporzionata alla criticità del servizio, dei dati e degli asset, agli esiti della valutazione del rischio e alle specificità delle attività istituzionali. Per gli ambienti di ricerca e sviluppo, eventuali scostamenti tecnici devono essere motivati, sottoposti ad analisi del rischio e accompagnati da misure compensative concordate con l'Area ICT, in coerenza col Regolamento di Ateneo per la sicurezza informatica.

2 – Responsabilità di governo e condizioni organizzative

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

- garantire l'adozione e la documentazione di pratiche di sviluppo sicuro del software.
- assicurare che siano installati esclusivamente software e sistemi operativi per i quali sia garantita la disponibilità di aggiornamenti di sicurezza, fatte salve motivate e documentate ragioni normative o tecniche;
- garantire che gli aggiornamenti di sicurezza rilasciati dal produttore siano installati senza ingiustificato ritardo, in coerenza con gli esiti della valutazione del rischio e con il piano di gestione delle vulnerabilità;
- garantire un adeguato processo di dismissione dei sistemi informativi e di rete non più idonei.

3 – Gestione del software e aggiornamenti di sicurezza

Sviluppo - Nell'ambito dello sviluppo del software e dell'integrazione applicativa l'Ateneo adotta un approccio basato sulla sicurezza in termini di security e privacy by design e by default.

Le modifiche agli ambienti di produzione sono autorizzate, testate, tracciate e reversibili, ove tecnicamente e organizzativamente possibile; gli ambienti di sviluppo, test e produzione sono separati in misura proporzionata al rischio.

Configurazione - L'Ateneo installa esclusivamente software, inclusi i sistemi operativi, per i quali è garantita la disponibilità di aggiornamenti di sicurezza, in accordo agli esiti della

valutazione del rischio, fatte salve motivate e documentate ragioni normative o tecniche che non lo consentano a fronte delle quali vanno previste adeguate misure compensative.

Manutenzione - Gli aggiornamenti di sicurezza rilasciati dal produttore sono installati senza ingiustificato ritardo, in coerenza con il piano di gestione delle vulnerabilità.

Dismissione - Per i sistemi informatici e di rete non più supportati o non aggiornabili è necessario avviare un processo di dismissione progressivo, compatibilmente con le risorse tecniche e finanziarie disponibili. In caso di impossibilità, anche temporanea a procedere alla dismissione, è necessaria una valutazione documentata del rischio, con misure compensative quali ad es. isolamento, segmentazione, limitazione degli accessi e rafforzamento del monitoraggio.

4 – Ciclo di vita sicuro dello sviluppo software

Nello sviluppo del software, l'Ateneo adotta e documenta pratiche di sviluppo sicuro del codice.

Il ciclo di vita sicuro del software integra la sicurezza dalla definizione dei requisiti alla progettazione, realizzazione, verifica, rilascio, esercizio, manutenzione e dismissione, in attuazione del Regolamento per la Cybersicurezza. In funzione del rischio e della criticità del servizio, devono essere previsti:

- requisiti di sicurezza e protezione dei dati definiti prima dello sviluppo o dell'acquisizione, con eventuale esecuzione della DPIA nei casi previsti;
- analisi delle minacce, architetture sicure, principio del minimo privilegio, difesa in profondità e impostazioni sicure per difetto;
- controllo delle versioni, revisione del codice e test di sicurezza prima del rilascio e dopo modifiche rilevanti;
- gestione protetta dei repository; presenza di un processo strutturato di sviluppo, test, build e deploy;
- criteri di accettazione, approvazione del rilascio, piano di rollback e gestione delle modifiche;
- raccolta e trattamento delle vulnerabilità, manutenzione per l'intera vita utile e dismissione sicura.

Le eccezioni devono essere motivate, approvate dal responsabile competente, registrate con durata definita e riesaminate. Nei contesti di ricerca e sviluppo si applicano i criteri di proporzionalità e le misure compensative previsti del Regolamento Cybersicurezza.

5 – Supply chain e componenti di terze parti

Lo sviluppo e la manutenzione sicura del software sono coordinati con la politica di sicurezza della supply chain (GV_PO-01e_Policy_Supply_Chain_ICT).

6 – Documentazione, evidenze e verifiche

Le attività svolte ai fini dello sviluppo, della configurazione, della manutenzione e della dismissione dei sistemi informativi e di rete 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 evidenze comprendono, in misura proporzionata: requisiti e valutazione del rischio; inventari e dipendenze; esiti di revisioni e test; registri delle versioni e delle modifiche; vulnerabilità, patch ed eccezioni; verifiche sui fornitori; incidenti e azioni correttive.

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 seguito di cambiamenti organizzativi, tecnologici o normativi significativi, o in seguito a incidenti di sicurezza.

Il riesame considera altresì gli aggiornamenti della mappatura dei servizi e del censimento degli asset, le determinazioni ACN applicabili, gli esiti del piano di gestione delle vulnerabilità, gli audit e le variazioni della supply chain.