Università di Genova

Politica – Gestione del Rischio Cybersecurity

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

Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e Direttivi NIS2
3 – Elenco dei sistemi rilevanti
4 – Valutazione, trattamento e piano di gestione del rischio
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 gestione del rischio di sicurezza informatica costituisce il presupposto per l'identificazione, l'analisi, la valutazione, il trattamento e il monitoraggio dei rischi cui sono esposti i sistemi informativi e di rete. A tal fine, l'organizzazione mantiene un elenco aggiornato dei sistemi informativi e di rete rilevanti e adotta un processo strutturato e documentato di valutazione e trattamento del rischio. Il processo è attuato in coerenza col Regolamento di Ateneo per la sicurezza informatica e secondo il modello di responsabilità distribuita definito dal Titolo I del medesimo Regolamento: tutti i soggetti ivi individuati concorrono, secondo le rispettive competenze e responsabilità, alle attività di identificazione, classificazione, valutazione, trattamento e monitoraggio del rischio cyber.

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 mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti;
- garantire che, nell'ambito dei processi di gestione del rischio dell'organizzazione, sia definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi, prevedendo il coinvolgimento dei soggetti individuati dal Titolo I del Regolamento di Ateneo per la sicurezza informatica, ciascuno per gli ambiti di competenza;
- assicurare che sia eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi, a intervalli pianificati e comunque almeno ogni due anni, nonché in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi, con approvazione da parte degli stessi;
- garantire che sia definito, documentato, eseguito e monitorato un piano di trattamento dei rischi per la sicurezza informatica, approvato dagli organi stessi. Tale attività prevede un raccordo con il GDPR, anche rispetto allo sviluppo di misure tecniche e organizzative adeguate alla protezione dei dati personali trattati, che tenga conto dei principi di disponibilità, di integrità e riservatezza.

3 – Elenco dei sistemi rilevanti

È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti, quale presupposto per la corretta impostazione dei processi di gestione del rischio.

4 – Valutazione, trattamento e piano di gestione del rischio

L'Ateneo gestisce il rischio di sicurezza informatica attraverso un piano organico, che ne disciplina l'identificazione, l'analisi, la valutazione, il trattamento e il monitoraggio nel tempo. In coerenza e in diretto collegamento col Regolamento di Ateneo per la sicurezza

informatica, la gestione del rischio si applica a tutte le strutture dell'Ateneo, compresi i contesti di ricerca scientifica, sviluppo, sperimentazione e didattica laboratoriale.

L'analisi e la gestione del rischio costituiscono un processo condiviso e ad evoluzione progressiva, cui concorrono tutti i soggetti individuati dal Titolo I del Regolamento, secondo le rispettive competenze e responsabilità; in particolare, Area ICT, Amministratori di Sistema, Responsabili di struttura e Responsabili scientifici delle attività di didattica, ricerca o dei laboratori assicurano la caratterizzazione degli asset, la valutazione dei rischi e l'attuazione delle misure di competenza. La valutazione del rischio tiene conto anche delle eventuali dipendenze da fornitori e partner terzi ed è condotta con periodicità pianificata, oltre che ogniqualvolta si verifichino incidenti significativi o mutamenti rilevanti nell'organizzazione o nel contesto delle minacce; i relativi esiti sono sottoposti all'approvazione dell'organo di amministrazione.

L'analisi del rischio coinvolge il DPO per gli aspetti inerenti alla protezione dei dati personali. Ad essa si può anche affiancare una DPIA nelle fattispecie previste con rischio elevato dei diritti e delle libertà degli interessati.

Per gli asset destinati alla ricerca scientifica e sviluppo, in prima applicazione e nelle more del completamento dell'analisi del rischio a livello delle diverse strutture, l'analisi comprende almeno: le caratteristiche e le finalità dell'asset secondo lo schema di censimento approvato dall'Ateneo; l'analisi delle vulnerabilità e dei rischi; il trattamento del rischio (definito per mezzo di prassi di trattamento standard).

Qualora, per vincoli tecnici o operativi documentati, le misure di sicurezza ordinarie non siano pienamente applicabili, la messa in sicurezza dell'ambiente è definita d'intesa con l'Area ICT, previa analisi di impatto del cyber rischio, mediante l'adozione di misure compensative concordate e proporzionate al livello di rischio.

Sulla base di tale valutazione, l'Ateneo definisce un piano di trattamento che individua le misure da adottare per ciascuna tipologia affine di rischio, le relative priorità, i responsabili dell'attuazione e le tempistiche previste, motivando adeguatamente l'eventuale accettazione di rischi residui; laddove specifiche misure non risultino attuabili per ragioni tecniche o normative documentate, sono previste soluzioni compensative che riducano il rischio residuo. Anche il piano di trattamento, incluse le decisioni relative ai rischi residui accettati, è approvato dagli Organi di Amministrazione e Direttivi NIS2.

5 – Documentazione ed evidenze

Le attività svolte ai fini della gestione del rischio 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. Rientrano tra le evidenze, in particolare, i dati e gli aggiornamenti dell'archivio degli asset rilevanti, gestiti attraverso un sistema informativo il più possibile integrato a livello delle diverse dimensioni previste (es. ruoli, asset, anagrafiche, sedi, ecc...).

Sono altresì conservati le valutazioni del rischio, gli esiti degli audit, i piani di trattamento e di adeguamento, nonché le motivazioni e le evidenze relative all'adozione di eventuali misure compensative, incluse quelle riferite agli ambienti di ricerca scientifica e sviluppo.

Università di Genova

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/normativi significativi, o in seguito a incidenti di sicurezza.