Università di Genova

Politica - Formazione del personale e consapevolezza

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

Sommario

1 – Principi generali
2 – Quadro di riferimento e raccordo con il Piano di formazione
3 – Governance, ruoli e responsabilità
4 – Pianificazione e articolazione dei percorsi formativi
5 – Attuazione, verifica, tracciabilità e monitoraggio
6 – Revisione e approvazione

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la formazione del personale e la diffusione della consapevolezza in materia di sicurezza informatica costituiscono misure essenziali per ridurre il rischio di comportamenti inadeguati, errori operativi, uso improprio delle risorse digitali e mancato riconoscimento di eventi potenzialmente avversi. A tal fine, l'organizzazione promuove lo sviluppo e il mantenimento di conoscenze e competenze adeguate affinché il personale, inclusi gli Organi di amministrazione e direttivi NIS2, sia in grado di svolgere i propri compiti tenendo conto dei rischi di sicurezza informatica.

La formazione è parte integrante del sistema di gestione della sicurezza informatica e della cultura organizzativa dell'Ateneo; è pianificata secondo criteri di adeguatezza organizzativa, gradualità, ragionevolezza e proporzionalità, in relazione ai ruoli, alle responsabilità e all'esposizione ai rischi cyber.

2 – Quadro di riferimento e raccordo con il Piano di formazione

La presente Policy dà attuazione agli obblighi in materia di formazione e consapevolezza previsti dalla normativa NIS2 e dal Regolamento di Ateneo per la sicurezza informatica, nonché alla misura PR.AT-01 delle specifiche di base adottate dall'Agenzia per la Cybersicurezza Nazionale.

Il Piano di formazione e sviluppo della consapevolezza in materia di cybersicurezza di UniGe (di seguito "Piano") costituisce lo strumento attuativo della presente Policy. Il Piano definisce destinatari, priorità, contenuti, modalità e canali di erogazione, finestre temporali, verifiche, tracciabilità e monitoraggio; è raccordato con il PIAO e con la programmazione della formazione del personale dell'Ateneo.

In caso di aggiornamento del Piano, le presenti previsioni operative si applicano senza necessità di modificare la Politica, purché ne siano rispettati principi, obiettivi e responsabilità.

3 – Governance, ruoli e responsabilità

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

- assicurare che sia definito un Piano di Formazione in materia di sicurezza informatica;
- garantire che il Piano includa la pianificazione delle attività formative, i destinatari, la frequenza, i contenuti e le modalità di verifica dell'apprendimento e/o della partecipazione;
- approvare il Piano e i relativi aggiornamenti, assicurando risorse adeguate e partecipando alla formazione loro destinata;
- promuovere la partecipazione del personale alle attività di formazione e sensibilizzazione in relazione ai ruoli svolti e ai rischi cui l'organizzazione è esposta;
- garantire il mantenimento di un registro aggiornato delle attività formative erogate, dei contenuti trattati, dei partecipanti e delle verifiche svolte, ove previste.

L'Area Direzionale e l'Area del personale in collaborazione con il RTD e la Commissione per la Cybersicurezza, predispongono e aggiornano il Piano. L'Area ICT partecipa alla progettazione della relativa formazione e ne valida i contenuti tecnici. L'Area del personale programma e organizza gli interventi rivolti al personale TABS; gestisce i canali di propria competenza e concorre alla tracciabilità e alla rilevazione delle presenze.

I dirigenti e i soggetti assimilati promuovono e verificano la partecipazione del personale delle strutture di afferenza.

Gli Amministratori di Sistema e il personale tecnico ICT partecipano alla formazione specialistica e contribuiscono, secondo competenza, ai moduli tecnici.

Sono altresì previste procedure per tracciare la frequenza a tale formazione da parte del personale docente e ricercatore.

Il personale destinatario partecipa alla formazione obbligatoria e alle verifiche previste.

4 – Pianificazione e articolazione dei percorsi formativi

L'Ateneo definisce, attua, aggiorna e documenta il Piano rivolto al personale e agli Organi di amministrazione e direttivi NIS2, differenziando la formazione in relazione ai ruoli ricoperti, alle responsabilità assegnate e al livello di esposizione ai rischi informatici.

In coerenza con il Piano, l'offerta è articolata almeno nei seguenti livelli di formazione obbligatoria:

- formazione per gli Organi di amministrazione e direttivi NIS2, i dirigenti e le figure assimilate, incentrata su governance, gestione del rischio, responsabilità NIS2, gestione e notifica degli incidenti e crisi informatiche;
- formazione tecnico - specialistica per Amministratori di Sistema, Incident Response Team, referenti CSIRT, personale ICT e referenti tecnici, progressivamente estendibile ai Responsabili scientifici delle attività di didattica, ricerca o laboratorio, sui principali processi e controlli di sicurezza;
- formazione e cybersecurity awareness per tutto il personale docente e tecnico amministrativo, bibliotecario, sociosanitario (TABS), sui principali rischi, sulla gestione sicura di credenziali, dispositivi, posta elettronica e dati, nonché sul riconoscimento e sulla segnalazione degli incidenti.

Per studenti e altro personale che collabora a qualsiasi titolo con l'Ateneo sono promosse campagne informative e di sensibilizzazione secondo il Regolamento e il Piano, senza sovrapposizione con gli obblighi formativi riservati ai destinatari individuati.

5 – Attuazione, verifica, tracciabilità e monitoraggio

È mantenuto, in formato elettronico strutturato, un registro aggiornato recante almeno l'identificazione del soggetto formato, la struttura di afferenza, il percorso o modulo, le date, i contenuti, il canale di erogazione e l'esito della verifica o il riferimento all'attestato. Le evidenze relative alla pianificazione, all'erogazione e alla partecipazione sono conservate in modo da garantirne disponibilità, integrità e tracciabilità, nel rispetto della disciplina sulla protezione dei dati personali.

Il monitoraggio considera almeno la copertura dei destinatari, lo stato dei completamenti, gli esiti delle verifiche e, ove applicabile, la qualità percepita. Le criticità e i mancati completamenti sono gestiti con solleciti e azioni correttive per struttura; gli esiti del monitoraggio alimentano il riesame del Piano e l'informativa periodica agli Organi.

La formazione sopra descritta può essere accompagnata da iniziative continuative di consapevolezza, quali specifica formazione mirata anche esterna o partecipazione a seminari, ecc.

6 – Revisione e approvazione

La presente politica è approvata dagli Organi di Amministrazione e direttivi NIS2 ed entra in vigore alla data di adozione.

È riesaminata con cadenza programmata, in coerenza con il riesame del Piano e con il ciclo di aggiornamento del PIAO, nonché a seguito di cambiamenti organizzativi, tecnologici o normativi significativi o di incidenti rilevanti.