Università di Genova

Politica - Protezione delle reti e delle comunicazioni

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

Sommario

1 – Principi generali
2 – Governance, ruoli e responsabilità
3 – Censimento delle reti e raccordo con gli asset ICT
4 – Accessi da remoto e sistemi accessibili
5 – Sistemi perimetrali e principi di protezione delle reti
6 – Documentazione ed evidenze
7 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la protezione delle reti e delle comunicazioni costituisce una misura essenziale per preservare la riservatezza, l'integrità e la disponibilità dei sistemi informativi e di rete. A tal fine, l'organizzazione adotta misure coerenti con il rischio per disciplinare gli accessi e per assicurare la presenza, l'aggiornamento, la manutenzione e la corretta configurazione dei sistemi di protezione. La configurazione dei vari sistemi deve essere coordinata, consistente e congruente con i criteri di protezione.

La presente politica si applica:

- Reti informatiche: tutte le reti di Ateneo, indipendentemente dal livello di criticità, incluse WAN, MAN, LAN, VLAN, VXLAN, che siano fisiche o logiche, cablate o wireless, compresi tutti i relativi apparati di rete;
- Sistemi informativi rilevanti:
    - On-premise - server fisici e virtuali ospitati nelle infrastrutture dell'Ateneo, applicazioni e componenti che erogano o supportano servizi digitali;
    - Cloud - sistemi e piattaforme erogati tramite fornitori esterni, inclusi servizi IaaS, PaaS e SaaS;
- Attività e Servizi iCT: servizi digitali erogati agli utenti interni o esterni, con indicazione delle finalità, dei destinatari e delle dipendenze da reti, sistemi e fornitori.
- Identità digitali (relative a persone fisiche o applicative).

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 definite e documentate le eventuali attività consentite e implementate adeguate misure di sicurezza per l'accesso / utilizzo;
- garantire il mantenimento di un elenco aggiornato dei sistemi informativi e di rete, con la descrizione delle relative modalità di accesso;
- assicurare che siano presenti, aggiornati, mantenuti e configurati in modo adeguato i sistemi di protezione.

3 – Accessi da remoto e sistemi accessibili

Per almeno i sistemi informativi e di rete rilevanti, l'Ateneo definisce e documenta le eventuali attività consentite da remoto e implementa adeguate misure di sicurezza per l'accesso. A tal fine, è mantenuto un elenco aggiornato di tali sistemi informativi e di rete ai quali è possibile accedere da remoto, con la descrizione delle relative modalità di accesso.

Gli accessi vanno autorizzati secondo necessità operative, minimo privilegio e separazione delle funzioni; utilizzano canali cifrati, autenticazione adeguata al rischio, preferibilmente a più fattori per accessi privilegiati o a risorse rilevanti, e sono soggetti a registrazione e riesame. Le connessioni di fornitori o terzi vanno limitate nel tempo e nell'ambito, tracciate e presidiate dal referente responsabile.

5 – Principi di protezione delle reti e dei sistemi

Le misure di protezione applicative agli asset indicati al par. 1 sono selezionate e graduate in funzione della classificazione degli asset stessi e dell'analisi del rischio. Si applicano, ove pertinenti, i seguenti principi generali:

- minima esposizione: sono consentiti solo i flussi di comunicazione necessari alla corretta erogazione dei servizi, con regole di filtraggio esplicite, motivate, documentate e periodicamente riesaminate;
- difesa in profondità: controlli preventivi, di rilevazione e di risposta sono distribuiti su più livelli, evitando dipendenze da un unico presidio;
  - segmentazione e segregazione: asset con livelli di classificazione differente sono posti in segmenti separati; i flussi di comunicazione tra segmenti diversi sono consentiti secondo necessità e rischio;
  - protezione del dato: v. politica descritta in GV_PO-01l_Policy_Sicurezza_Dati;
  - governo delle identità: v. politica descritta in GV_PO-01i_Policy_Accessi_Identità;
  - controllo degli accessi: v. politica descritta in GV_PO-01i_Policy_Accessi_Identità;
  - ciclo di vita sicuro del software: v. politica descritta in GV_PO-01m_Policy_Sviluppo_Sistemi;
  - configurazione sicura e ciclo di vita: apparati, firmware, sistemi operativi e regole sono inventariati, aggiornati, sottoposti a backup delle configurazioni e dismessi in modo controllato;
  - protezione delle comunicazioni: sono impiegati protocolli sicuri e cifratura adeguata per dati e credenziali in transito, specialmente su reti non fidate;
  - monitoraggio e tracciabilità: eventi e anomalie rilevanti sono registrati, protetti e analizzati secondo ruoli, tempi di conservazione e procedure di gestione degli incidenti;
  - resilienza: sono implementati ridondanza, continuità, capacità di isolamento e ripristino dei sistemi che supportano servizi istituzionali critici;
  - gestione di configurazioni particolari: configurazioni non standard, in particolare per ricerca e sperimentazione, sono motivate e autorizzate previa analisi del rischio, con misure compensative concordate e proporzionate.

Quando la valutazione evidenzi rischi significativi o vulnerabilità non tempestivamente mitigate e/o mitigabili, l'Area ICT può adottare, nei limiti delle competenze previste dal Regolamento, misure proporzionate quali limitazione dell'accesso di rete, segregazione

e/o isolamento del sistema, rafforzamento dell'autenticazione e disabilitazione di servizi non essenziali.

In fase di attuazione delle suddette misure, sono assicurate le idonee prassi di comunicazione, ai soggetti interessati, come previste dal Regolamento per la Cybersicurezza e della disposizioni normative.

6 – Documentazione ed evidenze

Le attività svolte ai fini 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 fonti di riferimento della documentazione sono, nell'ordine:

- le fonti regolatorie previste (Direttiva Europea NIS2; Decreto Legislativo NIS2, relativi decreti attuativi; determinazioni dell'Autorità NIS2, GDPR e normativa collegata, ecc…);
- Il Regolamento di Ateneo per la Cybersicurezza e il Regolamento dell'Università degli studi di Genova in materia di trattamento dei dati personali;
- Le Politiche cyber previste per i soggetti NIS2;
- Gli Allegati al Regolamento;
- Le Circolari, Direttive e Linee Guida ICT di Ateneo.

Le evidenze comprendono, secondo pertinenza: dati del censimento, responsabilità e autorizzazioni, schemi e dipendenze di rete, configurazioni e loro variazioni, regole perimetrali, verifiche degli accessi, aggiornamenti, esiti di monitoraggio, vulnerabilità, eccezioni e misure compensative. La documentazione è aggiornata in occasione di modifiche significative e resa disponibile per audit e riesami.

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 o in seguito a incidenti di sicurezza.

Il riesame considera altresì gli esiti dell'aggiornamento del censimento, dell'analisi del rischio, degli audit, del monitoraggio delle reti e delle vulnerabilità, nonché l'efficacia delle misure applicate e l'eventuale necessità di adeguamento organizzativo o finanziario.