Università di Genova

Politica - Continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche

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

Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e Direttivi NIS2
3 – Piani di continuità operativa, ripristino e gestione della crisi
4 – Coordinamento organizzativo
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 capacità di assicurare la continuità operativa dei servizi essenziali, ripristinare tempestivamente i sistemi informativi e di rete e gestire in modo coordinato le crisi informatiche costituisce un elemento essenziale della resilienza organizzativa. A tal fine, l'organizzazione definisce, attua, aggiorna e documenta piani dedicati alla continuità operativa, al ripristino in caso di disastro e alla gestione delle crisi informatiche, in coerenza con la criticità dei sistemi informativi e di rete rilevanti e con il profilo di rischio cui essi sono esposti.

Nei relativi Piani si dettagliano gli aspetti relativi alle infrastrutture centrali e alle infrastrutture gestite dalle strutture fondamentali.

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:

- approvare la presente Politica e i piani di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi, prevedendo altresì la costituzione di un Comitato di gestione della crisi nonché una procedura di comunicazione da adottare in tali casi, con coinvolgimento degli uffici responsabili;
- assicurare che la continuità operativa e la resilienza siano integrate nelle decisioni strategiche, organizzative e finanziarie dell'Ateneo;
- garantire l'assegnazione di risorse umane, tecnologiche e finanziarie adeguate alla gestione della Business Continuity ed al Disaster Recovery;
- sovrintendere all'attuazione degli obblighi e verificare periodicamente, sulla base di rendicontazioni e indicatori predisposti dalle strutture competenti, l'efficacia complessiva delle misure adottate;

3 – Piani di continuità operativa, ripristino e gestione della crisi

Per almeno i sistemi informativi e di rete rilevanti, l'Ateneo definisce, attua, aggiorna e documenta (ai sensi dell'indicatore Nis2 ID.IM-04 p. 1):

- un Piano di continuità operativa;
- un Piano di ripristino in caso di disastro.

Tali piani disciplinano almeno le finalità e l'ambito di applicazione, i ruoli e le responsabilità, i contatti principali e i canali di comunicazione interni ed esterni, le condizioni per l'attivazione e la disattivazione, nonché le risorse necessarie, inclusi backup e ridondanze; il piano di ripristino definisce inoltre l'ordine di ripristino delle operazioni e le procedure di ripristino per operazioni specifiche, compresi i relativi obiettivi, mentre il piano di gestione delle crisi informatiche disciplina anche le modalità di comunicazione tra i soggetti coinvolti e le autorità competenti.

La definizione delle priorità di continuità e ripristino è fondata sul censimento e sulla classificazione degli asset, sulla valutazione del rischio cyber e su una Business Impact Analysis (BIA) che individui almeno: processi e servizi essenziali; dipendenze da dati, infrastrutture, personale e fornitori; impatti massimi tollerabili; ordine di ripristino; obiettivi di tempo e punto di ripristino (RTO e RPO), ove applicabili; modalità operative alternative o degradate[1].

L'individuazione dei parametri di Business continuity come la BIA, il RTO e il RPO è svolto insieme alle Aree dirigenziali responsabili di un dato dominio di attività: es. didattica e servizi agli studenti, ricerca, gestione del personale e delle risorse finanziarie ecc…

Per i servizi cui sia attribuito un livello di cyber rischio elevato sono effettuati, tipicamente su base annuale, test di continuità operativa. Gli esiti sono documentati e alimentano il riesame dei piani e le azioni correttive. Gli scenari di prova includono, ove pertinenti, indisponibilità di sedi o personale, compromissione o perdita di dati, guasto infrastrutturale, indisponibilità di servizi cloud o di fornitori critici e interruzione delle comunicazioni, fenomeni fisici, atmosferici, calamità, ecc…

Nei contesti di ricerca e sviluppo, eventuali vincoli tecnici o operativi sono valutati d'intesa con l'Area ICT mediante analisi d'impatto del rischio e individuazione di misure compensative proporzionate, ferme restando le responsabilità dei Responsabili scientifici, degli Amministratori di sistema e delle strutture previste dal Regolamento.

4 – Coordinamento organizzativo

L'Ateneo assicura che i piani siano coerenti tra loro e coordinati con i processi di gestione degli incidenti, con le misure di backup e ripristino, con i flussi di comunicazione interni ed esterni e con i ruoli assegnati al personale e, ove opportuno, ai fornitori. In tal modo, la gestione della continuità operativa e della crisi informatica è integrata nel più ampio sistema di gestione della sicurezza informatica e della resilienza organizzativa.

Sulla base degli indirizzi degli Organi, Il costituendo Comitato di gestione della Crisi, le Aree dirigenziali competenti per la natura specifica di una data crisi e il RTD, coordinano le attività inerenti l'attuazione dei suddetti Piani (Continuità operativa; Ripristino in caso di disastro) e le relative attività di comunicazione interne ed esterne, previste anche ai sensi del D.lgs. 138/2024).

Per i dettagli specifici di gestione dell'incidente si rimanda agli specifici protocolli previsti nel Piano per la gestione degli incidenti di sicurezza informatica (RS.MA-01 p. 2).

5 – Documentazione ed evidenze

Le attività svolte ai fini della continuità operativa, del ripristino in caso di disastro e della gestione delle crisi informatiche sono supportate da adeguata documentazione ed

[1] La BIA (Business Impact Analysis) è l'analisi che identifica i processi e i servizi essenziali, valuta gli effetti di una loro interruzione e determina le priorità e i requisiti di ripristino. L'RTO indica il tempo massimo entro cui ripristinare un servizio. L'RPO indica la massima perdita di dati accettabile, espressa come intervallo temporale rispetto all'ultimo punto recuperabile.

evidenze. Tale documentazione è conservata secondo le modalità definite dall'organizzazione, in modo da garantirne disponibilità, integrità e tracciabilità.

La documentazione comprende almeno: versioni approvate dei piani; BIA e criteri di priorità; inventario delle dipendenze e dei contatti; esiti dei test e delle esercitazioni; decisioni e comunicazioni assunte durante la crisi; tempi effettivi di ripristino; scostamenti rispetto agli obiettivi; lezioni apprese e azioni correttive con responsabili e scadenze. Una copia aggiornata delle informazioni indispensabili all'attivazione deve essere accessibile anche in caso di indisponibilità dei sistemi ordinari, con adeguate misure di protezione.

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.

I Piani di continuità operativa e di ripristino in caso di disastro sono riesaminati periodicamente e sottoposti all'approvazione del Consiglio di amministrazione, in coerenza col Regolamento per la sicurezza informatica. Il riesame è comunque anticipato in caso di incidenti significativi, crisi, modifiche rilevanti del perimetro degli asset, esiti negativi delle prove o mutamenti sostanziali dell'esposizione alle minacce e ai rischi.