Decreto n. 4176 del 16.10.2025

Università di Genova

AREA LEGALE E GENERALE - SERVIZIO AFFARI GIURIDICI E ISTITUZIONALI
Settore affari generali e procedimenti elettorali
IL RETTORE E IL DIRETTORE GENERALE

Visto lo Statuto di Ateneo;

Visto il Regolamento generale di Ateneo;

Visto il Regolamento di Ateneo per l'amministrazione, la finanza e la contabilità;

Visto il Regolamento UE n. 679/2016 (GDPR);

Vista la Direttiva UE 2022/2555 (Direttiva NIS2), recepita a livello nazionale con il Decreto Legislativo n. 138/2024 (Decreto NIS2);

Visto il Piano Triennale dell'Informatica della Pubblica Amministrazione, aggiornamento 2025-2027 redatto dall'Agenzia Nazionale per l'Italia Digitale (AGID);

Vista l'individuazione dell'Università degli Studi di Genova come "soggetto importante" ai fini dell'attuazione della Direttiva NIS2, ai sensi dell'art. 3, comma 6, del D. Lgs. n. 138/2024, in base alla Determinazione del Direttore Generale dell'Agenzia Nazionale per la Cybersicurezza (ACN) n. 136432 del 12 aprile 2025;

Preso atto altresì che in base al cronoprogramma NIS2 saranno previste le seguenti prime attività, con specifico scadenziario relativo all'Università di Genova:

- Implementazione di una procedura relativa all'obbligo di notifica entro 24 ore in caso di incidente di cyber sicurezza effettivo o possibile, che rechi pregiudizio significativo alle attività dell'Ente o al benessere delle persone – entro 1/1/2026 - art. 42 co. 1 Decreto NIS2;
- Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi (ICT) - entro 01/01/2026 - art. 42 co. 2 Decreto NIS2;
- Obbligo adempimenti art. 23-24-29 Decreto NIS2 – entro 11.10.2026 - art. 42 co. 1 Decreto NIS2 ed in particolare
  - Art. 23 Organi di amministrazione e direttivi – compiti (tra cui formazione ai dipendenti e controllo attuazione misure di cui ai successivi articoli);
  - Art. 24 Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica;

Vista la delibera del Consiglio di Amministrazione del 28 maggio 2025, che ha definito le seguenti misure da attuare per implementare efficacemente le

direttive NIS2 nell'Università degli Studi di Genova e sviluppare un miglior processo di gestione correlato:

a) Informazione e formazione sulla *cybersecurity awareness*, commisurata ai diversi ruoli;
b) Integrazione delle linee guida vigenti in un Regolamento di Ateneo sulla sicurezza informatica, conforme alle Direttive NIS2, con definizione della struttura organizzativa della *cybersecurity*, coerente con l'assetto di Ateneo;
c) Aggiornamento delle *policy* per gli amministratori di sistema in coerenza con la Direttiva NIS2;
d) Completamento della mappatura dei rischi e definizione delle misure di mitigazione coerenti con il succitato regolamento (es. segmentazione rete, filtraggio avanzato, isolamento sistemi, continuità operativa, autenticazione a due fattori), da definire anche mediante il coinvolgimento delle strutture fondamentali, al fine di commisurare le prassi di protezione con l'esigenza di fruibilità e accessibilità dei servizi digitali;
e) Presidio della sicurezza della produttività individuale mediante la messa in sicurezza dei sistemi di autenticazione del personale e dei dati da esso gestiti in sistemi protetti di tipo "cloud first", con attenzione alla piena compliance dei dati gestiti da fornitori terzi rispetto all'aderenza dei criteri di protezione del cloud;

Considerata la necessità di costituire una *Task Force* per presidiare la sicurezza informatica dell'Ateneo e le correlate azioni di informazione / formazione, estendendo in modo capillare in Ateneo un approccio di gestione proattiva del *cyber* rischio;

Ritenuto indispensabile prevedere professionalità del settore accademico e tecnico-amministrativo;

DECRETANO

Art. 1 - Costituzione della *Task Force*

1. È istituita la *Task Force* per la Sicurezza Informatica di Ateneo (di seguito *Task Force*).
2. La *Task Force* ha l'obiettivo di
    a. definire le priorità e individuare le migliori prassi organizzative, tecnologiche e regolamentari ai fini della pianificazione, progettazione, gestione, monitoraggio e riesame della sicurezza informatica di Ateneo, supportando gli Organi di governo nelle opportune decisioni e deliberazioni, anche connesse agli adempimenti previsti a livello comunitario e nazionale;
    b. indirizzare le strutture di Ateneo dotate di autonomia organizzativa e gestionale nel percorso di condivisione delle conoscenze sul cyber rischio e di gestione proattiva dello stesso, in modo da garantire la sicurezza informatica delle infrastrutture, dei sistemi, delle informazioni / dati gestiti, in conformità con le specifiche condizioni di autonomia e di responsabilità previste nell'ambito dell'ordinamento delle Università e con l'assetto organizzativo di Ateneo.

Art. 2 - Composizione della *Task Force*

1. La *Task Force* è composta dai seguenti gruppi:

   a. **Gruppo di coordinamento** – Prof.ssa Paola GIRDINIO (IIET-01/A – Elettrotecnica), Coordinatrice; Prof. Alessandro ARMANDO (IINF-05/A – Sistemi di elaborazione delle informazioni); Prof. Sandro ZAPPATORE (IINF-03/A – Telecomunicazioni), Prof.ssa Marina RIBAUDO (INFO-01/A – Informatica); Prof. Gerolamo TACCOGNA (GIUR-06/A – Diritto amministrativo e pubblico); Dott. Enrico RUSSO (IINF-05/A – Sistemi di elaborazione delle informazioni); Dott. Paolo TESSITORE, Dirigente Area ICT; Dott. Claudio DI MARTINO, Responsabile Servizio Infrastrutture e Sistemi ICT; Dott. Paolo MORESCO, Responsabile Servizio Tecnologie per i Poli Territoriali; Ing. Agnese AROSIO, Servizio Infrastrutture e Sistemi ICT;

   b. **Gruppo tecnico - gestionale** – Ing. Agnese AROSIO, Servizio Infrastrutture e Sistemi ICT (Referente tecnico - gestionale); per il Servizio Infrastrutture e Sistemi ICT: Dott. Claudio DI MARTINO, Ing. Gianni VERDUCI, Dott. Massimo IVALDI; per Servizio Tecnologie per i Poli Territoriali: Dott. Paolo MORESCO, Dott. Daniele FABBRINI, Dott. Stefano OROCCHI; per l'Area legale e generale: Dott. Dott.ssa Anna RAPALLO; Dott.ssa Paola LOVISOLO;

   c. Altre figure ritenute necessarie per il raggiungimento degli obiettivi della Task Force saranno coinvolte nei tavoli di lavoro previsti, sulla base di quanto specificato all'art. 6.

Art. 3 - Compiti della Task Force

1. In coerenza con gli obiettivi previsti all'art. 1, la Task Force avrà i seguenti compiti, correlati alle disposizioni NIS2 e alle deliberazioni assunte dall'Ateneo:

I. In relazione alle disposizioni NIS2, sarà previsto in prima applicazione quanto segue (fatti salvi ulteriori adempimenti previsti per i soggetti importanti NIS2 che potranno essere emanati, e che verranno recepiti in termini di presidio dalla Task Force):

   a. Implementazione di una procedura per relativa all'Obbligo di notifica entro 24 ore in caso di incidente di cyber sicurezza effettivo o possibile, che rechi pregiudizio significativo alle attività dell'Ente o al benessere delle persone – entro 31.12.2025 - art. 42 co. 1 Decreto NIS2;

   b. Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi (ICT) - entro 01.01.2026 - art. 42 co. 2 Decreto NIS2;

   c. Obbligo adempimenti art. 23 - 29 Decreto NIS2 – entro 11/10/2026 - art. 42 co. 1 Decreto NIS2 ed in particolare:

      1. Art. 23 Organi di amministrazione e direttivi – compiti (tra cui formazione ai dipendenti e controllo attuazione misure di cui ai successivi articoli);
      2. Art. 24 Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica.

II. In relazione alle priorità previste dall'Ateneo, come da delibera del Consiglio di Amministrazione del 28 maggio 2025:

   a. Informazione e formazione sulla *cybersecurity awareness*, commisurata ai diversi ruoli;

b. Integrazione delle linee guida vigenti in un Regolamento di Ateneo sulla sicurezza informatica, conforme alle Direttive NIS2, con definizione della struttura organizzativa della cybersecurity, coerente con l'assetto di Ateneo;

c. Aggiornamento delle policy per gli amministratori di sistema in coerenza con la Direttiva NIS2;

d. Completamento della mappatura dei rischi e definizione delle misure di mitigazione coerenti con il succitato regolamento (es. segmentazione rete, filtraggio avanzato, isolamento sistemi, continuità operativa, autenticazione a due fattori), da definire anche mediante il coinvolgimento delle strutture fondamentali, al fine di commisurare le prassi di protezione con l'esigenza di fruibilità e accessibilità dei servizi digitali;

e. Presidio della sicurezza della produttività individuale mediante la messa in sicurezza dei sistemi di autenticazione del personale e dei dati da essi gestiti in sistemi protetti di tipo "cloud first", con attenzione alla piena compliance dei dati gestiti da fornitori terzi rispetto all'aderenza dei criteri di protezione del cloud.

Art. 5 - Durata

1. In prima applicazione la *Task Force* ha una durata allineata con il mandato del Rettore con decorrenza dalla data del presente decreto. Fino all'adozione di un nuovo provvedimento di designazione dei componenti, la *Task Force* continuerà ad operare al fine di garantire la continuità dell'azione amministrativa, in adempimento alle normative previste.

Art. 6 – Riporto e Procedure Operative

1. La *Task Force* si riunisce regolarmente, fissando le modalità di convocazione e le tempistiche.
2. La *Task Force* definisce le proprie procedure operative, garantendo la trasparenza e la partecipazione attiva dei membri.
3. La *Task Force* redige periodicamente un report delle attività svolte, da trasmettere agli Organi di governo al fine di supportare le deliberazioni conseguenti.
4. A tale fine la Task Force riporta al Rettore, e al Direttore Generale, in relazione agli specifici ruoli svolti dai componenti.

Art. 7 - Disposizioni conclusive.

1. Il presente decreto è pubblicato sull'albo e sul sito *web* di Ateneo, nella pagina https://ict-unige.it. Il documento informatico originale, sottoscritto con firma digitale, è conservato presso l'Area legale e generale.

IL RETTORE
F.to digitalmente
Prof. Federico DELFINO

IL DIRETTORE GENERALE
F.to digitalmente
Dott.ssa Tiziana BONACETO