Ministero dell'Università e della Ricerca

Consiglio Nazionale degli Studenti Universitari

Roma, 26 febbraio 2026

Alla **c.a.**

del **Ministro dell'Università e della Ricerca (MUR)**
On.Annamaria Bernini
gabinetto@pec.mur.gov.it
del **Segretario Generale del Ministero dell'Università e della Ricerca (MUR)**
prof.Marco Mancini
segretariatogenerale@pec.mur.gov.it

della **Presidente della Conferenza dei Rettori delle Università Italiane** (CRUI)
Prof.ssa Laura Ramaciotti
segreteria.crui@pec.it

LORO SEDI

Oggetto: Richiesta urgente di chiarimenti alle università statali sulle misure adottate per garantire la continuità didattica, la sicurezza dei sistemi informatici e la protezione dei dati personali a seguito dell'attacco informatico che ha colpito l'Università "Sapienza" di Roma tra la notte del 30 e 31 gennaio 2026.

Adunanza del 26 febbraio 2026

PREMESSO

Che a partire dalla notte tra il 30 e 31 gennaio 2026 l'Università La Sapienza di Roma è stata vittima di un grave attacco informatico che ha determinato il blocco del sito web ufficiale dell'Ateneo, dei sistemi interni di gestione della carriera studentesca e dei servizi digitali fondamentali per l'erogazione della didattica, la prenotazione degli esami, il pagamento delle tasse e l'accesso alle piattaforme di studio online.
La situazione ha costretto l'Ateneo al blocco immediato delle reti e dei sistemi digitali in via precauzionale, nonché all'attivazione di task force tecniche in collaborazione con l'Agenzia per la Cybersicurezza Nazionale per reclutare esperti e procedere alle attività di contenimento e ripristino. Diversi organi di stampa nazionali riportano che

l'incidente ha avuto natura sospettata di *ransomware,* coinvolgendo vari sistemi strategici dell'Ateneo e imponendo lo spegnimento delle infrastrutture digitali per tutelare l'integrità e la sicurezza dei dati. L'attacco ha determinato, e continua tuttora a determinare, l'interruzione prolungata di servizi digitali essenziali, con persistenti e significative ripercussioni sulla regolarità della vita accademica degli studenti, sulla gestione delle carriere, sulla comunicazione istituzionale e sull'accesso ai contenuti didattici online.

VISTO

- l'art. 34 della Costituzione della Repubblica Italiana, che tutela il diritto allo studio;
- la Legge 9 maggio 1989, n. 168 sul Sistema universitario nazionale;
- la Legge 30 dicembre 2010, n. 240 (Riforma del sistema universitario);
- il Regolamento (UE) 2016/679 (GDPR), in particolare gli artt. 5, 24, 25, 32, 33 e 34 in materia di sicurezza del trattamento, responsabilizzazione del titolare e notifica delle violazioni dei dati personali;
- il D.Lgs. 30 giugno 2003, n. 196 come modificato dal D.Lgs. 101/2018;
- il D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale), con specifico riferimento all'art.50-bis in materia di continuità operativa e piano di disaster recovery;
- il dlgs. 4 settembre 2024, n. 138 (attuazione della Direttiva (UE) 2022/2555 – NIS2), sul rafforzamento della sicurezza delle reti ICT e dei sistemi critici;
- le Linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) e le Linee guida dell'Agenzia per l'Italia Digitale (AgID) in materia di sicurezza ICT per le pubbliche amministrazioni;

CONSIDERATO

- che università statali italiane sono, in quanto enti pubblici autonomi, titolari del trattamento ai sensi del GDPR e pertanto tenute ad adottare misure tecniche e organizzative adeguate per garantire la sicurezza, l'integrità, la disponibilità e la riservatezza dei dati trattati;
- che l'interruzione di sistemi digitali e servizi online incide direttamente sull'erogazione del diritto allo studio e sulla regolarità delle carriere accademiche, con possibile pregiudizio per studenti, docenti e personale;

- che la normativa nazionale ed europea impone alle pubbliche amministrazioni l'adozione di piani di continuità operativa, di disaster recovery e di gestione degli incidenti informatici;
- che l'attacco alla Sapienza evidenzia rischi sistemici rispetto alla vulnerabilità delle infrastrutture ICT degli Atenei e alla tutela dei dati degli utenti;

RITENUTO

necessario assicurare piena trasparenza nei confronti della comunità accademica e verificare lo stato di aggiornamento e adeguatezza delle misure di sicurezza informatica adottate dalle università statali per prevenire e gestire eventi analoghi;

all'unanimità

IL CONSIGLIO NAZIONALE DEGLI STUDENTI UNIVERSITARI

CHIEDE

Con specifico riferimento ai fatti occorsi presso l'Università Sapienza di Roma tra la notte del 30 e 31 gennaio 2026.

Si chiede che il Ministero dell'Università e della Ricerca:
1. Promuova un'interlocuzione istituzionale con l'Ateneo interessato al fine di acquisire elementi utili circa:

- la natura dell'attacco informatico;
- le misure tecniche di contenimento adottate;
- lo stato del ripristino dei servizi digitali;
- eventuali interventi di rafforzamento già programmati.

2. Verifichi, in coordinamento con l'Agenzia per la Cybersicurezza Nazionale, l'eventuale impatto su:

- dati personali di studenti, docenti e personale;
- procedure amministrative e di gestione delle carriere;
- eventuali sistemi digitali connessi a procedure elettorali studentesche.

3. Valuti, in un'ottica di prevenzione futura, l'adeguatezza dei piani di continuità operativa e di disaster recovery adottati, anche al fine di individuare eventuali buone pratiche replicabili a livello nazionale.

4. Assicuri che non derivino pregiudizi per le carriere accademiche degli studenti, promuovendo misure compensative uniformi.

5. Incentivi una comunicazione istituzionale chiara e periodica verso la comunità accademica, nel rispetto della trasparenza e della tutela dei dati.

Con riferimento al sistema universitario nazionale che il Ministero:

1. Proceda a una verifica su base nazionale dello stato di attuazione dei piani di continuità operativa, di "disaster recovery" e di gestione degli incidenti informatici presso tutte le università statali.

2. Definisca e renda pubbliche misure minime obbligatorie di sicurezza ICT uniformi per tutti gli Atenei, prevedendo almeno:

a) In materia di gestione delle carriere e database amministrativi:
- cifratura dei dati secondo standard crittografici aggiornati;
- registrazione e conservazione degli accessi in maniera sicura;
- policy obbligatorie di backup periodico con test documentati di ripristino.

b) In materia di servizi email istituzionali:
- obbligo di protocolli che garantiscano congrui standard crittografici;
- sistemi di protezione contro phishing e malware;

3. Istituisca un monitoraggio periodico nazionale sul livello di sicurezza informatica degli Atenei, con relazione pubblica annuale sugli standard di conformità, vulnerabilità e misure di mitigazione adottate.

4. Definisca indicatori uniformi di rischio e protocolli standardizzati di risposta agli incidenti, al fine di ridurre l'impatto di eventuali attacchi su studenti, docenti e personale.

5. Valuti l'adozione di linee guida nazionali per la sicurezza delle procedure elettorali digitali, con particolare riferimento ai sistemi di voto elettronico e di gestione delle candidature.

6. Disponga misure uniformi di tutela delle carriere accademiche in caso di gravi interruzioni dei servizi digitali, prevedendo strumenti compensativi automatici e criteri omogenei su tutto il territorio nazionale.

IL PRESIDENTE

Lorenzo Bassi