Prot.n.468382 18.12.2020

Tit. I/5

Oggetto: Misure di sicurezza per l'erogazione di didattica a distanza e *meeting* in Zoom.

Gentili Colleghe e Colleghi,

Gentili Collaboratrici e Collaboratori,

recenti episodi di "incursioni web", durante lo svolgimento di attività didattica a distanza, mi costringono a chiedervi uno sforzo, individualmente minimo ma collettivamente assai prezioso, per tutelare il buon nome e l'immagine del nostro Ateneo.

Si tratta di un fenomeno già noto nel mondo informatico che, complice il *lockdown* e il ricorso sempre più frequente alla didattica a distanza, è purtroppo approdato anche nelle aule virtuali universitarie.

Circa un mese fa, nel corso di una lezione tenuta nella modalità a distanza e tramite la piattaforma Zoom, alcuni individui si sono infiltrati con interruzione dell'attività didattica del docente, sovrascrittura in video di immagini oscene e violente nonché offese volgari ai presenti.
Successivamente, nonostante il nostro Servizio informatico si sia prontamente attivato per prevenire simili situazioni, si sono verificati altri due episodi, probabilmente ad opera dei medesimi soggetti.

Quanto accaduto è sicuramente molto grave e, qualora dovesse ripetersi con una certa frequenza, potrebbe arrecare un danno di immagine all'Ateneo. Per questo motivo è stato immediatamente denunciato alle autorità competenti.

E' fondamentale tuttavia anche la vostra collaborazione. Tali "incursioni web" non sono affatto ineluttabili: si possono – e si devono – prevenire rispettando le misure minime di sicurezza informatica, come peraltro già da tempo richiesto a tutti i docenti e collaboratori coinvolti nella organizzazione di lezioni a distanza o *meeting on line* di qualsiasi tipo.

La messa in sicurezza a monte del sistema informatico di erogazione della didattica a distanza e di riunioni ed eventi telematici sarebbe possibile ma al momento non praticabile per due ordini di problemi: un notevole incremento della spesa, per la necessità di dotarsi di ulteriori licenze del software Zoom a carattere oneroso, ed un aggravio insostenibile di lavoro per gli addetti del servizio informatico che avrebbe come conseguenza la compromissione del livello di supporto informatico, attualmente garantito in altri ambiti.

Per questo motivo, mi appello al vostro impegno e senso di responsabilità nel rispetto puntuale e quotidiano delle indicazioni e delle procedure di indizione e gestione dei *meeting* Zoom fornite e costantemente aggiornate dalla competente Direzione Sistemi Informativi e Tecnologie.
Da parte mia ho già dato disposizioni affinché tali procedure siano portate a conoscenza di noi tutti, docenti e collaboratori, attraverso modalità di comunicazione più semplici ed efficaci.

Nei prossimi giorni saranno, pertanto, attivate campagne di informazione mirata sulla sicurezza dei *meeting*, supportate da infografica dedicata ed istruzioni semplificate (tutorial).
Vi anticipo da subito alcune sintetiche indicazioni, rinviandovi ai successivi comunicati della Direzione Sistemi Informativi e Tecnologie per tutte le istruzioni di dettaglio.

**Azioni generali**

- *Waiting room*: attivare sempre la *waiting room*.
- Microfoni, chat e condivisioni non attivi: è possibile ed all'occorrenza consigliato, impedire l'audio e lo scritto di una persona, autorizzandola solo se necessario; lo stesso vale per le condivisioni. Ciò permette di evitare l'intrusione audio, scritta e visiva nei *meeting* Zoom.
- evitare di pubblicizzare in rete link a *meeting* Zoom, a meno che non si seguano scrupolosamente gli accorgimenti sopra indicati.

**Lezioni**

- Salvo limitatissime eccezioni (*si veda punto seguente*), prevedere sempre l'opzione di accesso con le credenziali GIA, in dotazione a studentesse e studenti regolarmente immatricolati. In questo modo, essendo utenti noti all'Ateneo ed identificati, potranno accedere direttamente senza essere filtrati dalla *waiting room.* Questa impostazione deve essere configurata al momento della pianificazione del *meeting*.
- Nei pochi casi di lezioni che prevedano anche, in modo limitato, l'accesso di studentesse e studenti e/o ospiti esterni, si dovranno ammettere manualmente – quindi in modo controllato – tutti i soggetti esterni che non possiedono credenziali GIA. Dovrà quindi essere impostata la *waiting room,* ammettendoli dopo averne verificato l'identità.

**Eventi aperti al pubblico**

Per garantire la sicurezza negli eventi *on line* in cui i partecipanti non sono noti a priori oppure siano esterni, senza credenziali GIA d'Ateneo (convegni, seminari, presentazioni, etc.), la soluzione tecnicamente più sicura e più pratica, per pianificazione e gestione, è il Webinar:

- si tratta di una modalità di *meeting* che prevede uno o più relatori autorizzati ad un'interazione completa, mentre i partecipanti possono interagire solo in chat o, se in audio, solo tramite un moderatore.

In alternativa - per quanto modalità di più complessa gestione, che prevede una preparazione nei giorni precedenti all'evento - si può ricorrere al Meeting con iscrizione:

- in questo caso è necessario richiedere la formalizzazione di un'iscrizione al *meeting*, gestire gli iscritti e comunicare solo agli utenti, così identificati, il link al *meeting*.

Infine, nel rammentare che tutto il personale universitario è tenuto all'osservanza delle disposizioni normative e dei regolamenti interni (Statuto, Regolamenti d'Ateneo, Codice Etico, Codice di Comportamento dei Dipendenti e Codici Disciplinari), vi invito caldamente al rispetto delle indicazioni che saranno fornite dalla Direzione Sistemi Informativi e Tecnologie affinché, con l'impegno di tutti le nostre attività didattiche ed i nostri eventi on line, possano svolgersi in sicurezza.

Il Rettore
Prof. Pier Francesco Nocini