AVVISO

Ricognizione interna rivolta al personale *docente*, *dirigente* e *tecnico-amministrativo* dell'Ateneo per l'individuazione di dipendenti per attività di supporto specialistico all'Area dei Sistemi Informativi per l'adeguamento alla direttiva NIS2.

Università di Catania Area Risorse Umane	Rep DECRETI 4243
TIT VII	CL 3
Prot. 200924	24.10.2025

- ✓ Visto il D.Lgs. 30.3.2001, n. 165;
- ✓ Vista la legge 30.12.2010, n. 240;
- ✓ Vista la Direttiva (UE) 2022/2555" *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione*" (Direttiva NIS2), che aggiorna e rafforza il quadro legislativo in materia di sicurezza informatica, sostituendo la precedente Direttiva NIS;
- ✓ Visto il D.Lgs. n. 138/2024 (o "decreto NIS"), che recepisce la Direttiva NIS2 nell'ordinamento nazionale e designa l'Agenzia per la Cybersicurezza Nazionale (ACN) quale autorità competente per la supervisione e il coordinamento dell'attuazione della direttiva in Italia;
- ✓ Vista la Determinazione n. 136432 del 12 aprile 2025, con cui l'Agenzia per la Cybersecurity Nazionale ha inserito l'Università degli Studi di Catania nell'elenco dei soggetti NIS importanti, in relazione alla tipologia "Istituti di istruzione che svolgono attività di ricerca" di cui all'allegato IV del suddetto decreto NIS;
- ✓ Vista la Determinazione n. 164179 del 14 aprile 2025, con cui l'ACN ha definito le misure di sicurezza di base da adottare, nonché i requisiti per la notifica degli incidenti significativi;
- ✓ Considerato che, a seguito dell'individuazione quale soggetto NIS2 importante, l'Ateneo è vincolato al rispetto degli adempimenti previsti dall'art. 25 del D.Lgs. 138/2024 (Obblighi in materia di notifiche di incidente) e dagli artt. 23 e 24 del medesimo decreto (Organi di amministrazione e direttivi, Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica), rispettivamente entro 9 mesi e 18 mesi dalla comunicazione di inserimento tra i soggetti NIS importanti, pervenuta il 12 aprile 2025;
- ✓ Visto il D.D. n. 1474/2025 del 2/4/2025 con cui è stato costituito il gruppo di coordinamento "*Team NIS 2*" con competenze trasversali;
- ✓ Considerato che nell'ambito dei lavori del suddetto gruppo di coordinamento, tenuto conto della portata e della complessità degli adempimenti derivanti dalla direttiva sopra richiamata e dalle norme attuative, è emersa l'esigenza di procedere con un'attività di verifica strutturata dell'attuale livello di conformità dell'organizzazione alla normativa e, successivamente, con la fase di adeguamento;
- ✓ Considerato che è necessario primariamente verificare la presenza nell'organico dell'Università di un/una dipendente in possesso dell'adeguata esperienza nel campo della sicurezza informatica e di competenze in materia di nuove norme europee sulla Cybersicurezza, funzionali allo svolgimento della suddetta attività di verifica e di supporto dell'organizzazione in fase di adeguamento;

- ✓ Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE;
- ✓ Considerato che l'Università degli Studi di Catania, in qualità di titolare del trattamento dei dati personali raccolti per la gestione della presente procedura, tratta i dati raccolti in modo lecito, corretto e trasparente nei confronti dell'interessato, oltre che nel rispetto dei principi, delle condizioni e più in generale delle disposizioni del Regolamento (UE) 2016/679;

è avviata

una ricognizione interna *riservata* al personale *docente*, *dirigente* e *tecnico-amministrativo* dell'Ateneo con rapporto di lavoro a tempo *pieno* e *indeterminato* per individuare dipendenti con adeguata competenza ed esperienza professionale nel campo della sicurezza informatica e del contesto normativo europeo e nazionale sulla cybersicurezza, per attività di supporto specialistico all'Area dei Sistemi Informativi per l'adeguamento alla direttiva NIS2.

Il/la dipendente, in particolare, **potrà essere chiamato/a** ad espletare le seguenti **attività**:

1) **Analisi:**

   assessment strutturato del sistema informativo dell'organizzazione al fine di:

   - verificare la conformità ai requisiti previsti dalla Direttiva NIS2 e dal D.Lgs. 138/2024;
   - valutare l'adozione delle misure di base di sicurezza indicate dalla Determinazione ACN n. 164179/2025 per i soggetti importanti;
   - individuare i *gap* di conformità e definire un piano di adeguamento.

   L'attività di assessment è finalizzata a produrre:

   - un documento di *gap analysis*, ovvero il risultato di un'attività di valutazione sistematica volta a identificare le discrepanze tra lo stato attuale dell'organizzazione e i requisiti tecnici e organizzativi previsti dalla normativa che fornisca una visione chiara dei punti di non conformità e delle aree prioritarie di intervento. Si dovrà procedere all'identificazione dei *gap*, fornendo evidenza delle non conformità, delle carenze tecniche e organizzative e delle aree di rischio, alla classificazione e prioritizzazione dei *gap* e all'analisi del rischio associato;
   - un piano di *remediation*, ovvero un documento operativo che definisca le azioni correttive e migliorative necessarie per colmare i *gap* identificati nella fase di analisi e per orientare l'organizzazione nel percorso di adeguamento normativo e rafforzamento della postura di sicurezza. Dovranno essere indicate le azioni correttive, priorità e tempistiche, responsabilità, risorse necessarie e metriche di verifica.

2) **Adeguamento:**
implementazione delle misure di sicurezza di base per i soggetti importanti di cui alla Determinazione ACN n. 164179/2025, con particolare riferimento ai requisiti organizzativi, alla luce delle risultanze emerse nella precedente fase di analisi.

I principali ambiti di intervento riguarderanno:

- il processo di gestione degli incidenti e notifica al CSIRT (da implementare entro gennaio 2026);
- requisiti attinenti alla governance e all'organizzazione;
- sicurezza della supply chain;
- politiche di analisi e gestione dei rischi di cybersicurezza;
- continuità operativa e gestione delle crisi cyber;
- politiche di sicurezza nello sviluppo e gestione dei sistemi informativi.

Il/la dipendente dev'essere dotato/a di documentate competenze ed esperienze professionali attinenti alle attività descritte

Considerate le scadenze previste dalla normativa e la complessità degli adempimenti, è richiesta una disponibilità immediata e a tempo pieno ad impegnarsi sulle attività previste.

Il personale che sia in possesso delle competenze e delle esperienze professionali richieste potrà manifestare il proprio interesse inviando, **entro** venerdì **31 ottobre 2025, ore 12:00** all'indirizzo di posta elettronica *risorse.umane@unict.it*, il modello allegato, compilato e corredato di *curriculum*.

L'Amministrazione si riserva la facoltà di svolgere un ***colloquio***.

Le manifestazioni di interesse saranno valutate dalla direzione generale con il supporto del gruppo di coordinamento "*Team NIS 2*", tenendo conto anche delle motivazioni professionali e personali.

Il presente avviso è pubblicato all'Albo on-line dell'Ateneo, accessibile sul sito internet http://www.unict.it, ed è, altresì, disponibile sullo stesso sito alla sezione "Bandi, Gare e Concorsi".

Catania, 24.10.2025

Il Direttore generale
Dott. Rosario Corrado Spinella

Rosario Corrado Spinella
Università di Catania
Direttore generale
24.10.2025 10:01:38
GMT+02:00