Avviso di ricerca e selezione di personale

Data di pubblicazione dell'Avviso su web: 08/05/2025

Data di scadenza dell'Avviso: 29/05/2025

La **Fondazione Ugo Bordoni** (FUB), Istituzione di Alta Cultura e Ricerca soggetta alla vigilanza del Ministero delle Imprese e del Made in Italy riconosciuta dalla Legge 3/2003, nonché del decreto-legge 22 aprile 2023, n. 44, convertito con modificazioni dalla legge 21 giugno 2023, n. 74, ricerca la seguente posizione da inserire nell'**AREA Cloud e Dati** - Ambito: Cloud e sicurezza

ATTIVITÀ

Sono aperte **n. 4 posizioni per le attività che la FUB svolge nel contesto Cloud e Dati,** con riferimento alla collaborazione istituita in forma convenzionale tra FUB e MIMIT sui temi legati alla direttiva (UE) 2022/2555 (nota come NIS2). Il MiMIT è Autorità settoriale competente in materia di resilienza fisica delle reti di comunicazione elettronica ai sensi dell'art. 5 dello schema di decreto legislativo del 4 settembre 2024, n. 134 emanato in attuazione della citata direttiva e si rapporta con ACN che è l'autorità nazionale.

Le principali attività che i candidati andranno a svolgere sono di seguito elencate.

Supporto al MIMIT nell'ambito del regime convenzionale con la FUB per le seguenti attività:

1. **identificazione dei soggetti essenziali e importanti:**
    a. definizione e aggiornamento dell'elenco delle entità che rientrano nelle categorie di **soggetti essenziali** e **importanti**, ovvero aziende e organizzazioni che devono rispettare obblighi di sicurezza e segnalazione degli incidenti;
2. **vigilanza e controllo:**
    a. monitoraggio del rispetto degli obblighi di sicurezza e gestione del rischio da parte dei soggetti regolamentati;
    b. esecuzione di ispezioni, audit e valutazioni di conformità;
3. **definizione degli standard di sicurezza:**
    a. elaborazione di linee guida e regolamenti tecnici per la sicurezza delle reti e dei sistemi informativi;
    b. collaborazione con altre autorità nazionali ed europee per uniformare le misure di sicurezza;
4. **misure correttive:**
    a. applicazione di sanzioni amministrative in caso di violazioni della normativa;
    b. adozione di provvedimenti per la mitigazione dei rischi in situazioni di emergenza;
5. **promozione della cooperazione nazionale e internazionale:**

   a. collaborazione con enti europei come **l'ENISA** (Agenzia dell'Unione Europea per la Cybersecurity);
   b. coordinamento con altre autorità nazionali di cybersicurezza per la condivisione di informazioni e strategie;
6. **sensibilizzazione e formazione:**
   a. organizzazione di programmi di formazione per le aziende e gli enti regolamentati;
   b. promozione della cultura della cybersicurezza nel settore pubblico e privato.

REQUISITI e COMPETENZE

I requisiti minimi di cui i candidati dovranno essere in possesso sono un diploma di tecnico con almeno 5 anni di esperienza lavorativa, oppure una laurea di primo livello, con almeno 2 anni di esperienza lavorativa, conseguita in una delle seguenti classi STEM (Science, Technology, Engineering, Mathematics):

- ingegneria dell'informazione (L-08);
- scienze e tecnologie informatiche (L-31);
- matematica (L-35);
- fisica (L-30).

I candidati dovranno essere in possesso di:

- buona conoscenza della lingua inglese parlata e scritta, pari almeno al livello B1;
- fluente padronanza della lingua italiana parlata e scritta pari almeno a livello C1.

Le competenze e conoscenze tecnico-scientifiche richieste per la posizione includono:

- conoscenza dei sistemi operativi (Windows, Linux, ecc.) e delle architetture di rete;
- esperienza nella gestione delle patch e degli aggiornamenti di sistema per correggere le vulnerabilità note;
- conoscenza delle diverse tipologie di minacce informatiche (malware, phishing, ransomware, ecc.) e delle loro modalità di funzionamento;
- conoscenza su temi relativi alla crittografia e sicurezza delle reti (principi della crittografia, le tecniche di sicurezza delle reti, protocolli di comunicazione sicura);
- conoscenza approfondita del cloud computing: servizi cloud (IaaS, PaaS, SaaS), architetture cloud (microservizi, containerizzazione), piattaforme cloud (AWS, Azure, Google Cloud), modelli di deployment (public, hybrid, private);
- esperienza almeno biennale in ambito sviluppo e sicurezza delle infrastrutture cloud anche in progetti di migrazione al cloud;
- conoscenze inerenti le moderne infrastrutture Data Center (compresa normativa ANSI TIA-942) e di architetture per gli applicativi orientati al Cloud Computing;
- conoscenza dei fondamenti di sicurezza informatica e di architetture cloud per la sicurezza informatica;
- conoscenza delle direttive NIS e NIS2 e dei relativi adempimenti;
- conoscenza delle best practice organizzative in tema cloud e di sicurezza informatica (politiche e strategie per l'incident response, la continuità operativa, i meccanismi di gestione delle utenze e delle autenticazioni);

- conoscenza degli standard relativi al cloud e alla sicurezza informatica, con particolare riferimento alla ISO/IEC 27001 e alla resilienza infrastrutturale (ISO/IEC 22301).

Per la valutazione della posizione ricercata sono considerati elementi preferenziali:

- laurea magistrale conseguita in una delle seguenti classi STEM (Science, Technology, Engineering, Mathematics):
  - ingegneria dell'informazione (L-08);
  - scienze e tecnologie informatiche (L-31);
  - matematica (L-35);
  - fisica (L-30);
- conoscenza delle normative sulla protezione dei dati personali (GDPR) e della loro applicazione nel contesto della sicurezza informatica anche in contesti di audit IT;
- certificazioni in ambito cloud (es. CCSP, CSA CCSK/CCAH);
- esperienza con il framework Cloud Controls Matrix (CCM);
- esperienza con servizi, infrastrutture e ambienti cloud-native;
- esperienza nella ricerca di minacce e nell'identificazione di configurazioni errate;
- esperienza in Python, Golang e shell scripting;
- esperienza nell'analisi di dati su larga scala;
- familiarità con gli strumenti di automazione e orchestrazione del cloud per l'ottimizzazione dei processi di sicurezza;
- esperienza nell'analisi e nel reverse engineering di malware;
- tesi di laurea triennale e/o magistrale/specialistica in ambito Cyber Security e/o cloud;
- master universitario di I e/o II livello in ambito Cyber Security e/o cloud;
- certificazioni di competenza in ambito Cyber Security emesse da aziende leader del settore o enti internazionali di riferimento;
- esperienza in test di sicurezza per identificare le debolezze dei sistemi;
- partecipazione a gruppi di lavoro in contesti europei in ambito cyber security e cloud;
- conoscenza di strumenti per test di unità, test funzionali e test di carico.

CAPACITÀ ED ATTITUDINI INDIVIDUALI

Completano il profilo:

- attitudine al lavoro in gruppo;
- capacità di *problem solving* e orientamento al risultato;
- chiarezza nella scrittura di documentazione tecnica;
- capacità relazionali.

INQUADRAMENTO

Le figure saranno inserite all'interno dell'organizzazione con contratto full-time a tempo determinato con un livello di inquadramento nella 5° categoria come previsto dal C.C.N.L. Confapi e dal contratto integrativo della FUB.
Il contratto avrà durata pari a 12 mesi a partire dalla data di assunzione, con possibilità di rinnovo fino ad un massimo di ulteriori 12 mesi.

SEDE

Roma

Le candidature devono essere inviate all'indirizzo mail: ricercapersonale@fub.it entro e non oltre il **29 maggio 2025**, complete di:

- *curriculum vitae* (CV) in formato PDF. Il CV dovrà essere redatto in lingua italiana secondo lo standard del formato europeo, con espresso consenso al trattamento dei dati personali per le finalità connesse al presente avviso, ai sensi del D.Lgs. 196/2003 e s.m.i., e dichiarazione di veridicità effettuata ai sensi e per gli effetti del DPR 445/2000. Nel CV devono essere evidenti i requisiti formativi e professionali richiesti;
- certificato di titolo di studio comprensivo dell'elenco degli esami con relativa votazione o, in alternativa, dichiarazione sostitutiva contenente l'elenco degli esami con relativa votazione;
- in caso di titoli di studio conseguiti all'estero deve essere allegata al CV la dichiarazione di equipollenza rilasciata dalla competente autorità.

La ricerca e selezione del personale della Fondazione è rivolta a candidati di entrambi i sessi (D.Lgs. ti. 198/2006 e s.m.i.). Le caratteristiche delle attività sono compatibili con qualsiasi genere, età e condizione fisica (salvo, per quest'ultima, il necessario accertamento successivo ai fini della verifica dell'idoneità per l'effettivo espletamento delle mansioni). La selezione del personale della Fondazione avviene nel rispetto della normativa di riferimento e a garanzia dei principi di trasparenza, non discriminazione e parità di trattamento

I candidati che dimostrino di essere in possesso dei requisiti richiesti saranno chiamati a svolgere uno o più colloqui selettivi, volti a valutare il grado di competenza ed esperienza maturata, secondo quanto indicato nella Tabella criteri di valutazione e punteggi.

FUB
Fondazione Ugo Bordoni
Ricerca, Innovazione, Strategie

Tabella criteri di valutazione e punteggi

Requisito	Criterio di Valutazione	punteggio
Voto di laurea di primo livello	Voto di laurea	90 <= Voto < 105: 1 punto 106 <= Voto < 108: 2 punti Voto>= 109: 3 punti
Laurea di secondo livello o titolo equivalente	SI/NO	6
Per ciascuna competenza ed elemento preferenziale	Valutazione quantitativa	Da 0 a 3 punti per competenza fino ad un massimo di 78
Capacità attitudinali ed individuali	Valutazione qualitativa	Da 0 a 5