

Roma, 29/09/2022

Avviso di ricerca e selezione di personale

La **Fondazione Ugo Bordoni (FUB)**, Istituzione di Alta Cultura e Ricerca soggetta alla vigilanza del Ministero dello Sviluppo Economico riconosciuta dalla Legge 3/2003, è alla ricerca di **1 laureato** di secondo livello da inserire con il ruolo di **ricercatore** su progetti riguardanti la **cybersicurezza**.

Per la figura sopra indicata è previsto un contratto full-time con un inquadramento nel C.C.N.L. Confapi ad un livello commisurato all'esperienza lavorativa maturata nel settore oggetto della selezione. Il contratto prevede inoltre l'applicazione del contratto integrativo FUB.

La sede di lavoro è Roma.

Le candidature devono essere inviate all'indirizzo selezioni.personale@fub.it entro e non oltre il **28/10/2022**, 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 laurea Magistrale 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 avviene nel rispetto della normativa di riferimento e a garanzia dei principi di trasparenza, non discriminazione e parità di trattamento, secondo criteri e modalità di reclutamento approvati con apposito regolamento consultabile sul sito Internet della FUB.

I candidati che dimostrino di essere in possesso dei requisiti richiesti, come indicato nella *Tabella requisiti e titoli*, 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*.

Tabella requisiti e titoli

Figura professionale	Ricercatore di Cybersicurezza
Requisiti di ammissibilità	<ul style="list-style-type: none"> - Laurea Magistrale/Specialistica in Ingegneria Informatica o in Informatica o specifica dell'ambito Cyber Security o equipollenti con voto non inferiore a 105/110.
Titoli Preferenziali	<ul style="list-style-type: none"> - dottorato di ricerca in ambito Cyber security - master universitario di I e/o II livello in ambito Cyber security - certificazioni di competenza attinenti al profilo ricercato emesse da aziende leader del settore o enti internazionali di riferimento
Competenze ed esperienze	<ul style="list-style-type: none"> - conoscenza della lingua inglese con livello almeno B2 (il curriculum deve riportare l'autovalutazione della competenza linguistica secondo il quadro comune europeo per le lingue (QCER)) <p style="text-align: center;">COMPETENZE TECNICHE</p> <ol style="list-style-type: none"> 1. sviluppo software con utilizzazione di linguaggi di programmazione e tool di sviluppo quali C, Java, Python, Golang, GIT, Eclipse; 2. metodologie e strumenti di Vulnerability Assessment e Penetration Testing a livello di componenti e sistemi ICT; 3. reverse engineering di software e firmware; 4. tecnologie blockchain; 5. sicurezza di dispositivi in ambito IoT e/o in ambito automazione e controllo industriale (IACS); 6. sicurezza in ambito cloud; 7. strumenti automatizzati per la rilevazione e il contrasto di attacchi; 8. sicurezza di database SQL e No-SQL; 9. strumenti per l'esecuzione di test funzionali e test di carico; 10. sicurezza di sistemi operativi e applicazioni su dispositivi mobili; 11. sicurezza dell'hardware (vulnerabilità, tipi di attacchi, contromisure, piattaforme hardware sicure come TPM o similari). 12. strumenti di supporto allo sviluppo collaborativo (es. Maven, Git); 13. tecnologie e framework open-source per Web Application (es. React, Apache, Tomcat, Django); 14. database SQL (es. MySQL, Postgres); 15. strumenti per test di unità, test funzionali e test di carico;

	<p>16. progettazione e design di Web Application;</p> <p>17. tecnologie e metodologie per Big Data, Data Mining e Machine Learning;</p> <p>18. database No-SQL (es. MongoDB, Redis);</p> <p>19. tecnologie per la creazione di servizi cloud-native basati su container o micro-servizi;</p> <p>20. strumenti per l'analisi dei processi.</p> <p>21. valutazione e certificazione della sicurezza dei sistemi ICT;</p> <p>22. studio e applicazioni nell'ambito della sicurezza delle infrastrutture critiche, con particolare riferimento alle componenti hardware di reti TLC, dispositivi IoT e dispositivi per l'automazione e il controllo industriale (IACS).</p> <p>23. conoscenza del quadro normativo nazionale, europeo ed internazionale in merito alle politiche di sicurezza cibernetica</p> <p>24. partecipazione a gruppi di lavoro nazionali ed internazionali su tematiche relative a standard di sicurezza cibernetica</p> <p>25. collaborazione con organismi o enti di certificazione della sicurezza informatica</p>
Esperienze in settori preferenziali	- esperienze lavorative attinenti al profilo ricercato

Tabella criteri di valutazione e punteggi

Requisito	Criterio di Valutazione	punteggio
Dottorato di ricerca	SI/NO	5
Master	SI/NO	2 per master 1° livello, 3 per master 2° livello
Certificazioni	SI/NO	1 per ogni certificazione riconosciuta
Conoscenza della lingua inglese	corrispondenza con i livelli del QCER	1 (B2), 2 (C1), 3 (C2)
Per ciascuna competenza	Valutazione qualitativa	da 0 a 3
Esperienza pregressa	1 punto per ogni anno di esperienza (fino ad un massimo di 10)	da 0 a 10

Esperienza pregressa nella conduzione di progetti	1 punto per ogni anno di esperienza dimostrata di conduzione dei progetti (fino a un massimo di 5)	da 0 a 5