Roma, 11/03/2021

Avviso di ricerca e selezione di personale

La **Fondazione Ugo Bordoni** (FUB), riconosciuta dalla Legge 3/2003 come Istituzione di Alta Cultura e Ricerca soggetta alla vigilanza del Ministero dello Sviluppo Economico, nell'ambito delle attività di supporto alla Pubblica Amministrazione nel campo dell'ICT è alla ricerca di:

- **un laureato di secondo livello in Informatica o Ingegneria informatica con formazione e/o esperienze lavorative orientate alla cyber security**

da inserire su progetti di sviluppo software finalizzati alla digitalizzazione e innovazione della Pubblica amministrazione.

In allegato al presente avviso è possibile trovare una scheda descrittiva per il profilo sopra indicato.

Per la figura sopra indicata è previsto:

- in caso di esperienza lavorativa assente o non sufficientemente significativa per il profilo cercato, un contratto full-time a tempo determinato successivamente trasformabile a tempo indeterminato e caratterizzato da un inquadramento al livello 6 del C.C.N.L. Confapi con applicazione del contratto integrativo FUB; la retribuzione annua lorda è di circa 37.000 euro a cui si aggiungono, da contratto integrativo, buoni pasto giornalieri e un'assicurazione sanitaria integrativa con un'ampia copertura.
- In caso di esperienza lavorativa significativa per il profilo cercato, la Fondazione potrà valutare un diverso inquadramento contrattuale o tipologia di contratto commisurato all'esperienza effettivamente maturata nel settore oggetto della selezione; il contratto prevede inoltre l'applicazione del contratto integrativo FUB.

Per le figure ricercate nel presente avviso la sede di lavoro è **Roma**.

Tutte le candidature devono essere inviate all'indirizzo selezioni.personale@fub.it entro e non oltre il **06/04/2021**, 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 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.

Nel caso dovessero emergere, entro i prossimi 2 anni, ulteriori necessità di ampliamento di organico delle stesse figure oggetto del presente avviso, la Fondazione potrà attingere alle graduatorie stilate per questa selezione.

Figura professionale	**Laureato di secondo livello in Informatica o Ingegneria informatica con formazione e/o esperienze lavorative orientate alla cyber security**
Numero di posizioni aperte	1 posizione aperta
Requisiti minimi	• Laurea Magistrale/Specialistica in Ingegneria Informatica o in Informatica o specifica dell'ambito Cyber Security o equipollenti con voto non inferiore a 105/110
Breve Descrizione	La figura ricercata sarà inserita all'interno di progetti di Cyber Security nell'ambito delle attività che la FUB svolge a supporto della Pubblica Amministrazione. In particolare, la figura ricercata dovrà essere in possesso di competenze informatiche utili per contribuire ad attività quali: • supporto su tematiche di cyber security nell'ambito di progetti strategici e di digitalizzazione della Pubblica Amministrazione; • studio e applicazioni nell'ambito della valutazione e certificazione della sicurezza di componenti e sistemi ICT; • studio e applicazioni nell'ambito della sicurezza delle infrastrutture critiche, con particolare riferimento a IoT e componenti per l'automazione e il controllo industriale (IACS).
Inquadramento contrattuale	In caso di esperienza lavorativa assente o non sufficientemente significativa per il profilo cercato, un contratto full-time a tempo determinato successivamente trasformabile a tempo indeterminato e caratterizzato da un inquadramento al livello 6 del C.C.N.L. Confapi con applicazione del contratto integrativo FUB. In caso di esperienza lavorativa significativa per il profilo cercato, la Fondazione potrà valutare un diverso inquadramento contrattuale o tipologia di contratto commisurato all'esperienza effettivamente maturata nel settore oggetto della selezione; il contratto prevede inoltre l'applicazione del contratto integrativo FUB.
Lingue	• ottima conoscenza della lingua italiana. • buona conoscenza della lingua inglese.

Competenze ed esperienze minime	Per la posizione ricercata sono considerate necessarie:
	- conoscenza di base nel campo della Cyber Security;
	- conoscenza ed esperienza pratica relativamente a:
	  ○ almeno un linguaggio tra C++, Java, Python e JavaScript;
	  ○ sicurezza di sistemi operativi di tipo windows e linux-like.

Titoli, competenze e esperienze preferenziali	Per la valutazione della posizione ricercata sono considerati elementi preferenziali: - dottorato di ricerca in ambito Cyber Security; - tesi di laurea magistrale/specialistica in ambito Cyber Security; - tesi di laurea triennale in ambito Cyber Security; - master universitario di I e/o II livello in ambito Cyber Security;

	- certificazioni di competenza in ambito Cyber Security emesse da aziende leader del settore o enti internazionali di riferimento; - esperienza lavorativa in ambito Cyber Security, specialmente se relativa alla sicurezza e/o certificazione di componenti e sistemi ICT; - conoscenze ed esperienze pratiche relativamente a: o strumenti per l'individuazione in componenti, sistemi ICT e reti di potenziali vulnerabilità; o analisi e strumenti per verificare, con l'ausilio di penetration testing, la sfruttabilità di vulnerabilità potenziali sotto ipotesi predefinite caratterizzanti gli attacchi ritenuti possibili; o linguaggi di amministrazione dei sistemi operativi (Bash, VBScript e Jscript); o sviluppo software con utilizzazione di linguaggi di programmazione e tool di sviluppo quali C, Java, Python, Golang, GIT, Maven, Eclipse; o almeno un linguaggio di scripting tra Ruby, Perl e Python; o sicurezza dei principali servizi di rete (WEB, MAIL, VPN, DNS, SSH, RDP, NTP, SNMP); o protocolli di comunicazione basati su IP o protocolli di comunicazione al livello fisico e collegamento (es. IEEE 802.3, IEEE 802.11, IEEE 802.1X) o analisi di protocollo o firewall; o sicurezza dei dispositivi di rete (es. router e switch) con sistemi operativi Cisco IOS e/o Junos OS; o capacità di ricerca delle informazioni ottenibili dal deep web attraverso l'utilizzo dello strumento Tor e simili; o gestione infrastrutture a chiave pubblica; o strumenti per la prevenzione, l'individuazione e il contrasto delle intrusioni o analisi (statica e dinamica) dei malware; o analisi OSINT; o reverse engineering di software e firmware; o tecnologie blockchain; o sicurezza di dispositivi in ambito IoT e/o in ambito automazione e controllo industriale (IACS); o sicurezza in ambito cloud; o sicurezza di database SQL e No-SQL; o strumenti per l'esecuzione di test funzionali e test di carico; o sicurezza di sistemi operativi e applicazioni su dispositivi mobili; o sicurezza di sistemi operativi e applicazioni in ambienti mac OS o BSD. E' inoltre gradita la conoscenza ed esperienza pratica di: - tecnologie e framework open-source per Web Application (es. React, Apache, Tomcat, Django); - database SQL (es. MySQL, Postgres); - strumenti per test di unità, test funzionali e test di carico; - progettazione e design di Web Application; - tecnologie e metodologie per Big Data, Data Mining e Machine Learning; - database No-SQL (es. MongoDB, Redis); - tecnologie per la creazione di servizi cloud-native basati su container o micro-servizi; - strumenti per l'analisi dei processi.