ACN.AOO_ACN-US.REGISTRO
UNICO.0004064.26-01-2023.I

AVVISO DI SELEZIONE PER UN ADVISOR PER LE FUNZIONI DI DEPLOYABLE DIGITAL FORENSIC AND INCIDENT RESPONSE TEAM MANAGER

Entrare a far parte dell'Agenzia per la Cybersicurezza Nazionale significa mettere le proprie competenze al servizio dell'interesse generale partecipando a una missione che è vitale per il mantenimento della prosperità economica e della sicurezza del Paese all'interno del processo di trasformazione digitale. Noi lavoriamo dietro le quinte per aumentare la resilienza dei sistemi informatici, delle reti e dei servizi essenziali del Paese, collaborando e creando sinergie con la Pubblica Amministrazione, il settore privato e la ricerca nazionale.

Per lo svolgimento di **attività assolutamente necessarie all'operatività dell'Agenzia preordinate alle funzioni di tutela della sicurezza nazionale nello spazio cibernetico** è indetta una selezione per la costituzione di un rapporto di lavoro mediante la stipula di un contratto di diritto privato a tempo determinato. La prestazione lavorativa ha carattere di esclusività. La risorsa potrà anche essere impiegata su progetti ed attività connessi con l'investimento 1.5 del PNRR.

La figura ricercata sarà impiegata nel Servizio "Operazioni" deputato alla preparazione, prevenzione, gestione e risposta a eventi cibernetici di natura critica anche attraverso il CSIRT Italia, responsabile del monitoraggio e dell'analisi dei rischi delle minacce cyber a livello nazionale, delle emissioni di preallarme, allerte, annunci e della divulgazione di rilevanti informazioni agli operatori interessati.

In relazione alle esigenze da soddisfare, alle funzioni da attribuire e alle caratteristiche richieste, il candidato vincitore potrà svolgere funzioni e mansioni analoghe a quelle assegnate al personale dell'Agenzia inquadrato nel segmento di "**Consigliere**". Nell'ambito del contratto saranno definiti il trattamento giuridico ed economico e, in particolare, verranno indicate le disposizioni del regolamento del personale dell'Agenzia.

PROFILO RICERCATO	La ricerca è volta all'individuazione di un professionista in possesso di alta e particolare specializzazione nel campo della strutturazione, gestione e formazione continua di team, impiegati anche a contatto, per la risposta agli incidenti informatici, con particolare riferimento alle attività di ripristino dei sistemi colpiti e alla gestione delle successive fasi di *hardening* e miglioramento della postura generale dei soggetti.
DURATA	4 anni, rinnovabile fino ad un massimo di 8 anni.
SEDE DI LAVORO	Roma.
CANDIDATURE	Le candidature devono essere inoltrate utilizzando esclusivamente l'applicazione disponibile nella sezione "lavorare con noi" del sito dell'Agenzia www.acn.gov.it entro e non oltre le ore 18.00 del **14 febbraio 2023.** A tal fine il candidato dovrà preventivamente registrarsi indicando obbligatoriamente un indirizzo di posta elettronica certificata (PEC). Alla candidatura andrà allegato, **a pena di esclusione**, un CV in formato europeo, non superiore alle 5 pagine. **Non sono ammesse altre forme di partecipazione alla selezione**. Tutte le comunicazione inerenti la selezione saranno inviate all'indirizzo PEC indicato.
LETTERA DI REFERENZE	Le candidature devono essere supportate, **a pena di esclusione**, da una lettera di referenze rilasciata da un esponente di vertice di enti/organismi/società di rilievo nazionale e/o internazionale ovvero da docenti universitari nazionali o internazionali operanti nel settore oggetto della presente selezione. A tal fine i candidati nel modello di domanda devono indicare il nominativo del referee che dovrà inviare la lettera di referenze redatta in lingua italiana, francese, inglese o spagnola su carta intestata e debitamente firmata, entro il termine del **21 febbraio 2023** alla casella di posta elettronica referee@acn.gov.it.

N.B. Le candidature non supportate da una lettera di referenze **inviata direttamente dal referee** non verranno prese in considerazione. Nel caso in cui nella candidatura sia indicato più di un referee e pervengano più lettere di referenze, verrà presa in considerazione la prima lettera nell'ordine di priorità indicato nella domanda.

JOB DESCRIPTION

La figura ricercata sarà inserita nel Servizio "Operazioni", che ha il mandato di contribuire alla preparazione, prevenzione, gestione e risposta a eventi cibernetici per la *constituency* nazionale. In particolare, opererà all'interno della Divisione CSIRT ITALIA, che, tra le altre, assicura le funzioni di gestione di tutte le fasi di un incidente informatico, tra cui: la ricezione delle notifiche e segnalazioni; l'acquisizione, la validazione, la classificazione, il triage, la risposta di I e II livello (mitigazione e ripristino), il supporto alla definizione dei piani di rientro, la valutazione dell'impatto nazionale degli incidenti in corso e delle nuove vulnerabilità; il monitoraggio delle informazioni relative a nuove vulnerabilità, notizie di campagne malevole da fonti aperte e commerciali, l'arricchimento della *knowledge base*. In tale ambito potrà:

- curare l'avvio delle funzioni dei TEAM DFIR, anche in termini di personale, processi e requisiti delle capacità da sviluppare;
- gestire l'impiego dei TEAM DFIR a disposizione in base alla valutazione delle priorità;
- concordare e comunicare le strategie di correzione e i flussi di lavoro alle parti interessate da incidente informatico, tra cui personale tecnico, leadership esecutiva e terze parti in generale;
- coordinare e gestire le attività di analisi, contenimento e "*remediation*"dei TEAM DDFIR in caso di incidente e durante le normali attività d'istituto (formazione, processi, esercitazioni, *lesson learned*);
- coordinare le funzioni di risposta e governa i sottoprogetti per gli interventi su larga scala con funzioni di assegnazione delle risorse;
- esaminare i dati e assistere i team di risposta nell'implementazione di controlli di protezione avanzata in diverse tecnologie, tra cui *Active Directory*;
- coordinare le funzioni di risposta agli incidenti espletate anche da remoto in collaborazione con i Team di analisi di secondo livello;
- coordinare l'individuazione di potenziali impegni, partecipare alle riunioni di avvio e seguire l'andamento dei lavori fino alla correzione completa;
- coordinare il *mentoring* e la crescita del personale meno esperto.

REQUISITI CULTURALI E DI SPECIALIZZAZIONE PROFESSIONALE

1) Percorso di studi

Laurea magistrale ovvero titolo di studio universitario equivalente anche conseguito all'estero nell'ambito dell'Ingegneria Informatica, Ingegneria delle Telecomunicazioni, Scienze Informatiche e dell'Informazione, Matematica o Fisica.

2) Esperienza professionale

Esperienza professionale documentabile, di almeno 15 anni nel settore dell'*Information Tecnology*, di cui almeno 8 maturata nel campo della risposta agli incidenti informatici presso società/operatori privati, enti, organismi, preferibilmente anche in contesti internazionali. In tali posizioni deve aver maturato le seguenti esperienze:

a. responsabilità della gestione operativa di *Team di Incident Response* in un numero elevato di incidenti cyber sia su infrastrutture on-premise sia su infrastrutture *cloud*;

b. responsabilità della creazione e mantenimento di procedure e standard per l'esecuzione degli interventi in caso di incidenti informatici;

c. esperienza nella formazione tecnica del personale afferente ai team di risposta;

d. *design* e *delivery* di soluzioni di sicurezza e gestione dell'identità;

e. gestione dei rapporti con figure executive e tecniche per la realizzazione di progetti complessi anche durante la gestione di incidenti informatici;

f. supporto ai soggetti della *constituency* nella definizione di attività di *hardening* sia in attività post-incidente sia in attività preventive;

g. gestione dei rapporti con stakeholder esterni all'organizzazione.

3) Lettera di referenze

Le candidature devono essere supportate da una lettera di referenze, rilasciata dal responsabile o da un esponente di vertice di enti/organismi/società di rilievo nazionale e/o internazionale ovvero da docenti universitari nazionali o internazionali operanti nel settore oggetto della presente selezione. Non saranno prese in considerazione le candidature non supportate da una lettera di referenze **inviata direttamente dal referee** secondo le modalità previste nella sezione "candidature".

4) Conoscenza avanzata della lingua inglese (minimo B2)

5) Cittadinanza italiana

6) Non aver tenuto comportamenti incompatibili con i compiti da svolgere in Agenzia ovvero con le istituzioni democratiche o che non diano sicuro affidamento di scrupolosa fedeltà alla Costituzione repubblicana e alle ragioni di sicurezza dello Stato.

CONOSCENZE E COMPETENZE

a. Capacità di gestire *Team di digital forensic and incident response* (DFIR), in tutte le fasi di *preparation, detection & analysis, containment eradication & recovery, post-incident activity*;
b. capacità di presentare, revisionare e modificare i risultati delle attività di analisi e risposta ad incidenti informatici;
c. conoscenza approfondita dei più comuni sistemi di *Identity Management*;
d. conoscenza approfondita dei modelli utilizzati per la definizione di architetture di sistemi complessi in sicurezza (es. *Zero Trust, Just-in-time/Just-enough, network and duty segregation, Administrative access protection*);
e. spiccate capacità di *project management*;
f. capacità di produrre elaborati analitici efficaci, anche in lingua inglese;
g. capacità di presentare, revisionare e modificare i risultati delle attività di analisi e monitoraggio;
h. spiccate capacità di comunicazione scritta e verbale;
i. conoscenza dell'architettura normativa in materia di cybersicurezza nazionale.

ULTERIORI REQUISITI, CONOSCENZE E COMPETENZE

Ulteriori titoli di studio, certificazioni e pubblicazioni scientifiche in ambiti afferenti alla cyber security, la gestione di incidenti informatici, il *design* e l'*operations* di sistemi IT complessi.

PROCESSO DI SELEZIONE

Le candidature sono valutate da:
1. un Panel nominato con provvedimento del Direttore generale e composto da dipendenti dell'Agenzia ed, eventualmente, da esponenti del mondo accademico;
2. un Comitato composto dal Direttore generale, dal Vice Direttore generale e da un dirigente del Servizio Risorse umane e strumentali.

Il processo di selezione si articola nelle seguenti fasi e secondo i seguenti criteri di valutazione:

1) Esame cartolare fino a 35 punti:
a) Esperienza lavorativa documentabile (*fino a 15 punti*);
b) percorso di studi (Titolo di studio universitario, master, PhD., ulteriori titoli di studio e pubblicazioni - *fino a 7 punti*);
c) lingue straniere (*fino a 5 punti*);
d) articolazione del complessivo percorso professionale (*fino a 8 punti*).

Superano questa fase i candidati che conseguono nell'esame cartolare *almeno 25 punti*.

2) Intervista da parte del Panel fino a 35 punti
I candidati che superano l'esame cartolare verranno convocati per un'intervista - anche in modalità remota - finalizzato all'accertamento delle competenze professionali richieste nonché della padronanza della lingua inglese (ed eventualmente della buona conoscenza dell'ulteriore lingua). Nel corso dell'intervista, il candidato sarà chiamato a discutere con il Panel gli aspetti, attuali e prospettici, della posizione da ricoprire e il contributo che intende apportare all'Agenzia, anche dal punto di vista gestionale.

Superano questa fase i candidati che conseguono nell'intervista *almeno 20 punti*.

3) Selezione del profilo professionale più rispondente
I candidati selezionati a seguito dell'intervista vengono convocati per un colloquio dal Comitato, composto dal Direttore generale, il Vice Direttore generale e un Dirigente del Servizio Risorse Umane e strumentali dell'Agenzia, per discutere degli aspetti professionali della posizione da ricoprire ovvero delle funzioni da svolgere nonché per valutare il contributo, in termini di expertise professionale, che l'interessato intende apportare all'Agenzia, anche dal punto di vista gestionale. Nel corso del colloquio saranno inoltre discussi gli aspetti contrattuali del rapporto di lavoro che li potrebbe legare all'Agenzia. Il trattamento economico sarà determinato sulla base della eventuale posizione organizzativa da ricoprire, delle funzioni, degli incarichi e delle mansioni che sarà chiamato a svolgere e tenuto conto dei requisiti professionali posseduti e delle funzioni esercitate presso il precedente datore di lavoro. Il colloquio sarà valutato con l'attribuzione di un punteggio massimo di **30 punti**. Ai fini dell'assunzione verranno considerati, in ordine di punteggio complessivo, esclusivamente i candidati che abbiano conseguito complessivamente nelle tre fasi almeno **80 punti**.
L'Agenzia si riserva, in ogni caso, di non dar seguito alla stipula del contratto, nonché di utilizzare la graduatoria finale della selezione entro un anno dalla data di approvazione per eventuali ulteriori specifiche esigenze.

La presente selezione è indetta ai sensi dell'art. 12, comma 2, lett. b), del D.L. 14 giugno 2021, n. 82, convertito, con modificazioni, dalla L. 4 agosto 2021, n. 109, dell'art. 91 del Regolamento del Personale dell'Agenzia (d.P.C.M. 9 dicembre 2021, n. 224) e della determina del Direttore generale n. 3838 del 25 gennaio 2023.

L'Agenzia si riserva di verificare, in qualsiasi momento, l'effettivo possesso dei requisiti previsti dal presente avviso di selezione disponendo l'esclusione dalla selezione ovvero procedendo alla risoluzione del rapporto di lavoro di coloro che risultino sprovvisti di uno o più dei requisiti.

L'Unità organizzativa responsabile del procedimento è il Servizio Risorse umane e strumentali dell'Agenzia. Il responsabile del procedimento è il Capo *pro tempore* di tale Servizio.

I dati forniti dai candidati sono trattati, anche in forma automatizzata, per le finalità di gestione della selezione. Per i candidati che saranno assunti il trattamento proseguirà per le finalità inerenti alla gestione del rapporto di lavoro. Base giuridica del trattamento è pertanto rispettivamente l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato e l'esecuzione di un contratto di cui l'interessato è parte (art. 6.1 b) Reg. (UE) 2016/679, di seguito GDPR).

Titolare del trattamento è l'Agenzia per la Cybersicurezza Nazionale - via di Santa Susanna n. 15, 00184 ROMA (di seguito, ACN).

Il conferimento dei dati richiesti è obbligatorio ai fini della valutazione dei requisiti di partecipazione e di assunzione; in caso di rifiuto a fornire i dati, l'Agenzia non dà corso alla selezione.

Per il trattamento ACN potrà avvalersi di società terze situate sul territorio comunitario, tenute alla riservatezza e legate ad essa da un contratto che garantisca un adeguato livello di sicurezza dei dati ed il rispetto dei requisiti imposti dall'art. 28 del GDPR.

I dati forniti possono essere comunicati ad altre amministrazioni pubbliche situate sul territorio nazionale, a fini di verifica di quanto dichiarato dai candidati o negli altri casi previsti da leggi e regolamenti, le quali li tratteranno in qualità di autonomi titolari del trattamento. Non è previsto il trasferimento di dati all'estero.

I dati relativi alle persone successivamente assunte saranno trattati da ACN per tutta la durata del rapporto di lavoro e per l'ulteriore tempistica richiesta dalla normativa applicabile in materia giuslavoristica, pensionistica e fiscale.

Al soggetto interessato competono il diritto di accesso ai propri dati personali e gli altri diritti riconosciuti dalla normativa applicabile, tra i quali il diritto di ottenere la rettifica o l'integrazione dei dati, la cancellazione, la trasformazione in forma

anonima o il blocco di quelli trattati in violazione di legge nonché il diritto di opporsi in tutto o in parte, per motivi legittimi, al loro trattamento.

ACN ha nominato un Responsabile per la protezione dei dati (DPO). Tali diritti potranno essere fatti valere scrivendo direttamente ad ACN od inoltrando un'email all'indirizzo dpo@acn.gov.it.

Ove infine il soggetto interessato dovesse ritenere lesi i propri diritti, è inoltre possibile rivolgersi direttamente all' autorità di controllo competente per il proprio paese di residenza (in Italia Garante per la protezione dei dati personali - Piazza Venezia n. 11 - Roma - protocollo@gpdp.it) o adire la giurisdizione ordinaria.

IL DIRETTORE GENERALE
Roberto Baldoni