



Agenzia per la Cybersicurezza Nazionale

50 ASSUNZIONI DI LAUREATI PER L'INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

Articolo 1

Requisiti di partecipazione e di assunzione

L'Agenzia per la Cybersicurezza Nazionale (di seguito Agenzia) indice i seguenti concorsi pubblici per l'assunzione a tempo indeterminato di:

- A. 15 Esperti** per le funzioni tecnico/amministrative di **“Certificazione e ispezione” con esperienza nell'applicazione di schemi di certificazione Common Criteria / ITSEC e/o come auditor ISO;**
- B. 10 Esperti** per le funzioni di **“Tecnico hardware e tecnico di telecomunicazioni” con esperienza nello sviluppo hardware (PCB, logiche programmabili, ASIC), in sistemi embedded e/o in ambito reti di telecomunicazioni;**
- C. 15 Esperti** per le funzioni di **“Tecnico software” con esperienza nello sviluppo software e/o nella sicurezza informatica;**
- D. 4 Esperti** per le funzioni di gestione e realizzazione di **“Programmi industriali, tecnologici e di ricerca” con esperienza in programmi di investimento di rilevanza nazionale ed europea nel campo della cyber security;**
- E. 3 Esperti** per le funzioni di **“Tecnico crittografo” con esperienza nell'ambito della crittografia teorica o applicata;**
- F. 3 Esperti** per le funzioni **operative di “Cybersecurity” con conoscenze in ambito della gestione degli incidenti informatici (triage, indicatori di compromissione, best practices di sicurezza informatica), dell'analisi malware, dell'analisi forense e cyber threat intelligence, dell'analisi e valorizzazione di dati e della gestione del rischio cyber.**

I vincitori lavoreranno a Roma. Le persone selezionate nei concorsi di cui alle lettere A, B, C ed E saranno utilizzate prevalentemente per le esigenze di funzionamento del Centro di valutazione e certificazione nazionale (CVCN)¹ dell'Agenzia. Le persone selezionate nel concorso di cui alla lettera D saranno utilizzate prevalentemente per la realizzazione e gestione di programmi industriali, tecnologici e di ricerca di rilevanza nazionale ed europea (PNRR e

¹ Il CVCN è la struttura strategica nell'ambito del perimetro di sicurezza nazionale cibernetica cui è affidato il compito di effettuare la certificazione, qualificazione e valutazione di beni, sistemi e servizi ICT destinati ad essere impiegati su infrastrutture ICT che supportano la fornitura di beni e servizi essenziali o di funzioni essenziali per lo Stato, anche ai fini dell'attività ispettiva e di verifica.



Agenzia per la Cybersicurezza Nazionale

fondi strutturali) e quelle di cui alla lettera F saranno utilizzate prevalentemente per le esigenze del *Computer Security Incident Response Team* (CSIRT) Italia nell'ambito delle attività di monitoraggio e analisi dei rischi e delle minacce cyber a livello nazionale, l'emissione di preallarmi, allerte, annunci e la divulgazione di rilevanti informazioni agli operatori interessati.

Sono richiesti i seguenti requisiti.

1. Laurea magistrale/specialistica, conseguita con un punteggio di almeno 105/110 o votazione equivalente, in una delle seguenti classi:

ingegneria delle telecomunicazioni (30S/LM-27); ingegneria elettronica (32S/LM-29); ingegneria informatica (35S/LM-32); ingegneria dell'automazione (29S/LM-25); informatica (23S/LM-18); sicurezza informatica (LM-66); matematica (45S/LM-40); fisica (20S/LM-17); ingegneria gestionale (34S/LM-31); altra laurea equiparata a uno dei suddetti titoli ai sensi del Decreto Interministeriale 9 luglio 2009

ovvero

diploma di laurea di "vecchio ordinamento", conseguito con un punteggio di almeno 105/110 o votazione equivalente, in una delle seguenti discipline:

ingegneria delle telecomunicazioni; ingegneria elettronica; ingegneria informatica; informatica; scienze dell'informazione; matematica; fisica; ingegneria gestionale; altra laurea a esso equiparata o equipollente per legge.

È consentita la partecipazione ai possessori di **titoli di studio conseguiti all'estero o di titoli esteri conseguiti in Italia** con votazione corrispondente ad almeno 105/110, riconosciuti equivalenti a uno dei titoli sopraindicati ai fini della partecipazione ai pubblici concorsi. **La richiesta di riconoscimento dell'equivalenza deve essere presentata alla Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica, entro la data di svolgimento della prima prova di concorso.**

Per la partecipazione ai concorsi di cui alle lettere A, B, C, D ed E è inoltre richiesta un'esperienza lavorativa, documentabile e successiva alla laurea prevista al punto 1, della durata di almeno 2 anni, maturata in attività di lavoro dipendente o autonomo nel campo espressamente indicato per ciascuna lettera del bando.

2. Cittadinanza italiana.

3. Idoneità fisica alle mansioni.

4. Godimento dei diritti civili e politici.

5. Non aver tenuto comportamenti incompatibili con le funzioni da svolgere nell'Agenzia ovvero con le istituzioni democratiche o che non diano sicuro affidamento di



Agenzia per la Cybersicurezza Nazionale

scrupolosa fedeltà alla Costituzione repubblicana e alle ragioni di sicurezza dello Stato (cfr. art. 8).

Il requisito di cui al punto 1 deve essere posseduto alla data di scadenza stabilita per la presentazione della domanda; l'equivalenza del titolo di studio e gli altri requisiti devono essere posseduti alla data di assunzione.

I requisiti richiesti dal presente bando potranno essere verificati dall'Agenzia in qualsiasi momento, anche successivo allo svolgimento delle prove di concorso e all'eventuale assunzione.

L'Agenzia **dispone l'esclusione dal concorso, non dà seguito all'assunzione o procede alla risoluzione del rapporto d'impiego di coloro che risultino sprovvisti di uno o più dei requisiti previsti dal bando.** Le eventuali difformità riscontrate rispetto a quanto dichiarato o documentato dagli interessati vengono segnalate all'Autorità giudiziaria.

Articolo 2

Domanda di partecipazione e termine per la presentazione

La domanda deve essere presentata **entro il termine perentorio delle ore 16:00 del 25 marzo 2022 (ora italiana)**, utilizzando esclusivamente l'applicazione disponibile sul sito internet della Agenzia www.acn.gov.it. **Non sono ammesse altre forme di presentazione della domanda di partecipazione al concorso.**

La data di presentazione della domanda è attestata dal sistema informatico che, allo scadere del termine di cui al comma 1, non permetterà più l'accesso e l'invio della domanda. Per evitare un'eccessiva concentrazione degli accessi all'applicazione a ridosso della scadenza del termine, si consiglia di presentare la domanda con qualche ora di anticipo, tenuto anche conto del tempo necessario per completare l'*iter* di registrazione propedeutico alla candidatura.

È consentita la partecipazione ad uno solo dei concorsi di cui all'articolo 1. Se un candidato avanza domanda di partecipazione per più di un concorso, l'Agenzia prende in considerazione **l'ultima candidatura presentata in ordine di tempo.** A tal fine, fa fede la data di presentazione della domanda registrata dal sistema informatico.

Non sono tenute in considerazione e comportano quindi l'esclusione dal concorso le candidature dalle quali risulti il **mancato possesso di uno o più requisiti prescritti** per la partecipazione al concorso.

L'Agenzia comunica agli interessati il provvedimento di esclusione.



Agenzia per la Cybersicurezza Nazionale

L'Agenzia non assume responsabilità per il mancato o ritardato recapito di comunicazioni dirette ai candidati che sia da imputare a disguidi postali o telematici, all'indicazione nella domanda *on-line* di un indirizzo errato o incompleto oppure a omessa o tardiva segnalazione da parte del candidato del cambiamento di indirizzo.

I nominativi dei candidati ammessi alla prova scritta vengono resi disponibili, sul sito internet dell'Agenzia www.acn.gov.it, almeno 15 giorni prima della data prevista per la prova.

L'ammissione alle prove avviene con la più ampia riserva in ordine al possesso dei requisiti di partecipazione richiesti dal bando.

Il giorno della prova scritta i candidati dovranno confermare il possesso dei requisiti dichiarati nella domanda di partecipazione sottoscrivendo una specifica dichiarazione, previa esibizione di un documento di identità (cfr. art. 6). Le dichiarazioni rese e sottoscritte hanno valore di autocertificazione ai sensi del decreto del Presidente della Repubblica n. 445/2000 (Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), con ogni conseguenza anche di ordine penale in caso di mendacio e applicazione delle sanzioni previste dall'art. 76 del decreto.

Ogni variazione dei recapiti indicati dal candidato nella domanda per la ricezione delle eventuali comunicazioni relative al concorso deve essere tempestivamente comunicata all'Agenzia, mediante posta elettronica, al seguente indirizzo: recruitment@acn.gov.it. Al medesimo indirizzo possono essere inoltrate eventuali richieste di chiarimento in merito alla procedura concorsuale.

I candidati che hanno necessità, in relazione alla specifica condizione di disabilità, di **strumenti di ausilio e/o di tempi aggiuntivi** per lo svolgimento delle prove (ai sensi dell'art. 20, L. n. 104/1992 e dell'art. 16, comma 1, L. n. 68/1999) dovranno farne richiesta compilando il "Quadro A" dell'applicazione. I medici di cui si avvarrà l'Agenzia valuteranno la richiesta esclusivamente sulla base del nesso causale tra la patologia dichiarata nel "Quadro A" e le modalità di svolgimento di ciascuna prova. Qualora l'Agenzia riscontri, anche successivamente, la non veridicità di quanto dichiarato disporrà l'esclusione dal concorso, non darà seguito all'assunzione o procederà alla risoluzione del rapporto di impiego eventualmente instaurato.

Articolo 3 Preselezione per titoli

Nel caso in cui le domande di partecipazione a ciascun concorso siano più di **600**, l'Agenzia procederà a una **preselezione per titoli** per individuare **600 candidati** da ammettere alla relativa prova scritta (cfr. art. 5). A tal fine, l'Agenzia provvederà alla formazione di **graduatorie preliminari redatte sulla base del punteggio attribuito al titolo di cui al**



Agenzia per la Cybersicurezza Nazionale

punto 1 dell'art. 1, che deve essere posseduto alla data di scadenza stabilita per la presentazione delle domande:

laurea magistrale/specialistica/di "vecchio ordinamento" con voto (o titolo e voto equivalenti):

- | | |
|-------------------------------|---------|
| – da 105/110 a 106/110 | punti 1 |
| – da 107/110 a 109/110 | punti 2 |
| – da 110/110 a 110/110 e lode | punti 3 |

Nelle graduatorie preliminari i candidati vengono classificati in ordine decrescente di punteggio, calcolato unicamente sulla base di quanto dichiarato nella domanda di partecipazione. Ai fini della determinazione del punteggio, verrà preso in considerazione **un solo titolo di laurea magistrale/specialistica/di "vecchio ordinamento" utile** ai fini della partecipazione al concorso.

Per ciascun concorso vengono convocati a sostenere la prova scritta (cfr. art. 5) i candidati classificatisi nelle **prime 600 posizioni nonché gli eventuali *ex aequo* nell'ultima posizione utile**. L'ammissione alle prove avviene con la più ampia riserva in ordine al possesso dei requisiti di partecipazione previsti dal bando e dei titoli dichiarati ai fini della preselezione.

I **risultati** conseguiti nella preselezione con l'indicazione dell'eventuale ammissione alla prova scritta vengono resi disponibili esclusivamente sul sito internet dell'Agenzia www.acn.gov.it. Tale comunicazione assume valore di notifica ad ogni effetto di legge.

Il punteggio conseguito ai fini della preselezione non concorre alla formazione del punteggio complessivo utile ai fini della graduatoria di merito dei concorsi.

Articolo 4 Convocazioni

Il calendario e il luogo di svolgimento della prova scritta vengono resi noti tramite avviso sulla Gazzetta Ufficiale della Repubblica italiana "4^a Serie speciale (Concorsi ed Esami)" di uno dei **martedì o venerdì del mese di aprile 2022**.

Con le stesse modalità e gli stessi tempi - qualora per motivi organizzativi non sia ancora possibile determinare data e luogo di svolgimento della prova scritta - viene indicata la Gazzetta Ufficiale sulla quale l'avviso verrà successivamente pubblicato.

Nel caso in cui, dopo la pubblicazione del calendario, circostanze straordinarie e imprevedibili rendano necessario rinviare lo svolgimento della prova scritta, la notizia del rinvio e del nuovo calendario viene prontamente diffusa mediante avviso sulla Gazzetta Ufficiale.



Agenzia per la Cybersicurezza Nazionale

Tutte le informazioni relative ai concorsi sono disponibili anche sul sito internet dell'Agenzia www.acn.gov.it. L'Agenzia non assume responsabilità in ordine alla diffusione di informazioni inesatte da parte di fonti non autorizzate.

Articolo 5 Commissioni e prove di concorso

Per i concorsi di cui all'art.1 l'Agenzia nomina una o più Commissioni con l'incarico di sovrintendere alle prove.

Le **prove** consistono in una prova scritta e in una prova orale sulle materie indicate nei programmi allegati e **si svolgono a Roma**.

La prova scritta prevede lo **svolgimento di tre quesiti a risposta sintetica** sulle materie indicate nei programmi allegati e di un **breve elaborato in lingua inglese** su argomenti di attualità.

I quesiti, che possono avere per oggetto l'esame di un **caso pratico**, devono essere scelti dal candidato tra quelli proposti dalla Commissione, secondo quanto specificamente indicato in ciascuno dei programmi allegati. La durata complessiva della prova scritta verrà stabilita dalla Commissione **fino a un massimo di quattro ore**.

Nella valutazione dei quesiti la Commissione verifica: le conoscenze tecniche (applicazione delle conoscenze generali al caso specifico); la capacità di sintesi; l'attinenza alla traccia (pertinenza; completezza); la chiarezza espressiva (proprietà linguistica; correttezza espositiva); la capacità di argomentare (sviluppo critico delle questioni; qualità delle considerazioni/soluzioni proposte). Nella valutazione dell'elaborato in lingua inglese la Commissione verifica il livello di conoscenza dell'inglese come strumento di lavoro.

Per lo svolgimento della prova scritta **non è consentito** l'uso di telefoni cellulari, calcolatrici elettroniche, *personal computer, smartphone, tablet, smartwatch* e strumenti ad essi assimilabili, né di manuali, appunti di ogni genere, dizionari di lingua inglese; **è consentita** la consultazione di testi normativi non commentati né annotati, esclusivamente in forma cartacea.

La **prova scritta** è corretta garantendo l'anonimato dei candidati. **Vengono valutate esclusivamente le prove dei candidati che abbiano svolto tutti e tre i quesiti, secondo le indicazioni dei programmi allegati.**

I tre quesiti sulle materie dei programmi allegati sono valutati fino a un **massimo di 60 punti**, attribuendo a ognuno fino a un massimo di 20 punti. La prova è superata da coloro che ottengono **un punteggio di almeno 12 punti in ciascuno dei quesiti**; sono, tuttavia, ammessi alla prova orale i candidati che hanno conseguito in uno dei tre quesiti un punteggio di almeno 10 punti, **purché il punteggio complessivo non sia inferiore a 36 punti**.



Agenzia per la Cybersicurezza Nazionale

L'elaborato in lingua inglese è corretto solo per i candidati che hanno ottenuto il punteggio minimo di 36 punti nei quesiti ed è **valutato fino a un massimo di 3 punti**.

La votazione complessiva della prova scritta risulta dalla somma dei due punteggi utili (quesiti sulle materie dei programmi allegati ed elaborato in lingua inglese).

I risultati della prova scritta, con l'indicazione dell'eventuale ammissione alla prova orale e della data di convocazione, **vengono resi disponibili a ciascun candidato esclusivamente sul sito internet dell'Agenzia www.acn.gov.it**. Tale comunicazione ha valore di notifica a ogni effetto di legge.

La prova orale consiste in un colloquio sulle materie indicate nei programmi allegati e in una **conversazione in lingua inglese**; possono formare oggetto di colloquio l'argomento della tesi di laurea e le esperienze professionali maturate.

Il colloquio, nel quale potranno essere discussi con il candidato anche **casi pratici**, tende ad accertare: le conoscenze tecniche; la capacità espositiva; la capacità di cogliere le interrelazioni tra gli argomenti; la capacità di giudizio critico. La conversazione in lingua inglese è volta a verificarne il livello di conoscenza in relazione a un utilizzo dell'inglese come strumento di lavoro.

La prova orale viene valutata con l'attribuzione di un punteggio **massimo di 60 punti** ed è superata dai candidati che conseguono una votazione di **almeno 36 punti**.

I risultati della prova orale vengono resi disponibili a ciascun candidato sul sito internet dell'Agenzia www.acn.gov.it. Tale comunicazione ha valore di notifica a ogni effetto di legge.

Articolo 6

Identificazione dei candidati per la partecipazione alle prove

Per sostenere le prove i candidati devono essere muniti di carta di identità o di uno dei documenti di riconoscimento previsti dall'art. 35 del d.P.R. n. 445/2000.

Il documento deve essere in corso di validità secondo le previsioni di legge. **Sono esclusi i candidati non in grado di esibire un valido documento di identità.**

Articolo 7

Graduatorie

Il punteggio complessivo dei candidati idonei è determinato dalla somma delle votazioni riportate nelle prove scritta e orale.



Agenzia per la Cybersicurezza Nazionale

Sono considerati idonei i candidati che hanno conseguito i punteggi minimi previsti per le prove di cui all'art. 5.

Le Commissioni formano le graduatorie di merito seguendo l'ordine decrescente di punteggio complessivo.

L'Agenzia approva le graduatorie finali sulla base delle graduatorie di merito; qualora più candidati risultino in posizione di *ex aequo*, viene data preferenza al candidato più giovane.

L'Agenzia, nel caso di rinuncia alla nomina o di mancata presa di servizio da parte dei candidati classificati in posizione utile all'assunzione, si riserva la facoltà di coprire i posti rimasti vacanti seguendo l'ordine di graduatoria.

L'Agenzia si riserva la facoltà di utilizzare le graduatorie finali dei concorsi di cui all'art. 1 entro **due anni** dalla rispettiva data di approvazione.

Le graduatorie finali dei vincitori vengono pubblicate sul sito internet dell'Agenzia www.acn.gov.it. Tale pubblicazione assume valore di notifica a ogni effetto di legge. Per tutelare la *privacy* degli interessati, i nominativi dei candidati idonei, classificati in posizione non utile all'assunzione, verranno pubblicati solo in caso di utilizzo delle graduatorie, ai sensi del comma precedente.

Articolo 8 Autocertificazioni richieste per l'assunzione

Ai fini dell'assunzione dovrà essere autocertificato il possesso dei requisiti di partecipazione al concorso e di assunzione, secondo le modalità previste nel d.P.R. n. 445/2000. Per la verifica del possesso del requisito di cui all'art. 1, punto 5 (compatibilità con le funzioni da svolgere presso l'Agenzia), sarà richiesto di rendere dichiarazioni relative all'eventuale sussistenza di condanne penali, di sentenze di applicazione della pena su richiesta, di sottoposizione a misure di sicurezza o di carichi pendenti. Saranno oggetto di valutazione discrezionale tutte le sentenze di condanna anche in caso di intervenuta prescrizione, provvedimento di amnistia, indulto, perdono giudiziale, riabilitazione, sospensione della pena, beneficio della non menzione nonché i procedimenti penali pendenti.

Ai candidati verrà richiesto di autocertificare di aver tenuto condotta incensurabile e comunque di non aver adottato comportamenti nei confronti delle istituzioni democratiche che non diano sicuro affidamento di scrupolosa fedeltà alla Costituzione repubblicana e alle ragioni di sicurezza dello Stato. In relazione allo specifico contesto di impiego e laddove sussista per l'Agenzia l'esigenza di abilitare il candidato alla trattazione di informazioni classificate ai



Agenzia per la Cybersicurezza Nazionale

sensi dell'art. 42 della L. n. 124/2007, l'Agenzia si riserva la possibilità di avviare, ai sensi dell'art. 25 del d.P.C.M. n. 5/2015, le procedure per il rilascio del nulla osta di sicurezza (NOS).

Articolo 9 Nomina e assegnazione

I candidati classificati in posizione utile all'assunzione dovranno comunicare all'Agenzia - qualora non abbiano già provveduto nella domanda *on-line* - un indirizzo di Posta Elettronica Certificata (PEC) al quale verranno indirizzate, a ogni effetto di legge, le comunicazioni di avvio del procedimento di nomina e assegnazione ed eventuali altre comunicazioni. **Il possesso di un indirizzo PEC è indispensabile per avviare il procedimento di assunzione.**

L'Agenzia procede all'assunzione dei candidati utilmente classificati che siano in possesso dei requisiti di cui all'art. 1. Essi sono nominati in prova come:

- Esperto al 2° livello stipendiale, per il concorso di cui alla lett. A;
- Esperto al 2° livello stipendiale, per il concorso di cui alla lett. B;
- Esperto al 2° livello stipendiale, per il concorso di cui alla lett. C;
- Esperto al 2° livello stipendiale, per il concorso di cui alla lett. D;
- Esperto al 2° livello stipendiale, per il concorso di cui alla lett. E;
- Esperto al 1° livello stipendiale, per il concorso di cui alla lett. F.

Al termine del periodo di prova della durata di sei mesi, le persone nominate, se riconosciute idonee, conseguono la conferma della nomina con la stessa decorrenza di quella in prova; nell'ipotesi di esito sfavorevole, il periodo di prova è prorogato, per una sola volta, di altri sei mesi.

L'accettazione della nomina non può essere in alcun modo condizionata.

Le persone nominate devono prendere servizio presso la sede di lavoro cui sono assegnate entro il termine comunicato; eventuali proroghe del termine sono concesse solo per giustificati motivi. Se rinunciano espressamente alla nomina o, in mancanza di giustificati motivi, non prendono servizio entro il termine, decadono dalla nomina, come previsto dal Regolamento del Personale dell'Agenzia.

Articolo 10 Trattamento dei dati personali

Ai sensi della normativa europea e nazionale in materia di *privacy*, si informa che i dati forniti dai candidati sono trattati, anche in forma automatizzata, per le finalità di gestione del concorso. Per i candidati che saranno assunti il trattamento proseguirà per le finalità inerenti alla gestione del rapporto di lavoro.



Agenzia per la Cybersicurezza Nazionale

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 procede all'esclusione dal concorso o non dà corso all'assunzione.

I dati idonei a rivelare lo stato di salute dei candidati sono trattati per l'adempimento degli obblighi previsti dalle leggi n. 104/1992 e n. 68/1999. I dati di cui all'art. 8 del presente bando sono trattati per l'accertamento del requisito di assunzione, secondo quanto previsto dalle norme regolamentari dell'Agenzia, relativo alla compatibilità dei comportamenti tenuti dagli interessati con le funzioni da svolgere in Agenzia, con le istituzioni democratiche o che non diano sicuro affidamento di scrupolosa fedeltà alla Costituzione repubblicana e alle ragioni di sicurezza dello Stato.

I dati forniti possono essere comunicati ad altre amministrazioni pubbliche a fini di verifica di quanto dichiarato dai candidati o negli altri casi previsti da leggi e regolamenti i quali li tratteranno in qualità di autonomi titolari del trattamento. I dati personali forniti per la candidatura vengono registrati in una piattaforma informatica della Banca d'Italia che a tal fine viene nominata Responsabile del trattamento; inoltre, i dati possono essere comunicati anche alle società - in qualità di Responsabili del trattamento - di cui l'Agenzia si avvale per particolari prestazioni professionali, consulenze o servizi strettamente connessi con lo svolgimento del concorso.

Agli interessati competono il diritto di accesso ai dati personali e gli altri diritti riconosciuti dalla legge 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 della legge nonché il diritto di opporsi in tutto o in parte, per motivi legittimi, al loro trattamento.

Tali diritti potranno essere fatti valere nei confronti del Titolare del trattamento, Agenzia per la Cybersicurezza Nazionale - Servizio Risorse umane e strumentali - via di Santa Susanna n. 15, 00184 ROMA (e-mail: risorseumane@acn.gov.it).

Per le violazioni della vigente disciplina in materia di *privacy* è possibile rivolgersi, in qualità di Autorità di controllo, al Garante per la protezione dei dati personali - Piazza Venezia n. 11 - Roma.

Articolo 11 Responsabile del procedimento

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.

IL DIRETTORE GENERALE
Roberto Baldoni



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

15 Esperti per le funzioni tecnico/amministrative di **“Certificazione e Ispezione” con esperienza nell’applicazione di schemi di certificazione Common Criteria / ITSEC e/o come auditor ISO**

lett. A dell’art. 1 del bando

PROVA SCRITTA

Svolgimento di tre quesiti a risposta sintetica (su tre delle quattro materie del programma), scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma) su:

Contesto giuridico nazionale

- Regolamento concernente le procedure, le modalità e i termini da seguire ai fini delle valutazioni da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione (DPR n. 54/2021)
- Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell’informazione (DPCM 30 ottobre 2003)
- Golden Power (art. 1-bis, D.L. n. 21/2012): ambito di applicazione e procedimento istruttorio a seguito dell’avvio del CVCN

Contesto tecnico/giuridico europeo

- Regolamento eIDAS (Reg. UE 2014/910): iniziative nazionali di implementazione
- Cybersecurity Act (Reg. UE 2019/881), limitatamente al Quadro di certificazione della cybersicurezza
- Direttiva europea NIS (UE 2016/1148) e decreto di recepimento nell’ordinamento nazionale D.Lgs. n. 65/2018
- Iniziative europee in materia di schemi di certificazione ai sensi del Cybersecurity Act

Standard, norme e metodologie

- Framework Nazionale per la Cybersecurity e la Data Protection
- Common Criteria for Information Technology Security Evaluation (ISO/IEC 15048) e relativa metodologia (ISO/IEC 18045)
- Information Technology Security Evaluation Criteria (ITSEC)
- Metodologie di risk assessment
- Altre metodologie e linee guida per i test di sicurezza (NIST, OSSTMM, OWASP, CIS)
- Principi generali degli standard ISO: ISO 27001:2013, ISO 17025:2017, ISO 17065:2012



Agenzia per la Cybersicurezza Nazionale

Metodologie ispettive

- Audit ISO 27001
- Audit ISO 9001
- Audit ISO 17025
- Attività di ispezione e verifica demandate all'Agenzia per la Cybersicurezza Nazionale

Prova in lingua inglese

PROVA ORALE

Oltre a tutti gli argomenti previsti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le esperienze professionali maturate potranno formare oggetto della prova orale.



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

10 Esperti per le funzioni di “Tecnico hardware e Tecnico di telecomunicazioni” con esperienza nello sviluppo hardware (PCB, logiche programmabili, ASIC), in sistemi embedded e/o in ambito reti di telecomunicazioni

lett. **B** dell’art. 1 del bando

PROVA SCRITTA

Svolgimento di tre quesiti a risposta sintetica (su tre delle cinque materie del programma), scelti tra i dieci proposti dalla Commissione (due per ogni materia del programma) su:

Elettronica e Progettazione Hardware

- Elettronica Analogica e Digitale
- Lettura e comprensione di schemi elettrici
- Conoscenza generale componentistica elettronica
- Linguaggi di descrizione dell’hardware e logiche programmabili
- Utilizzo strumentazione elettronica di test e tecniche di misura
- Tecniche e strumenti di Reverse Engineering dell’hardware

Sistemi Embedded

- Linguaggio C/C++
- Architettura dei Sistemi Embedded e IoT
- Sistemi Operativi Real Time
- Architetture firmware e tecniche di dumping delle memorie
- Elementi di Side Channel Analysis e Fault Injection
- Conoscenza dei principali protocolli di comunicazione hardware (SPI, UART, I2C, CAN, etc)

Fondamenti di informatica e sviluppo software

- Linguaggi di Programmazione (imperativi, di scripting e orientati agli oggetti)
- Sistemi Operativi (Windows, Linux, OSX, Android, iOS)
- Algoritmi e Strutture Dati
- Algoritmi di Crittografia Simmetrica e Asimmetrica



Agenzia per la Cybersicurezza Nazionale

Sistemi e reti per l'automazione industriale

- Sistemi di controllo industriale (SCADA, ICS)
- Elementi di Industrial IoT
- Elementi di cybersecurity in ambito industriale (IEC 62443, NIST SP 800-82)
- Protocolli di telecomunicazione in ambito industriale (IEC 60870-5-104, Modbus, OPC, etc.)
- Nuove architetture e servizi TLC in ambito industriale: 5G (MEC, URLCC, mMTC) e WiFi 6

Reti di Telecomunicazione Mobili

- Protocolli e Standard (UMTS/LTE/5G)
- Architetture logiche end-to-end per le reti 4G e 5G
- Radio Access Network 4G e 5G, Open RAN
- Multi-access edge computing
- Architetture di rete Core (PC/EPC, 5GC-SBA), SDN, NFV
- Tecnologie DevOps (OpenStack, Kubernetes)
- Operation Support System e sistemi di orchestrazione (MANO)
- Sicurezza dei protocolli di segnalazione

Prova in lingua inglese

PROVA ORALE

Oltre ai tre argomenti scelti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le esperienze professionali maturate potranno formare oggetto della prova orale.



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

15 Esperti per le funzioni di “Tecnico software” con esperienza in ambito sviluppo software e/o nella sicurezza informatica

lett. C dell’art. 1 del bando

PROVA SCRITTA

Svolgimento di tre quesiti a risposta sintetica (su tre delle quattro materie del programma), scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma) su:

Fondamenti di informatica e sviluppo software

- Linguaggi di Programmazione (imperativi, di scripting e orientati agli oggetti)
- Tecnologie web
- Sistemi Operativi (Windows, OSX, Linux, Android, iOS)
- Algoritmi e Strutture Dati
- Database Relazionali e NoSQL
- Architettura degli Elaboratori e linguaggi macchina
- Reti di Calcolatori e protocolli di rete

Sicurezza delle reti e dei sistemi ICT

- Metodologie e Strumenti di Vulnerability Assessment e Penetration Testing in ambito reti ICT/OT
- Tecniche di Analisi Forense (computer/network/mobile forensics)
- Algoritmi di Crittografia Simmetrica e Asimmetrica
- Conoscenza dei Protocolli e delle Reti Industriali (SCADA, ICS)

Sicurezza del Software

- Tecniche per lo sviluppo di codice sicuro
- Sicurezza delle applicazioni web: strumenti e metodologie (OWASP)
- Contromisure Software per Fault Injection e Side Channel Analysis
- Tipologie di vulnerabilità software (buffer overflow, use-after-free, etc.)
- Tipologie di vulnerabilità in applicazioni web (OWASP Top 10)
- Metodologie e strumenti di fuzzing
- Metodologie e strumenti di Reverse Engineering



Agenzia per la Cybersicurezza Nazionale

Architetture cloud

- Strategia nazionale sul cloud computing
- NIST Definition of Cloud Computing (SP 800-145)
- Principi generali degli standard ISO relativi al cloud computing (cenni su materiale liberamente consultabile): ISO 17788:2014, ISO 17789:2014, ISO 27017:2015
- Architetture Cloud: tipologie di servizi e modelli di deployment
- Tecnologie di virtualizzazione
- OWASP DevSecOps Guideline
- Principi generali su framework applicabili (COBIT, ITIL)

Prova in lingua inglese

PROVA ORALE

Oltre a tutti gli argomenti previsti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le esperienze professionali maturate potranno formare oggetto della prova orale.



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

4 Esperti per le funzioni di gestione e realizzazione di “Programmi industriali, tecnologici e di ricerca” con esperienza in programmi di investimento di rilevanza nazionale ed europea nel campo della cyber security

lett. **D** dell’art. 1 del bando

PROVA SCRITTA

Svolgimento di tre quesiti a risposta sintetica sulle tre materie del programma, scelti tra i sei proposti dalla Commissione (due per ogni materia del programma) su:

Architetture di sicurezza e sistemi IT

- Elementi di architetture di sicurezza e sistemi IT
- Elementi di gestione del rischio nei sistemi IT
- Elementi di gestione della privacy
- Standard di sicurezza

Programmi di innovazione tecnologica e gestione progettuale

- Opportunità di finanziamento Comunitario
- Elementi di trasferimento tecnologico
- Livelli di maturità tecnologica
- Pratiche di gestione progettuale
- Elementi di pianificazione finanziaria e operativa
- Metodologie di monitoraggio e controllo

Tecnologie emergenti

- Blockchain e Distributed Ledger Technology
- Quantum Computing
- Augmented / Virtual Reality
- IoT

Prova in lingua inglese



Agenzia per la Cybersicurezza Nazionale

PROVA ORALE

Oltre a tutti gli argomenti previsti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le eventuali esperienze professionali maturate potranno formare oggetto della prova orale.



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

3 Esperti per le funzioni di “Tecnico crittografo” con esperienza nell’ambito della crittografia teorica o applicata

lett. **E** dell’art. 1 del bando

Svolgimento di tre quesiti a risposta sintetica (su tre delle quattro materie del programma), scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma) su:

Fondamenti di informatica e sviluppo software

- Linguaggi di Programmazione (imperativi, di scripting e orientati agli oggetti)
- Sistemi Operativi (Windows, Linux, OSX, Android, iOS)
- Algoritmi e Strutture Dati
- Sicurezza protocolli di rete (SSL/TLS, IPSEC, ...)
- Architettura degli elaboratori e linguaggi macchina

Crittografia Simmetrica e Algoritmi di Hashing

- Block Ciphers e Block Cipher Modes
- Stream Ciphers
- Message Digest e Hash
- Crittoanalisi Lineare
- Crittoanalisi Differenziale
- Elementi di Contromisure Software per Side Channel Analysis

Crittografia Asimmetrica

- Teoria dei Gruppi
- Elementi di Algebra Astratta
- Logaritmo Discreto e Diffie-Hellman
- Fattorizzazione Intera e RSA
- Crittografia a Curve Ellittiche
- Algoritmi di firma digitale
- Elementi di crittoanalisi
- Elementi di Contromisure Software per Side Channel Analysis



Agenzia per la Cybersicurezza Nazionale

Applicazioni Crittografiche

- Crittografia Post-Quantum
- Blockchain, criptovalute e voto elettronico
- Lattice e crittografia Lattice-based
- Crittografia Omomorfica
- Zero-knowledge proof

PROVA ORALE

Oltre a tutti gli argomenti previsti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le eventuali esperienze professionali maturate potranno formare oggetto della prova orale.



Agenzia per la Cybersicurezza Nazionale

PROGRAMMA

3 Esperti per le funzioni **operative di “Cybersecurity”** con **conoscenze** in ambito della **gestione degli incidenti informatici** (triage, indicatori di compromissione, best practices di sicurezza informatica), dell'**analisi malware**, dell'**analisi forense e cyber threat intelligence**, dell'**analisi e valorizzazione di dati** e della **gestione del rischio cyber**

lett. F dell'art. 1 del bando

PROVA SCRITTA

Svolgimento di tre quesiti a risposta sintetica (su tre delle quattro materie del programma), scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma) su:

La sicurezza dei dati, dei sistemi e delle applicazioni

- La sicurezza sotto i profili di disponibilità, confidenzialità e integrità
- La sicurezza del *software*, delle reti e dei sistemi
- Gli algoritmi, i protocolli e le applicazioni della crittografia
- Le tipologie di attacchi *cyber* e le relative tattiche, tecniche e procedure
- La gestione degli incidenti di sicurezza e le attività di *digital forensic* e *security assessment*
- L'innovazione tecnologica applicata alla *cyber security*

La gestione dei dati, delle informazioni e della conoscenza

- La raccolta, la correlazione e il ciclo di vita degli indicatori di compromissione
- Il *triage* delle informazioni e la prioritizzazione delle minacce
- Metodi, modelli e protocolli per lo scambio informativo
- I *framework* per il *threat modeling* e la gestione della conoscenza
- Metodi e tecniche per il trasferimento efficace della conoscenza ai diversi *stakeholder*

La Cyber Threat Intelligence

- Il ciclo di *intelligence* e i livelli della *threat intelligence*
- Profilazione degli attori della minaccia e *reverse targeting*
- Metodologie di analisi strutturate
- Metodologie per la gestione dei *bias* cognitivi
- La *Social media intelligence*, l'*Open source intelligence* e il *Deep/Dark web monitoring*
- L'analisi strategica: la minaccia ibrida e la *cyber warfare*



Agenzia per la Cybersicurezza Nazionale

Il contesto organizzativo e normativo

- Modelli di *governance* per la *business continuity*, la *data protection* e il *cyber risk management*
- I *framework* per le attività di *red team testing*
- La protezione *cyber* delle infrastrutture critiche informatizzate
- L'ordinamento dell'architettura nazionale *cyber* e i *cybersecurity framework* internazionali
- I modelli organizzativi per la difesa proattiva (ISAC, CERT, CSIRT)
- La protezione della *supply chain*: presidi organizzativi e normativi

Prova in lingua inglese

PROVA ORALE

Oltre a tutti gli argomenti previsti per la prova scritta e alla conversazione in lingua inglese:

Architettura normativa in materia di cybersicurezza

- Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), D.LGS. n. 65/2018 NIS e D.LGS. n. 207/2021 (attuazione della direttiva UE 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche)
- Strategia europea in materia di cybersicurezza
- Autorità nazionali ed europee competenti in materia di cybersicurezza
- Legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021)

L'argomento della tesi di laurea e le eventuali esperienze professionali maturate potranno formare oggetto della prova orale.