Agenzia per la Cybersicurezza Nazionale

90 ASSUNZIONI DI ESPERTI CON ORIENTAMENTO TECNICO SCIENTIFICO

Articolo 1
Posti e posizioni messe a concorso

1. L'Agenzia per la cybersicurezza nazionale (di seguito Agenzia) indice i seguenti concorsi pubblici per l'assunzione a tempo pieno e indeterminato di:

A) 8 Esperti	**con orientamento in *cloud* e *edge computing* e in sistemi di telecomunicazione di nuova generazione;**
B) 12 Esperti	**con orientamento in sistemi di Intelligenza Artificiale;**
C) 10 Esperti	**con orientamento in ispezioni di cybersicurezza;**
D) 3 Esperti	**con orientamento in crittografia;**
E) 10 Esperti	**con orientamento in valutazione della sicurezza e certificazione di sistemi e componenti OT e ICT;**
F) 12 Esperti	**con orientamento in gestione e realizzazione di programmi industriali, tecnologici e di ricerca nel campo della cybersicurezza o dell'ICT;**
G) 10 Esperti	**con orientamento in gestione e realizzazione di progetti IT;**
H) 12 Esperti	**con orientamento in gestione del rischio cyber;**
I) 5 Esperti	**con orientamento in analisi della minaccia cyber;**
J) 8 Esperti	**con orientamento in *data analysis* e produzione di statistiche sulla minaccia cyber**.

Articolo 2
Requisiti di partecipazione

1. Per la partecipazione ai concorsi di cui all'articolo 1, comma 1, sono richiesti i seguenti requisiti:

   a. **Concorso di cui alla lettera A) - 8 Esperti con orientamento in *cloud* e *edge computing* e in sistemi di telecomunicazione di nuova generazione**:

   - **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria aerospaziale e astronautica (LM-20); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettrica (LM-28); Ingegneria elettronica (LM-29); Ingegneria energetica e nucleare (LM-30); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;

- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro o tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: sistemi di certificazione della sicurezza ICT, cloud e/o telecomunicazioni; architetture di sicurezza cloud e delle telecomunicazioni; progettazione, studio e amministrazione di architetture di sicurezza cloud e/o delle telecomunicazioni; esecuzione di test di sicurezza in ambito ICT, cloud e/o telecomunicazioni; applicazione di metodologie di valutazione della sicurezza ICT basate su standard internazionali. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

b. **Concorso di cui alla lettera B) - 12 Esperti con orientamento in sistemi di Intelligenza Artificiale:**

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria aerospaziale e astronautica (LM-20); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettrica (LM-28); Ingegneria elettronica (LM-29); Ingegneria energetica e nucleare (LM-30); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente.

c. **Concorso di cui alla lettera C) - 10 Esperti con orientamento in ispezioni di cybersicurezza:**

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria aerospaziale e astronautica (LM-20); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettrica (LM-28); Ingegneria elettronica (LM-29); Ingegneria energetica e nucleare (LM-30); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Ingegneria meccanica (LM-33); Matematica (LM-40); Sicurezza informatica (LM-66); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in qualità di auditor ISO 27001, con particolare riferimento alla valutazione della conformità a requisiti di cybersicurezza. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui

si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività di auditor svolte in periodi coincidenti.

d. **Concorso di cui alla lettera D) - 3 Esperti con orientamento in crittografia**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria informatica (LM-32); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente.

e. **Concorso di cui alla lettera E) - 10 Esperti con orientamento in valutazione della sicurezza e certificazione di sistemi e componenti OT e ICT**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria aerospaziale e astronautica (LM-20); Ingegneria civile (LM-23); Ingegneria dei sistemi edilizi (LM-24); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettrica (LM-28); Ingegneria elettronica (LM-29); Ingegneria energetica e nucleare (LM-30); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Ingegneria meccanica (LM-33); Ingegneria navale (LM-34); Ingegneria per l'ambiente e il territorio (LM-35); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: consulenza nell'ambito Common Criteria; consulenza nell'ambito della sicurezza di sistemi di controllo industriale; consulenza nell'ambito di sistemi di certificazione della sicurezza ICT; progettazione di sistemi di controllo industriale o reti ICT; amministrazione di sistemi di controllo industriale; amministrazione di apparati di sicurezza di reti ICT/OT; esecuzione di test di sicurezza in ambito ICT o su sistemi di controllo industriale; applicazione di metodologie di valutazione della sicurezza ICT basate su standard internazionali. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

f. **Concorso di cui alla lettera F) - 12 Esperti con orientamento in gestione e realizzazione di programmi industriali, tecnologici e di ricerca nel campo della cybersicurezza o dell'ICT**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria dell'automazione (LM-25); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Ingegneria meccanica (LM-33); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: gestione di progetti industriali, tecnologici o di ricerca applicata, con partecipazione a rilevanti iniziative nazionali, europee o internazionali, di trasferimento tecnologico, nel campo della cybersicurezza o, più in generale, dell'ICT; attività di supporto alla gestione di risorse e pianificazione delle attività. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

g. **Concorso di cui alla lettera G) - 10 Esperti con orientamento in gestione e realizzazione di progetti IT**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria dell'automazione (LM-25); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Ingegneria meccanica (LM-33); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: progettazione e sviluppo di sistemi IT e di soluzioni che prevedono l'adozione di principi e metodologie propri dei *framework* Agile e/o PMP e/o Prince2; progettazione, prototipazione e/o adozione di nuove soluzioni basate su tecnologie di *Artificial Intelligence/Machine Learning* (AI/ML), *High Performance Computing* (HPC), *Data Science*. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è

svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

h. **Concorso di cui alla lettera H) - 12 Esperti con orientamento in gestione del rischio cyber**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria civile (LM-23); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Matematica (LM-40); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: gestione del rischio cyber, ivi compresa l'attività di *risk assessment*. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

i. **Concorso di cui alla lettera I) - 5 Esperti con orientamento in analisi della minaccia cyber**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione equivalente/equipollente, in una delle seguenti classi di laurea: Scienze della Difesa e della Sicurezza (LM/DS); Fisica (LM-17); Informatica (LM-18); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria informatica (LM-32); Matematica (LM-40); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;
- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: *cyber threat intelligence*, *threat modeling* o analisi geopolitica della minaccia cyber. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

j. **Concorso di cui alla lettera J) - 8 Esperti con orientamento in *data analysis* e produzione di statistiche sulla minaccia cyber**:

- **laurea magistrale, con un punteggio di almeno 105/110** o votazione

equivalente/equipollente in una delle seguenti classi di laurea: Fisica (LM-17); Informatica (LM-18); Ingegneria dell'automazione (LM-25); Ingegneria della sicurezza (LM-26); Ingegneria delle telecomunicazioni (LM-27); Ingegneria elettronica (LM-29); Ingegneria gestionale (LM-31); Ingegneria informatica (LM-32); Matematica (LM-40); Modellistica matematico-fisica per l'ingegneria (LM-44); Sicurezza informatica (LM-66); Scienze statistiche (LM-82); Tecniche e metodi per la società dell'informazione (LM-91); Data science (LM-Data); altra laurea equivalente/equipollente o equiparata ad uno dei suddetti titoli ai sensi della normativa vigente;

- **esperienza professionale, anche di tipo autonomo, di almeno un biennio**, documentabile tramite attestazione del datore di lavoro ovvero tramite idonea documentazione contrattuale e/o fiscale, successiva alla laurea richiesta dalla presente lettera, in uno o più dei seguenti ambiti: statistica e/o data science e/o AI, applicata alla *cybersecurity*; consulenza e/o supporto tecnico-specialistico nell'implementazione di procedure informatiche, metodi statistici ed algoritmi di AI per previsione e analisi predittiva e/o elaborazione del *Natural Language Processing* (NLP) e/o rilevamento delle anomalie e/o automazione dei processi e/o visualizzazione e ottimizzazione dei dati. L'esperienza professionale biennale è valutata anche cumulativamente sia sotto il profilo temporale sia sotto il profilo dell'ambito in cui si è svolta. Ai fini del computo sotto il profilo temporale si prendono in considerazione una sola volta le attività differenti svolte in periodi coincidenti.

2. Per tutti i concorsi di cui all'articolo 1, comma 1, è consentita la partecipazione, con riserva, ai possessori di **titoli di studio conseguiti all'estero o di titoli esteri conseguiti in Italia** riconosciuti equivalenti/equipollenti, ai sensi della normativa vigente, ad uno dei titoli sopraindicati ai fini della partecipazione ai pubblici concorsi. **La richiesta di riconoscimento dell'equivalenza e dell'equipollenza** deve essere presentata a cura dei candidati vincitori entro quindici giorni dalla pubblicazione della graduatoria finale.

3. Per **tutti i concorsi** di cui **all'articolo 1, comma 1**, sono altresì richiesti:
   a) **cittadinanza italiana**;
   b) **godimento dei diritti civili e politici;**
   c) **non essere esclusi dall'elettorato politico attivo;**
   d) **idoneità fisica all'impiego;**
   e) **non essere stato destituito o dispensato dall'impiego presso una pubblica amministrazione** per persistente insufficiente rendimento o dichiarato decaduto per aver conseguito la nomina o l'assunzione mediante la produzione di documenti falsi o viziati da nullità insanabile, ovvero licenziato ai sensi della vigente normativa di legge o contrattuale;
   f) **aver tenuto condotta incensurabile e comunque 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 nonché non avere tenuto comportamenti incompatibili con le funzioni da espletare** (articolo 9, decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 224, recante il "*Regolamento del*

personale dell'Agenzia per la cybersicurezza nazionale");

g) **non aver riportato condanne penali con sentenza passata in giudicato e di non avere in corso procedimenti penali, né procedimenti amministrativi per l'applicazione di misure di sicurezza o di prevenzione, nonché precedenti penali a proprio carico iscrivibili nel casellario giudiziale**, ai sensi dell'articolo 3, decreto del Presidente della Repubblica 14 novembre 2002, n. 313.

4. Tutti i requisiti, eccetto l'equivalenza/equipollenza del titolo di studio, devono essere posseduti alla data di scadenza stabilita per la presentazione della domanda. Tutti i requisiti devono, comunque, essere posseduti anche al momento dell'assunzione.
5. 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.
6. L'Agenzia **dispone l'esclusione dal concorso e 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 presente bando**. Le eventuali difformità riscontrate rispetto a quanto dichiarato o documentato dagli interessati verranno segnalate all'autorità giudiziaria.

Articolo 3
Termine e modalità di presentazione della domanda di partecipazione

1. Il candidato dovrà inviare la domanda di partecipazione alla procedura selettiva **esclusivamente per via telematica**, autenticandosi con SPID/CIE/CNS/eIDAS, compilando il *format* elettronico di candidatura sul Portale «*inPA*» disponibile all'indirizzo: https://www.inpa.gov.it, previa registrazione del candidato sullo stesso Portale. Per la partecipazione alla procedura selettiva il candidato deve essere in possesso di un indirizzo di posta elettronica certificata (PEC) a lui intestato. La registrazione, la compilazione e l'invio on-line della domanda devono essere **completati entro le ore 18:00 del quarantacinquesimo giorno successivo alla pubblicazione del presente bando** sul Portale «*inPA*» (https://www.inpa.gov.it) e sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi). **Saranno accettate esclusivamente le domande inviate prima dello spirare di tale termine perentorio**.
2. La data di presentazione on-line della domanda di partecipazione alla procedura selettiva sarà certificata e comprovata da apposita ricevuta scaricabile al termine della procedura di invio, dal Portale «*inPA*» (https://www.inpa.gov.it). Allo scadere del termine ultimo per la presentazione della domanda, il Portale non consentirà l'accesso alla procedura di candidatura né l'invio della domanda di partecipazione.
3. **È consentita la partecipazione a uno solo dei concorsi di cui all'articolo 1, comma 1**.
4. Ai fini della partecipazione alla procedura selettiva, in caso di più invii della domanda di partecipazione, si terrà conto unicamente dell'ultima domanda di partecipazione inviata in ordine

cronologico, intendendosi le precedenti revocate in modo integrale e definitivo, nonché prive d'effetto.

5. In caso di malfunzionamento, parziale o totale della piattaforma digitale, accertato dall'Agenzia, che impedisca l'utilizzazione della stessa per la presentazione della domanda di partecipazione o degli eventuali allegati, sarà disposta una proroga del termine di scadenza per la presentazione della domanda corrispondente a quello della durata del malfunzionamento. Dell'accertato malfunzionamento e del corrispondente periodo di proroga verrà data comunicazione con avviso pubblicato sul Portale «*inPA*» (https://www.inpa.gov.it) e sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi).
6. Non saranno considerate valide le domande inviate con modalità diverse da quelle prescritte e quelle compilate in modo difforme o incompleto rispetto a quanto indicato nel presente bando di concorso.

Articolo 4
Domanda di partecipazione

1. Nel *format* elettronico di presentazione della domanda, il candidato deve dichiarare, a pena di esclusione, ai sensi degli articoli 46 e 47, decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e consapevole delle sanzioni penali previste dal successivo articolo 76 per le ipotesi di falsità in atti e di dichiarazioni mendaci:
   a) il cognome e il nome, la data e il luogo di nascita;
   b) il codice fiscale;
   c) l'indirizzo di residenza o di domicilio, se diverso dalla residenza, con l'esatta indicazione del numero di codice di avviamento postale, nonché il recapito telefonico e il recapito di posta elettronica certificata (PEC), con l'impegno di far conoscere tempestivamente le eventuali variazioni;
   d) la cittadinanza italiana;
   e) il comune nelle cui liste elettorali è iscritto, oppure i motivi della non iscrizione o della cancellazione dalle liste medesime;
   f) di non essere stato destituito o dispensato dall'impiego presso una pubblica amministrazione per persistente insufficiente rendimento o dichiarato decaduto per aver conseguito la nomina o l'assunzione mediante la produzione di documenti falsi o viziati da nullità insanabile, ovvero licenziato ai sensi della vigente normativa di legge o contrattuale;
   g) il godimento dei diritti civili e politici;
   h) il concorso al quale intende partecipare;
   i) di aver tenuto condotta incensurabile e comunque 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 nonché non avere tenuto comportamenti incompatibili con le funzioni da espletare (articolo 9, decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 224);

j) di non aver riportato condanne penali con sentenza passata in giudicato e di non avere in corso procedimenti penali, né procedimenti amministrativi per l'applicazione di misure di sicurezza o di prevenzione, nonché precedenti penali a proprio carico iscrivibili nel casellario giudiziale, ai sensi dell'articolo 3, decreto del Presidente della Repubblica 14 novembre 2002, n. 313. In caso contrario, devono essere indicati i procedimenti penali e/o amministrativi per l'applicazione di misure di sicurezza o di prevenzione, in corso, precisando l'autorità giudiziaria presso la quale penda l'eventuale procedimento;

k) di essere in possesso dell'idoneità fisica all'impiego;

l) il possesso del titolo di studio di cui all'articolo 2, comma 1, del presente bando, previsto per lo specifico concorso per il quale si presenta la domanda di partecipazione, con l'indicazione della data di conseguimento, della votazione riportata, dell'Università che lo ha rilasciato;

m) per i titoli di studio conseguiti all'estero, gli estremi del provvedimento con il quale il titolo stesso è stato riconosciuto equivalente/equipollente al corrispondente titolo italiano o la dichiarazione che il candidato provvederà a richiedere l'equivalenza/equipollenza secondo le modalità e i tempi indicati nell'articolo 2, comma 2, del presente bando;

n) di possedere la specifica esperienza professionale richiesta per i concorsi di cui all'articolo 1, comma 1, lettere A), C), E), F), G), H), I) e J);

o) di aver preso visione e di accettare in modo pieno e incondizionato le informazioni, disposizioni e condizioni del presente bando, ivi incluso l'articolo 12.

2. I candidati devono specificare, in apposito spazio disponibile sul *format* elettronico, la richiesta di ausili e/o tempi aggiuntivi in funzione della propria necessità che andrà opportunamente documentata ed esplicitata con apposita dichiarazione resa dalla Commissione medico-legale dell'ASL di riferimento o da equivalente struttura pubblica. La concessione e l'assegnazione di ausili e/o tempi aggiuntivi sarà determinata a insindacabile giudizio dell'Agenzia, sulla scorta della documentazione esibita e dell'esame obiettivo di ogni specifico caso. I medici di cui si avvarrà l'Agenzia valuteranno la richiesta esclusivamente sulla base del nesso causale tra la patologia dichiarata e le modalità di svolgimento di ciascuna prova. In ogni caso, i tempi aggiuntivi non eccederanno il 50% del tempo assegnato per la prova. Tutta la documentazione di supporto alla dichiarazione resa dovrà essere caricata sul Portale «*inPA*» (https://www.inpa.gov.it) durante la fase di inoltro della candidatura quando richiesto, i file dovranno essere in formato pdf. L'omesso inoltro di tale documentazione non consentirà di fornire adeguatamente l'assistenza richiesta.

3. I candidati con diagnosi di disturbi specifici di apprendimento (DSA) dovranno fare esplicita richiesta, in apposito spazio disponibile sul *format* elettronico, della misura dispensativa, dello strumento compensativo e/o dei tempi aggiuntivi necessari in funzione della propria esigenza che dovrà essere opportunamente documentata ed esplicitata con apposita dichiarazione resa dalla Commissione medico-legale dell'ASL di riferimento o da equivalente struttura pubblica. L'adozione delle richiamate misure sarà determinata a insindacabile giudizio dell'Agenzia, sulla

scorta della documentazione esibita e dell'esame obiettivo di ogni specifico caso, e comunque nell'ambito delle modalità individuate dal decreto 9 novembre 2021 del Ministro per la pubblica amministrazione.

4. Eventuali gravi limitazioni fisiche sopravvenute successivamente alla data di scadenza del bando, che potrebbero prevedere la concessione di ausili e/o tempi aggiuntivi, dovranno essere documentate con certificazione medica che sarà valutata dalla Commissione esaminatrice, la cui decisione, sulla scorta della documentazione sanitaria che consenta di quantificare il tempo aggiuntivo ritenuto necessario, resta insindacabile e inoppugnabile. La documentazione dovrà essere inviata all'indirizzo recruitment@acn.gov.it, con l'indicazione nell'oggetto: "*Concorso per 90 Esperti con orientamento tecnico scientifico, Lettera* (da specificare a cura del candidato) – *Documentazione riservata*".
5. L'Agenzia effettua controlli sulla veridicità delle dichiarazioni rese dai candidati utilmente collocati in graduatoria. Qualora il controllo accerti la falsità del contenuto delle dichiarazioni, il candidato sarà escluso dalla selezione, ferme restando le sanzioni penali previste dall'articolo 76, decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
6. L'Agenzia non è responsabile in caso di smarrimento o di mancato recapito delle proprie comunicazioni inviate al candidato quando ciò sia dipendente da dichiarazioni inesatte o incomplete rese dallo stesso circa il proprio recapito, oppure da mancata o tardiva comunicazione del cambiamento del predetto recapito rispetto a quello indicato nella domanda, nonché da eventuali disguidi imputabili a fatto di terzo, a caso fortuito o forza maggiore.
7. Per le richieste di assistenza di tipo informatico legate alla procedura di iscrizione on-line, i candidati devono utilizzare esclusivamente, previa lettura della guida alla compilazione della domanda presente nella *home page* e delle relative FAQ, l'apposito modulo di assistenza presente sul Portale «*inPA*» (https://www.inpa.gov.it). Non è garantita la soddisfazione entro il termine di scadenza previsto per l'invio della domanda di partecipazione delle richieste inviate nei tre giorni antecedenti il medesimo termine. Le richieste pervenute in modalità differenti da quelle sopra indicate non potranno essere prese in considerazione.

Articolo 5
Comunicazioni ai candidati

1. Le comunicazioni personali relative alla presente procedura saranno inviate dall'Agenzia all'indirizzo PEC personale del candidato. L'Agenzia non assume alcuna responsabilità derivante da inesatte indicazioni del recapito da parte del candidato, ovvero, da mancata o tardiva comunicazione di cambiamento dell'indirizzo PEC.
2. Le comunicazioni di carattere pubblico concernenti la procedura selettiva, compreso il calendario della prova d'esame e le graduatorie finali, saranno effettuate mediante pubblicazione:
   a) sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*»

(https://www.acn.gov.it/portale/lavora-con-noi);

b) sul Portale «*inPA*» (https://www.inpa.gov.it).

3. Non sono tenute in considerazione e determinano, 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, tramite PEC, il **provvedimento di esclusione**.
4. **I candidati non esclusi sono comunque ammessi alla procedura selettiva con la più ampia riserva in ordine al possesso dei requisiti di partecipazione richiesti dal presente bando.**
5. L'Agenzia non assume responsabilità in ordine alla diffusione di informazioni inesatte da parte di fonti non autorizzate.
6. La pubblicazione delle comunicazioni relative alla **convocazione alle prove d'esame** sarà effettuata nel rispetto dei termini di preavviso previsti di **almeno quindici giorni prima** dell'effettuazione **della prova scritta e della prova orale**.
7. Tutte le comunicazioni effettuate sul Portale «*inPA*» (https://www.inpa.gov.it) e sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi) hanno valore di notifica a tutti gli effetti nei confronti dei candidati che hanno presentato domanda di partecipazione al concorso.
8. Eventuali richieste di informazioni e chiarimenti in merito al concorso potranno essere trasmesse al responsabile del procedimento individuato nel Capo *pro tempore* del Servizio Risorse Umane, strumentali e amministrazione generale dell'Agenzia, all'indirizzo recruitment@acn.gov.it, con l'indicazione nell'oggetto: "*Concorso per 90 Esperti con orientamento tecnico scientifico, Lettera* (da specificare a cura del candidato) – *Documentazione riservata*".

Articolo 6
Commissioni e prova scritta

1. L'Agenzia, per i concorsi di cui all'articolo 1, nomina più Commissioni competenti per l'espletamento di tutte le fasi del concorso, compresa la formazione delle graduatorie di merito.
2. L'Agenzia nomina, altresì, un Comitato test con l'incarico di predisporre i quesiti a risposta multipla comuni a tutti i concorsi. Ciascuna Commissione verifica, recepisce e approva le domande predisposte dal Comitato test e predispone, altresì, i quesiti a risposta multipla e i quesiti a risposta sintetica specifici per ciascun profilo.
3. **Ciascuna Commissione predispone due versioni di prova da sorteggiare in sede di esame di fronte ai candidati**.
4. Per ciascun concorso di cui all'articolo 1, comma 1, la prova d'esame, che si svolgerà a Roma mediante l'ausilio di strumenti informatici appositamente messi a disposizione del candidato, consiste in un **test a risposta multipla** e in **due quesiti a risposta sintetica** sulle materie indicate negli specifici programmi allegati al presente bando.

5. La **prova scritta** per tutti i concorsi si articola nel seguente modo:

A) TEST A RISPOSTA MULTIPLA

Il test è composto da **50 domande** ed è articolato in **tre sezioni** finalizzate all'accertamento della conoscenza delle materie qui di seguito indicate:

- Materie di cui ai punti 1 e 2 degli specifici programmi allegati, comuni a tutti i concorsi (*Sezione 1*: domande da 1 a 20);
- Materie di cui ai punti 3, 4, e 5 degli specifici programmi allegati (*Sezione 2*: domande da 21 a 40);
- Lingua inglese, livello B2, comune a tutti i concorsi (*Sezione 3*: domande da 41 a 50).

Alla predisposizione delle domande:

- da 1 a 20 (*Sezione 1*) e da 41 a 50 (*Sezione 3*) provvede il Comitato Test;
- da 21 a 40 (Sezione 2) provvede ciascuna specifica Commissione.

Il test è corretto in forma anonima e automatizzata.

Al test viene attribuito un punteggio massimo di 25 punti.

I criteri di attribuzione del punteggio sono i seguenti:

- ✓ per ogni risposta esatta: 0,50 punto;
- ✓ per ogni risposta errata: -0,25 punti;
- ✓ per ogni riposta non data: -0,15 punti.

I candidati sono classificati in ordine decrescente in base al punteggio complessivo del test.

Il test a risposta multipla si intende superato da coloro che si collocano nelle seguenti posizioni:

- nelle prime 80 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. A);
- nelle prime 120 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. B);
- nelle prime 100 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. C);
- nelle prime 30 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. D);
- nelle prime 100 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. E);
- nelle prime 120 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. F);
- nelle prime 100 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. G);
- nelle prime 120 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. H);
- nelle prime 50 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. I);
- nelle prime 80 ed *ex aequo* per il concorso di cui all'articolo 1, comma 1, lett. J);

B) QUESITI A RISPOSTA SINTETICA

Nella stessa giornata, al termine del test a risposta multipla tutti i candidati devono svolgere **due quesiti a risposta sintetica.**

La Commissione, al riguardo, predisporrà sei quesiti, due per ciascuna materia di cui ai punti 3, 4 e 5 degli specifici programmi allegati. I quesiti potranno avere per oggetto anche l'esame di un caso pratico.

I candidati dovranno svolgere **due elaborati a scelta su due diverse materie.**

Sono valutati i quesiti a risposta sintetica dei soli candidati che si sono collocati nelle posizioni utili sopra indicate nel test a risposta multipla.

Costituiscono causa di esclusione: l'aver svolto più di due quesiti; l'aver svolto due quesiti sulla medesima materia; o, più in generale, l'aver operato in qualunque altro modo che possa aver reso riconoscibile il proprio elaborato.

I due elaborati sono valutati fino a un **massimo di 60 punti**, attribuendo a ognuno fino a un massimo di 30 punti. La prova è superata da coloro che ottengono **un punteggio di almeno 15 punti in ciascuno degli elaborati**; sono, tuttavia, ammessi alla prova orale i candidati che hanno conseguito **in uno dei due quesiti un punteggio di almeno 13 punti, purché il punteggio complessivo non sia inferiore a 30 punti**.
Vengono valutate esclusivamente le prove dei candidati che abbiano svolto tutti e due i quesiti, secondo le predette indicazioni.

Nella valutazione dei quesiti le Commissioni verificano: 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).

Per lo svolgimento della prova scritta **non è consentito** l'uso di carta da scrivere, pubblicazioni, manuali, codici, codici commentati, raccolte normative, linee guida, vocabolari, testi, appunti di ogni genere, dizionari, nonché matite, penne o altri oggetti idonei alla scrittura, telefoni cellulari, calcolatrici elettroniche, *personal computer*, *smartphone*, *tablet*, *smartwatch* o altri dispositivi assimilabili idonei alla memorizzazione o trasmissione di dati. Durante lo svolgimento delle prove i candidati non possono comunicare tra loro.

La **prova scritta** è corretta garantendo l'anonimato dei candidati.

La durata complessiva della prova scritta è stabilita in **quattro ore**: 1 ora per lo svolgimento del test a risposta multipla e 3 ore per lo svolgimento dei quesiti a risposta sintetica.

6. **La votazione complessiva della prova scritta** risulta dalla somma dei due punteggi utili (test e quesiti).
7. I risultati della prova d'esame, comprensivi dell'esito del test a risposta multipla anche per i candidati che non si sono collocati in posizione utile ai sensi del precedente comma 5 lett. A),

saranno pubblicati in forma anonimizzata, attraverso l'indicazione del codice meccanografico di ciascun candidato generato in fase di presentazione della domanda di partecipazione, sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi) e sul Portale «*inPA*» (https://www.inpa.gov.it) ove sarà pubblicato un *link* di rinvio al sito istituzionale dell'Agenzia. Tale pubblicazione assume valore di notifica ad ogni effetto di legge.

8. Sul Portale «*inPA*» saranno pubblicate le modalità con cui saranno resi visibili il test a risposta multipla, i quesiti a risposta sintetica e i relativi punteggi attribuiti. Ai sensi del precedente comma 5, lett. A), i punteggi dei quesiti a risposta sintetica saranno presenti solo per gli elaborati dei candidati valutati in quanto utilmente collocati nel test a risposta multipla.

Articolo 7
Prova orale

1. **Per tutti i concorsi di cui all'articolo 1, comma 1, almeno quindici giorni prima dello svolgimento della prova orale,** verrà **pubblicato** sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi) e sul Portale «inPA» il **calendario con l'indicazione della modalità, della sede, del giorno e dell'ora in cui si svolgerà la prova orale.** Tale pubblicazione ha valore di notifica ad ogni effetto di legge.
2. I candidati ammessi alla prova orale dovranno inviare un *curriculum vitae*, entro 10 giorni dalla pubblicazione del calendario della prova orale, tramite mail all'indirizzo recruitment@acn.gov.it, con l'indicazione nell'oggetto: "*Concorso per 90 Esperti con orientamento tecnico scientifico, Lettera* (da specificare a cura del candidato) – *CV*".
3. **Per tutti i concorsi di cui all'articolo 1, comma 1, la prova orale consiste in un colloquio su tutte le materie indicate negli specifici programmi allegati** e in una **conversazione in lingua inglese**. Possono, altresì, formare oggetto di colloquio le esperienze professionali e/o di studio maturate. Il colloquio, nel quale potranno essere discussi con il candidato anche casi pratici, tende ad accertare: le conoscenze tecniche; la capacità comunicativa ed espositiva; la capacità di cogliere le interrelazioni tra gli argomenti; la capacità di giudizio critico. La conversazione in lingua inglese è volta a verificare il livello di conoscenza "B2" in relazione a un utilizzo dell'inglese come strumento di lavoro anche in considerazione dell'orientamento e del programma relativo allo specifico concorso.
4. **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**.
5. La Commissione, al termine di ciascuna sessione della prova orale, provvederà ad affiggere l'elenco dei candidati in forma anonimizzata, attraverso l'indicazione del codice meccanografico generato in fase di presentazione della domanda di partecipazione, con la relativa votazione attribuita.

Articolo 8
Diario delle prove d'esame

1. I candidati regolarmente iscritti on-line e non esclusi sono tenuti a presentarsi per sostenere le prove concorsuali a Roma nella sede, nel giorno e nell'ora comunicati ai sensi dell'articolo 5, comma 6.
2. I candidati devono presentarsi con un **valido documento di riconoscimento** e la **ricevuta rilasciata dal sistema informatico** al momento della compilazione *on-line* della domanda. Sono esclusi dallo svolgimento della prova d'esame i candidati che non sono in grado di esibire un valido documento di riconoscimento.
3. **L'assenza dalla sede di svolgimento della prova d'esame nella data e nell'ora stabilita, per qualsiasi causa, anche se dovuta a forza maggiore, comporta l'esclusione dal concorso.**

Articolo 9
Graduatorie

1. Sono considerati idonei i candidati che hanno conseguito i punteggi minimi previsti all'articolo 6, comma 5, e all'articolo 7, comma 4.
2. La Commissione forma le graduatorie di merito seguendo l'ordine decrescente di punteggio complessivo.
3. 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.
4. 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.
5. L'Agenzia si riserva la facoltà di utilizzare le graduatorie finali dei concorsi di cui all'articolo 1, comma 1, entro **due anni** dalla rispettiva data di approvazione.
6. **Le graduatorie finali dei vincitori e degli idonei, classificati in posizione non utile all'assunzione, nonché gli elenchi dei non idonei,** con l'indicazione del punteggio complessivo della prova scritta (test e quesiti) e quello della prova orale, **saranno pubblicate in forma anonimizzata**, attraverso l'indicazione del codice meccanografico di ciascun candidato generato in fase di presentazione della domanda di partecipazione sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) e alla Sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi) e sul Portale «*inPA*» (https://www.inpa.gov.it) sarà pubblicato un *link* di rinvio al sito istituzionale dell'Agenzia. Tale pubblicazione assume valore di notifica a ogni effetto di legge.

Articolo 10
Impiego e adempimenti

1. I vincitori dei concorsi di cui all'articolo 1, comma 1, lavoreranno a Roma e saranno impiegati, in particolare, in attività di carattere ispettivo, di analisi e di ricerca, studio, programmazione e progettazione nel campo di ogni profilo selezionato, svolgendo incarichi connotati da particolari livelli tecnici e di professionalità connessi alle specifiche funzioni dell'Agenzia.
2. 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 nonché inviata, tramite mail all'indirizzo recruitment@acn.gov.it, con l'indicazione nell'oggetto: "*Concorso per 90 Esperti con orientamento tecnico scientifico, Lettera* (da specificare a cura del candidato) – *Documentazione esperienza lavorativa*", la documentazione comprovante l'esperienza professionale richiesta per i concorsi di cui all'articolo 1, comma 1, lettere A), C), E), F), G), H), I) e J).
3. In relazione allo specifico contesto di impiego e laddove sussista per l'Agenzia l'esigenza di abilitare i vincitori dei predetti concorsi alla trattazione di informazioni classificate ai sensi dell'art. 42 della legge 3 agosto 2007, n. 124, l'Agenzia si riserva la possibilità di avviare, ai sensi dell'art. 25 del d.P.C.m. 6 novembre 2015, n. 5, le procedure per il rilascio del nulla osta di sicurezza (NOS).

Articolo 11
Assunzione e inquadramento

1. Le comunicazioni di avvio del procedimento di assunzione e inquadramento ed eventuali altre comunicazioni verranno indirizzate alla PEC fornita dal candidato in sede di presentazione della domanda.
2. I candidati utilmente classificati che siano in possesso dei requisiti di cui all'articolo 2, comma 1, del presente bando sono assunti, in prova, come:
   a) **Esperto, livello economico 1**, per il concorso di cui all'articolo 1, comma 1, lett. B) e D);
   b) **Esperto, livello economico 2**, per i concorsi di cui all'articolo 1, comma 1, lett. A); C); E); F); G); H); I) e J).
3. Al termine del periodo di prova della durata di sei mesi, le persone assunte, se riconosciute idonee, conseguono la conferma dell'assunzione con la stessa decorrenza di quella in prova.
4. L'accettazione dell'assunzione non può essere in alcun modo condizionata.
5. Le persone assunte 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 all'assunzione o in mancanza di giustificati motivi non prendono servizio entro il predetto termine, decadono dall'assunzione, come previsto dal d.P.C.m. n. 224 del 2021.

Articolo 12
Trattamento dei dati personali

1. Ai sensi dell'art. 13 del Regolamento (UE 2016/679 GDPR), si informano i candidati che i dati da loro forniti comunque raccolti saranno trattati dall'Agenzia, in qualità di titolare del trattamento, anche in forma automatizzata, per le sole finalità di gestione del concorso. Per i candidati che saranno assunti il trattamento proseguirà per le finalità inerenti alla gestione del rapporto di lavoro.
2. 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.
3. Soggetti autorizzati al trattamento sono le persone preposte alla procedura di selezione individuate nell'ambito della procedura medesima.
4. I dati forniti dai candidati compresi quelli sensibili e giudiziari (articoli 9 e 10, del GDPR) sono trattati, anche in forma automatizzata, per le finalità di gestione della selezione. In particolare, i dati idonei a rivelare lo stato di salute dei candidati sono trattati per l'adempimento degli obblighi previsti dalla legge 5 febbraio 1992, n. 104 e dalla legge 12 marzo 1999, n. 68. I dati di cui all'articolo 10 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.
5. Base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6.1 lett. e) del GDPR), l'assolvimento degli obblighi e l'esercizio dei diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (articoli 9.2 lett. b) del GDPR), il perseguimento di interessi pubblici rilevanti sulla base del diritto dell'Unione o degli Stati membri (articolo 9.2 lett. g) del GDPR) e le finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (articolo 9.2 lett. h) del GDPR).
6. Per il trattamento l'Agenzia potrà avvalersi di ulteriori società terze situate sul territorio dell'Unione europea, 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'articolo 28 del GDPR (c.d. Responsabili del trattamento).
7. 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.
8. Il trattamento dei dati ricevuti o raccolti dall'Agenzia per le finalità di selezione del personale avrà

durata pari alla durata del procedimento di selezione. Successivamente, i dati verranno rimossi dal sistema informatico utilizzato per le finalità di selezione e verranno esclusivamente conservati, senza alcun ulteriore trattamento, nell'archivio dell'Agenzia conformemente alla disciplina archivistica e per le altre finalità previste dalla normativa vigente, compresa la difesa in giudizio dell'Agenzia.

9. I dati relativi invece alle persone successivamente assunte saranno trattati dall'Agenzia per tutta la durata del rapporto di lavoro e per l'ulteriore tempistica richiesta dalla normativa applicabile in materia giuslavoristica, archivistica, pensionistica e fiscale.
10. Ai soggetti interessati spetta il diritto di accesso ai propri dati personali e gli altri diritti riconosciuti dalla normativa applicabile, tra i quali - ove previsto - 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 (articoli 15-22 del GDPR).
11. L'Agenzia ha nominato un Responsabile per la protezione dei dati (DPO). Tali diritti potranno essere fatti valere scrivendo direttamente all'Agenzia od inoltrando un'e-mail all'indirizzo dpo@acn.gov.it.
12. Ove, infine, il soggetto interessato dovesse ritenere lesi i propri diritti, è possibile rivolgersi direttamente al Garante per la protezione dei dati personali (Piazza Venezia n. 11 - Roma - protocollo@gpdp.it) o all'autorità di controllo competente per il proprio Paese di residenza, o anche adire la giurisdizione ordinaria.

Articolo 13
Responsabile del procedimento

1. L'Unità organizzativa responsabile del procedimento, anche ai fini dell'accesso agli atti, è il Servizio Risorse umane, strumentali e amministrazione generale dell'Agenzia. Il responsabile del procedimento è il Capo *pro tempore* di tale Servizio.

Articolo 14
Pubblicazione del bando

1. Il presente bando è pubblicato sul Portale «*inPA*» (https://www.inpa.gov.it) e sul sito istituzionale dell'Agenzia alla Sezione «*Amministrazione Trasparente/Bandi di concorso*» (https://www.acn.gov.it/portale/bandi-di-concorso) nonché alla sezione «*Lavora con noi*» (https://www.acn.gov.it/portale/lavora-con-noi).

Bruno Frattasi
28.07.2025
16:17:09
GMT+02:00

IL DIRETTORE GENERALE
Bruno Frattasi

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA A)

8 ESPERTI CON ORIENTAMENTO IN CLOUD ED EDGE COMPUTING E IN SISTEMI DI TELECOMUNICAZIONE DI NUOVA GENERAZIONE

1. **Architettura nazionale ed europea in materia di cybersicurezza**
   - Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
   - Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
   - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
   - Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).
2. **Fondamenti di informatica**
   - Linguaggi di Programmazione.
   - Fondamenti di Sistemi Operativi.
   - Algoritmi e Strutture Dati.
   - Fondamenti di *networking*. Il modello ISO OSI.
   - Architettura degli elaboratori.
3. **Sicurezza del software e dei sistemi**
   - Sicurezza delle applicazioni web: strumenti e metodologie (OWASP).
   - Sicurezza sotto i profili di disponibilità, integrità e riservatezza.
   - Tipologie di attacchi *cyber*.
   - La gestione del rischio *cyber*.
   - Metodologie e linee guida per i test di sicurezza (NIST, OSSTMM, OWASP, CIS).
4. **Architetture e sistemi abilitanti**
   - *Architetture Cloud* ed *Edge Computing*.
   - Architetture di sicurezza e sistemi IT.
   - Sistemi di sicurezza (IPS/IDS, *Firewall*, WAF, *Endpoint protection*, etc.).
   - Sistemi di virtualizzazione.
   - Sistemi di autenticazione.

5. Reti di Telecomunicazione

- Standard reti mobili cellulari (GSM, 4G/5G).
- Reti cellulari private con particolare attenzione a soluzioni architetturali per il 5G.
- Architetture reti non-3GPP (es.: Wi-FI, reti ad-hoc).
- Fondamenti reti fisse ottiche (es.: GPON).
- Fondamenti di virtualizzazione per le reti: *Software Defined Networking* (SDN), *Network Function Virtualization* (NFV), *OpenRAN*, *Network Slicing*, Architettura ETSI MANO (*NFV Management Orchestration*).

PROVA SCRITTA

La prova scritta consiste:

- **Test a risposta multipla** sulle materie di cui ai punti 1, 2, 3, 4 e 5 del programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai punti 3, 4 e 5 del programma.

PROVA ORALE

La prova orale verterà su:

- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA B)

12 ESPERTI CON ORIENTAMENTO IN SISTEMI DI INTELLIGENZA ARTIFICIALE

1. **Architettura nazionale ed europea in materia di cybersicurezza**
   - Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
   - Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
   - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
   - Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).
2. **Fondamenti di informatica**
   - Linguaggi di Programmazione.
   - Fondamenti di Sistemi Operativi.
   - Algoritmi e Strutture Dati.
   - Fondamenti di *networking*. Il modello ISO OSI.
   - Architettura degli elaboratori.
3. **Fondamenti di cybersicurezza - Metodologie per la gestione del rischio cyber**
   - Tipologie di attacchi cyber e principali tool e tecniche utilizzate nell'ambito del *Vulnerability Assessment* e *Penetration Testing*.
   - Protocolli per la sicurezza delle reti (SSL/TLS, IPSEC, etc.).
   - Aspetti di cybersicurezza dei sistemi basati su tecnologia *Cloud* ed *Edge*.
4. **Teoria dell'Intelligenza Artificiale e Machine Learning**
   - Algoritmi di apprendimento supervisionato e non supervisionato.
   - Reti neurali artificiali e metodi di apprendimento.
   - Tecniche e metodi di valutazione di modelli.
   - Fondamenti di AI generativa.
   - Fondamenti di *Natural Language Processing* basato su *machine learning*.
   - Fondamenti di *Reinforcement Learning*.
   - Fondamenti di *Safety* e *Security* dei modelli AI.

5. Sistemi di Intelligenza artificiale

- Metodi e linguaggi di programmazione.
- Ciclo di vita dei modelli AI.
- *Framework* di sviluppo e di ottimizzazione dei modelli AI.
- Tecnologie di sviluppo e di erogazione di applicazioni AI, anche in contesto cloud ed embedded.
- Architetture, tecnologie e paradigmi computazionali per l'*High Performance Computing* (HPC).
- Fondamenti di cybersecurity dei sistemi AI.
- Metodologie e linee guida per i test di cybersicurezza su sistemi AI (NIST, OWASP, CSA).

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai punti 1, 2, 3, 4 e 5 del programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai punti 3, 4 e 5 del programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- AI Act (Regolamento (UE) 2024/1689);
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate;
- eventuale approfondimento dell'argomento della tesi di laurea.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA C)

10 ESPERTI CON ORIENTAMENTO IN ISPEZIONI DI CYBERSICUREZZA

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. Attività di verifica e ispezione di competenza dell'Agenzia per la cybersicurezza nazionale

- Perimetro di sicurezza nazionale cibernetica (PSNC).
- Accreditamento dei laboratori di prova (LAP) e relativa Determinazione del Direttore generale dell'ACN n. 10829 del 11 agosto 2022.
- NIS2, con particolare riferimento alla Determinazione del Direttore generale dell'ACN n. 164179 del 14 aprile 2025.

4. Attività di *audit*

- Linee guida per audit di sistemi di gestione (ISO 19011).
- Conoscenza dello standard internazionale ISO 27001 e connessi processi di audit.

5. Gestione del rischio

- Conoscenza dello standard internazionale ISO 31000 (principi e linee guida per la gestione del rischio).

- Conoscenza dello standard internazionale ISO 27005 (linee guida per la gestione dei rischi relativi alla sicurezza delle informazioni, alla cybersecurity e alla protezione della privacy).

PROVA SCRITTA

La prova scritta consiste:

- **Test a risposta multipla** sulle materie di cui ai punti 1, 2, 3, 4 e 5 del programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai punti 3, 4 e 5 del programma.

PROVA ORALE

La prova orale verterà su:

- tutte le materie previste per la prova scritta;
- principi di cybersicurezza:
  - la sicurezza sotto i profili della disponibilità, riservatezza e integrità;
  - la sicurezza del software, delle reti e dei sistemi e relative soluzioni tecnologiche (IDS/IPS, Firewall, WAF, VPN, *Endpoint protection*, SIEM, etc.);
  - sistemi di autenticazione;
  - i protocolli e le applicazioni della crittografia;
  - le attività di *security assessment*;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA D)

3 ESPERTI CON ORIENTAMENTO IN CRITTOGRAFIA

1. **Architettura nazionale ed europea in materia di cybersicurezza**
   - Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
   - Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
   - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
   - Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).
2. **Fondamenti di informatica**
   - Linguaggi di Programmazione.
   - Fondamenti di Sistemi Operativi.
   - Algoritmi e Strutture Dati.
   - Fondamenti di *networking*. Il modello ISO OSI.
   - Architettura degli elaboratori.
3. **Crittografia Simmetrica, Algoritmi di Hashing e Generatori di Numeri Casuali**
   - Cifrari a blocchi e modalità di operazione.
   - Cifrari a flusso.
   - Funzioni di *hash* e codici di autenticazione dei messaggi (MAC).
   - Generatori di numeri casuali (RNG).
   - Elementi di crittoanalisi e attacchi *side-channel*.
4. **Crittografia a Chiave Pubblica Classica e Post-Quantum**
   - Logaritmo discreto e Diffie-Hellman su campi e curve ellittiche.
   - Fattorizzazione di interi e RSA.
   - Algoritmi di firma digitale.
   - Elementi di crittoanalisi e attacchi *side-channel*.
   - Algoritmi crittografici *post-quantum* (KEM, firma digitale).

- Crittografia quantistica e distribuzione quantistica delle chiavi (QKD).

5. Applicazione crittografiche per la cybersicurezza

- Sicurezza protocolli di rete (SSL/TLS, IPSEC, etc.).
- Implementazioni di algoritmi simmetrici e a chiave pubblica.
- *Public Key Infrastructure* (PKI).
- Cifratura in ambito cloud.
- Protocolli e applicazioni della crittografia (MPC, ZKP, OT, VCs, etc.).
- *Blockchain, smart contract* e valute digitali.

PROVA SCRITTA

La prova scritta consiste:

- **Test a risposta multipla** sulle materie di cui ai punti 1, 2, 3, 4 e 5 del programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai punti 3, 4 e 5 del programma.

PROVA ORALE

La prova orale verterà su:

- tutte le materie previste per la prova scritta;
  - tutte le materie previste per la prova scritta;
  - principi di cybersicurezza:
    - la sicurezza sotto i profili della disponibilità, riservatezza e integrità;
    - la sicurezza del software, delle reti e dei sistemi e relative soluzioni tecnologiche (IDS/IPS, Firewall, WAF, VPN, *Endpoint protection*, SIEM, etc.);
    - sistemi di autenticazione;
    - le attività di *security assessment*;
  - una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA E)

10 ESPERTI CON ORIENTAMENTO IN VALUTAZIONE DELLA SICUREZZA E CERTIFICAZIONE DI SISTEMI E COMPONENTI OT E ICT

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. Standard, norme e metodologie

- Principi generali sui *Common Criteria for Information Technology Security Evaluation* (ISO/IEC 15048:2022) e relativa metodologia (ISO/IEC 18045).
- Principi generali degli standard ISO 27001, ISO 17025, ISO 17065.
- Metodologie di test a tempo fisso (FitCEM): principi generali ed esempi.
- *Framework* di sicurezza per sistemi di controllo industriale. Principi generali della norma ISA/IEC 62443.

4. Principi di cybersecurity

- Sicurezza delle informazioni: riservatezza, integrità e disponibilità.
- Sicurezza delle reti.
- Sicurezza dei sistemi operativi.
- Sicurezza delle applicazioni.

- Attacchi *cyber*: tattiche, tecniche e procedure.
- La gestione del rischio *cyber*.
- Crittografia come strumento di cybersicurezza.

5. Architetture di sicurezza IT e OT

- Architetture di sicurezza e sistemi IT (IDS/IPS, Firewall, WAF, VPN, *Endpoint protection*, SIEM, etc.).
- Architetture Cloud: aspetti di sicurezza, tipologie di servizi e modelli di deployment.
- Architetture ICS: *Purdue Model* e aspetti di sicurezza dei sistemi di controllo industriale.
- Principali protocolli in ambito ICS e aspetti di sicurezza.
- Sistemi di virtualizzazione: aspetti di sicurezza.
- Sistemi di autenticazione.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- tecniche e metodologie di cybersicurezza:
  - *framework* Nazionale per la Cybersecurity e la *Data Protection*;
  - linguaggi di programmazione (imperativi, di scripting, orientati agli oggetti) e tecniche per lo sviluppo di codice sicuro;
  - sicurezza delle applicazioni web: strumenti e metodologie (OWASP);
  - tipologie di vulnerabilità software (*buffer overflow, use-after-free*, etc.);
  - tipologie di vulnerabilità in applicazioni web (OWASP Top 10);
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA F)

12 ESPERTI CON ORIENTAMENTO IN GESTIONE E REALIZZAZIONE DI PROGRAMMI INDUSTRIALI, TECNOLOGICI E DI RICERCA NEL CAMPO DELLA CYBERSICUREZZA O DELL'ICT

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. Fondamenti di cybersicurezza

- Principi e controlli di sicurezza.
- Sistemi di sicurezza.
- Tipologie di attacchi *cyber*.
- Il ruolo dei SOC, CSIRT e ISAC.
- Metodologie e *framework* di analisi e gestione del rischio cyber.

4. Gestione progettuale

- Metodologie di gestione progettuale.
- Elementi di pianificazione finanziaria e operativa.
- Gestione del *team* di lavoro, gestione degli *stakeholder*.
- Utilizzo di strumenti di pianificazione, controllo e monitoraggio.
- Tecniche e modelli di reportistica.

- Gestione dei conflitti e delle scadenze.

5. Programmi di innovazione tecnologica e tecnologie emergente

- Elementi di Autonomia Tecnologica.
- Elementi e approcci di trasferimento tecnologico (es. incubazione, accelerazione e promozione di nuova imprenditorialità).
- *Machine Learning, Artificial Intelligence*, ivi inclusi modelli supervisionati, non supervisionati e large-language model.
- *Quantum Computing, Quantum Communication* e *Quantum Sensing*.
- *High Performance Computing*.
- *Cybersecurity* applicata alle tecnologie spaziali.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA G)

10 ESPERTI CON ORIENTAMENTO IN GESTIONE E REALIZZAZIONE DI PROGETTI IT

1. **Architettura nazionale ed europea in materia di cybersicurezza**
   - Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
   - Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
   - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
   - Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).
2. **Fondamenti di informatica**
   - Linguaggi di Programmazione.
   - Fondamenti di Sistemi Operativi.
   - Algoritmi e Strutture Dati.
   - Fondamenti di *networking*. Il modello ISO OSI.
   - Architettura degli elaboratori.
3. **Informatica e cybersicurezza**
   - Architettura degli elaboratori, sistemi operativi, basi dati relazionali e NoSQL.
   - Fondamenti di algoritmi e linguaggi di programmazione.
   - Reti di comunicazione e sistemi di sicurezza.
   - Sistemi di gestione centralizzati (*Active Directory*, Sistemi IAM, OAuth 2.0, SAML, *Kerberos*, etc.).
   - Metodologie e *framework* di analisi e gestione del rischio *cyber*.
   - Ambienti di esecuzione e di gestione (DevOps, *Continuous Integration*, *Continuous Delivery*).
   - Attività di monitoraggio di eventi cyber e risposta e gestione di incidenti.
4. **Programmazione, architetture dati e intelligenza artificiale**
   - Analisi e progettazione del *software*.
   - Architetture a servizi e microservizi.
   - Tecniche per lo sviluppo di codice sicuro.

- Architetture delle piattaforme dati, tecniche e strumenti di acquisizione e gestione di big-data.
- Elementi di modellazione statistica, *Machine Learning*, *Artificial Intelligence*.
- Problemi di classificazione e predizione, elaborazione del linguaggio naturale.
- Modelli supervisionati, non supervisionati, *Large-Language Model*.

5. IT project management

- Elementi di gestione di un progetto IT.
- Gestione del *team* di lavoro.
- Utilizzo di strumenti di controllo e monitoraggio.
- Le metodologie e il ciclo di sviluppo: definizione dei requisiti, progettazione, realizzazione, collaudo e go-live.
- Modelli e processi di gestione applicativa.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA H)

12 ESPERTI CON ORIENTAMENTO IN GESTIONE DEL RISCHIO CYBER

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. Fondamenti di cybersicurezza

- Rappresentazione delle informazioni.
- Modello funzionale "*Purdue Model for Control Hierarchy*" (in relazione all'OT).
- Sistemi di sicurezza (IPS/IDS, Firewall, WAF, *Endpoint protection*).
- Sistemi di autenticazione.
- Sistemi di gestione centralizzati (*Active Directory*, Sistemi IAM, OAuth 2.0, SAML, Kerberos).
- Sicurezza sotto i profili di disponibilità, integrità e confidenzialità.
- Sicurezza delle applicazioni *web*: strumenti e metodologie (OWASP).

4. Modellazione librerie per la gestione del rischio cyber

- Basi dati relazionali e NoSQL.
- Tipologie di minacce informatiche e loro impatti (ad es. *ransomware*, DDoS, *phishing*).
- *Framework* per la descrizione dei tipici passi utilizzati dagli attaccanti per l'esecuzione di attacchi informatici (*Cyber Kill Chain*).

- *Framework* per la modellazione/descrizione delle TTP utilizzate dagli attaccanti e relative contromisure difensive (*MITRE ATT&CK* e *MITRE D3FEND*).
- Controlli di mitigazione del rischio cyber e loro applicazione, anche con riferimento a standard/norme di settore (ad es. NIST 800-53, CIS, CCM, ISO/IEC 27002, IEC 62443, CSF2.0).
- Metodologie e approcci per la correlazione di rischi e integrazione/fusione di informazioni provenienti da fonti differenti.
- Metodi e modelli per il supporto alle decisioni manageriali.
- Metodi per la modellazione di interdipendenze e rischi tra diversi sistemi.
- Correlazione tra servizi/*asset* (ICT e OT), minacce e controlli di mitigazione dei rischi *cyber*.
- Scenari di rischio: concetti abilitanti, progettazione e loro utilizzo per l'identificazione di sequenze/combinazioni di eventi *cyber* avversi e conseguente riduzione del rischio *cyber*.
- Utilizzo di *dashboard* e strumenti di *business intelligence* per il *reporting*.

5. Gestione del rischio cyber

- Il processo generale di gestione del rischio (UNI ISO 31000).
- La gestione dei rischi legati alla sicurezza delle informazioni (ISO/IEC 27001 e ISO/IEC 27005).
- Campo di applicazione e contesto nella gestione del rischio.
- Identificazione del rischio.
- Analisi del Rischio.
- Ponderazione del Rischio.
- Trattamento del rischio.
- *Reporting*: esempi e relativi contenuti.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA I)

5 ESPERTI CON ORIENTAMENTO IN ANALISI DELLA MINACCIA CYBER

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. *Cyber Threat Intelligence* e *Cyber Threat Modeling*

- Il ciclo di intelligence: livelli tattico, operativo e strategico.
- *Framework* e modelli di analisi della minaccia: *MITRE ATT&CK*, *Kill Chain*, *Diamond Model*.
- Identificazione e analisi di TTP (*Tactics, Techniques and Procedures*).
- Indicatori di compromissione (IoC) e indicatori di attacco (IoA).
- Analisi del comportamento degli attori della minaccia: motivazioni, obiettivi, capacità.
- Collegamenti tra *Cyber Threat Actors* e loro evoluzione nel tempo.

4. Analisi strategica e previsione della minaccia

- Framework per il supporto decisionale in ambito cyber a livello politico-strategico.
- Normativa nazionale ed europea in materia di cybersicurezza (PSNC, NIS2, L90, DORA).
- *Cyber diplomacy* e cooperazione internazionale (es. NATO, UE, ONU).
- Dottrina cyber dei principali Paesi avanzati (es. USA, Russia, Cina, etc).

- Approcci e metodologie per l'analisi strategica *cyber*.
- Analisi multilivello degli eventi (tecnico, operativo, strategico).
- Metodi per la contestualizzazione geopolitica e settoriale delle minacce.
- *Supply chain security*: strategie, normative e approcci di mitigazione del rischio.
- Il processo di attribuzione *cyber*.

5. Innovazione tecnologica e rischio *cyber*

- Fondamenti di AI, *Blockchain* e *Quantum Computing*.
- *Artificial Intelligence* e *cybersecurity*: utilizzo in ambito prevenzione e risposta *cyber*.
- Blockchain e cybersicurezza: potenzialità e rischi in ambito cybersicurezza.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.

PROGRAMMA

CONCORSO DI CUI ALL'ARTICOLO 1, COMMA 1, LETTERA J)

8 ESPERTI CON ORIENTAMENTO IN DATA ANALYSIS E PRODUZIONE DI STATISTICHE SULLA MINACCIA CYBER

1. Architettura nazionale ed europea in materia di cybersicurezza

- Agenzia per la cybersicurezza nazionale (decreto-legge 14 giugno 2021 n. 82).
- Perimetro di sicurezza nazionale cibernetica (decreto-legge 21 settembre 2019, n. 105; decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81; decreto del Presidente della Repubblica 5 febbraio 2021, n. 54; decreto del Presidente del Consiglio dei ministri 15 giugno 2021; decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92).
- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (legge 28 giugno 2024, n. 90).
- Normativa in materia di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva (UE) 2022/2555 (NIS 2) recepita con decreto legislativo 4 settembre 2024, n. 138).

2. Fondamenti di informatica

- Linguaggi di Programmazione.
- Fondamenti di Sistemi Operativi.
- Algoritmi e Strutture Dati.
- Fondamenti di *networking*. Il modello ISO OSI.
- Architettura degli elaboratori.

3. Data Analysis e Statistica applicata alla cyber security

- Fondamenti di statistica descrittiva e inferenziale applicata all'analisi di dati di cybersicurezza.
- Tecniche di *data preparation* e *data cleaning*.
- Analisi esplorativa dei dati e individuazione di anomalie e *outlier*.
- Visualizzazione dei dati (*data visualization*).
- Modellazione statistica per l'analisi predittiva delle minacce informatiche.
- Metriche e KPI per la misurazione della minaccia *cyber*.

4. Tecnologie e strumenti per la manipolazione e l'analisi dei dati

- Linguaggi e strumenti per l'analisi dei dati: Python (*pandas*, *numpy*, *scikit-learn*), R, SQL.
- Database relazionali e NoSQL.
- Tecniche e strumenti per l'estrazione e la trasformazione dei dati da sorgenti eterogenee.
- Pipeline di analisi dei dati e automazione dei *workflow* analitici.

- Utilizzo di dashboard e strumenti di business intelligence (es. *Power BI, Tableau, Grafana*) per il *reporting*.

5. Cyber Threat Landscape e analisi delle minacce

- Tipologie di minacce informatiche (*ransomware*, DDoS, *phishing*, etc.).
- *Framework* e modelli di analisi della minaccia: *MITRE ATT&CK, Kill Chain, Diamond Model*.
- Indicatori di compromissione (IoC): classificazione, raccolta, ciclo di vita.
- Correlazione tra eventi di sicurezza e profilazione della minaccia.

PROVA SCRITTA

La prova scritta consiste:
- **Test a risposta multipla** sulle materie di cui ai seguenti punti 1, 2, 3, 4 e 5 del presente programma e di Lingua inglese - Livello B2;
- **Due quesiti a risposta sintetica a scelta** tra i sei proposti dalla Commissione, sulle materie di cui ai seguenti punti 3, 4 e 5 del presente programma.

PROVA ORALE

La prova orale verterà su:
- tutte le materie previste per la prova scritta;
- una conversazione in lingua inglese volta a verificare il livello di conoscenza B2 anche in relazione a un utilizzo dell'inglese come strumento di lavoro;
- eventuale esposizione delle esperienze professionali e/o di studio maturate.