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

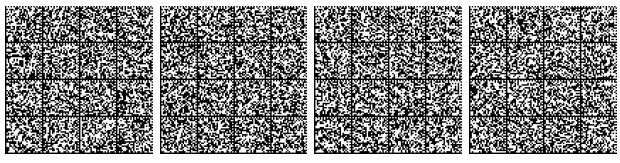
- Regolamento concernente le procedure, le modalità e i termini da seguire ai fini delle valutazioni da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione (DPR n. 54/2021)
- Schema nazionale per la valutazione e certificazione della sicurezza nel settore della 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



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

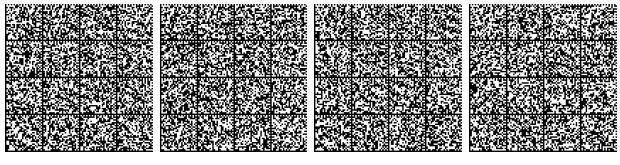
PROVA ORALE

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.



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

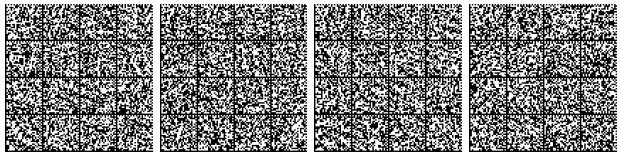
- Elettronica Analogica e Digitale
- Lettura e comprensione di schemi elettrici
- Conoscenza generale componentistica elettronica
- Linguaggi di descrizione dell'hardware e logiche programmabili
- Utilizzo strumentazione elettronica di test e tecniche di misura
- Tecniche e strumenti di Reverse Engineering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



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

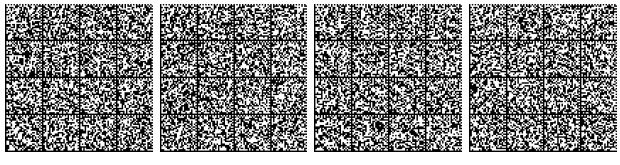
PROVA ORALE

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.



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

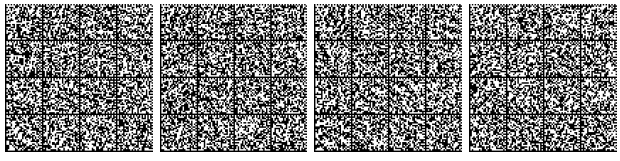
- Linguaggi di Programmazione (imperativi, di scripting e orientati agli oggetti)
- Tecnologie web
- Sistemi Operativi (Windows, OSX, Linux, Android, iOS)
- Algoritmi e Strutture Dati
- Database Relazionali e NoSQL
- Architettura degli Elaboratori e linguaggi macchina
- Reti di Calcolatori e protocolli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



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.

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

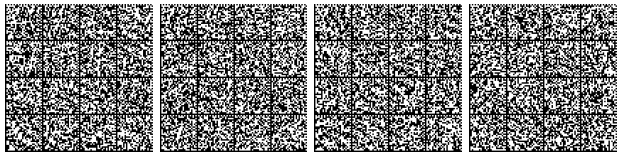
PROVA ORALE

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.



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

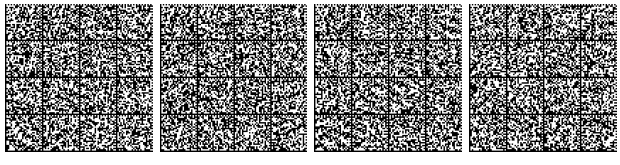
- Linguaggi di Programmazione (imperativi, di scripting e orientati agli oggetti)
- Sistemi Operativi (Windows, Linux, OSX, Android, iOS)
- Algoritmi e Strutture Dati
- Sicurezza protocolli di rete (SSL/TLS, IPSEC, …)
- Architettura degli elaboratori e linguaggi macchina

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



Applicazioni Crittografiche

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

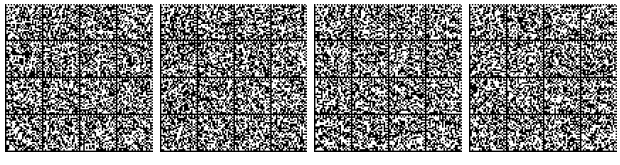
PROVA ORALE

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.



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*

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.

22E01638