ICT Security Specialist - SS.22

1. Descrizione del profilo:

È la figura che, rispondendo all'ICT Security Manager, assicura l'implementazione della politica di sicurezza delle informazioni aziendali, valuta i rischi di sicurezza delle informazioni ed i requisiti per soddisfare gli obiettivi di controllo e monitoraggio dell'IT security. Implementa e presidia soluzioni di sicurezza, proponendo ed implementando i necessari aggiornamenti. È riconosciuto come l'esperto tecnico della sicurezza ICT dai colleghi e consiglia, supporta e fornisce addestramento e consapevolezza sul tema della cyber security.

I compiti principali saranno:

- analizzare i rischi relativi alla sicurezza delle informazioni e alle minacce cyber;
- contribuire all'acquisizione di informazioni inerenti la comparsa di nuovi pericoli;
- svolgere attività di monitoraggio, audit tecnici e normativi relativi alla sicurezza delle informazioni;
- fornire supporto e definire procedure per l'applicazione di soluzioni di sicurezza delle informazioni;
- consigliare, supportare, informare e fornire addestramento e consapevolezza sulle minacce cyber e sulla sicurezza delle informazioni;
- emettere preallarmi, allerte, annunci;
- gestire e documentare eventuali incidenti di sicurezza delle informazioni;
- redigere documentazione e reportistica utile al conseguimento o al mantenimento di certificazioni o al soddisfacimento di normative;
- mantenere e far evolvere i presidi e le tecnologie di protezione / sicurezza nell'ambito di riferimento;
- contribuire alla definizione degli standard di sicurezza.

2. Livello di inquadramento contrattuale

È prevista l'assunzione con **contratto a tempo indeterminato,** CCNL Industria metalmeccanica privata e della installazione di impianti, con inquadramento contrattuale e retributivo dal livello C3 (campo professionale C "Ruoli tecnico specifici") al livello B3 (campo professionale B "Ruoli specialistici e gestionali"), commisurato alle esperienze e competenze del candidato.

3. Requisiti specifici del profilo per partecipare alla selezione

Per partecipare alla procedura di selezione è necessario dimostrare di possedere:

- diploma di istruzione secondaria di secondo grado di durata quinquennale;

- comprovata esperienza lavorativa di almeno 24 mesi (in parte anche in modalità tirocinio ordinario) nel settore dell'IT Security (vedi punto "4. Conoscenze acquisite ").

4. Conoscenze acquisite

Per partecipare alla procedura di selezione è necessario dimostrare di possedere sufficienti conoscenze di:

- gestione degli incidenti informatici (triage, indicatori di compromissione, best practice di sicurezza informatica);
- analisi malware, analisi forense e cyber threat intelligence, analisi e valorizzazione di dati e della gestione del rischio cyber;
- metodi e tecniche per la sicurezza dei dati, dei sistemi e delle applicazioni software (disponibilità, confidenzialità e integrità, crittografia, tipologie di attacchi cyber e le relative tattiche, tecniche e procedure);
- modelli di governance per la business continuity, la data protection e il cyber risk management;
- normative, leggi e regolamenti di riferimento (es. standard ISO 27001, protezione dati personali, regolamentazione AgID);
- modelli organizzativi per la difesa proattiva (ISAC, CERT, CSIRT);
- in merito all'esercizio di attività pregresse di detenere conoscenze inerenti alla gestione dei sistemi IT, del networking e dei dispositivi IOT;
- conoscenza della lingua inglese.

5. Skill richiesti

- autonomia nelle attività
- capacità di elaborare linee guida e report
- capacità di lavorare in gruppo
- gestione dell'imprevisto
- problem solving
- senso critico

6. Costituiranno ulteriori elementi positivi di valutazione

- Diploma di Laurea triennale preferibilmente in materie scientifiche;
- Possesso di certificazioni specifiche in relazione alla sicurezza delle informazioni (CompTIA +, CompTIA Network +, CompTIA Security +, CISSP, CSX, CISA, CISM, ISO27001 LA, CEH, ...);
- conoscenza dell'architettura normativa nazionale cyber e i cybersecurity framework internazionali, come per es.:
  - il 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);
  - la strategia europea in materia di cybersicurezza;

  - le autorità nazionali ed europee competenti in materia di cybersicurezza;
  - la legge istitutiva dell'Agenzia per la cybersicurezza nazionale (D.L. n. 82/2021);
  - la strategia nazionale di cybersicurezza 2022-2026;
- conoscenza di framework per le attività di red e blue team testing;
- metodi e tecniche per la protezione cyber delle infrastrutture critiche materiali ed immateriali;
- Partecipazione ad eventi specifici sui temi inerenti la cyber security da discutere durante il colloquio.