JOB DESCRIPTION FUNZIONARIO

Sicurezza Informatica e Intelligenza Artificiale

AREA DEI FUNZIONARI E DELLA ELEVATA QUALIFICAZIONE

<table>
<tr><td>Area</td><td colspan="2">Funzionari e della Elevata Qualificazione</td></tr>
<tr><td>Profilo professionale</td><td colspan="2">Specialista Sicurezza Informatica e Intelligenza Artificiale</td></tr>
<tr><td rowspan="8">Competenze trasversali (Rif. D.M. 28 Giugno 2023)</td><td>Capire il contesto pubblico</td><td>Livello di complessità</td></tr>
<tr><td>• Consapevolezza del contesto
• Soluzione dei problemi
• Consapevolezza digitale
• Orientamento all'apprendimento</td><td>• 3
• 3
• 3
• 3</td></tr>
<tr><td>Interagire nel contesto pubblico</td><td>Livello di complessità</td></tr>
<tr><td>• Comunicazione
• Collaborazione
• Orientamento al servizio
• Gestione delle emozioni</td><td>• 3
• 3
• 3
• 3</td></tr>
<tr><td>Realizzare il valore pubblico</td><td>Livello di complessità</td></tr>
<tr><td>• Affidabilità
• Accuratezza
• Iniziativa
• Orientamento al risultato</td><td>• 3
• 3
• 3
• 3</td></tr>
<tr><td>Gestire le risorse pubbliche</td><td>Livello di complessità</td></tr>
<tr><td>• Gestione dei processi
• Guida del gruppo
• Sviluppo dei collaboratori
• Ottimizzazione delle risorse</td><td>• 3
• 1-3
• 1-3
• 3</td></tr>
<tr><td>Scopo organizzativo</td><td colspan="2">Garantire la gestione, l’evoluzione e la messa in sicurezza dell’infrastruttura tecnologica dell’Ente, assicurando il corretto funzionamento dei sistemi informativi, la cybersicurezza, la continuità operativa e il supporto tecnico avanzato agli utenti interni.
Funzionario esperto nella governance dei processi al fine di rafforzare la resilienza dell’Ente e la sicurezza delle infrastrutture ICT dell’Ente in accordo alle normative di settore. E’ in grado di mettere in atto misure organizzative finalizzate all’analisi dei rischi, gestione degli incidenti per garantire l’affidabilità, la continuità operativa, la protezione dei dati e dei sistemi informatici, assicurando la conformità alle normative vigenti e il supporto tecnico-specialistico alle strutture interne. E’ in grado inoltre di implementare soluzioni basate su modelli di AI al fine di ottimizzare e innovare i processi dell’Ente, la gestione dei dati con il rispetto delle regole imposte dalla compliance normativa di settore.</td></tr>
<tr><td>Conoscenze e competenze richieste</td><td colspan="2">• Conoscenza approfondita di sistemi operativi server (Windows Server, Linux) e infrastrutture di rete (TCP/IP, VLAN, VPN, firewall, routing).</td></tr>
</table>

	• Conoscenza dei principi di cybersecurity: gestione vulnerabilità, hardening, autenticazione multilivello, crittografia, monitoraggio eventi, audit di sicurezza. • Esperienza nell'amministrazione di Active Directory, DNS, DHCP, GPO e servizi di directory. • Conoscenza di virtualizzazione (AHV, KVM), containerizzazione e sistemi di storage (SAN/NAS). • Capacità di gestione e monitoraggio di sistemi di backup, disaster recovery, business continuity. • Conoscenza della normativa di riferimento: GDPR, misure minime AgID, Linee guida sulla sicurezza ICT, standard ISO/IEC 27001 e NIS2. • Capacità di utilizzo di strumenti SIEM, sistemi di logging centralizzato, antivirus/EDR, firewall di nuova generazione. • Competenze nell'analisi e risoluzione di incidenti di sicurezza (incident response) • Conoscenza della sicurezza nei modelli AI, AI governance e machine learning applicato alla cybersecurity. • Competenze informatiche relative all'uso degli applicativi di ufficio e di specifici applicativi web in relazione ai processi gestiti • Conoscenze linguistiche
Autonomia operativa e responsabilità	• Elevata capacità di analisi di problemi complessi in ambito ICT e sicurezza. • Autonomia nell'impostare, eseguire e monitorare interventi tecnici su sistemi critici. • Capacità di programmazione e pianificazione delle attività di manutenzione, aggiornamento e potenziamento dell'infrastruttura. • Responsabilità nella gestione dei sistemi centrali, dei dati e della sicurezza informatica dell'Ente. • Gestione delle priorità in situazioni di emergenza, incidenti di sicurezza o criticità operative. • Capacità di comunicazione tecnica verso colleghi, dirigenti, fornitori e stakeholder informatici. • Capacità di gestione dei conflitti e delle situazioni di stress durante eventi critici ICT. • Abitudine all'aggiornamento continuo in un settore altamente dinamico come la cybersecurity.
Risorse Umane	• Capacità di gestione delle risorse sottoposte e di coordinamento di gruppi di lavoro • Capacità di coordinare tecnici, collaboratori e gruppi di lavoro su progetti ICT complessi. • Supporto tecnico-specialistico alle altre unità organizzative, con funzione di riferimento interno per la sicurezza informatica.
Relazioni interne ed esterne	• Relazioni interne di natura negoziale e complessa

	• Costanti rapporti con tutte le unità dell'Ente al fine di gestire processi intersettoriali • Relazioni esterne con altre istituzioni, private e pubbliche • Relazioni interne trasversali e continuative con tutte le unità dell'Ente per la gestione dei sistemi informativi condivisi. • Rapporti con fornitori ICT, provider di servizi, system integrator e consulenti di sicurezza. • Rapporti con enti pubblici, CERT, istituzioni e organismi nazionali per attività di sicurezza informatica, segnalazione incidenti e compliance normativa.