

Il tuo futuro nel nostro. Il tuo talento per i nostri valori!

Vuoi entrare a far parte della Società garante della fede pubblica in Italia ed essere protagonista di importanti progetti per la trasformazione del Paese?

Siamo alla ricerca di risorse altamente motivate, proattive, dotate di una forte passione, integrità e che condividano la nostra mission ed i nostri valori.

Ci impegniamo a creare un ambiente sicuro e inclusivo, basato sul rispetto reciproco e sulla valorizzazione delle diversità, offrendo pari opportunità di lavoro a tutti i candidati qualificati.

CHI SIAMO?

Siamo una realtà industriale e tecnologica unica, poliedrica ed in continua evoluzione. Racchiudendo tradizione ed innovazione, progettiamo, sviluppiamo e realizziamo prodotti di sicurezza e soluzioni tecnologiche integrate a tutela della fede pubblica, a supporto dello Stato, delle Imprese e dei Cittadini.

4 siti produttivi, oltre 1.600 dipendenti, l'Istituto Poligrafico e Zecca dello Stato (IPZS) sviluppa soluzioni per l'identità digitale dei cittadini

N. 2 Network & Security

DI COSA TI OCCUPERAI?

Presso la Struttura IT ti occuperai principalmente di gestire l'installazione, configurazione, supervisione e manutenzione dei sistemi network e degli apparati di security IT includendo attività quali l'integrazione sistemistica HW/SW, la gestione delle reti, la gestione di aggiornamenti, le evoluzioni infrastrutturali delle reti e il supporto tecnico/operativo ai team di IT System Specialist Application e di sviluppo applicativo.

Sarai inoltre coinvolto nelle seguenti attività:

- Gestire le eventuali problematiche network e di sicurezza connesse ad una specifica tecnologia applicativa, ai sistemi middleware e all'integrazione con i database relazionali;
- Mantenere contatti diretti con il produttore delle tecnologie network e di sicurezza;
- Collaborare con le strutture interessate per la stesura della documentazione tecnica di progetto, curandone l'implementazione finale;
- Implementare le azioni preventive mirate ad assicurare il servizio di rete e ad ottimizzare le prestazioni dei flussi di comunicazione sia interni sia verso l'esterno;
- Applicare le procedure di qualità per reti cablate e wireless e garantire un adeguato livello di sicurezza della rete;
- Gestire le problematiche di rete effettuando i relativi test di performance e resilienza ai fault;
- Gestire l'erogazione di servizi di comunicazione in rete ed il relativo supporto operativo per la parte dati (eventualmente integrata con la fonia VoIP), verificando l'adeguatezza dei sistemi di rete e garantendo la gestione del rischio in linea con le direttive aziendali;

- Produrre documenti di design, procedure e relazioni scritte inerenti le soluzioni utilizzate sulla base dei requisiti di progetto ed alle fasi di gestione operativa, fornendo il supporto necessario per le fasi di Audit di Certificazione e verifica Normativa.

CHI CERCHIAMO?

REQUISITI NECESSARI:

Diploma di istruzione secondaria superiore

- Pregressa esperienza nel ruolo o in ruoli similari all'interno di realtà aziendali strutturate e/o di consulenza;

Conoscenze:

1. Architetture di sicurezza (sia in configurazione cluster che non ridondata), basate soprattutto sulle architetture dei prodotti Radware, Check Point, Imperva, Cisco, F5, Fortinet e di log management (es. RSA, HP, Qradar)
2. Tematiche legate al design e deploy (dimensionamento sulla base dei requisiti, disegno logico/fisico, valutazione degli impatti connessi agli aspetti evolutivi e d'integrazione, ecc) all'amministrazione, manutenzione, configurazione, tuning e monitoring di architetture network (router, load balancer, apparati di ottimizzazione del traffico di rete, proxy, sistemi di autenticazione, ecc) ai sistemi di sicurezza (web application firewall, firewall, intrusion prevention, intrusion detection) ai sistemi di log management e SIEM, nonché alla loro corretta interazione, integrazione ed interoperabilità sia funzionale che operativa
3. Integrazione di sistemi IT hardware eterogenei in architetture di rete complesse
4. Architetture di reti LAN/WAN per la definizione, realizzazione, configurazione e supporto network
5. Metodi di crittografia più comuni, dell'implementazione dei protocolli di sicurezza e dei sistemi NAC
6. Gestione della sicurezza e di rischio e la relativa normativa di riferimento
7. Modello di riferimento OSI e vari strati fisico, datalink, rete, trasporto, sessione, presentazione, applicazione
8. Funzionamento di un sistema di comunicazione complesso basato su IP anche di una rete senza fili (wireless)
9. Configurazione di reti locali virtuali (VLAN) o segmentate e di VPN
10. Aspetti chiave della sicurezza di rete, firewall, politiche dei controlli di accesso e di gestione dei log in ottemperanza alla normativa vigente e privacy
11. Attività di Vulnerability Assessment e Penetration Test (VAPT) adottando contromisure (Hardening) relative alle principali vulnerabilità sui sistemi
12. tecnologie Datacenter Software Defined (es. Broadcom NSX-T, Cisco ACI)

Completa il profilo la buona conoscenza della lingua inglese

Si richiede la disponibilità alla **reperibilità**.

REQUISITI PREFERENZIALI:

- Possesso di certificazioni e Fortinet NS 4;
- Possesso di certificazione CCSA/CCSE;
- Possesso di certificazioni F5 101, F5-CA o superiori
- Possesso di certificazione Cisco CCDP o altre certificazioni tecniche sui prodotti e sistemi relativi alle competenze specialistiche
- certificazioni Cisco CCNA/CCNP

Nella valutazione si terrà inoltre conto delle seguenti:

CAPACITA' ED ATTITUDINI INDIVIDUALI

- Ottime capacità di Problem Setting e Problem Solving
- Forte Orientamento al Risultato
- Forte Orientamento all'Innovazione e al Digital Mindset
- Spiccata attitudine alla Collaborazione e al lavoro in Team
- Ottima capacità di Pianificazione e Organizzazione
- Motivazione e apertura al Cambiamento
- Buone doti Comunicative

La ricerca è rivolta a candidati di entrambi i sessi (D.Lgs. n. 198/2006 e s.m.i.). Le caratteristiche delle attività sono compatibili con qualsiasi genere, età e condizione fisica (salvo, per quest'ultima, il necessario accertamento successivo ai fini della verifica dell'idoneità per l'effettivo espletamento delle mansioni).

COSA OFFRIAMO?

Tempo Indeterminato full-time, inquadramento previsto fino al gruppo "A" (a seconda del livello di esperienza maturato) ai sensi del vigente CCNL per le Aziende Grafiche e Affini e delle Aziende Editoriali anche Multimediali.

Sede: **Roma**

L'azienda, per esigenze tecnico organizzative, si riserva la facoltà di estendere la presente ricerca ad altre sedi e/o presidi IPZS.

RITIENI DI ESSERE IL CANDIDATO IDEALE? ECCO COSA FARE PER CANDIDARTI

Potrai candidarti dal **30/05/2025** alle ore 23:59 del **29/06/2025** cliccando su “candidati ora” o direttamente dal link <https://selezione.pa.randstad.it/networksecurityipzs>

Non sono ammesse altre forme di invio delle domande di partecipazione alla selezione e, pertanto, non saranno ritenute valide le domande presentate con modalità e tempistiche diverse da quella indicata, a pena di esclusione.

Il Poligrafico e la società incaricata Randstad Italia S.p.A. che si occuperà della ricezione delle domande e dello svolgimento dell'iter pre-selettivo, non si assumono alcuna responsabilità circa la mancata ricezione delle domande per qualsiasi motivo imputabile a terzi, a caso fortuito e forza maggiore.

PROCESSO DI SELEZIONE

Il processo di selezione prevede vari la preselezione da parte della società Randstad Italia S.p.A incaricata, che curerà la fase preselettiva volta all'individuazione dei candidati da ammettere alla fase selettiva.

Una seconda fase di selezione nella quale il Poligrafico condurrà colloqui tecnico / motivazionali. Verrà ritenuto idoneo chi otterrà un punteggio pari ad almeno 2/5, sia alla valutazione tecnica che alla valutazione motivazionale.

Laddove necessario potranno essere previste, sia nella fase di pre-selezione che nella fase di selezione delle prove tecniche e/o logico - attitudinali, che si intenderanno superate con il raggiungimento del punteggio minimo previsto – cosiddetto punteggio soglia – pari al 51% del punteggio massimo. Resta inteso che in fase di pre-selezione accederanno alle prove tecniche solo i candidati che abbiano i requisiti sopra richiesti.

È IMPORTANTE SAPERE CHE:

La mancata allegazione del cv sarà causa di esclusione dalla selezione.

Le competenze specialistiche richieste e i requisiti preferenziali, qualora presenti, devono essere espressamente indicati nel CV – specificando le date di inizio e fine (mese e anno) sia del percorso formativo sia delle singole esperienze professionali, nonché il possesso delle competenze/conoscenze richieste.

Eventuali dati incompleti non potranno essere tenuti in considerazione ai fine della valutazione.

Le competenze specialistiche e i requisiti preferenziali devono essere maturati alla data di scadenza dei termini per la presentazione della candidatura.

L'Azienda si riserva di verificare in qualsiasi momento l'effettivo possesso dei requisiti previsti dal presente avviso, nonché dei titoli dichiarati, attraverso la richiesta della documentazione necessaria o di informazioni su di essa e di disporre, in qualsiasi momento, l'esclusione dei candidati nel caso di non veridicità delle dichiarazioni rese.

La società si riserva la facoltà di prorogare, modificare o revocare la presente ricerca in caso di:

- Mancata ricezione di candidature corrispondenti ai requisiti necessari richiesti;
-



- Nuove esigenze organizzative aziendali che richiedano la sospensione/cancellazione degli inserimenti pianificati e ad oggi approvati o la variazione del numero di ingressi previsti;

La presentazione della domanda implica inoltre l'accettazione di tutte le disposizioni del presente avviso.

I dati personali saranno trattati dalla società Randstad Italia S.p.A. in qualità di Titolare ai sensi e per gli effetti della normativa Privacy vigente.

L'Informativa ex art. 13 del Regolamento UE 2016/679 è presente sul sito www.randstad.it nella sezione Informativa Privacy.