**ALLEGATO “A” AL CAPITOLATO TECNICO**

**LOTTI 1 e 2**

**PROFILI PROFESSIONALI**

(RETTIFICATO)

# INDICE

## 1. PREMESSA

Le figure professionali proposte per lo svolgimento dei servizi oggetto del **Lotto 1** dovranno rispettare i profili di seguito descritti e sintetizzati nella tabella di correlazione tra figure professionali e servizi/attività.

| Servizi / Attività | TEM | CET | SPP | SSS | SIM | SIJ | DBS | DBJ | SRS | SRJ | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Servizi di Monitoraggio Sistemi e Reti | X | | | X | X | X | X | X | | | |
| Servizi di Conduzione Operativa Sistemi | X | | | X | X | X | X | X | | | |
| Servizi di Sviluppo e Integrazione Architetture e Sistemi | X | X | X | X | X | X | X | X | | | |
| Servizi di Conduzione Operativa Reti | X | | | | | | | | X | X | |
| Servizi di Rete: progettazione e sviluppo | X | | X | | | | | | | | |
| Manutenzione Hardware | X | | | | X | X | | | | | |
| Servizi di Service e Performance Management | X | | | | | | | | | | |

### Legenda

TEM: ICT Operation Manager

CET: Enterprise Architect

SPP: System Architect

SSS: System Administrator Senior

SIM: System Administrator Middle

SIJ: System Administrator Junior

DBS: Database Administrator Senior

DBJ: Database Administrator Junior

SRS: Network Specialist Senior

SRJ: Network Specialist Junior

Le figure professionali proposte per lo svolgimento dei servizi oggetto del **Lotto 2** dovranno rispettare i profili di seguito indicati:

1. Security Project Manager
2. Governance & risk compliance (GRC) consultant
3. Security architect & engineer
4. Security Advisor senior

5. Security Advisor junior
6. Security specialist
7. Security specialist H24
8. Security Analyst senior
9. Security Analyst junior
10. Vulnerability researcher / Ethical Hacker senior
11. Vulnerability researcher / Ethical Hacker junior
12. Incident handler / response senior
13. Incident handler / response junior
14. Digital forensic
15. CyberSecurity & Privacy Legal Advisor

È richiesto che il Fornitore indichi nell'Offerta il mix di risorse che si impegna ad utilizzare per l'erogazione dei servizi remunerati a canone.
Qualunque sia l'organizzazione che il Fornitore intenda proporre per i diversi team, nel formulare la propria Offerta, in particolare **per il Lotto 1** tenga presente la tabella di correlazione tra i servizi e le figure professionali, ferma restando la facoltà per il Fornitore stesso di proporre il mix di figure professionali ritenuto più funzionale alle finalità e agli obiettivi di qualità della fornitura.

Per entrambi i Lotti si precisa che:

- la cultura equivalente può corrispondere, indicativamente: a 4 anni di esperienza lavorativa addizionale in ambito informatico oppure **(per il Lotto 2)** a 3 di esperienza in ambito specialistico della sicurezza informatica;
- nei profili professionali vengono a volte indicate competenze/certificazioni su ambienti tecnologici diversi. È evidente che tali conoscenze devono essere presenti nel complesso delle risorse professionali richieste al fornitore sulle diverse attività e/o servizi e non in un'unica persona e possono essere intese come fra loro alternative, in funzione del servizio di assegnazione e delle esigenze progettuali. Le certificazioni richieste devono essere valide, mantenute valide per tutta la durata della fornitura e comunque **non più vecchie di 3 anni** ad eccezione delle certificazioni che per loro stessa natura non scadono ancorché conseguite prima dei 3 anni.
- rimane fermo l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico avvenute in corso d'opera, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi anche mediante percorsi formativi organizzati internamente o inserendo nei gruppi di lavoro risorse con skills adeguate, senza alcun onere aggiuntivo per l'Amministrazione. Pertanto, le competenze e conoscenze tecniche delle figure che seguono non sono da considerarsi esaustive delle esigenze della fornitura, in quanto la Committente potrà richiedere, competenze specifiche in relazione ad ulteriori tematiche, prodotti, sistemi e metodologie.
- requisito fondamentale è individuare figure professionali con una forte propensione alla comunicazione e ai rapporti personali, con l'attitudine ad operare nella Pubblica Amministrazione.

**LOTTO 1 - DESCRIZIONE DEI PROFILI PROFESSIONALI**

Nei paragrafi seguenti è fornita la descrizione dei profili professionali minimi da impiegare nella fornitura, diversificati, ove significativo, in base al servizio/attività di competenza.

## 1.1 ICT OPERATION MANAGER

| Qualifica professionale | ICT Operation Manager - TEM |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 12 anni di cui almeno 7 nella funzione |
| Esperienze consolidate | - Comprovata esperienza in progetti complessi e/o di grandi dimensioni<br>- Conduzione di progetti strategici<br>- Comprovata esperienza nel coordinamento di risorse umane<br>- Comprovata esperienza nel garantire, per conto del Fornitore, gli SLA definiti e concordati con l'Amministrazione.<br>- Stima di risorse per realizzazione di progetto<br>- Comprovata esperienza nel garantire l'applicazione degli standard tecnologici e delle policy di sicurezza definite dall'Amministrazione.<br>- Tecniche di gestione progetti<br>- Spiccate capacità relazionali |
| Conoscenze | - Conoscenze approfondite di tecniche per project e risk management<br>- Conoscenze approfondite su metodologie di analisi, metodologie di documentazione e metodologie di pianificazione<br>- Conoscenze approfondite su Piano di Qualità, la definizione degli standard di progetto, delle procedure e delle metriche<br>- Conoscenza delle principali tendenze evolutive delle architetture tecnologiche per sistemi enterprise;<br>- Conoscenza a livello senior dei sistemi operativi Windows, Linux e Unix;<br>- Conoscenza a livello senior delle problematiche di clustering;<br>- Conoscenza a livello senior delle architetture applicative.NET e J2EE;<br>- Conoscenza a livello senior delle infrastrutture informatiche applicative datacenter oriented;<br>- Conoscenza a livello senior delle architetture applicative a Container;<br>- Conoscenza a livello senior delle architetture applicative in Cloud;<br>- Conoscenza a livello senior delle problematiche di business continuity;<br>- Conoscenza a livello senior delle problematiche d'integrazione in ambienti tecnologici complessi;<br>Si richiede il possesso di almeno una delle seguenti certificazioni:<br>• ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente<br>• Certificazioni Microsoft per System Engineer |

## 1.2 ENTERPRISE ARCHITECT

| Qualifica professionale | Enterprise Architect - CET |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 12 anni di cui almeno 7 nella funzione |
| Esperienze consolidate | - Analisi e progettazione di sistemi informativi, package, procedure complesse<br>- Redazione di specifiche e documentazione di progetto<br>- Stesura documentazione e manualistica tecnica<br>- Stima di risorse per realizzazione di progetto<br>- Tecniche di gestione progetti<br>- Progettazione test integrati<br>- Capacità di analisi e risoluzione problemi<br>- Spiccate capacità relazionali<br>- Certificazioni nei diversi ambiti tecnologici, ad esempio:<br>SuSe, Red Hat o altra certificazione di una distribuzione Linux;<br>Microsoft server e database;<br>VMWare (VCAP, VCDX);<br>Oracle (DBA Professional/Master, Enterprise manager, ecc.);<br>IBM (Certified specialist, ecc.);<br>Red Hat Openshift o Kubernetes<br>Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP)<br>ITIL expert/intermediate level |
| Conoscenze in ambito system architecture | - Disegno di architetture tecnologiche complesse (multivendor, container,multicloud);<br>- Attività di dimensionamento sistemi e capacity planning;<br>- Conoscenza delle principali tendenze evolutive delle architetture tecnologiche<br>- Conoscenze approfondita degli elementi tecnologici che costituiscono un sistema complesso (sia On Prem che Cloud-based o a Container);<br>- Conoscenza approfondita degli strumenti tecnologici di CD/CI (Azure, DevOps, Jenkins, GitLab, GitHub, Ansible,…)<br>- Metodologia per l'analisi, il disegno e la revisione dell'IT Service Management;<br>- Analisi delle necessità di impianto delle applicazioni in ambienti complessi. |
| Conoscenze approfondite in ambito System Administration | - Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster;<br>- Gestione delle procedure di startup e shutdown; |
| Conoscenze approfondite in ambito Database e prodotti middleware | - Database administration (Oracle Db, Sql server, mysql, postgress slq, Mongo DB, Cassandra ecc.)<br>- Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, Jboss, Microsoft IIS, ecc..);<br>- Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, Plone, ecc.)<br>- Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages. |
| Conoscenze approfondite in ambito SAN e Backup | - Tipologie di Raid<br>- Tecnologie e best practice di integrazione tra host e apparati di storage<br>- Mobilità dei dati |

| | |
|---|---|
| | - SCSI e FC – LUN e associazione con File System<br>- Zoning e LUN Masking<br>- Multipathing<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Orchestrazione del backup<br>- Data loss prevention<br>- Data retention e deduplica<br>- Offline Backup<br>- Object Storage |
| Conoscenze approfondite in ambito networking | - Amministrazione Sistemi operativi degli apparati di rete<br>- Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità<br>- Disegno e progettazione di reti TCP/IP complesse<br>- Implementazione di infrastrutture gestionali per reti complesse<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sicurezza delle reti. |
| Conoscenze approfondite nell'ambito delle tecnologie di virtualizzazione | - Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN<br>- Disegno e implementazione di server, storage e modalità di backup e restore<br>- Supporto di ambienti enterprise. |
| Conoscenze approfondite in ambito sicurezza | - Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.<br>- Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.<br>- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi<br>- Tecniche di ridondanza ed alta affidabilità<br>- Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways<br>- Amministrazione sistemi Antivirus;<br>- Analisi di problematiche complesse ed individuazione del componente in errore<br>- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>- Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799)<br>- Conduzione di assesment di sicurezza logica, fisica e organizzativa. |
| Conoscenze approfondite in ambito Operation Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log |
| Conoscenze approfondite in ambito Service Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management<br>- Metodologia per l'analisi, il disegno, la revisione dell'IT Service Management |

### 1.3 SYSTEM ARCHITECT

| Qualifica professionale | System Architect - SPP |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 8 anni di cui almeno 4 nella funzione |
| Esperienze consolidate | - Analisi e progettazione di sistemi informativi, package, procedure complesse<br>- Redazione di specifiche di progetto<br>- Stima di risorse per realizzazione di progetto<br>- Tecniche di gestione progetti<br>- Controllo realizzazione procedure<br>- Progettazione test integrati<br>- Capacità di analisi e risoluzione problemi<br>- Spiccate capacità relazionali<br>- Certificazioni nei diversi ambiti tecnologici |
| Conoscenze Linux | Comprovate competenze nell'ambito dei sistemi GNU/Linux ed esperienza di almeno 2 anni nell'installazione e configurazione di Linux su sistemi server e/o<br>infrastrutture professionali.<br>Possiede almeno una delle seguenti conoscenze o ha effettuato una delle esperienze:<br>- progettazione di Sistemi Informativi basati integralmente su FLOSS (Free Libre<br>Open Source Software);<br>- partecipazione a progetti di sviluppo di software Open Source;<br>- certificazione SuSe, Red Hat o altra certificazione di una distribuzione Linux<br>- conoscenza del mondo dell'Open Source Community e dei relativi tool. |
| Conoscenze sistemi operativi Microsoft | Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting di server e client in ambienti Microsoft. In particolare è richiesta una specifica competenza sulle configurazioni cluster Windows MSCS e NLB, sulla tecnologia .NET, sul database SQL Server e Share Point.<br>Certificazioni possedute:<br>- Certificazioni Microsoft per Systems Engineer – Windows Server<br>- Certificazioni Microsoft per Database Administrator - SQL Server<br>- Certificazioni Microsoft per App Builder for Microsoft .NET<br>- Certificazioni Microsoft per Systems Administrator on Microsoft Windows Server |
| Conoscenze Application Server IBM WebSphere | Specifiche competenze sull'application server WebSphere con particolare riguardo alle attività di analisi delle problematiche complesse ed individuazione del componente in errore comprovate dal possedere la certificazione IBM WebShere Application Server "IBM Certified System Administrator – WebSphere" |
| Conoscenze Application server Microsoft IIS | - Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting del sistema Microsoft Internet Information Services in ambiente Microsoft Windows Server. |

| | |
|---|---|
| | - Richiesta specifica conoscenza dell'application server in tutte le sue componenti. |
| Conoscenze Application server Open | - Conoscenza specialistica in tema di installazione, personalizzazione, tuning e<br>troubleshooting degli application server Apache Tomcat in ambiente Linux/Unix.<br>- Richiesta specifica conoscenza degli application server in tutte le sue componenti. |
| Conoscenze specifiche in ambito CMS – MS SharePoint | Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting di servizi di gestione dei contenuti in ambienti Microsoft Sharepoint. In particolare è richiesta una specifica competenza sulle tecniche di integrazione dei servizi e di sviluppo di smart application "APP" e della piattaforma in tutte le sue componenti. |
| Conoscenze specifiche in ambito Microsoft Exchange e Zimbra | - Conoscenza specialistica in tema di installazione, personalizzazione, tuning e<br>troubleshooting del sistema Microsoft Exchange in ambiente Microsoft Windows Server e Zimbra in ambiente Linux.<br>Richiesta specifica conoscenza della piattaforma in tutte le sue componenti. |
| Conoscenze nell'ambito delle tecnologie di virtualizzazione | - Conoscenza approfondita della tecnologia VMWare, con particolare riferimento a<br>piattaforma ESX/ESXi, in ambienti complessi con storage su SAN.<br>- Esperienza nel disegno e implementazione di soluzioni di virtualizzazione dei client<br>(VDI), dei server e delle applicazioni attraverso le maggiori tecnologie di virtualizzazione (VMWARE, CITRIX e Microsoft Hyper-V).<br>- Supporto di ambienti enterprise (hardware x86, VMWare Virtual Infrastructure,<br>amministrazione di sistemi Windows e Linux) utilizzando best practices standard e processi operativi (ITIL like).<br>- Esperienza nell'installazione, personalizzazione e test di prodotto, applicazione di patch e service pack.<br>- Esperienza nel disegno e implementazione di server, storage e modalità di backup e restore (VMWARE consolidated backup).<br>- Possiede le certificazioni VMWare VCP-DCV |
| Conoscenze Oracle RDBMS e Oracle Fusion Middleware | Skill specifico nella gestione di database large-scale e di applicazioni "enterprise".<br>Conseguimento dei titoli previsti dal programma Oracle Certified Professional.<br>Conoscenza approfondita in tema di installazione, tuning, personalizzazione e trouble shooting di prodotti Oracle del tipo:<br>- Oracle RDBMS (RAC);<br>- Oracle Enterprise MGR, Grid Control;<br>Certificazione: Varie Piattaforme Oracle |
| Conoscenze nell'ambito delle tecnologie Java | Possiede conoscenze specialistiche delle applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Web Services (JAX-RS e JAX-WS), Java Servlet, JavaServer Faces (JSF), JavaServer Pages (JSP), Enterprise JavaBeans (EJB), nonché i client Java che li utilizzano.<br>Possiede certificazioni Oracle o equivalenti in ambito Java. |

| | |
|---|---|
| Conoscenza piattaforme di Backup | Possiede conoscenze approfondite dell'infrastruttura e dei prodotti di backup (Tivoli, Commvault, ecc..) con una esperienza di almeno 5 anni maturata sulle problematiche relative. |
| Conoscenze altre piattaforme Enterprise | Possiede conoscenze approfondite dell'infrastruttura e dei prodotti SAP e SAS con una esperienza di almeno 5 anni maturata sulle problematiche relative. |

### 1.4 SYSTEM ADMINISTRATOR SENIOR

| Qualifica professionale | System Administrator Senior - SSS |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 10 anni, di cui almeno 5 nella funzione |
| Esperienze consolidate | - Problem determination e problem solving<br>- Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi<br>- Tecniche di gestione progetti<br>- Elaborazione e redazione di specifiche di progetto e di studi di fattibilità<br>- Conoscenze di best practices ITIL<br>- Tecniche di progettazione e dimensionamento di architetture hardware/software<br>- Tecniche di pianificazione<br>- Tecniche e strumenti di monitoraggio<br>- Tecniche di analisi del rischio<br>- Controllo della qualità del servizio<br>- Controllo dello stato di avanzamento delle attività<br>- Progettazione, analisi e realizzazione di architetture di BC/DR<br>- Sistemista DB/DC in ambiente open e loro sottosistemi<br>- Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati<br>- Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo.<br>- Operativi (UNIX, Linux, Windows) e con altri middleware (DB2, CICS, Oracle, WebSphere)<br>- Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei<br>- Architetture client/server e web<br>- Architetture a Container e Cloud<br>- Protocollo e architettura di rete TCP/IP<br>- Ambienti LAN e WAN |
| Conoscenze specifiche approfondite | - Architetture di BC/DR<br>- Tematiche applicative gestionali, preferibilmente in ambito Pubblica Amministrazione<br>- Tecniche di problem solving<br>- assistenza alla risoluzione dei problemi che gli utenti possono incontrare nell'interazione con i servizi di business dell'Amministrazione<br>- supporto per l'utilizzo corretto dei servizi di business |
| System Administration | - Gestione Data Center, con particolare riguardo alle tecnologie HP, IBM, FUJITSU e DELL<br>- Sistemi di gestione Blade<br>- Amministrazione e gestione Sistemi Operativi Microsoft |

| | |
|---|---|
| | - Installazione, configurazione, personalizzazione/tuning e gestione del sistema operativodei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali Red Hat, SuSe,)<br>- Configuration management<br>- Analisi e progettazione di sistemi informativi, package e procedure complesse<br>- Configurazione e personalizzazione/tuning di cluster dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali Red Hat, SuSe)<br>- Personalizzazione protezione file di sistema (es. password, group, hosts)<br>- Gestione delle procedure di startup e shutdown;<br>- Conoscenza (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti:<br>Database Management System RDBMS: DB2 - Oracle – SQL Server – MySQL – PostgreSQL<br>Database Management System NoSQL: Mongo DB, Cassandra<br>Application Server: IBM Websphere - Oracle Application Server - Apache/Tomcat – Jboss, Oracle Fusion Middleware<br>Business Intelligence : Business objects– prodotti di ETL (ad esempio Power Center e InfoSphere)<br>Web server: Apache,<br>Oracle application HR, OFA, OGL, OHS<br>Oracle portal, Oracle login server<br>UCM, Content Server e Bea Web Logic<br>- Prodotti di analisi log (es. Webtrend)<br>Conoscenza approfondita delle tecniche di eliminazione delle vulnerabilità dei sistemi. |
| Amministrazione Database in ambiente open e prodotti middleware | - Database administration (DB2, Oracle, SQL, mysql, PostGresSQL, MongoDB, Cassandra)<br>- Analisi performance e tuning Database<br>- Supporto allo sviluppo applicativo<br>- Studio metodologie di recovery/backup: utilities, concurrent copy, flash copy,<br>time finder, mirroring (SRDF)<br>- Personalizzazione e utilizzo tools<br>- Application Server administration (Oracle iAS, Oracle Web Logic, jboss,ecc..)<br>- Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal,<br>OpenCMS, WebSphere Portal Server, Liferay, ecc.)<br>- Oracle Identity Management<br>- Oracle Active Data Guard<br>- Architetture SOA/cooperazione applicativa e modelli concettuali correlati (XML, SOAP, WSDL, UDDI)<br>- Business Intelligence: metodologie di progettazione e amministrazione prodotti<br>(business object, ecc.).<br>- Amministrazione di sistemi di collaborazione (es. MS Sharepoint, MS Teams) |

| | |
|---|---|
| Test integrati | - Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati (DB2, Oracle, ..).<br>- Progettazione e realizzazione di test integrati con altre piattaforme (Superdome,<br>System P, Intel), con altri Sistemi Operativi (UNIX, Linux, Windows) e con altri middleware (DB2, CICS, Oracle, WebSphere).<br>- Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo.<br>- Redazione di specifiche di progetto |
| Conoscenze in ambito SAN e Backup | - Concetti e tipologie di Raid<br>- Padronanza dei comandi necessari per i diversi host collegati ai box EMC2, IBM<br>- Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor)<br>- Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage<br>- Concetti di mobilità dei dati<br>- Multipathing<br>- Zoning e LUN Masking<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Concetti di orchestrazione del backup<br>- Concetti di data loss prevention<br>- Concetti di data retention e deduplica<br>- Offline Backup<br>- Object Storage |
| Conoscenze in ambito networking | - Amministrazione Sistemi operativi degli apparati di rete<br>- Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità<br>- Disegno e progettazione di reti TCP/IP complesse<br>- Implementazione di infrastrutture gestionali per reti complesse<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Reti di trasporto ottiche, tecnologia DWDM, Cisco Ons 15454<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sistemi di network monitoring proprietari ( Cisco Works, ecc.) ed open source (Zabbix, NAGIOS, MRTG, ecc)<br>- Sistemi di Analisi e Problem determination proprietari ed Open Source (Tcpdump, Wireshark, Flow tools ecc.)<br>- Sicurezza delle reti<br>- Sicurezza perimetrale (Cisco Pix-Firewall, Cisco FW-Blade, Iptables) e logica (sistemi<br>IDS ed IPS proprietari ed Open Source - Snort, ecc., Vpn , Nac, Ldap, 802.1x ecc.)<br>- Protocolli di crittografia (IPSEC, PPtp, L2tp,ecc.)<br>- Infrastruttura PKI (certificati digitali, ecc.)<br>- Partecipazione ad analisi e disegno di progetti di reti WIRELESS, LAN, WAN in |

| | |
|---|---|
| | presenza di architetture diverse (SNA, TCP/IP) e con supporto di traffico multimediale<br>- Installazione personalizzazione e utilizzo di: VTAM, TCP/IP, MPLS, PPP, ISDN, NCP,<br>Router, Switch, Access server, protocolli di routing (RIP, OSPF), Multicast, VoIP,<br>applicativi video on demand, QoS |
| Conoscenze nell'ambito delle tecnologie di virtualizzazione | - Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e<br>gestione) delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti<br>complessi con storage su SAN<br>- Disegno e implementazione di server, storage e modalità di backup e restore (anche su infrastruttura virtuale)<br>- Supporto di ambienti enterprise (hardware x86, VMWare Virtual Infrastructure, amministrazione di sistemi Windows e Linux) |
| Conoscenze specifiche in ambito Microsoft | - Amministrazione Sistemi operativi Windows<br>- Progettazione ed implementazione di infrastrutture basate su piattaforme Microsoft<br>- Amministrazione e configurazione:<br>- Active directory e directory services<br>- Active directory server role<br>- Group policy ed impatto sui client del dominio<br>- Network access e remote access<br>- Windows deployment services<br>- Terminal services<br>- Windows registry<br>- Windows services<br>- Remote desktop<br>- Certificate management<br>- Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e<br>gestione) di:<br>sistema operativo Windows Server<br>.Net Framework<br>cluster Windows MSCS<br>Network Load Balancing (NLB)<br>Personalizzazione, configurazione delle componenti di back office, configurazione e<br>personalizzazione/tuning file system Microsoft, anche in ambiente cluster<br>Configurazione e personalizzazione/tuning cluster Microsoft<br>Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti:<br>- SQL server, IIS, Microsoft SharePoint, Microsoft Exchange, Microsoft System Center Configuration Manager SCCM , Microsoft Data Protection Manager, Microsoft Teams, Microsoft Forefront Identity Manager |
| Conoscenze in ambito sicurezza e log management | - Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.<br>- Protocolli applicativi di base quali http, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. |

| | |
|---|---|
| | - Principali vulnerabilità/tipi di attacchi di rete e dei sistemi<br>- Tecniche di ridondanza ed alta affidabilità<br>- Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways<br>- Amministrazione sistemi di Log Management SIEM (es. RSA Envision)<br>- Amministrazione sistemi Antivirus (es. McAfee)<br>- Analisi di problematiche complesse ed individuazione del componente in errore<br>- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>- Approfondita conoscenza dei principali standard di sicurezza (ITSEC, CC, BS7799)<br>- Conduzione di assessment di sicurezza logica, fisica e organizzativa. |
| Conoscenza piattaforme di CD/CI | Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting delle piattaforme di CD/CI. Richiesta specifica conoscenza delle tecnologie Azure, DevOps, GitLab, GitHub, Ansible, Maven, Docker, Terraform, ecc… |
| Conoscenza piattaforme di Containerizzazione | Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting delle piattaforme di Containerizzazione, con particolare riferimento alle<br>funzioni di automation, orchestration e provisioning. Richiesta specifica conoscenza di<br>tipologie e architetture di Containerizzazione basate su piattaforma Kubernates (es. OpenShift) |
| Conoscenza piattaforme Cloud Computing | Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting della piattaforme di Cloud Computing, con particolare riferimento alle<br>funzioni di automation, orchestration e provisioning. Richiesta specifica conoscenza di<br>tipologie e architetture di Cloud Computing basate su piattaforme Amazon Web Services (AWS), Azure Microsoft, Google Cloud Platform (GCP) |
| Conoscenze in ambito Service Management | - Metodi di Business Process Rengineering<br>- Conoscenza approfondita sui processi e sui principali prodotti disponibili per la<br>razionalizzazione di:<br>Service Desk<br>Incident management<br>Problem management<br>Change Management<br>Service Request Management<br>Knowledge management<br>- Competenze di data modeling, disegno e sviluppo di procedure ETL<br>- Esperienza nell'attività di integrazione tra diversi sistemi informativi<br>- Esperienza nell'attività di predisposizione e conduzione di sessioni formative e di coaching<br>- Partecipazione a progetti di Service Management dell' IT<br>- Conoscenza approfondita delle principali metodologie e best practices sul Service<br>Management IT (Cobit, ITIL, ISO 20000) |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente ;<br>- Certificazioni Microsoft per System Engineer |

| | |
|---|---|
| | - Certificazioni Microsoft per Technology Specialist SQL Server;<br>- Oracle OCP DBA - SAP Certified<br>- VMware Certified Professional (VCP)<br>- LBL®LoadBalancer Application Availability Infrastructure 1° e 2° livello;<br>- Trend Micro Certified Security Expert (TCSE);<br>- CCA - Citrix Certified Administrator<br>- Red Hat Certified Engineer (RHCE)<br>- Red Hat Certified Specialist in OpenShift Administration<br>- Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP) |

### 1.5 SYSTEM ADMINISTRATOR MIDDLE

| Qualifica professionale | System Administrator – SIM |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 6 anni, di cui almeno 4 nella funzione |
| Esperienze consolidate | - Interazione e relazione con gli utenti;<br>- Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici;<br>- Problem determination e problem solving;<br>- Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi;<br>- Elaborazione e redazione di specifiche di progetto e di studi di fattibilità;<br>- Metodologie di project management e di best practices ITIL;<br>- Tecniche di progettazione e dimensionamento di architetture hardware/software;<br>- Tecniche di pianificazione;<br>- Tecniche e strumenti di monitoraggio;<br>- Tecniche di analisi del rischio;<br>- Controllo della qualità del servizio;<br>- Controllo dello stato di avanzamento della attività;<br>- Progettazione test integrati;<br>- Certificazioni nei diversi ambiti tecnologici |
| Conoscenze in ambito System Administration | - Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster;<br>- Personalizzazione di file di sistema (es. password, group, hosts)<br>- Gestione delle procedure di startup e shutdown;<br>- Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico. |
| Conoscenze in ambito Database e prodotti middleware | - Database administration (Oracle Db, Sql server, mysql, postgress slq, MongoDB, Cassandra ,ecc.)<br>- Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, jboss, Microsoft IIS, ecc..);<br>- Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, Plone, ecc.)<br>- Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages: |

| | |
|---|---|
| | - Ottimizzazione delle strutture dati. |
| Conoscenze approfondite in ambito SAN e Backup | - Tipologie di Raid<br>- Tecnologie e best practice di integrazione tra host e apparati di storage<br>- Mobilità dei dati<br>- SCSI e FCS – LUN e associazione con File System<br>- Zoning e LUN Masking<br>- Multipathing<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Orchestrazione del backup<br>- Data loss prevention<br>- Data retention e deduplica<br>- Offline Backup<br>- Object Storage |
| Conoscenze in ambito networking | - Amministrazione Sistemi operativi degli apparati di rete<br>- Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità<br>- Disegno e progettazione di reti TCP/IP complesse<br>- Implementazione di infrastrutture gestionali per reti complesse<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sicurezza delle reti. |
| Conoscenze nell'ambito delle tecnologie di virtualizzazione | - Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN<br>- Disegno e implementazione di server, storage e modalità di backup e restore<br>- Supporto di ambienti enterprise. |
| Conoscenze specifiche in ambito Microsoft | - Amministrazione Sistemi operativi Windows<br>- Progettazione ed implementazione di infrastrutture basate su piattaforme Microsoft<br>- Amministrazione e configurazione:<br>- Active directory e directory services<br>- Active directory server role<br>- Group policy ed impatto sui client del dominio<br>- Network access e remote access<br>- Windows deployment services<br>- Terminal services<br>- Windows registry<br>- Windows services<br>- Remote desktop<br>- Certificate management<br>- Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e<br>gestione) di:<br>sistema operativo Windows Server<br>.Net Framework<br>cluster Windows MSCS<br>Network Load Balancing (NLB) |

| | |
|---|---|
| | Personalizzazione e configurazione componenti di back office, configurazione e<br>personalizzazione/tuning file system Microsoft, anche in ambiente cluster<br>Configurazione e personalizzazione/tuning cluster Microsoft<br>Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti:<br>- SQL server<br>- IIS<br>- Microsoft SharePoint<br>- Microsoft Exchange<br>- Microsoft System Center Configuration Manager SCCM<br>- Microsoft Data Protection Manager<br>- Microsoft Teams<br>- Microsoft ISA, TMG e successive<br>- Microsoft Forefront Identity Manager |
| Conoscenze in ambito sicurezza | - Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.<br>- Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.<br>- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi<br>- Tecniche di ridondanza ed alta affidabilità<br>- Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways<br>- Amministrazione sistemi Antivirus;<br>- Analisi di problematiche complesse ed individuazione del componente in errore<br>- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>- Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799)<br>- Conduzione di assessment di sicurezza logica, fisica e organizzativa. |
| Conoscenze in ambito Operation Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log |
| Conoscenze in ambito Service Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management<br>- Controllo dei Processi IT e delle relative procedure operative |
| Conoscenze in ambito Client | - Architetture dei sistemi client Microsoft e Linux<br>- principali prodotti di software distribution e di remote desktop control<br>- sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android)<br>- web browser (es. Internet Explorer, Firefox, Chrome, Safari)<br>- antivirus (es. MCAfee, Norton, Kaspersky ecc.)<br>- Sistemi di virtualizzazione (es. XenApp, XenDesktop) |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente;<br>- RedHat Certified Engineer RHCE;<br>- Certificazioni Microsoft per System Engineer<br>- SAP NetWeaver Security;<br>- VMware Certified Professional (VCP)<br>- CCA - Citrix Certified Administrator<br>- IBM Certified Specialist - Open System Storage Solutions; |

| | |
|---|---|
| | - IBM Certified System Administrator - WebSphere App. Server Network Deployment;<br>- LBL®LoadBalancer Application Availability Infrastructure 1° livello. |

### 1.6 SYSTEM ADMINISTRATOR JUNIOR

| Qualifica professionale | System Administrator Junior – SIJ |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui almeno 1 nella funzione |
| Esperienze consolidate | - Interazione e relazione con gli utenti;<br>- Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici;<br>- Problem determination e problem solving;<br>- Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi;<br>- Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità;<br>- Metodologie di project management e di best practices ITIL;<br>- Certificazioni nei diversi ambiti tecnologici |
| Conoscenze base in ambito System Administration | - Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster;<br>- Personalizzazione di file di sistema (es. password, group, hosts)<br>- Gestione delle procedure di startup e shutdown;<br>- Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico. |
| Conoscenze base in ambito Database e prodotti middleware | - Database administration (Oracle Db, Sql server, mysql, postgress slq, ecc.)<br>- Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, jboss,Microsoft IIS, ecc..);<br>- Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, ecc.)<br>- Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages;<br>- Ottimizzazione delle strutture dati. |
| Conoscenze base in ambito SAN e Backup | - Tipologie di Raid<br>- Tecnologie e best practice di integrazione tra host e apparati di storage<br>- Mobilità dei dati<br>- SCSI e FCS – LUN e associazione con File System<br>- Zoning e LUN Masking<br>- Multipathing<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Orchestrazione del backup<br>- Data loss prevention<br>- Data retention e deduplica |
| Conoscenze base in ambito networking | - Amministrazione Sistemi operativi degli apparati di rete<br>- Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità |

| | |
|---|---|
| | - Disegno e progettazione di reti TCP/IP complesse<br>- Implementazione di infrastrutture gestionali per reti complesse<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sicurezza delle reti. |
| Conoscenze base nell'ambito delle tecnologie di virtualizzazione | - Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN<br>- Disegno e implementazione di server, storage e modalità di backup e restore<br>- Supporto di ambienti enterprise. |
| Conoscenze base in ambito sicurezza | - Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.<br>- Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.<br>- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi<br>- Tecniche di ridondanza ed alta affidabilità<br>- Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways<br>- Amministrazione sistemi Antivirus;<br>- Analisi di problematiche complesse ed individuazione del componente in errore<br>- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>- Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799)<br>- Conduzione di assessment di sicurezza logica, fisica e organizzativa. |
| Conoscenze base in ambito Operation Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log |
| Conoscenze base in ambito Service Management | - Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management<br>- Controllo dei Processi IT e delle relative procedure operative |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- ITIL® V3 foundation o ITIL® V4 equivalente ;<br>- Red Hat Certified System Administrator (RHCSA);<br>- Certificazioni Microsoft per System Administrator;<br>- VMware Certified Professional (VCP)<br>- CCA - Citrix Certified Administrator |

## 1.7 DATABASE ADMINISTRATOR SENIOR

| Qualifica professionale | Database Administrator Senior - DBS |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 10 anni, di cui almeno 5 nella funzione |
| Esperienze consolidate | - Problem determination e problem solving<br>- Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi<br>- Tecniche di gestione progetti<br>- Elaborazione e redazione di specifiche di progetto e di studi di fattibilità<br>- Conoscenze di best practices ITIL<br>- Tecniche di progettazione e dimensionamento di architetture hardware/software<br>- Tecniche di pianificazione<br>- Tecniche e strumenti di monitoraggio<br>- Tecniche di analisi del rischio<br>- Controllo della qualità del servizio<br>- Controllo dello stato di avanzamento delle attività<br>- Progettazione, analisi e realizzazione di architetture di BC/DR<br>- Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati<br>- Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo.<br>- Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei |
| Conoscenze | - Conoscenza a livello operativo dei sistemi Windows, Linux e Unix;<br>- Conoscenza a livello senior dei sistemi Oracle, SQL Server, MySql e PostGreSQL, MongoDB, Cassandra;<br>- Conoscenza a livello operativo delle problematiche di networking;<br>- Conoscenza a livello senior delle problematiche di clustering in ambito database;<br>- Conoscenza a livello senior delle architetture applicative .NET e J2EE in ambito database;<br>- Conoscenze a livello senior delle piattaforme software enterprise (SAP, SAS e BO) in ambito database;<br>- Conoscenza a livello senior delle problematiche di monitoring e performance tuning in ambito database;<br>- Conoscenza a livello senior delle problematiche di storage su architetture SAN in ambito database;<br>- Conoscenza a livello senior delle problematiche di consolidation in ambito database;<br>- Conoscenza a livello senior delle problematiche di business continuity e disaster recovery in ambito database. |
| Conoscenze in ambito SAN e Backup | - Concetti e tipologie di Raid<br>- Padronanza dei comandi necessari per i diversi host collegati ai box EMC2, IBM<br>- Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor)<br>- Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage<br>- Concetti di mobilità dei dati |

| | |
|---|---|
| | - Multipathing<br>- Zoning e LUN Masking<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Concetti di orchestrazione del backup<br>- Concetti di data loss prevention<br>- Concetti di data retention e deduplica<br>- Offline Backup<br>- Object Storage |
| Conoscenze in ambito Service Management | - Metodi di Business Process Rengineering<br>- Conoscenza approfondita sui processi e sui principali prodotti disponibili per la razionalizzazione di:<br>Service Desk<br>Incident management<br>Problem management<br>Change Management<br>Service Request Management<br>Knowledge management<br>- Competenze di data modeling, disegno e sviluppo di procedure ETL<br>- Esperienza nell'attività di integrazione tra diversi sistemi informativi<br>- Esperienza nell'attività di predisposizione e conduzione di sessioni formative e di coaching<br>- Partecipazione a progetti di Service Management dell' IT<br>- Conoscenza approfondita delle principali metodologie e best practices sul Service Management IT (Cobit, ITIL, ISO 20000) |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente ;<br>- Certificazioni Microsoft per Database Administrator - SQL Server<br>- Oracle OCP DBA<br>- Oracle Certified Associate PL/SQL Developer;<br>- Managing Oracle on Linux Certified Expert;<br>- SAP NetWeaver Sys. Admin. Oracle. |

### 1.8 DATABASE ADMINISTRATOR JUNIOR

| Qualifica professionale | Database Administrator Junior - DBJ |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui almeno 2 nella funzione |
| Esperienze consolidate | - Problem determination e problem solving<br>- Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi<br>- Tecniche di gestione progetti<br>- Elaborazione e redazione di specifiche di progetto e di studi di fattibilità<br>- Conoscenze di best practices ITIL<br>- Tecniche di progettazione e dimensionamento di architetture hardware/software<br>- Tecniche e strumenti di monitoraggio<br>- Controllo della qualità del servizio<br>- Controllo dello stato di avanzamento delle attività<br>- Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei |
| Conoscenze | - Conoscenza a livello operativo dei sistemi Windows, Linux e Unix;<br>- Conoscenza a livello operativo dei sistemi Oracle, SQL Server, MySql e PostGreSQL;<br>- Conoscenza a livello operativo delle problematiche di networking;<br>- Conoscenza a livello operativo delle problematiche di clustering in ambito database;<br>- Conoscenza a livello operativo delle architetture applicative .NET e J2EE in ambito database;<br>- Conoscenza a livello operativo delle problematiche di monitoring e performance tuning in ambito database. |
| Conoscenze in ambito SAN e Backup | - Concetti e tipologie di Raid<br>- Padronanza dei comandi necessari per i diversi host collegati ai box<br>- Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor)<br>- Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage<br>- Concetti di mobilità dei dati<br>- Multipathing<br>- Zoning e LUN Masking<br>- Disaster Recovery e funzioni di alta affidabilità degli storage<br>- Remote Mirroring e aggiornamento Sincrono-Asincrono<br>- Concetti di orchestrazione del backup<br>- Concetti di data loss prevention<br>- Concetti di data retention e deduplica |
| Conoscenze in ambito Service Management | - Conoscenza base sui processi e sui principali prodotti disponibili per la razionalizzazione di:<br>Service Desk<br>Incident management<br>Problem management<br>Change Management<br>Service Request Management<br>Knowledge management |

| | |
|---|---|
| | - Competenze di data modeling, disegno e sviluppo di procedure ETL<br>- Esperienza nell'attività di integrazione tra diversi sistemi informativi<br>- Partecipazione a progetti di Service Management dell' IT |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- ITIL® V3 foundation o ITIL® V4 equivalente ;<br>- Certificazioni Microsoft per Database Administrator - SQL Server<br>- Oracle OCP DBA |

### 1.9 NETWORK SPECIALIST SENIOR

| Qualifica professionale | Network Specialist Senior - SRS |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 7 anni di cui almeno 3 nella funzione |
| Esperienze consolidate | - Problem determination e problem solving<br>- Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi<br>- Tecniche di gestione progetti<br>- Elaborazione e redazione di specifiche di progetto e di studi di fattibilità<br>- Conoscenze di best practices ITIL<br>- Tecniche di pianificazione<br>- Tecniche e strumenti di monitoraggio<br>- Tecniche di analisi del rischio<br>- Controllo della qualità del servizio<br>- Controllo dello stato di avanzamento delle attività<br>- Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo.<br>- Architetture client/server e web<br>- Protocollo e architettura di rete TCP/IP<br>- Ambienti LAN e WAN |
| Conoscenze approfondite | Possiede un'approfondita conoscenza di molteplici architetture tecnologiche e protocolli di rete locale e geografica, e si mantiene aggiornato continuamente sulle loro evoluzioni. È in grado di analizzare i requisiti di comunicazione dei progetti e di disegnare sistemi di rete via cavo e/o senza fili, tenendo conto delle esigenze degli utenti e dei sistemi. È responsabile dell'installazione, configurazione e collegamento tra loro degli apparati di rete, prestando attenzione a garantire sicurezza, prestazioni elevate ed affidabilità dei servizi prestati. Garantisce il presidio ed il buon funzionamento della rete, attraverso la configurazione e l'uso degli appositi strumenti di monitoraggio. È in grado di intervenire in caso di gravi problemi sulla rete, sa analizzarne a fondo le cause e sa trovare e proporre soluzioni alternative per il ripristino dei servizi.<br>Le attività di questa figura professionale sono:<br>-progettare, in collaborazione con i tecnici dell'Amministrazione, le architetture necessarie all'evoluzione dell'infrastruttura di rete, garantendo il rispetto delle policies regionali;<br>-realizzare configurazioni complesse su apparati di rete locale e geografica, anche per gestire protocolli di trasporto multimediali;<br>- ricercare errori e guasti, anche con l'aiuto di strumenti HW e SW dedicati;<br>- risolvere problemi nelle configurazioni; analizzare le prestazioni degli apparati;<br>- collaborare alla gestione degli strumenti di Network Management su piattaforma Open Source e OpenVMS; |

| | |
|---|---|
| | - gestire in autonomia malfunzionamenti complessi sui circuiti di telecomunicazione;<br>- gestire le configurazioni d'interfaccia con i fornitori di connettività, approfondendo le tecnologie di routing dinamico e di gestione del Virtual Routing and Forwarding;<br>- dedicare attenzione agli aspetti di sicurezza interna e perimetrale, dando supporto alla gestione del firewall;<br>- collaborare alla gestione dei Domain Name System pubblici. |
| Conoscenze approfondite in ambito networking | - Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (BGP, IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sicurezza delle reti. |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- CISCO CCIE<br>- CISCO CCNP<br>- Ulteriori certificazioni specifiche di prodotto nell'ambito networking |

### 1.10 NETWORK SPECIALIST JUNIOR

| Qualifica professionale | Network Specialist Junior - SRJ |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui almeno 1 nella funzione |
| Esperienze consolidate | - Interazione e relazione con gli utenti;<br>- Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici;<br>- Problem determination e problem solving;<br>- Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi;<br>- Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità;<br>- Metodologie di project management e di best practices ITIL; |
| Conoscenze approfondite | Conosce le architetture tecnologiche ed i protocolli di rete locale e geografica più diffusi, e si mantiene aggiornato continuamente sulle loro evoluzioni. Sulla base dei documenti di progetto, è in grado di installare, configurare e collegare alle infrastrutture di cablaggio strutturato gli apparati di rete, le postazioni di lavoro ed i server. Verifica il buon funzionamento della rete, attraverso l'uso degli appositi strumenti di monitoraggio. In caso di problemi, si rapporta con gli utenti, con gli altri tecnici che lavorano sulle infrastrutture informatiche dell'Amministrazione e con i fornitori di servizi di connettività, segnalando malfunzionamenti e guasti, che segue fino alla risoluzione.<br>Le attività di questa figura professionale sono:<br>- gestire in autonomia guasti e malfunzionamenti su cablaggi o reti locali e geografiche;<br>- garantire l'help desk specialistico di secondo livello per problematiche di rete;<br>- predisporre la configurazione iniziale ed installare nuovi apparati di rete, su indicazione dei tecnici regionali e dello specialista senior;<br>- mantenere continuamente aggiornata la documentazione online sugli apparati di rete, sui circuiti e sui sistemi di trouble ticketing;<br>- gestire i disservizi sui servizi di telecomunicazione in caso di malfunzionamenti dei circuiti, con apertura delle chiamate verso i fornitori di connettività. |
| Conoscenze base in ambito networking | - Tecniche di bilanciamento del traffico<br>- Tecniche di ridondanza ed alta affidabilità<br>- Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…)<br>- Protocolli di routing (BGP, IGRP, OSPF,…)<br>- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)<br>- Apparati di rete (switch, bridge, router, ecc..)<br>- Sistemi di network management<br>- Sicurezza delle reti. |
| Certificazioni | Si richiede il possesso di una o più delle seguenti certificazioni:<br>- CISCO CCNA<br>- Ulteriori certificazioni specifiche di prodotto nell'ambito networking |

## 2. LOTTO 2 – DESCRIZIONE DEI PROFILI PROFESSIONALI

Nei paragrafi seguenti è fornita la descrizione dei profili professionali minimi da impiegare nella fornitura, diversificati, ove significativo, in base al servizio/attività di competenza.
Tali figure dovranno possedere preferibilmente le principali certificazioni professionali in ambito sicurezza informatica quali:

- ITIL® V3 / ITIL® V4;
- Auditor IEC/ISO 270xx family
- Certificazione privacy
- CISSP - Certified Information Systems Security Professional
- CompTIA A+
- CompTIA Security+
- CREST Certified Incident Manager
- CSX-P - Cybersecurity Practitioner Certification
- SSCP - Systems Security Certified Practitioner
- Certificazioni di vendor SIEM specifici (es. IBM, MicroFocus/OpenText, ecc)
- Cyber Defense
- Offensive Operations
- Certified Ethical Hacker (C|EH o CEH)
- Certified Hacking Forensic Investigator (C|HFI)
- Certificazioni vendor neutral
- Certificazioni di vendor specifici (es. Checkpoint, Fortinet, TrendMicro, BitDefender, ecc)
- Cloud Security
- GIAC Certified Incident Handler (GCIH)
- CSX Forensics Analysis Certificate
- GIAC Certified Forensic Analyst
- GIAC Reverse Engineering Malware
- CTIA - Certified Threat Intelligence Analyst
- GCTI - GIAC Cyber Threat Intelligence
- CSA - Certified SOC Analyst
- Digital Forensics
- Incident Response.

### 2.1 SECURITY PROJECT MANAGER

| | |
|---|---|
| Qualifica professionale | Security project manager |
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 4 nella funzione |
| Profilo professionale | **Progettazione** |

| | |
|---|---|
| | Assiste nella definizione, implementazione e gestione dei progetti di sicurezza informatica sulla base di obiettivi ed esigenze dell'Ente<br>Sviluppa progetti in materia di sicurezza informatica e ne coordina le fasi sino al completamento entro i limiti di tempo e budget assegnati, anche coordinando la comunicazione tra i vari attori coinvolti nel processo |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni<br>Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica<br>ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.2 GOVERNACE & RISK COMPLIANCE (GRC) CONSULTANT

| Qualifica professionale | Governace & risk compliance (GRC) consultant |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 8 anni, di cui 5 nella funzione |

| | |
|---|---|
| Profilo professionale | **Progettazione**<br>Sviluppa e partecipa all'implementazione di progetti per la riduzione del rischio tecnologico, la governance della sicurezza e la conformità alle policy dell'Ente ed alle normative vigenti ed agli standard ISO<br>**Analisi dei rischi**<br>Effettua analisi e valutazioni del rischio di sicurezza informatica<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate<br>**Policy e strategie**<br>Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi<br>Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente<br>Redige ed aggiorna le policy e le procedure di gestione degli incidenti<br>**Processi**<br>Migliora il livello di sicurezza informatica dell'Ente attraverso il miglioramento dei processi di gestione della sicurezza<br>Supporta l'Ente nella progettazione di processi conformi agli standard (ISO27001, GDPR, ecc….) per la gestione degli incidenti<br>Documenta e segnala criticità nei processi esistenti, fornisce indicazioni per il loro miglioramento, fornisce reportistica sulle attività di miglioramento |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni<br>Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica<br>ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali |

| | |
|---|---|
| | Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.3 SECURITY ARCHITECT & ENGINEER

| Qualifica professionale | Security architect & engineer (Specialista infrastrutture e di processo della sicurezza delle informazioni) |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 8 anni, di cui 5 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati<br>**Policy e strategie**<br>Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione<br>Supporta la pianificazione delle strategie in materia di sicurezza dei sistemi e delle informazioni<br>Redige ed aggiorna le policy e le procedure di gestione degli incidenti<br>**Processi**<br>Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati<br>Progetta misure di sicurezza per proteggere reti e sistemi<br>**Tecnologie e sistemi di sicurezza**<br>Progetta, sviluppa per l'Ente infrastrutture informatiche sicure sfruttando tecnologie e sistemi di sicurezza informatica ed applicando le best practices del settore<br>Supervisiona i processi di change management in chiave di sicurezza dei sistemi<br>Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni<br>Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |

| | |
|---|---|
| | ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.4 SECURITY ADVISOR SENIOR

| Qualifica professionale | Security Advisor senior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 3 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate<br>**Policy e strategie**<br>Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi<br>Supporta la pianificazione delle strategie in materia di sicurezza dei sistemi e delle informazioni<br>Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente<br>Redige ed aggiorna le policy e le procedure di gestione degli incidenti<br>**Processi** |

| | |
|---|---|
| | Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati<br>Progetta misure di sicurezza per proteggere reti e sistemi<br>Tecnologie e sistemi di sicurezza<br>Supervisiona i processi di change management in chiave di sicurezza dei sistemi<br>Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza<br>**Analisi dei sistemi**<br>Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore<br>**Awareness**<br>Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices<br>**Operations**<br>Svolge il ruolo di facilitatore per la gestione della sicurezza informatica nell'operatività dei sistemi e delle postazioni di lavoro |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Comprovata esperienza nella definizione e progettazione di architetture di sicurezza<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità<br>Competenze sulle metodologie e sui tool di analisi forense |

## 2.5 SECURITY ADVISOR JUNIOR

| Qualifica professionale | Security Advisor junior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui 1 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate<br>**Policy e strategie**<br>Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi<br>**Processi**<br>Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati<br>Progetta misure di sicurezza per proteggere reti e sistemi<br>**Tecnologie e sistemi di sicurezza**<br>Supervisiona i processi di change management in chiave di sicurezza dei sistemi<br>Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza<br>Analisi dei sistemi<br>Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore<br>**Awareness**<br>Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices<br>**Operations**<br>Svolge il ruolo di facilitatore per la gestione della sicurezza informatica nell'operatività dei sistemi e delle postazioni di lavoro |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi |

| | |
|---|---|
| | Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità<br>Competenze sulle metodologie e sui tool di analisi forense |

## 2.6 SECURITY SPECIALIST

| Qualifica professionale | Security specialist |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 4 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati<br>**Policy e strategie**<br>Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione<br>**Processi**<br>Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati<br>Progetta misure di sicurezza per proteggere reti e sistemi<br>**Analisi dei sistemi**<br>Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore<br>Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza<br>**Awareness**<br>Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices<br>**Response e contromisure**<br>A seguito delle minacce di sicurezza rilevate o di eventuali incidenti, suggerisce e sviluppa contromisure<br>Simula scenari di perdita di dati per valutare l'efficacia dei piani di ripristino esistenti<br>**Operations**<br>Installa, configura e gestisce apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc. |

| | |
|---|---|
| | Configura, gestisce ed utilizza sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc. per identificare tempestivamente minacce ed eventi di sicurezza<br>Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Fornisce competenze e leadership al team di gestione degli incidenti<br>Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica<br>ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.7 SECURITY SPECIALIST H24

| Qualifica professionale | Security specialist H24 |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 4 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati<br>**Policy e strategie**<br>Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione<br>**Processi**<br>Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati<br>Progetta misure di sicurezza per proteggere reti e sistemi<br>**Analisi dei sistemi**<br>Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza<br>**Awareness**<br>Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices<br>**Response e contromisure**<br>A seguito delle minacce di sicurezza rilevate o di eventuali incidenti, suggerisce e sviluppa contromisure<br>Simula scenari di perdita di dati per valutare l'efficacia dei piani di ripristino esistenti<br>**Operations**<br>Installa, configura e gestisce apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Configura, gestisce ed utilizza sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... per identificare tempestivamente minacce ed eventi di sicurezza<br>Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Fornisce competenze e leadership al team di gestione degli incidenti<br>Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente |

| | |
|---|---|
| | Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica<br>ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.8 SECURITY ANALYST SENIOR

| Qualifica professionale | Security Analyst senior (malware analyst, Intrusion detection, etc ) |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 4 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate |

| | |
|---|---|
| | **Policy e strategie**<br>Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente<br>Tecnologie e sistemi di sicurezza<br>Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza<br>**Analisi dei sistemi**<br>Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza<br>**Operations**<br>Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Effettua attività di reverse engineering per analizzare malware ed il relativo potenziale impatto nel corso di attacchi o a seguito di incidente di sicurezza<br>Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati<br>**VA & PT**<br>Analizza i report sulle vulnerabilità per determinare i livelli di rischio e consigliare soluzioni per mitigarlo |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse |

| | |
|---|---|
| | Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.9 SECURITY ANALYST JUNIOR

| Qualifica professionale | Security Analyst junior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui 2 nella funzione |
| Profilo professionale | **Analisi dei rischi**<br>Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate<br>**Tecnologie e sistemi di sicurezza**<br>Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza<br>**Analisi dei sistemi**<br>Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza<br>**Operations**<br>Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Effettua attività di reverse engineering per analizzare malware ed il relativo potenziale impatto nel corso di attacchi o a seguito di incidente di sicurezza<br>Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati<br>**VA & PT**<br>Analizza i report sulle vulnerabilità per determinare i livelli di rischio e consigliare soluzioni per mitigarlo |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate |

| | |
|---|---|
| | Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.10 VULNERABILITY RESEARCHER / ETHICAL HACKER SENIOR

| Qualifica professionale | Vulnerability researcher / Ethical Hacker senior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 4 nella funzione |
| Profilo professionale | **VA & PT**<br>Analizza i sistemi esposti e la struttura della rete dell'Ente ed identifica potenziali siti di penetrazione. Evidenzia le aree a più alto rischio di sicurezza. Fornisce feedback e suggerimenti per il rimedio o la mitigazione delle vulnerabilità.<br>Effettua analisi di vulnerabilità e penetration test<br>Implementa nuove metodologie di test da applicare, in accordo con l'Ente per le verifica dei sistemi |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate |

| | |
|---|---|
| | Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di individuare le metodologie e i tool di attacco più appropriati per effettuare penetration testing<br>Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) |

## 2.11 VULNERABILITY RESEARCHER / ETHICAL HACKER JUNIOR

| Qualifica professionale | Vulnerability researcher / Ethical Hacker junior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 3 anni, di cui 1 nella funzione |
| Profilo professionale | **VA & PT**<br>Analizza i sistemi esposti e la struttura della rete dell'Ente ed identifica potenziali siti di penetrazione. Evidenzia le aree a più alto rischio di sicurezza. Fornisce feedback e suggerimenti per il rimedio o la mitigazione delle vulnerabilità.<br>Effettua analisi di vulnerabilità e penetration test<br>Implementa nuove metodologie di test da applicare, in accordo con l'Ente per le verifica dei sistemi |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità<br>Capacità di individuare le metodologie e i tool di attacco più appropriati per effettuare penetration testing<br>Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software |

| | |
|---|---|
| | Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) |

## 2.12 INCIDENT HANDLER / RESPONSE SENIOR

| Qualifica professionale | Incident handler / response senior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 8 anni, di cui 5 nella funzione |
| Profilo professionale | **Policy e strategie**<br>Redige ed aggiorna le policy e le procedure di gestione degli incidenti<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Fornisce competenze e leadership al team di gestione degli incidenti<br>Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati<br>Identifica e gestisce le problematiche operative durante i processi di risposta agli incidenti, suggerisce e implementa azioni correttive<br>In caso di incidente di sicurezza, agisce quale punto di collegamento tra il personale del SOC, dell'IT e la committenza |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence |

| | |
|---|---|
| | Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

### 2.13 INCIDENT HANDLER / RESPONSE JUNIOR

| Qualifica professionale | Incident handler / response junior |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 5 anni, di cui 3 nella funzione |
| Profilo professionale | **Policy e strategie**<br>Redige ed aggiorna le policy e le procedure di gestione degli incidenti<br>**Gestione incidenti**<br>Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione<br>Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati<br>Identifica e gestisce le problematiche operative durante i processi di risposta agli incidenti, suggerisce e implementa azioni correttive<br>In caso di incidente di sicurezza, agisce quale punto di collegamento tra il personale del SOC, dell'IT e la committenza |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa<br>Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc...<br>Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... |

| | |
|---|---|
| | Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...<br>Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità |

## 2.14 DIGITAL FORENSIC

| Qualifica professionale | Digital forensic |
|---|---|
| Titolo di studio | Laurea in discipline tecniche o cultura equivalente |
| Anzianità lavorativa | Minimo 6 anni, di cui 5 nella funzione |
| Profilo professionale | Effettua raccolte ed analisi di dati relativi ad attacchi informatici e attività illecite sui sistemi dell'Ente<br>E' responsabile del rilevamento, della raccolta e dell'analisi di tutte le potenziali prove di reato informatico su sistemi, reti e dispositivi<br>Sottopone le prove raccolte al personale dell'Ente, collabora e supporta l'Ente nello svolgimento di indagini da parte delle Forze di polizia e nell'attivazione di azioni penali. Supporta ed assiste l'avvocatura dell'Ente nel comprendere le implicazioni di quanto rilevato in merito alle prove raccolte.<br>Fornisce competenze avanzate per il l'analisi dei dati relativi agli incidenti di sicurezza, criminalità informatica, pirateria informatica, frode, archiviazione e distribuzione di contenuti illegali<br>Fornisce consulenza in merito a normative e standard in caso di violazione di sicurezza<br>Assiste l'Ente durante le indagini penali in caso di richieste tecniche da parte delle forze di Polizia o della Magistratura<br>Redige relazioni tecniche che possano essere utilizzate in tribunale |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |

| | |
|---|---|
| Conoscenze approfondite in ambito sicurezza | Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Competenze sulle metodologie e sui tool di analisi forense |

## 2.15 CYBERSECURITY & PRIVACY LEGAL ADVISOR

| Qualifica professionale | CyberSecurity & Privacy Legal Advisor |
|---|---|
| Titolo di studio | Laurea in discipline tecniche / giuridiche o cultura equivalente |
| Anzianità lavorativa | Minimo 6 anni, di cui 5 nella funzione |
| Profilo professionale | **Policy e strategie**<br>Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente<br>**Legal**<br>Eroga consulenza normativa in materia di sicurezza informatica<br>Verifica la conformità delle policy e delle procedure dell'Ente rispetto alla normativa in materia di protezione dei dati personali e di cybersecurity<br>Redige DPIA, Accordi sul trattamento dei dati, privacy policy, informative, valutazione in merito alla base giuridica dei trattamenti<br>Assiste l'Ente durante eventuali indagini penali inerenti reati informatici |
| Conoscenze e competenze | Capacità di comprendere le esigenze del committente<br>Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate<br>Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica |
| Conoscenze approfondite in ambito sicurezza | Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi<br>Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)<br>Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali<br>Conoscenza delle metodologie di analisi, valutazione e gestione del rischio<br>Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza<br>Competenze sulle metodologie e sui tool di analisi forense |