La figura tecnica necessaria per l'area IT deve coprire una serie esigenze inerenti alla gestione degli apparati aziendali, ai sistemi informatici in generale ed alla loro integrazione nell'ambito dei progetti industria 4.0. Deve inoltre dare supporto nel processo di digitalizzazione dei dati aziendali (sistema ERP aziendale, MES, ecc..). Di seguito è riportato un elenco delle competenze di base richieste:

- Conoscenza del funzionamento dei sistemi informatici: essere in grado di capire come i vari hardware interagiscono e come essi e i software lavorano insieme.
- Conoscenza dei principali **linguaggi di programmazione** per applicazioni e software.
- Conoscenza dei più diffusi programmi di diagnostica per la localizzazione della sorgente dei problemi.
- Esperienza nell'ambito delle tecnologie per lo **smart working.**
- Capacità di **disaster recovery** e **business continuity**.
- Conoscenze di base in ambito della tutela della privacy e protezione dei dati;
- Esperienza con i sistemi operativi più utilizzati dalle aziende.
- Esperienza con i vari **sistemi di storage** (SAN e NAS).
- Ottima conoscenza del funzionamento dei principali modelli di **database relazionali** (DBMS: Oracle, Microsoft SQL Server, MySQL, PostgreSQL...) e **non relazionali** (NoSQL: MongoDB, Cassandra…); competenza nei diversi sistemi operativi; conoscenza dei principali linguaggi di codifica per banche dati; conoscenza della normativa sulla protezione dei dati;

In aggiunta deve saper:

- Verificare periodicamente lo stato di software e hardware per **identificare e risolvere i problemi** che li riguardano.
- Installare e configurare nuove tecnologie e aggiornamenti.
- Fornire **supporto tecnico** al personale all'interno dell'azienda.
- **Gestire gli account** dei collaboratori (email, accessi al gestionale e ai software) e supporto in caso di problematiche.
- Utilizzare di programmi diagnostici e troubleshooting.

Nell'ambito della cyber security vanno aggiunte e mansionate competenze più specifiche relative a:

- Gestione dei **sistemi di prevenzione** aziendali.
- Monitoraggio della corretta esecuzione delle **practice di sicurezza**.
- **Implementazione di misure atte a proteggere i dati e le informazioni** sensibili dell'azienda (come **firewall** e sistemi di **crittografia**).
- Aggiornamento dei **security tool** utilizzati.
- Individuazione delle intrusioni (i cosiddetti **Data Breach**) e di attività non autorizzate.
- Raccolta delle informazioni sugli incidenti al fine di siolare i parametri utili per prevedere e neutralizzare eventuali problematiche future.
- Studiare ed eventualmente redigere o aggiornare **security policies** aziendali.

Per fare ciò è necessario possedere le seguenti competenze in aggiunta a quanto specificato in precedenza:

- Competenze di **Data Mining**, **Statistical Analysis** e **Malware Analysis**.

- Conoscenza delle principali piattaforme per il **penetration testing** (come **Metasploit**, **Nmap** e **Wireshark**).
- Conoscenza degli strumenti di **Information Gathering**.
- Conoscenza di base dei principali **linguaggi di scripting.**
- Abilità in ambito **Ethical Hacking.**