

Analisi dei fabbisogni formativi ICT Cybersecurity 2026

Analisi regionale e locale

1

QUADRO DI SINTESI

Il mercato della cybersecurity è in forte espansione; in Italia il settore vale oltre 2,78 miliardi di euro e una stima di 100.000 esperti necessari per colmare il "gap" di talenti nei prossimi anni¹

I 3 Pilastri della crescita in Italia:

1. *Motori degli investimenti*: la Pubblica Amministrazione, il settore Finance (banche e assicurazioni) e l'aumento degli attacchi ransomware spingono le aziende ad aumentare i budget.
2. *Normative stringenti*: l'entrata a regime della Direttiva NIS2 (che impone severi obblighi di sicurezza a energia, trasporti, sanità e finanza) sta costringendo le organizzazioni ad assumere specialisti certificati.
3. *Fabbisogno di figure specializzate*: alle aziende mancano profili operativi e strategici, tra cui Security Analyst, Risk Manager e CISO.

L'analisi dei fabbisogni formativi in cybersecurity in Toscana risponde da un lato, alla necessità di adeguamento normativo stringente, dovuto alla Direttiva NIS 2; dall'altro, alla necessità di proteggere un tessuto produttivo caratterizzato da MPMI e da una fitta rete di enti locali.

La Regione Toscana ha sviluppato un ecosistema pubblico-privato, focalizzato su queste competenze: da strutture che offrono strumenti di self-assessment e mappatura del gap tecnologico a centri di competenza tecnologica, come di seguito:

- **C3T (Centro di Competenza Cybersecurity Toscano)**: nato dalla collaborazione tra Regione e università toscane, mette a disposizione l'**Osservatorio Toscano sulla Cyber Security**. Fornisce alle imprese strumenti gratuiti di Cybersecurity Readiness per misurare empiricamente la maturità aziendale e definire i piani di riqualificazione

¹ <https://www.osservatori.net/comunicato/cybersecurity-data-protection/cybersecurity-italia-mercato-crescita/>

- **CSIRT Regionale (Computer Security Incident Response Team):** un team dedicato (gestito operativamente dal consorzio Medis) che centralizza la telemetria degli incidenti sul territorio, fungendo da "motore" per indirizzare la formazione specifica dove si concentrano i reali attacchi informatici.

L'analisi dei fabbisogni in Toscana dovrà necessariamente declinarsi in base alle peculiarità dei settori chiave del territorio:

1. Piccole e Medie Imprese (manifatturiero, artigianato, filiere settoriali)

- **Contesto:** strutture snelle, spesso prive di un reparto IT dedicato, fortemente esposte a ransomware e truffe via email.
- **Fabbisogno Formativo:** corsi di cyber-higiene per impiegati amministrativi (focalizzati su frodi di pagamento e CEO fraud). Formazione per i titolari sull'analisi del rischio della catena di fornitura (Supply Chain) richiesta dai grandi committenti internazionali.

2. Settore Turistico e Ricettivo

- **Contesto:** raccolta massiva di dati personali, numeri di carte di credito e utilizzo diffuso di canali di prenotazione terzi (OTA).
- **Fabbisogno Formativo:** moduli specifici sulla conformità **GDPR** applicata al turismo, gestione sicura dei POS digitali e protezione delle reti Wi-Fi destinate agli ospiti.

3. Enti Locali e Comuni del Territorio

- **Contesto:** Frammentazione dei sistemi informativi dei piccoli Comuni toscani e obbligo di conformità ai requisiti di sicurezza dettati dall'Agenzia per la Cybersicurezza Nazionale (ACN) e dalla NIS 2.
- **Fabbisogno Formativo:** formazione obbligatoria per amministratori e tecnici comunali sulla gestione del patrimonio informativo e sui processi di Incident Response cooperativi con lo CSIRT regionale.

4. Settore Sanitario (Aziende USL ed ESTAR)

- **Contesto:** Alta criticità dei dati sensibili e forte spinta verso la telemedicina.
- **Fabbisogno Formativo:** corsi specialistici sullo sviluppo sicuro del software e sull'analisi dei rischi legati ai dispositivi medicali connessi (IoT).

L'intelligenza artificiale sta modificando il mercato del lavoro tecnologico anche in Italia, ma nella cybersecurity l'effetto non coincide con una semplice sostituzione delle competenze umane tramite automazione. La diffusione di strumenti generativi, codice prodotto con assistenti software, servizi cloud e sistemi integrati aumenta i processi digitali da controllare e rende più complessa la gestione del rischio.

Per questo, la domanda di lavoro cyber tende a spostarsi verso profili capaci di unire competenze tecniche, conoscenza normativa, sicurezza applicativa, governo dei fornitori e risposta agli incidenti.

L'AI può ridurre attività ripetitive di monitoraggio o produzione documentale, ma amplia il bisogno di figure in grado di verificare gli output automatici, proteggere ambienti ibridi e tradurre il rischio tecnico in decisioni organizzative.

I profili più richiesti uniscono competenze tecniche, normative e di intelligenza artificiale.

ANALISI TERRITORIALE E PROGETTUALE IN TOSCANA

1. Premessa e finalità del documento
2. Contesto territoriale e scenario digitale
3. Evoluzione della domanda di competenze cybersecurity
4. Analisi dei fabbisogni formativi delle imprese
5. Competenze richieste e aree prioritarie di formazione
6. Profili professionali emergenti
7. Prospettive occupazionali in Toscana
8. Il ruolo di Hub per competenze, innovazione e competitività del territorio: gli ecosistemi per l'innovazione
9. Considerazioni conclusive

3

1. Premessa e finalità del documento

La progressiva trasformazione digitale dei processi produttivi, organizzativi e commerciali ha reso la cybersecurity un elemento strategico per la competitività delle imprese e per la protezione del patrimonio informativo.

L'aumento delle minacce informatiche, la diffusione di servizi digitali, l'utilizzo di infrastrutture cloud e la crescente interconnessione dei sistemi aziendali hanno determinato una forte richiesta di competenze specialistiche in grado di prevenire, individuare e gestire i rischi cyber.

Il presente documento ha l'obiettivo di analizzare i fabbisogni formativi e professionali nell'ambito della cybersecurity, con particolare riferimento al contesto regionale toscano e all'ecosistema di innovazione rappresentato dal Polo Tecnologico di Navacchio.

L'analisi è finalizzata a:

- individuare le competenze maggiormente richieste dalle imprese;
- evidenziare eventuali carenze formative presenti nel mercato del lavoro;
- definire aree di intervento formativo coerenti con le esigenze aziendali;
- delineare le principali prospettive occupazionali del settore.

2. Contesto territoriale e scenario digitale

La Toscana presenta un sistema economico caratterizzato dalla presenza di imprese manifatturiere, aziende tecnologiche, startup innovative, centri di ricerca e realtà impegnate nei processi di innovazione digitale.

La crescita dell'economia digitale ha favorito lo sviluppo di nuovi servizi e modelli produttivi, aumentando tuttavia la necessità di garantire adeguati livelli di sicurezza informatica.

Il territorio regionale sta evidenziando un particolare interesse verso:

- digitalizzazione dei processi aziendali;
- sviluppo di soluzioni software e piattaforme digitali;
- utilizzo di tecnologie cloud;
- applicazioni IoT e sistemi connessi;

- protezione dei dati aziendali e personali.

3. Evoluzione della domanda di competenze cybersecurity

La cybersecurity non rappresenta più un ambito esclusivamente tecnico riservato ai reparti IT, ma una funzione strategica che coinvolge l'intera organizzazione.

Le imprese necessitano di figure capaci di:

- proteggere infrastrutture e sistemi informativi;
- analizzare vulnerabilità e minacce;
- gestire incidenti informatici;
- applicare metodologie di sicurezza nello sviluppo software;
- garantire conformità normativa;
- supportare i processi decisionali attraverso la valutazione del rischio.

La richiesta di personale qualificato risulta in crescita sia presso aziende ICT specializzate sia presso imprese tradizionali che stanno affrontando percorsi di trasformazione digitale.

4. Analisi dei fabbisogni formativi delle imprese

L'analisi evidenzia una domanda articolata di competenze suddivisibile in quattro principali aree.

4.1 Cultura aziendale della sicurezza

Formazione su:

- riconoscimento delle minacce informatiche;
- phishing e tecniche di ingegneria sociale;
- gestione sicura delle credenziali;
- protezione delle informazioni aziendali;
- corretto utilizzo degli strumenti digitali.

4.2 Competenze tecniche specialistiche

Le principali esigenze riguardano:

- sicurezza delle reti informatiche;
- configurazione sicura dei sistemi;
- analisi delle vulnerabilità;
- monitoraggio degli eventi di sicurezza;
- gestione degli incidenti;
- sicurezza cloud;
- sicurezza applicativa.

4.3 Competenze organizzative e normative

Sono richieste competenze relative a:

- gestione del rischio informatico;
- protezione dei dati personali;
- governance della sicurezza;
- procedure aziendali;
- continuità operativa e disaster recovery.

4.4 Competenze trasversali

Il professionista cybersecurity deve possedere anche:

- capacità analitiche;

- problem solving;
- capacità comunicative;
- capacità di lavorare in team multidisciplinari.

Competenze prioritarie di formazione

AREA FORMATIVA	COMPETENZE
Fondamenti di cybersecurity	Conoscenza delle principali minacce e contromisure
Network security	Protezione delle infrastrutture di rete
Vulnerability assessment	Individuazione e gestione delle vulnerabilità
Secure software development	Sviluppo di applicazioni più sicure
Cloud security	Gestione sicura degli ambienti cloud
Incident response	Analisi e gestione degli attacchi informatici
Cyber risk management	Valutazione e trattamento del rischio
Normativa e compliance	Applicazione di principi GDPR e sicurezza organizzativa

5

5. Profili professionali emergenti

Le esigenze del mercato stanno determinando una crescente richiesta delle seguenti figure:

PROFILO	FUNZIONE
Cybersecurity Specialist	Implementazione delle strategie di sicurezza
Security Analyst	Analisi degli eventi e delle minacce
SOC Analyst	Monitoraggio operativo della sicurezza
Security Engineer	Progettazione di sistemi protetti
Ethical Hacker	Individuazione preventiva delle vulnerabilità
Cloud Security Specialist	Sicurezza degli ambienti cloud
Incident Response Specialist	Gestione delle emergenze informatiche
Cyber Risk Analyst	Analisi e gestione del rischio

6. Prospettive occupazionali in Toscana

Il settore cybersecurity presenta prospettive occupazionali positive grazie alla crescente necessità delle imprese di rafforzare la propria sicurezza digitale.

Le opportunità riguardano:

- aziende ICT;
- società di consulenza tecnologica;
- imprese manifatturiere digitalizzate;
- startup innovative;
- organizzazioni pubbliche e private.

In particolare, risultano favoriti i profili in grado di combinare competenze informatiche con capacità di analisi del rischio e conoscenza dei processi aziendali.

La formazione specialistica in cybersecurity può rappresentare un importante strumento di inserimento lavorativo e riqualificazione professionale.

Risultati attesi

- incremento delle competenze cybersecurity disponibili sul territorio;
- maggiore capacità delle imprese di gestire i rischi digitali;
- sviluppo di nuove professionalità

6

7. Il ruolo di Hub per competenze, innovazione e competitività del territorio: gli ecosistemi per l'innovazione

La cybersecurity rappresenta una sfida che nessuna organizzazione può affrontare in modo isolato. La complessità delle minacce, la velocità dell'evoluzione tecnologica e la necessità di competenze specialistiche richiedono un approccio basato sulla collaborazione tra diversi attori.

In questo scenario assumono un ruolo fondamentale gli ecosistemi territoriali dell'innovazione, capaci di mettere in relazione:

- imprese;
- startup;
- centri di competenza;
- istituzioni;
- enti di formazione;
- professionisti.

Il territorio toscano dispone di condizioni favorevoli per sviluppare un modello integrato di crescita delle competenze digitali, nel quale la cybersecurity diventi un elemento abilitante per l'innovazione e la competitività.

All'interno di questo modello i Poli tecnologici possono svolgere una funzione di collegamento e accelerazione, favorendo la creazione di reti, competenze e opportunità, perché non rappresentano soltanto uno spazio fisico per imprese innovative, ma un ambiente nel quale si sviluppano relazioni, conoscenza e collaborazione.

Molte aziende, soprattutto PMI, hanno la necessità di migliorare il proprio livello di sicurezza digitale ma non dispongono internamente delle competenze necessarie.

I Poli possono favorire:

- incontro tra domanda e offerta tecnologica;
- accesso a specialisti;
- individuazione di soluzioni innovative;

- accompagnamento nei percorsi di trasformazione digitale.

La sicurezza digitale non riguarda esclusivamente i responsabili IT.

Una strategia efficace richiede consapevolezza diffusa all'interno delle organizzazioni.

I Poli possono promuovere:

- seminari per imprese;
- incontri divulgativi;
- workshop pratici;
- programmi di sensibilizzazione;
- iniziative rivolte a manager e personale non tecnico.

Uno dei principali ostacoli alla crescita della cybersecurity è la carenza di professionisti qualificati.

I Poli possono contribuire allo sviluppo di percorsi formativi attraverso la collaborazione con:

- Centri di competenza;
- ulteriori enti formativi;
- aziende tecnologiche.

Possibili iniziative:

- percorsi formativi sperimentali e tecnica specialistica
- percorsi per giovani talenti;
- formazione continua per professionisti;
- programmi upskilling-reskilling

La cybersecurity evolve rapidamente e richiede capacità di sperimentazione continua.

I Poli possono favorire:

- challenge tecnologiche;
- hackathon;
- programmi startup;
- collaborazione tra aziende consolidate e nuove imprese innovative.

Un modello collaborativo composto da:

Imprese

Contribuiscono attraverso:

- casi d'uso reali;
- fabbisogni tecnologici;
- opportunità occupazionali.

Università e ricerca

Contribuiscono attraverso:

- competenze scientifiche;
- ricerca applicata;
- formazione avanzata.

Poli Tecnologici

Svolgono il ruolo di:

- coordinamento;
- facilitazione;
- networking;
- trasferimento tecnologico.

8

Istituzioni

Supportano:

- strategie territoriali;
- programmi di finanziamento;
- sviluppo delle competenze.

10. Considerazioni conclusive

La cybersecurity rappresenta una grande opportunità per costruire un nuovo modello di sviluppo territoriale basato sulla conoscenza e sull'innovazione, che coinvolga l'ecosistema tutto dell'innovazione regionale.

La sfida non riguarda soltanto la protezione dei sistemi digitali, ma la costruzione delle competenze necessarie per governare il futuro tecnologico della Toscana.

L'analisi evidenzia come la cybersecurity costituisca un settore strategico per lo sviluppo economico e occupazionale della Toscana.

La crescente digitalizzazione delle imprese rende necessario investire nella formazione di competenze specialistiche capaci di rispondere alle nuove esigenze del mercato.

Il rafforzamento dell'offerta formativa in ambito cybersecurity rappresenta quindi un'opportunità per sostenere l'innovazione delle imprese, ridurre il divario tra domanda e offerta di lavoro e favorire la crescita di nuove professionalità qualificate nel territorio regionale.

