FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBERPRO TRAIN

Formazione professionale in cybersicurezza

Per pubbliche amministrazioni e PMI

Lorenzo Scatena
Segretario Generale, Fondazione Amaldi

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI

CYBERPRO TRAIN

Formazione professionale in cybersicurezza

per Pubbliche Amministrazioni e PMI

Forum Cyber4.0

Roma 05.06.2025

Lorenzo Scatena - Valerio Roscani

RAFFORZARE LA RESILIENZA CIBERNETICA DELL'EUROPA

CyberPro Train è un progetto europeo co-finanziato dal **Digital Europe Programme** per far fronte all'enorme richiesta di professionisti della cybersicurezza in Europa.

Il rischio: Minacce ai sistemi digitali

L'obbligo: Direttiva NIS2 e il ***Cyber Resilience Act***

L'opportunita: fornire a professionisti delle **PMI** e della **Pubblica Amministrazione** le competenze tecniche avanzate necessarie per proteggere infrastrutture critiche e dati sensibili.

PERCHÉ È IMPORTANTE

L'Unione Europea soffre nel 2025 di una **carenza di oltre 260.000 professionisti** della cybersicurezza.

Settori critici come salute, energia e trasporti sono particolarmente vulnerabili ad attacchi cyber.

Aziende e istituzioni pubbliche hanno sempre di più **bisogno urgente di personale formato** per rispettare i nuovi standard normativi e garantire la sicurezza dei propri sistemi.

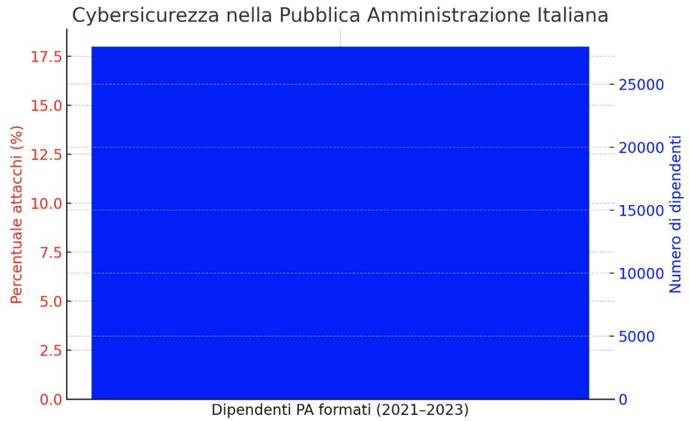
SFIDE NELLA PUBBLICA AMMINISTRAZIONE

Nella PA italiana, le difficoltà derivano da una molteplicità di fattori, tra cui:

1. **Frammentazione istituzionale**: la cybersicurezza è spesso gestita a livello locale o regionale, senza un coordinamento centralizzato efficace. Questo ostacola l'adozione di standard formativi comuni (Bergamaschi et al., 2020).

2. **Basso livello di competenze digitali**: studi dell'AgID (Agenzia per l'Italia Digitale) mostrano come una parte significativa del personale pubblico possegga competenze digitali di base, ma sia impreparata su tematiche avanzate come il phishing, la gestione degli accessi e la protezione dei dati (AgID, 2021).

3. **Vincoli burocratici e budgetari**: la formazione è spesso considerata un costo, non un investimento. Le rigidità nella spesa pubblica rendono difficile l'aggiornamento continuo del personale (Cerrillo i Martínez, 2018).



Fonte: AgID

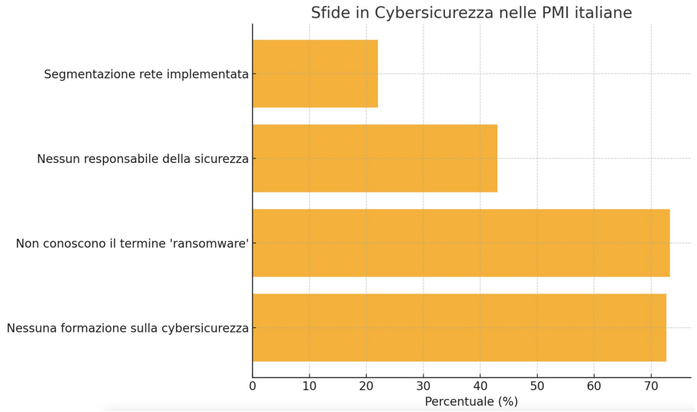
SFIDE NELLA PMI

Le PMI italiane rappresentano oltre il 90% del tessuto imprenditoriale nazionale, ma si trovano spesso in una condizione di vulnerabilità in ambito cyber per i seguenti motivi:

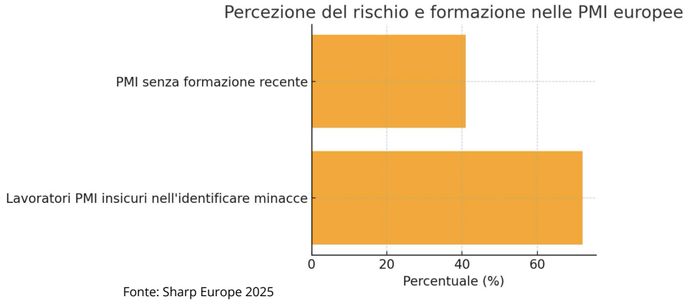
1. **Limitate risorse economiche e umane**: molte PMI non dispongono di un reparto IT dedicato, né di risorse per assumere esperti in cybersicurezza (ENISA, 2022).

2. **Bassa percezione del rischio**: svariati studi (es. Bocchi et al. (2021) evidenziano come molte PMI sottovalutino la probabilità e l'impatto degli attacchi informatici, trascurando la formazione interna.

3. **Assenza di cultura della sicurezza**: la sicurezza informatica è spesso vista come un problema tecnico o economico e non organizzativo. Manca un approccio integrato che coinvolga l'intera struttura aziendale (Furnell & Esmael, 2017).

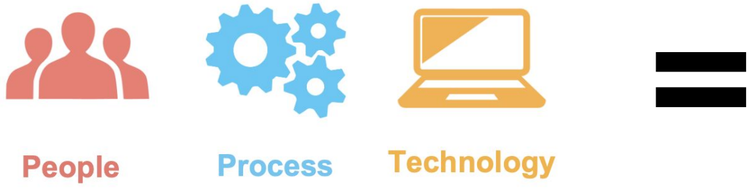


Fonte: Grenke Italia 2023



Fonte: Sharp Europe 2025

PROSPETTIVE E RACCOMANDAZIONI



Fonte: ENISA Cybersecurity for SMEs3

Per superare queste difficoltà, la letteratura propone alcune direttrici d'azione comuni:

- Adozione di programmi formativi **modulari e personalizzati**, pensati per differenti livelli di competenza e ruoli (Sommestad et al., 2014).
- **Collaborazioni pubblico-privato**: la sinergia tra PA, università e aziende può facilitare la diffusione di buone pratiche e competenze specialistiche.

AgID. (2021). *Linee guida per la formazione del personale pubblico in materia di competenze digitali*.

Bergamaschi, M., De Marco, M., & Braccini, A.M. (2020). *Cybersecurity governance in Italian public administration*. Journal of Information Security.

Bocchi, A., Lorusso, L., & Satta, L. (2021). *Cybersecurity in SMEs: A Case for Cultural Change*. Economia e Politica Industriale.

Cerrillo i Martínez, A. (2018). *Public administration and cybersecurity: managing risks and threats*. Government Information Quarterly.

ENISA. (2022). *Cybersecurity for SMEs – Challenges and Recommendations*.

Furnell, S., & Esmael, R. (2017). *The Role of Security Culture in Effective Cybersecurity Governance*. Computers & Security.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). *Variables influencing information security policy compliance: a systematic review of quantitative studies*. Information Management & Computer Security.

LA NOSTRA SOLUZIONE

Corsi di formazione modulari, **online** e **gratuiti** altamente professionalizzanti in formato sincrono e asincrono

Bootcamp con i maggiori player del settore

Formazione on-the job in data contour e SOC di aziende le ader di cybersicure

Un **Digital Handbook europeo** sulla cybersicurezza con best practices e lessons learned

- IT EXPERT NELLE PMI
- FUNZIONARI PUBBLICI CHE GESTISCONO DATI SENSIBILI O SERVIZI DIGITALI
- PROFESSIONISTI DI CYBERSICUREZZA
- OPERATORI IT NEI SETTORI DELLE INFRASTRUTTURE CRITICHE

FORMAZIONE STRUTTURATA PER AFFRONTARE SFIDE REALI

TRE verticali (Spazio, ITC, TLC)

Moduli Base

- Fondamenti di sicurezza informatica
- Fondamenti di sistemi operativi e database
- Reti e protocolli TCP/IP
- Introduzione alle normative e buone pratiche

Moduli Avanzati

- Sicurezza informatica – livello avanzato
- Gestione avanzata di sistemi operativi e database
- Sicurezza architetturale avanzata
- Sicurezza avanzata delle reti

Moduli su Tecnologie Strategiche

- Sicurezza avanzata nel Cloud
- Intelligenza Artificiale per la cybersicurezza

CARATTERISTICHE DEI CORSI

Formazione **modulare** e **flessibile**

Approccio **pratico** e basato su **casi reali**

Certificazione con modello **Open Badge**

Piattaforma dedicata e intuitiva

REGISTRATI ORA!

Unisciti a noi per contribuire
a **colmare il divario**
di competenze nella **cybersicurezza**
in Italia e in Europa.

Scannerizza il QR Code per entrare
in contatto con Cyberpro Train!

FONDAZIONE E. AMALDI · TESEAS · TIM · ABCorporation · S2GRUPO · Innovation Hive · 220.M.OJA · KIM3CN