# P.E.K.I.T. Security (solo certificazione)

***Permanent Education and Knowledge on Information Technology Project***

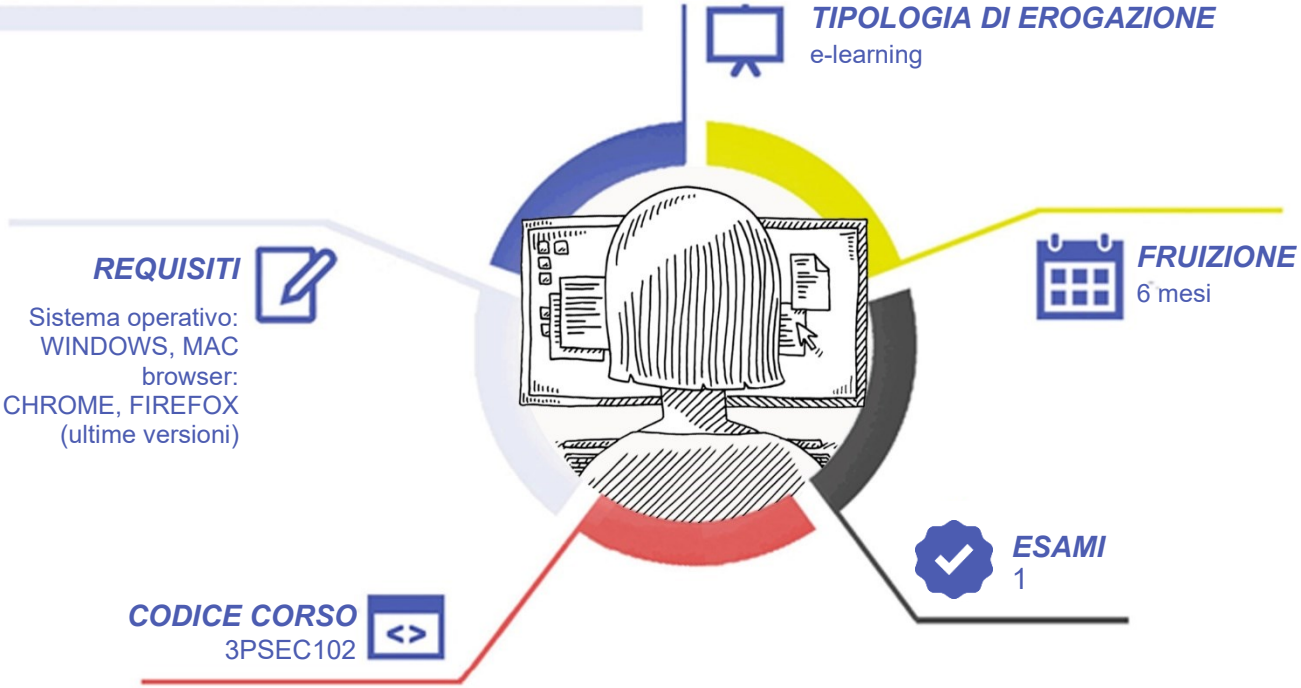
## A CHI SI RIVOLGE

Tutte le fasce di utenza, dai ragazzi della scuola primaria fino agli adulti e agli anziani.

## OBIETTIVI

PEKIT Security certifica le conoscenze, le competenze e le procedure necessarie a garantire la sicurezza dei sistemi informatici. Queste abilità sono proprie della figura professionale dell'Ethical Hacker. I contenuti si distinguono in 4 aree principali:

- Le reti informatiche: teoria, hardware, protocolli e strumenti di diagnostica
- Gli attacchi informatici: classificazione, fasi e tecniche di attacco, virus e malware.
- Concetti di base di sicurezza informatica: crittografia, firewall e dispositivi di sicurezza
- L'attività di Ethical Hacking: il penetration test, distribuzioni di Linux e i principali strumenti utilizzati dall'ethical hacker.



Interattiva editore

# PEKIT

## COMPETENZE CERTIFICATE

**1 Concetti di base**

1. **Concetti di base di sicurezza informatica:** I principi di base della sicurezza informatica - Gestione del rischio - Organizzazione della sicurezza - Standard ed enti di standardizzazione
2. **Nozioni di base sul funzionamento delle reti:** Classificare le reti - Il modello ISO/OSI
3. **L'hardware di rete:** I principali tipi di segnale e di mezzo trasmissivo - La scheda di rete - Gli apparati di connessione
4. **I principali protocolli di rete:** I protocolli di rete locale - L'architettura TCP/IP
5. **Diagnostica di rete e strumenti utili:** Comandi e funzionalità utilizzati per amministrare la rete

**2 Gli attacchi informatici**

1. **Nozioni generali sugli attacchi informatici:** La figura dell'hacker – Le fasi di un attacco informatico
2. **Il malware:** Gli antivirus - Le principali tipologie di malware
3. **Classificazione degli attacchi**: Le categorie generali di attacco - Le principali tecniche di attacco

**3 Sicurezza informatica**

1. **L'utilizzo delle password:** Scegliere e gestire una password - Gli attacchi alle password
2. **Crittografia:** Le tecniche di crittografia - Gestire le chiavi - Principali algoritmi di crittografia
3. **Soluzioni di sicurezza in rete:** I firewall - Altri dispositivi di sicurezza

**4 L'attività di Ethical Hacking**

1. **Concetti di base sull'attività di Ethical Hacking:** Il penetration test - Modalità di svolgimento del penetration test - Apetti legali, contrattuali e normative - I report relativi all'attività svolta
2. **Strumenti utilizzati nelle attività di penetration test:** Le distribuzioni Linux dedicate al penetration test - I principali programmi utilizzati per le attività di penetration test

Syllabus rev. 1.0

## SUPERAMENTO

La certificazione PEKIT Security si consegue superando l'esame proposto, composto da 36 quesiti da risolvere entro un tempo massimo di 45 minuti. Il superamento dell'esame esame si ottiene al raggiungimento della soglia minima del 75% del punteggio massimo teorico.

## CERTIFICAZIONI

Le certificazioni e i corsi online P.E.K.I.T sono titoli validi ai fini dell'aggiornamento delle graduatorie di II e III fascia. Per ciascuna certificazione informatica sono riconosciuti 0,5 punti. È possibile sommare fino ad un massimo di 4 titoli, ottenendo così un riconoscimento complessivo pari a 2 punti.

## RICONOSCIMENTI

La certificazione PEKIT si attiene al **DigComp 2.1 | 2017** che definisce i parametri per la valutazione del livello di competenza digitale dei cittadini europei ed è stato sviluppato dal Joint Research Centre (JRC) – The European Commission's science and knowledge service dell'Unione Europea.
La certificazione PEKIT è inoltre riconosciuta dal **MIUR** con provvedimento A00DGPERS_6235 del 25/06/2010.

## I VANTAGGI DELL'E-LEARNING

*- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali*
*- Accessibilità ovunque e in ogni momento - Possibilità di rivedere le lezioni anche dopo aver terminato il corso*