

Corso  
Completamente  
Finanziato

Borsa  
di Studio

**ITS** | UMBRIA  
ACADEMY

**POST-DIPLOMA**

Biennio accademico 2025\_27



Corsi Area

# CYBERSECURITY

## Tecnico superiore in cybersecurity

### PROFILO PROFESSIONALE

Il corso forma specialisti nella **protezione dei sistemi informatici** e degli asset informativi. Le competenze acquisite includono lo **sviluppo e la gestione di policy di sicurezza** allineate con la strategia aziendale e la gestione del rischio.

Il percorso fornisce le competenze per **analizzare e mitigare le minacce di natura tecnica, umana e organizzativa, consentendo di individuare e risolvere vulnerabilità su infrastrutture IT e applicazioni. Inoltre, il corso include la gestione della risposta agli incidenti, applicando tecniche di prevenzione, rilevamento e analisi forense per investigare su dispositivi compromessi e identificarne le cause.**

### ARTICOLAZIONE DEL PERCORSO

**Durata:** Corso gratuito biennale (1800/2000 ore tra formazione e tirocinio di cui più dell'80% in laboratorio o aziende)

**Impegno:** 30-35 ore settimanali in aula, fino a 40 ore settimanali in tirocinio

**Frequenza:** Obbligatoria per l'80% del monte orario

### TITOLO DI STUDIO CONSEGUITO

Diploma di Istruzione Terziaria di V livello EQF rilasciato dal Ministero dell'Istruzione.

**SEDE PERUGIA**

**FUTURA** LA SCUOLA  
PER L'ITALIA DI DOMANI



### TITOLO DI ACCESSO

Diploma di Scuola Secondaria di Secondo Grado o Diploma IFTS.

### DURATA

1800/2000 ore distribuite in 2 anni di cui 800 di tirocinio aziendale

### METODOLOGIA DIDATTICA

Docenti che provengono dalle imprese e tirocini in azienda. Metodologia didattica applicativa e laboratoriale.

### SERVIZIO PLACEMENT

Un'azione personalizzata e continuativa con elevate percentuali di assunzione

	UNITA' FORMATIVA	ORE
<b>PARTE TRASVERSALE</b>	COMPORTAMENTO ORGANIZZATIVO INGLESE INFORMATICA INFORMATICA AVANZATA TECNICHE DI PROGRAMMAZIONE INTERNET TECHNOLOGIES	
<b>PARTE SPECIALISTICA</b>	HUMAN SECURITY SECURITY OF OPERATIONAL TECHNOLOGY SICUREZZA DEL CLOUD AMMINISTRAZIONE DI SISTEMA VULNERABILITY ASSESSMENT SECURITY ANALYST DATA SECURITY SOFTWARE SECURITY CONNECTION SECURITY DIGITAL FORENSICS RISK MANAGEMENT INCIDENT RESPONSE	
<b>TOTALE FORMAZIONE AULA E LABORATORIO</b>		<b>1200</b>
<b>TIROCINIO IN AZIENDA</b>		<b>800</b>
<b>TOTALE</b>		<b>2000</b>

## COSA SA FARE

- Identifica minacce cyber e implementa misure difensive.
- Esegue risk assessment, vulnerability assessment, e penetration testing.
- Organizza infrastrutture IT secondo le migliori pratiche di sicurezza.
- Gestisce e protegge dati sensibili all'interno di aziende e pubbliche amministrazioni.
- Gestisce la risposta agli incidenti, con tecniche di prevenzione, rilevamento e analisi dei malware per identificare e neutralizzare le minacce.
- Esegue analisi forense per investigare su dispositivi compromessi e determinare le cause degli attacchi informatici.

