

## PROGRAMMA DEL CORSO DI RETI DI CALCOLATORI E CYBERSECURITY

### SETTORE SCIENTIFICO

INF/01

### CFU

12

### OBIETTIVI

*/\*\*/*

Obiettivo del corso è di apprendere la struttura e le meccaniche dietro il funzionamento di una rete di elaboratori, con particolare attenzione verso la rete Internet.

Inoltre, il corso ha come obiettivo l'apprendimento delle nozioni di base della sicurezza informatica.

Apprendere la struttura di una rete di elaboratori, le meccaniche fondamentali della rete Internet e i più diffusi protocolli di rete. Padroneggiare le nozioni fondamentali della sicurezza informatica, imparando a riconoscere le principali tipologie di attacco informatico e le relative contromisure. Acquisire familiarità con i principali protocolli di crittografia.

### DESCRIZIONE

*/\*\*/*

Il corso è suddiviso in due moduli:

Reti di calcolatori e Internet Sicurezza informatica

Nel primo modulo, verrà esplorata l'architettura delle reti di calcolatori e delle reti di massa come Internet, con particolare attenzione alla struttura dello stack protocollare e dei principali protocolli di rete per le comunicazioni attraverso Internet. In questo modulo, verranno esaminati protocolli di uso fondamentale come HTTP e IP, e verranno introdotti concetti a basso livello come le comunicazioni attraverso reti cablate e wireless.

Nel secondo modulo, verranno presentati i più utilizzati e diffusi paradigmi di sicurezza, con particolare attenzione agli algoritmi crittografici a chiave simmetrica e asimmetrica. Verranno introdotte le nozioni di hashing sicuro e i principali protocolli per le comunicazioni sicure in Internet. Infine, verranno presentate le più diffuse applicazioni pratiche della cybersecurity, come il multimedia forensics, le comunicazioni anonime e la blockchain.