**V ANNO**

| **Disciplina: Sistemi e Reti** | | **Ore settimanali: 4 (di cui 3 in compresenza)** | |
| --- | --- | --- | --- |
| **NUCLEO** | **COMPETENZE** | **OBIETTIVI MINIMI D’APPRENDIMENTO** | **CONTENUTI** |
| Il livello delle applicazioni  Il protocollo HTTP  VLAN: Virtual Local Area Network  Tecniche crittografiche per la protezione dei dati  Reti, sicurezza, DMZ e Trusted  Reti mobili e sicurezza  Modello client/server e distribuito per i servizi di rete. | * Configurare, installare e gestire sistemi di elaborazione dati e reti * Scegliere dispositivi e strumenti in base alle loro caratteristiche funzionali. * Descrivere e comparare il funzionamento di dispositivi e strumenti elettronici e di telecomunicazione * Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare * Analizzare il valore, i limiti e i rischi delle varie soluzioni tecniche per la vita sociale e culturale con particolare attenzione alla sicurezza nei luoghi di vita e di lavoro, alla tutela della persona, dell’ambiente e del territorio | * Individuare le tipologie di applicazione di rete * Comprendere il concetto di porta e di socket * Comprendere il protocollo Telnet e il suo utilizzo * Comprendere i meccanismi del protocollo HTTP * Utilizzare i comandi FTP * Individuare il formato del messaggio HTTP * Individuare pregi e difetti delle VLAN * Riconoscere VLAN tagged, untagged e ibride * Applicare le VLAN in base alla tipologia di rete richiesta * Riconoscere le tecniche monoalfabetiche per trasposizione e sostituzione * Individuare i campi di applicazione delle firma digitale * Saper distinguere tra i cifrari DES, 3-DES e IDEA * Saper garantire la sicurezza informatica e la riservatezza dei dati personali * Configurare una DMZ * Connettere un Access Point a una rete LAN * Saper definire le topologie delle reti wireless * Individuare i dispositivi connessi a una rete wireless * Individuare i possibili attacchi alla sicurezza di una rete wireless * Autenticare dispositivi wireless con server Radius * Utilizzare sistemi di protezione WPA2 PSK e WPA2 TKIP * Prendere i dovuti provvedimenti per la protezione dai principali tipi di attacco informatico * Individuare le caratteristiche di server farm, partitioning e cloning | * Il livello delle applicazioni nel modello ISO-OSI e TCP/IP * Il Web * FTP * Le Email * DNS * Telnet * HTTP * Le VLAN * Il protocollo VTP e l’Inter-VLAN Routing * La crittografia simmetrica * La crittografia asimmetrica * Sistemi di autenticazione * La sicurezza nei sistemi informativi * La sicurezza delle connessioni con SSL/TLS * VPN * Firewall, proxy, ACL e DMZ * Le connessioni wireless * L’autenticazione nelle reti wireless * La trasmissione wireless * L’architettura delle reti wireless * Le applicazioni e i sistemi distribuiti * Architettura dei sistemi Web * Amministrazione di una rete * Active Directory * La sicurezza della rete |
| **Metodi** | **Strumenti** | **Verifiche** | **Valutazione** |
| * Lezioni frontali. * Lettura e commento dei libri di testo. * Discussioni di gruppo. * Lavoro individuale e di gruppo. * Metodo intuitivo-deduttivo. * Lezioni interattive e dialogate alla scoperta di relazioni, nessi, regole. * Lavoro guidato e individualizzato per gli alunni con difficoltà di apprendimento. * Cooperative learning. * Peer to peer. * Classi virtuali. | * Libro di testo, eserciziario. * Sussidi didattici di supporto. * Lavagna e/o L.I.M. * Piattaforme multimediali. * Internet. | **PROVE SCRITTE**   * Prove chiuse * Prove aperte * Prove miste * Relazioni su esercitazioni svolte in simulazione   **PROVE ORALI**   * Interrogazioni (esposizione orale o con supporto informatico in modalità DAD) * Interventi * Prodotti multimediali   **COMPITO AUTENTICO** | **Griglie di valutazione**  Per la valutazione delle UDA si farà riferimento alle griglie approvate in sede dipartimentale e già allegate al PTOF  Per la verifica delle competenze trasversali si prevede di realizzare un compito autentico. |