POLO SCIENTIFICO TECNOLOGICO PROFESSIONALE "E. FERMI & G. GIORGI" LUCCA

INDIRIZZO: Informatica e Telecomunicazioni

DISCIPLINA: SISTEMI e RETI A.S. 2016/'17

Classe 5AIF

Docente: Lucia GIAMMARIO
ITP: Luciano CARLOTTI

Linee guida Secondo biennio e quinto anno

I risultati di apprendimento sopra riportati in esito al percorso quinquennale costituiscono il riferimento delle attività didattiche della disciplina nel secondo biennio e quinto anno. La disciplina, nell'ambito della programmazione del Consiglio di classe, concorre in particolare al raggiungimento dei seguenti risultati di apprendimento, relativi all'indirizzo, espressi in termini di competenza:

- 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;
- gestire progetti secondo le procedure e gli standard previsti dai sistemi aziendali di gestione della qualità e della sicurezza
- 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

MODULO 1: Problematiche di instradamento e sistemi di interconnessione nelle reti geografiche

U1- Le reti geografiche

OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
• Conoscere le varie modalità di inoltro dei pacchetti • Conoscere i protocolli principali e il loro utilizzo • Saper descrivere le varie tecnologie • Saper programmare un router •	• Il livello fisico • Il protocollo X.21 • Il protocollo fisico EIA RS-232C • Il livello data link • Il protocollo PPP • Architettura di una WAN • Le tecniche di commutazione: circuito, messaggio, pacchetto • Le tecnologie WAN • La rete PSTN • Velocità di trasmissione • I protocolli X/Y/Z-Modem • Programma di comunicazione • Linea commutata e dedicata • Reti digitali • La rete ISDN (cenni) • La rete Frame Relay • La rete ATM • Le reti DSL: ADSL,SDSL, HDSL,VDSL • I servizi SAT ADSL	• Configurazione router • Introduzione alla programmazione dei router Cisco: - user mode - privileged mode - configurazioni e IOS • Salvataggio e ripristino del file di configurazione • Configurazione delle interfacce

MODULO 2: Tecnologie informatiche per garantire la sicurezza e l'integrità dei dati e dei sistemi.

U1- Strategie per la sicurezza interna

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Conoscere problematiche e rischi afferenti alla gestione della rete privata	• Il fenomeno degli hackers e dei crackers • Misure fisiche di sicurezza • Processi organizzativi • Sicurezza interna	

U2- Protocolli per la sicurezza

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Conoscere potenzialità e limiti dei protocolli che implementano la sicurezza	• Protocollo Ipsec • Protocollo SSL/TLS	

Modulo3: Tecniche crittografiche applicate alla protezione dei sistemi e delle reti.

U1- Servizi di crittografia

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Descrivere i requisiti di sicurezza delle comunicazioni tra cui l'integrità, l'autenticazione e la riservatezza. • Descrivere la crittografia, la crittoanalisi e la crittologia. •	• Autenticazione, Integrità • Riservatezza, Non ripudio • Metodi di cifratura • Crittografia, Crittoanalisi e Crittologia	• Prova di cifratura

U2- Integrità di base, Autenticità e Riservatezza

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Descrivere l'importanza delle funzioni hash . • Descrivere le caratteristiche e le funzioni l'algoritmo MD5 e SHA • Descrivere come abilitare l'autenticità con HMAC. • Descrivere i componenti di gestione delle chiavi. • Descrivere la funzione degli algoritmi DES, 3DES e AES, SEAL, RC e DH	• Funzione hash • Integrità con MD5 and SHA-1 • Autenticazione con HMAC • Caratteristiche di gestione delle chiavi • Algoritmi di Crittografia simmetrica • Tecniche di crittografia Simmetrica • Scambio di chiavi Diffie-Hellman	

U3- Crittografia a Chiave pubblica

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Spiegare le differenze tra crittografia simmetrica e asimmetrica • Spiegare la funzionalità delle firme digitali • Descrivere il ruolo delle Autorità di Certificazione e dei Certificati Digitali	• Algoritmi a chiave asimmetrica • Chiave pubblica e privata • Crittografia a chiave pubblica • Firma digitale • Il framework PKI • Le autorità di certificazione • La gestione dei certificati • I protocolli standard ed i protocolli alternativi	• Analisi di un certificato digitale

Modulo 4: Reti private virtuali.

U1-Le reti VPN

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Descrivere i benefici di una VPN ed i loro benefici. • Configurare una VPN site-to-site con tunnel GRE Configurare le ACL crypto utilizzando CLI. • Configurare una mappa crittografica utilizzando CLI. • Spiegare come il panorama aziendale sta cambiando per supportare il telelavoro. • Configurare un server VPN • Collegare un client VPN utilizzando un software specifico	• Caratteristiche generali • Tipi di VPN: remote access, site to site • Il tunnel GRE • Gestione della sicurezza, autenticazione, crittografia, tunnelling	• Configurazione su Packet Tracer di una VPN site-t-site tra due router Cisco 2811

U2- Tecnologie di implementazione di una VPN

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Descrivere il protocollo IPsec e le sue funzioni di base. • Descrivere le fasi di negoziazione e configurazione di IPsec. • Preparare IPsec per rendere compatibili le ACL. • Confrontare l' accesso remoto con IPsec e SSL • Spiegare come SSL viene utilizzato per stabilire una connessione VPN sicura.	• Protocollo Ipsec • Protocollo SSL (cenni)	**ACL**

Modulo 5: Strumenti e protocolli per la gestione ed il monitoraggio delle reti

U2- M*onitoraggio delle reti*

OBIETTIVI:	CONTENUTI:	LABORATORIO:
• Saper utilizzare tecniche e strumenti per il monitoraggio delle reti • Comprendere la necessità di prevenire i malfunzionamenti e risolverli rapidamente	• Concetto di monitoraggio di una rete • Le utility di monitoraggio	• I comandi di monitoraggio di una rete: ping, traceroute, arp, nslookup, ipconfig, netstat