Fondazione ITS Academy Energia di Reggio Calabria

IV corso ITS per
"Tecnico Superiore in system administration, cybersecurity e AI per l'efficientamento energetico"
biennio 2026/2028

Piano di Studi

Ambito 1. Formazione di base

UFC n.	Titolo Unità Formativa / Modulo	Ore	Teoria	Pratica	Verif.
1	Inglese tecnico per l'ICT	**60**	30	28	2
2	Sicurezza sui luoghi di lavoro	**20**	6	13	1
3	Organizzazione aziendale e autoimprenditorialità	**20**	6	13	1
4	Comunicazione, personal branding e redazione del CV per professionisti ICT	**20**	6	13	1
5	Project Management e metodologie Agile	**20**	6	13	1
TOTALE Ore Formazione di base		**140**			

Ambito 2. Formazione specialistica

UFC n.	Unità Formativa / Modulo	Ore	Teoria	Pratica	Verif.
6	Architettura degli elaboratori e Fondamenti Sistemi Operativi	**40**	10	28	2
7	Fondamenti di programmazione e scripting per l'automazione IT	**50**	16	32	2
8	Algoritmi e strutture dati per l'elaborazione dei dati	**30**	10	18	2
9	Basi di dati relazionali e non relazionali	**30**	10	18	2
10	Fondamenti di Networking e protocolli TCP/IP	**40**	10	28	2
TOTALE Ore Formazione specialistica		**190**			

Ambito 3. Reti, sistemi e amministrazione

UFC n.	Unità Formativa / Modulo	Ore	Teoria	Pratica	Verif.
11	Progettazione delle reti: cablaggio, apparati e Wi-Fi	**40**	10	28	2
12	Amministrazione di sistemi Server	**40**	15	23	2
13	Gestione utenti, autenticazione e sicurezza degli accessi	**40**	10	28	2
14	Amministrazione di database con MySQL	**40**	10	28	2
15	Web server e application server	**30**	10	18	2
16	Cloud Computing, Storage e gestione dei dati	**40**	10	28	2
17	Virtualizzazione e containerizzazione	**30**	10	18	2

18	Monitoraggio, performance e troubleshooting	**20**	8	10	2
TOTALE Ore Reti, sistemi e amministrazione		**280**			

Ambito 4. Cybersecurity

19	Fondamenti e Governance della Sicurezza. L'Analisi del rischio	**30**	10	18	2
20	Vulnerability Assessment e Penetration Test	**40**	10	28	2
21	Hardening dei sistemi e protezioni perimetrali	**30**	10	18	2
22	Sicurezza Reti Wireless e 5G	**40**	10	28	2
23	Sandbox, Malware Analysis e Threat Detection	**30**	10	18	2
24	Disaster Recovery e Business Continuity Management	**40**	10	28	2
25	SOC, SIEM/SOAR e Threat Intelligence	**40**	10	28	2
26	Gestione delle vulnerabilità nei sistemi AI e Incident Response	**30**	10	18	2
27	Sicurezza dell'AI e Security-for-AI	**20**	6	13	1
28	Etica, normativa e responsabilità nella sicurezza (GDPR, NIS2)	**20**	6	13	1
TOTALE Ore Cybersecurity		**320**			

Ambito 5. Trasformazione digitale AI-based per l'efficientamento energetico

UFC n.	Unità Formativa / Modulo	Ore	Teoria	Pratica	Verif
29	Fondamenti di intelligenza artificiale ed AI generativa	**20**	6	13	1
30	Machine Learning e Large Language Model	**30**	10	18	2
31	Dispositivi intelligenti per l'automazione industriale e l'efficienza energetica	**40**	15	24	1
32	Sistemi SCADA, HMI e supervisione dei processi di efficienza energetica	**40**	10	28	2
33	Sistemi di automazione e AI Agents per l'efficientamento energetico	**30**	10	18	2
34	Normativa, Etica e sicurezza dell'IA	**20**	6	12	2
TOTALE Ore Trasformazione digitale AI-based per l'efficientamento energetico		**180**			

Programmazione dettagliata

Ambito 1. Formazione di base

UFC 1 – Inglese tecnico per l'ICT – ore 60	
Teoria	• To Be; To Have; • Tempi verbali: present simple, present continuous, past simple, past continuous, used to, present perfect, present perfect continuous, future tenses (present continuous, be-going-to, will); • Verbi modali: can/could, have to/must, should, may/might; • If-clauses; • Like/would like; • WH-questions; • Sostantivi: genere e numero, contabili e non contabili, nomi formati con il gerundio (infinito sostantivato); • The Possessive Case; • Articoli: determinativo, indeterminativo; • Pronomi: personali (soggetto e complemento), indefiniti e dimostrativi; • Quantifiers: some, any, a lot of, much, many, a little, a few; • Some/any compounds; • Aggettivi: possessivi, dimostrativi, qualificativi, numerali cardinali/ordinali, indefiniti; • Avverbi: tempo, luogo, frequenza; • Preposizioni: luogo, tempo, movimento; • Adjectives; • Lessico tecnico ICT: networking, sistemi, cybersecurity, cloud, intelligenza artificiale; • Comprensione di documentazione tecnica in lingua inglese (manuali, guide, RFC, vendor documentation); • Redazione di email tecniche, report e brevi documenti in inglese; • Terminologia utile per colloqui tecnici e principali certificazioni internazionali di settore.
Laboratorio	• Attività di listening, speaking, writing e reading comprehension; • Esercitazioni pratiche per il conseguimento della certificazione linguistica di Livello B1/B2.
Competenze in uscita	Livello B1 (Livello Soglia) *Indica un'autonomia di base in contesti quotidiani e lavorativi.* • Ascolto e Lettura: Saper comprendere i punti chiave di argomenti familiari (lavoro, scuola, tempo libero). Riuscire a seguire testi chiari su tematiche d'interesse. • Parlato (Interazione e Produzione): Essere in grado di muoversi con disinvoltura in situazioni che possono verificarsi viaggiando in paesi anglofoni. Saper descrivere esperienze, avvenimenti e sogni, ed esprimere brevi opinioni o progetti. • Scrittura: Saper scrivere testi semplici e coerenti su argomenti noti. Livello B2 (Livello Intermedio Superiore) *Indica una padronanza più fluida e articolata, spesso richiesta per scopi accademici o professionali.* • Ascolto e Lettura: Essere in grado di comprendere le idee principali di testi complessi (sia concreti che astratti), comprese discussioni tecniche sul proprio campo professionale. • Parlato (Interazione e Produzione): Saper interagire con scioltezza e spontaneità, rendendo possibile una conversazione naturale con i madrelingua senza sforzo. Saper esporre tesi, argomentazioni ed esprimere opinioni dettagliate, indicando vantaggi e svantaggi di varie opzioni. • Scrittura: Saper produrre testi chiari, dettagliati ed elaborati su un'ampia gamma di argomenti.

UFC 2 - Sicurezza sui luoghi di lavoro (Rischio Alto) – ore 20	
Teoria	(*Accordo Stato-Regioni 21/12/2011 – Formazione lavoratori rischio alto)* *Modulo giuridico-normativo* • Il D. Lgs. 81/2008: struttura, campo di applicazione, sistema sanzionatorio; • Soggetti della prevenzione: datore di lavoro, dirigente, preposto, lavoratore, RSPP, RLS, MC; • Obblighi e responsabilità di ciascuna figura;

	• Il sistema istituzionale: ASL/ARPA, Ispettorato del Lavoro, INAIL; *Modulo rischi e prevenzione* • Concetti di pericolo, rischio, danno, prevenzione e protezione; • La valutazione dei rischi e il DVR: struttura e contenuti obbligatori; • Rischi fisici, chimici, biologici, ergonomici e psicosociali; • Dispositivi di Protezione Individuale (DPI): criteri di scelta e utilizzo; • Segnaletica di sicurezza; • Procedure di emergenza, evacuazione e primo soccorso.
Laboratorio	• Lettura e analisi di un DVR reale relativo a un'impresa impiantistica; • Riconoscimento dei rischi in un ambiente di lavoro simulato (cantiere/locale macchine); • Corretta scelta e indossamento dei DPI specifici per lavori su impianti elettrici e ascensori; • Simulazione di evacuazione e gestione emergenza; • Prova pratica di primo soccorso: BLS (Basic Life Support), uso del defibrillatore (cenni); • Esercitazione su segnaletica e procedure di messa in sicurezza di un impianto.
Competenze in uscita	• Conoscere il quadro normativo del D. Lgs. 81/2008 e i ruoli dei soggetti della prevenzione; • Identificare pericoli e valutare i rischi in un ambiente di lavoro impiantistico; • Applicare le misure di prevenzione e protezione e utilizzare correttamente i DPI; • Gestire situazioni di emergenza e applicare le procedure di primo soccorso di base.
Il rilascio dell'attestato "Formazione dei Lavoratori - Rischio Alto. Formazione Generale e Formazione Specifica" è INDEROGABILMENTE subordinato al raggiungimento del 90% di ore di presenza, nonché al superamento del test scritto e della prova pratica.	

UFC 3 - Autoimprenditorialità e creazione di start-up – ore 20	
Teoria	*L'imprenditore e l'ecosistema imprenditoriale* • Che cos'è un'impresa: forme giuridiche (ditta individuale, SRL, SRL semplificata, società di persone); • Il Registro delle Imprese e i requisiti per le imprese installatrici ai sensi del D.M. 37/2008; • L'ecosistema delle start-up innovative in Italia: definizione giuridica, agevolazioni fiscali, investor; • Incubatori, acceleratori e bandi pubblici per l'innovazione nel settore energetico; *Il Business Plan* • Struttura di un Business Plan per un'impresa impiantistica o una ESCO; • Analisi di mercato; • Il modello di business Canvas applicato al settore: proposta di valore, segmenti di clientela, canali, flussi di ricavi; • Cenni di analisi SWOT. *Aspetti economici e finanziari dell'avvio d'impresa* • Costi di avvio: attrezzature, certificazioni, assicurazioni, iscrizione albi; • Fonti di finanziamento: capitale proprio, finanziamenti bancari, microcredito, bandi pubblici; • Il break-even point; • Cenni di fiscalità per il professionista tecnico: regime forfettario, IVA, fatturazione elettronica.
Laboratorio	• Sviluppo del Business Model Canvas; • Ricerca e analisi di bandi pubblici attivi nel settore energetico/impiantistico; • Redazione di un Business Plan sintetico (executive summary + piano economico semplificato); • Simulazione di pitch: presentazione del proprio progetto imprenditoriale alla classe, con feedback strutturato.
Competenze in uscita	• Individuare la forma giuridica e i requisiti normativi per avviare un'impresa nel settore impiantistico ed energetico, identificando le principali fonti di finanziamento disponibili; • Redigere un Business Model Canvas e un Business Plan sintetico per un'impresa o start-up analizzando il mercato di riferimento (opportunità, concorrenza e posizionamento competitivo); • Presentare in modo efficace un'idea imprenditoriale a interlocutori tecnici e non tecnici.

UFC 4 - Comunicazione, personal branding e redazione del CV per professionisti ICT – ore 20	
Teoria	• Le organizzazioni e i gruppi di lavoro: ruoli, leadership, dinamiche interpersonali; • Stress lavoro-correlato: riconoscimento e strategie di gestione; • La comunicazione organizzativa interna: riunioni, report, cantiere; • Cenni di comunicazione istituzionale con enti;

	• Il Colloquio di Lavoro; • La redazione del CV e della lettera motivazionale; • LinkedIn e personal branding professionale.
Laboratorio	• Redazione del proprio CV tecnico e ottimizzazione del profilo LinkedIn; • Simulazione di colloqui tecnici: presentazione delle competenze ICT; • Creazione di un portfolio tecnico: GitHub, progetti, certificazioni; • Role-playing su dinamiche comunicative in team tecnici.
Competenze in uscita	• Riconoscere i ruoli, le dinamiche di gruppo e gli stili di leadership all'interno di un'organizzazione tecnica, adottando comportamenti funzionali al lavoro in team; • Gestire la comunicazione organizzativa in contesti tecnici; • Redigere un CV Europass e una lettera motivazionale efficaci per il settore ICT; • Costruire e ottimizzare un'identità professionale online (LinkedIn, GitHub).

UFC 5 - Project Management e metodologie Agile – ore 20	
Teoria	*Project Management tradizionale* • Project Management: definizione, ciclo di vita del progetto, organizzazione del team; • Framework PMI: aree di conoscenza (scope, time, cost, quality, risk, communication); • Strumenti di pianificazione: GANTT (struttura, dipendenze, percorso critico), RACI (ruoli e responsabilità); • Gestione dei rischi di progetto ICT: identificazione, valutazione (probabilità × impatto), mitigazione, risk register; • Rischi specifici nei progetti di cybersecurity e AI: rischio di data breach durante un pentest, rischio di bias in un modello AI in produzione, rischio di non conformità normativa (GDPR, NIS2, AI Act). *Agile Project Management* • Metodologia Scrum: ruoli (Product Owner, Scrum Master, Development Team), artefatti (Product Backlog, Sprint Backlog, Increment), cerimonie (Sprint Planning, Daily Standup, Sprint Review, Retrospective); • Metodologia Kanban: principi, board, WIP limit, flusso continuo, metriche (lead time, cycle time); • Scrum vs Kanban: criteri di scelta in funzione del tipo di progetto ICT. *Strumenti e tecniche applicative* • Tecniche di prioritizzazione: matrice MoSCoW (Must have, Should have, Could have, Won't have); • Analisi SWOT applicata ai progetti ICT; • Strumenti digitali per il PM: Jira (backlog, sprint board, epics), Trello (kanban board, card), Notion e Confluence (documentazione e knowledge base) — panoramica e criteri di scelta.
Laboratorio	• Pianificazione di un progetto ICT reale assegnato (es. implementazione di un sistema SCADA con integrazione IoT), redazione del GANTT, compilazione della matrice RACI con ruoli del team tecnico; • Applicazione della matrice MoSCoW per la prioritizzazione dei requisiti del progetto assegnato: identificazione dei Must have tecnici e dei requisiti di sicurezza non negoziabili; • Redazione di un risk register per il progetto assegnato: identificazione dei rischi ICT/cybersecurity/AI, valutazione probabilità × impatto, definizione delle misure di mitigazione.
Competenze in uscita	• Pianificare un progetto ICT con strumenti GANTT e RACI, gestire i rischi con un risk register strutturato e identificare i rischi specifici dei progetti di cybersecurity e AI; • Applicare le metodologie Scrum e Kanban a progetti ICT, conducendo le cerimonie Agile e gestendo il backlog con criteri di prioritizzazione MoSCoW; • Utilizzare Jira, Trello e Confluence per la gestione operativa di progetti tecnici in modalità Agile.

Ambito 2. Formazione specialistica

UFC 6 – Architettur5a degli elaboratori e sistemi operativi – ore 40	
Teoria	• Architettura degli elaboratori: modello di von Neumann, CPU, memoria, I/O, bus; • Introduzione ai sistemi operativi: funzioni, storia, tipologie; • Processi e thread: concetti di base; programmazione concorrente: semafori, monitor, message passing; • Gestione delle risorse: scheduling, deadlock, memoria principale e secondaria, file system; • File system e permessi su Linux: gestione pratica da riga di comando; • Installazione e configurazione di Linux e Windows in macchina virtuale; • Comandi da terminale: navigazione, gestione file, permessi, gestione utenti avanzata;

	• Container: cos'è Docker, differenza tra immagine e container, avvio e gestione di un container.
Laboratorio	• Installazione e configurazione di Ubuntu e Windows 10/11 in VirtualBox/VMware; • Gestione file, permessi e utenti da riga di comando Linux (bash); • Creazione e gestione di processi: comandi ps, top, kill, nice; • Avvio e gestione di un container Docker: build, run, stop, log; • Simulazione di deadlock e analisi dello scheduling su esempi pratici; • Configurazione di un sistema di backup automatico con script bash,
Competenze in uscita	• Comprendere i principi di funzionamento di un elaboratore secondo l'architettura di von Neumann; • Installare e configurare un sistema operativo Linux e Windows in ambiente virtuale; • Gestire file, permessi e utenti da riga di comando; • Avviare e gestire un container Docker per un'applicazione semplice.

UFC 7 – Fondamenti di programmazione e scripting per l'automazione IT – ore 50	
Teoria	• Logica di programmazione: variabili, condizioni, cicli, funzioni in Python; • Gestione di errori ed eccezioni; programmazione orientata agli oggetti (cenni); • Git e GitHub: commit, push, pull, branch, merge, gestione di un repository condiviso; • Scripting Bash e PowerShell per l'automazione di task ripetitivi (backup, pulizia file, report); • Pianificazione automatica di script: cron (Linux) e Task Scheduler (Windows); • Chiamate a API REST: lettura di risposte JSON con Python, autenticazione bearer token; • Introduzione a librerie Python per l'automazione ICT: requests, paramiko, psutil.
Laboratorio	• Esercizi progressivi di programmazione Python: dalla sintassi base alle funzioni; • Creazione e gestione di un repository GitHub: versionamento del codice e collaborazione; • Script Bash per automazione: backup automatico, rotazione log, report di sistema; • Script PowerShell per amministrazione Windows: gestione utenti, report, patch; • Pianificazione cron e Task Scheduler su casi reali assegnati; • Chiamata a API REST pubblica (es. API meteo, OpenAI API) e lettura JSON con Python.
Competenze in uscita	• Scrivere programmi Python (variabili, cicli, condizioni, funzioni, gestione errori); • Usare Git e GitHub per versionare codice e collaborare su un repository; • Scrivere ed eseguire script Bash/PowerShell per automatizzare task ripetitivi; • Effettuare chiamate API REST e leggere risposte JSON.

UFC 8 – Algoritmi e strutture dati per l'elaborazione dei dati – ore 30	
Teoria	• Cos'è un algoritmo e perché l'efficienza conta (approccio intuitivo) • Strutture dati di base: array, liste, stack, code, dizionari e tabelle hash • Algoritmi di ricerca: ricerca lineare e ricerca binaria • Algoritmi di ordinamento: bubble sort, insertion sort, selection sort, merge sort, quick sort • Applicazione pratica delle strutture dati nel linguaggio Python • Analisi della complessità: concetto intuitivo di $O(n)$, $O(\log n)$, $O(n^2)$
Laboratorio	• Implementazione e confronto degli algoritmi di ordinamento su dataset reali • Utilizzo di array, liste, stack, code e dizionari in Python per risolvere problemi pratici • Esercitazioni su ricerca binaria e ricerca in strutture complesse • Analisi delle prestazioni: confronto dei tempi di esecuzione al variare della dimensione del dataset • Progetto: implementazione di un sistema di logging e analisi dati con strutture dati ottimizzate
Competenze in uscita	• Implementare e usare array, liste, stack, code, dizionari/tabelle hash • Applicare algoritmi di ricerca e ordinamento • Scegliere la struttura dati più adatta a un problema pratico • Valutare intuitivamente l'efficienza di una soluzione

UFC 9 – Basi di dati relazionali e non relazionali – ore 30

Teoria	• Ruolo dei database nei sistemi software; differenze tra file system e DBMS; • Modello relazionale: tabelle, chiavi primarie ed esterne, vincoli di integrità; • Normalizzazione: prime tre forme normali con esempi pratici; • Query SQL: SELECT, FROM, WHERE, JOIN, subquery, funzioni aggregate (GROUP BY, HAVING); • Progettazione concettuale: analisi requisiti, diagrammi ER e schema relazionale; • DBMS pratico: installazione e configurazione di MySQL/PostgreSQL; backup e restore; • Introduzione a NoSQL: differenze RDBMS vs NoSQL, modelli documento/key-value/colonne; • Scenari d'uso: quando scegliere SQL vs NoSQL; demo con MongoDB.
Laboratorio	• Installazione e configurazione di MySQL; creazione di database, utenti e permessi; • Progettazione di un database relazionale per un caso reale assegnato: analisi requisiti, ER, schema SQL; • Esercitazioni SQL: query complesse, join, subquery, funzioni aggregate; • Backup e restore di un database MySQL; automazione con cron; • Demo MongoDB: insert, find, update, query semplici su un dataset JSON; • Progetto finale: database per un sistema di monitoraggio energetico.
Competenze in uscita	• Scrivere query SQL per la gestione e l'analisi dei dati; • Progettare un database relazionale dalla raccolta dei requisiti allo schema SQL; • Comprendere le differenze tra database relazionali e non relazionali e scegliere la tecnologia più adatta; • Effettuare backup e ripristino di un database.

UFC 10 – Fondamenti di Networking e protocolli TCP/IP - ore 40	
Teoria	• Modello ISO/OSI e modello TCP/IP a confronto; • Indirizzamento IP (IPv4: classi, subnetting, CIDR; cenni IPv6); • Protocolli di livello trasporto: TCP e UDP, porte e socket; • Protocolli applicativi fondamentali: HTTP/HTTPS, FTP, SMTP, DNS, DHCP; • ARP e risoluzione degli indirizzi; routing di base; • Strumenti di diagnostica di rete: ping, traceroute, ipconfig/ifconfig, netstat, nslookup; • Standard IEEE 802: 802.3 Ethernet, 802.11 Wi-Fi — cenni; • Concetti di sicurezza di rete: firewall, VPN, IDS/IPS — panoramica introduttiva.
Laboratorio	• Analisi del traffico di rete con Wireshark: cattura e interpretazione dei pacchetti TCP/IP, HTTP, DNS; • Esercitazioni di subnetting con simulatore Cisco Packet Tracer o GNS3; • Configurazione base di un router e di uno switch virtuale in simulatore; • Diagnostica di rete: identificazione e risoluzione di problemi di connettività con gli strumenti da riga di comando; • Test di protocolli applicativi: interrogazione DNS, tracciamento di route, analisi HTTP.
Competenze in uscita	• Comprendere e configurare l'indirizzamento IP e i protocolli fondamentali della suite TCP/IP; • Utilizzare strumenti di diagnostica di rete per identificare problemi di connettività; • Analizzare il traffico di rete con Wireshark; • Conoscere i concetti di base di sicurezza di rete.

Ambito 3. Reti, Sistemi e Amministraizone

UFC 11 – Progettazione delle reti: cablaggio, apparati e Wi-Fi – ore 40	
Teoria	• Mezzi trasmissivi: cavi a coppie simmetriche (UTP/STP), fibra ottica (monomodale/multimodale); • Cablaggio strutturato: standard TIA/EIA 568A, ISO/IEC 11801; topologie fisiche; • Indirizzamento IP e subnetting (IPv4/IPv6); assegnazione degli indirizzi in una rete; • Apparati di rete: switch (L2/L3), router, access point, firewall — funzioni e differenze; • VLAN: segmentazione logica della rete; trunking e inter-VLAN routing; • Reti Wi-Fi: standard 802.11 (a/b/g/n/ac/ax), progettazione della copertura, analisi del sito; • Sicurezza Wi-Fi: WPA2/WPA3, 802.1X, rogue AP; NAT e VPN — concetti e casi d'uso; • Strumenti di monitoraggio: ping, traceroute, SNMP — concetti base.
Laboratorio	• Crimpatura di cavi UTP (T568A/B) e verifica con cable tester; • Configurazione di switch gestito: VLAN, trunking, spanning tree (cenni) su Cisco Packet Tracer; • Configurazione di router: routing statico, NAT, DHCP;

	• Progettazione e simulazione di una rete aziendale completa in Packet Tracer: 3 VLAN, Wi-Fi, firewall base; • Configurazione di una rete Wi-Fi: SSID, sicurezza WPA2/WPA3, canali; analisi del sito con app (es. Wi-Fi Analyzer); • Configurazione di una VPN client-to-site (concetti e demo).
Competenze in uscita	• Progettare e implementare il cablaggio strutturato di un edificio; • Configurare apparati di rete (switch, router, access point), VLAN e reti Wi-Fi; • Configurare indirizzamento IP, NAT e i principi di base della sicurezza di rete; • Analizzare e risolvere problemi di connettività.

UFC 12 – Amministrazione di sistemi Server – ore 40	
Teoria	• Installazione e configurazione di sistemi operativi server: Windows Server 2022, Ubuntu Server, Rocky/AlmaLinux; • Gestione utenti, gruppi e permessi a livello di sistema operativo server; • Gestione dei servizi di sistema: systemd, avvio/arresto/monitoraggio; • File system server: partizionamento, RAID software, gestione dello storage locale; • Active Directory / servizi di dominio: struttura, OU, Group Policy (cenni); • Gestione remota: SSH, RDP, PowerShell Remoting; • Automazione: script di manutenzione, cron job, task scheduler; • Hardening di base: disabilitazione servizi non necessari, aggiornamenti automatici, log di sistema (syslog, journald).
Laboratorio	• Installazione di Windows Server 2022 e Ubuntu Server in VirtualBox; • Configurazione dei servizi di base: DNS, DHCP, NTP su Linux; • Installazione e configurazione di Active Directory su Windows Server: creazione OU, utenti, GPO; • Gestione remota: connessione SSH, RDP e PowerShell Remoting a server virtuali; • Script di manutenzione: backup automatico, pulizia log, report di sistema; • Hardening di base di un server Linux: ssh senza password, firewall ufw, fail2ban; • Configurazione RAID 1 software su Linux: mdadm.
Competenze in uscita	• Installare, configurare e amministrare sistemi operativi server Windows e Linux; • Gestire utenti, permessi, servizi, storage e aggiornamenti su un server; • Automatizzare compiti di amministrazione ricorrenti tramite script e scheduler; • Applicare tecniche di hardening di base a un server.

UFC 13 – Gestione utenti, autenticazione e sicurezza degli accessi – ore 40	
Teoria	• Modelli di identità digitale: identificazione, autenticazione, autorizzazione (AAA); • Directory service: LDAP, Active Directory, sincronizzazione utenti (Azure AD Connect — cenni); • Meccanismi di autenticazione: password policy, MFA (TOTP, FIDO2/passkey); • Single Sign-On (SSO): SAML 2.0, OAuth 2.0, OpenID Connect — concetti; • Modelli di controllo degli accessi: RBAC, ABAC, principio del privilegio minimo; • Gestione del ciclo di vita dell'identità: provisioning/deprovisioning; • IAM su cloud: esempio pratico su AWS IAM o Microsoft Entra ID; • Audit degli accessi: log di accesso, revisione periodica permessi; • Vulnerabilità legate all'identità: credential stuffing, phishing, session hijacking — contromisure.
Laboratorio	• Configurazione di AD con politiche di password avanzate: lunghezza, complessità, scadenza, lockout; • Implementazione di MFA su un servizio cloud (es. Microsoft 365 o AWS) con TOTP; • Configurazione di SSO tra due applicazioni (demo con Keycloak o Azure AD); • Configurazione RBAC su AWS IAM: creazione di ruoli, policy, utenti con permessi minimi; • Revisione degli accessi: script per audit dei log di autenticazione e report degli account inattivi; • Simulazione di attacco credential stuffing e configurazione delle contromisure.
Competenze in uscita	• Applicare i principi fondamentali di gestione delle identità e degli accessi (autenticazione, MFA, RBAC); • Configurare Active Directory con politiche di password e MFA; • Riconoscere le vulnerabilità più comuni legate agli account utente; • Effettuare audit degli accessi e rivedere i permessi.

UFC 14 – Amministrazione di database con MySQL – ore 40	
Teoria	• SELECT avanzato: join multipli, subquery correlate, funzioni di finestra (ROW_NUMBER, RANK); • Transazioni: ACID, BEGIN/COMMIT/ROLLBACK, isolation level; • Indici: tipologie (B-tree, full-text), creazione, analisi delle prestazioni con EXPLAIN; • Sicurezza del database: gestione account, privilegi minimi, cifratura dei dati at rest e in transit; • Backup e ripristino: mysqldump, xtrabackup — pianificazione e automazione; • Replica MySQL: concetti e configurazione master-slave (cenni); • Performance tuning: ottimizzazione delle query, configurazione del buffer pool, slow query log; • Progettazione avanzata: pattern architetturali (CQRS, event sourcing — cenni).
Laboratorio	• Query SQL avanzate su database reale: join multipli, subquery, funzioni aggregate; • Analisi delle prestazioni: uso di EXPLAIN per ottimizzare query lente; • Configurazione della sicurezza: creazione utenti con privilegi minimi, abilitazione SSL/TLS; • Backup automatizzato con cron e mysqldump; ripristino da backup; • Monitoraggio del slow query log e ottimizzazione delle query più lente; • Progetto finale: database per un sistema di monitoraggio energetico con query di analisi.
Competenze in uscita	• Scrivere query SQL avanzate per la gestione e l'analisi dei dati; • Ottimizzare le prestazioni di un database MySQL; • Proteggere un database: gestione account, cifratura, backup; • Pianificare e automatizzare il backup e il ripristino.

UFC 15 – Web server e application server – ore 30	
Teoria	• Architettura client-server e ruolo di web server/application server nello stack applicativo; • Installazione e configurazione di Apache HTTP Server e Nginx: virtual host, reverse proxy, load balancing; • Certificati SSL/TLS: configurazione HTTPS, rinnovo automatico (Let's Encrypt/Certbot); • Application server: Tomcat, Node.js, Gunicorn/uWSGI — concetti e configurazione; • Deploy di applicazioni web: gestione processi, porte, log applicativi; • Hardening di base: header di sicurezza HTTP (HSTS, CSP, X-Frame-Options), disabilitazione moduli non necessari; • Troubleshooting: errori 502/503/504, timeout, errori di configurazione; • Deploy tramite container Docker (cenni).
Laboratorio	• Installazione e configurazione di Nginx come reverse proxy per un'applicazione Python (Flask); • Configurazione HTTPS con Let's Encrypt/Certbot su un server reale o in VM; • Hardening di un web server Nginx: configurazione dei security header, disabilitazione versioni vulnerabili; • Deploy di un'applicazione Node.js con Gunicorn e gestione con systemd; • Troubleshooting: identificazione e risoluzione di errori 502/504 e timeout; • Deploy di una semplice applicazione web tramite Docker e Nginx come reverse proxy.
Competenze in uscita	• Installare e configurare un web server e un application server, gestendo certificati SSL/TLS; • Applicare tecniche di hardening a un web server; • Risolvere i problemi più comuni di un web server e di un application server; • Effettuare il deploy di un'applicazione web in ambiente server.

UFC 16 – Cloud Computing, Storage e gestione dei dati – ore 40	
Teoria	• Definizione e modelli di servizio cloud: IaaS, PaaS, SaaS — differenze e casi d'uso; • Modelli di deployment: public, private, hybrid, multi-cloud; • Panoramica dei principali provider: AWS, Azure, GCP — orientamento nel panorama attuale; • Creazione e gestione di VM su cloud: AWS EC2 o Azure VM — pratica; • Deploy su piattaforma PaaS: AWS Elastic Beanstalk o Azure App Service — demo; • Servizi di storage cloud: object storage (S3), block storage (EBS), file storage (EFS) — pratica su S3; • Strategie di backup e disaster recovery in ambienti cloud; • Shared responsibility model: responsabilità del provider vs del cliente; • Principi di sicurezza nel cloud: IAM, cifratura at rest e in transit, VPC; • Ottimizzazione dei costi cloud: concetti di reserved instances, spot instances, rightsizing.

Laboratorio	• Creazione account AWS Free Tier/Azure; provisioning di una VM Linux e Windows; • Deploy di una piccola applicazione Python su Elastic Beanstalk o Azure App Service; • Configurazione di un bucket S3: permessi, versionamento, lifecycle policy; • Strategia di backup: configurazione di snapshot automatici di una VM e backup su S3; • Configurazione di un VPC con subnet pubblica e privata, security group e NACL; • Analisi dei costi: utilizzo di AWS Cost Explorer per ottimizzare le risorse.
Competenze in uscita	• Creare e gestire risorse di calcolo e storage in un ambiente cloud (IaaS/PaaS); • Comprendere le responsabilità condivise in materia di sicurezza cloud; • Configurare backup e disaster recovery in ambienti cloud; • Ottimizzare i costi di un'infrastruttura cloud.

UFC 17 – Virtualizzazione e containerizzazione – ore 30	
Teoria	• Concetti di virtualizzazione: hypervisor tipo 1 (VMware ESXi, Hyper-V, KVM) e tipo 2 (VirtualBox); • Creazione, configurazione e gestione di macchine virtuali: snapshot, clonazione, migrazione; • Containerizzazione: differenze tra VM e container; architettura Docker (daemon, client, registry); • Docker: immagini, Dockerfile, container, volumi persistenti, reti Docker; • Gestione del ciclo di vita dei container: build, run, stop, log, exec; • Docker Compose: orchestrazione multi-container — pratica; • Sicurezza delle immagini container: uso di immagini verificate, scansione vulnerabilità (Trivy); • Kubernetes: concetti base (pod, deployment, service, namespace).
Laboratorio	• Installazione di VMware Workstation/VirtualBox e creazione di VM Linux e Windows; • Snapshot, clonazione e migrazione di una VM in VirtualBox; • Scrittura di un Dockerfile per containerizzare un'applicazione Python/Node.js; • Docker Compose: orchestrazione di un'applicazione web con database (app + MySQL + Nginx); • Scansione di vulnerabilità di un'immagine Docker con Trivy; • Demo Kubernetes: deploy di un'applicazione su un cluster k3s locale,
Competenze in uscita	• Creare e gestire macchine virtuali e container Docker; • Scrivere Dockerfile e Docker Compose per applicazioni multi-container; • Scegliere tra virtualizzazione e containerizzazione in base al contesto; • Applicare la sicurezza di base alle immagini container.

UFC 18 – Monitoraggio, performance e troubleshooting – ore 20	
Teoria	• Metriche fondamentali di sistema: CPU, RAM, I/O disco, banda di rete • Strumenti di monitoraggio locale: top/htop, vmstat, iostat, iotop, iftop • Strumenti di monitoraggio centralizzato: panoramica di Zabbix, Nagios, Grafana + Prometheus • Log di sistema: syslog, journald, logrotate; log delle applicazioni web • Configurazione di alert e soglie di allarme; escalation delle notifiche • Metodologia di troubleshooting: isolamento del problema, ipotesi, verifica, documentazione • Bottleneck analysis: identificazione dei colli di bottiglia prestazionali • Documentazione degli incidenti: incident report, root cause analysis
Laboratorio	• Installazione e configurazione di uno stack Grafana + Prometheus su VM Linux • Configurazione di un agente node_exporter per raccogliere metriche di sistema • Creazione di dashboard Grafana: grafico CPU, RAM, disco, rete • Configurazione di alert in Grafana: notifica via email/webhook quando la CPU supera l'80% • Analisi dei log con journald e grep: identificazione di errori e anomalie • Simulazione di un problema di performance (CPU spike, saturazione disco) e risoluzione guidata
Competenze in uscita	• Monitorare le prestazioni di un sistema e configurare alert • Analizzare i log di sistema e applicativi per individuare anomalie • Applicare un metodo strutturato di troubleshooting e documentare gli interventi • Configurare uno stack di monitoraggio Grafana + Prometheus

Ambito 4. Cybersecurity

UFC 19 – Reti e Comunicazione Digitale – ore 20	
Teoria	• Fondamenti di sicurezza: panoramica su minacce, vulnerabilità, rischi informatici; • Principi base di crittografia: simmetrica (AES), asimmetrica (RSA), hashing (SHA-256); • Applicazioni pratiche: cifratura dei dati, autenticazione, firma digitale, certificati X.509; • Framework di governance della sicurezza: ISO/IEC 27001, NIST Cybersecurity Framework; • Metodologie di analisi del rischio: risk assessment, risk matrix, DREAD, STRIDE; • Politiche di sicurezza aziendale: ruoli (CISO, DPO, Security Officer), documentazione; • Principi del modello Zero Trust; • Normative di riferimento: panoramica GDPR, NIS2, AI Act.
Laboratorio	• Cifratura e hashing con OpenSSL: generazione chiavi RSA, cifratura AES, calcolo hash SHA-256; • Creazione e analisi di un certificato X.509 con OpenSSL; • Compilazione di una risk matrix per un'infrastruttura ICT assegnata: identificazione degli asset, minacce, impatti; • Analisi STRIDE applicata a un sistema web: identificazione delle minacce per categoria; • Redazione di una policy di sicurezza aziendale semplificata: password policy, acceptable use policy.
Competenze in uscita	• Comprendere e applicare i principi fondamentali di sicurezza e crittografia; • Orientarsi nei principali framework di governance della sicurezza (ISO 27001, NIST CSF); • Impostare una prima valutazione del rischio (risk assessment); • Applicare il modello Zero Trust in un contesto di progettazione di rete.

UFC 20 – Vulnerability Assessment e Penetration Test – ore 40	
Teoria	• Principi di Ethical Hacking: metodologia, autorizzazione, responsabilità legale; • Fasi del penetration test: reconnaissance, scanning, exploitation, post-exploitation, reporting; • Tecniche di Social Engineering: phishing, spear-phishing, pretexting, vishing; • Metodologie di Sniffing e analisi del traffico di rete; • Vulnerability Assessment: metodologie, strumenti (Nessus, OpenVAS, Nmap); • Penetration Testing su sistemi e reti: strumenti (Metasploit, Burp Suite, Nikto); • Tecniche di Persistenza e Privilege Escalation; • Testing su applicazioni web: OWASP Top 10 (SQL injection, XSS, CSRF, SSRF); • Testing su applicazioni mobile: cenni (Android/iOS); • Analisi e Prevenzione dei Malware; • Standard e normative di sicurezza: PTES, OWASP Testing Guide; • Metodologie di documentazione e reporting del pentest.
Laboratorio	• Reconnaissance: utilizzo di Nmap, Shodan, theHarvester su target autorizzato; • Scanning delle vulnerabilità con OpenVAS su macchina virtuale Metasploitable; • Exploitation: utilizzo di Metasploit su vulnerabilità nota (CVE) in ambiente controllato; • SQL injection su applicazione DVWA (Damn Vulnerable Web Application); • XSS reflected e stored su DVWA: identificazione e exploitazione; • Privilege escalation su Linux: tecnica sudo, SUID, cron job vulnerabile; • Redazione di un report di penetration test professionale per un caso assegnato.
Competenze in uscita	• Condurre, in laboratorio controllato e autorizzato, una vulnerability assessment di base; • Comprendere le fasi di un penetration test e documentare i risultati in un report tecnico; • Identificare le vulnerabilità OWASP Top 10 nelle applicazioni web; • Applicare tecniche di privilege escalation su sistemi Linux in ambiente controllato:

UFC 21 – Hardening dei sistemi e protezioni perimetrali – ore 30	
Teoria	• Sicurezza delle reti: minacce (sniffing, spoofing, DoS/DDoS, man-in-the-middle) • Protocolli di sicurezza: SSL/TLS, VPN (IPsec, OpenVPN, WireGuard), IDS/IPS • Firewall: tipologie (stateful, application-layer, NGFW), configurazione delle regole • Segmentazione di rete: DMZ, zone di sicurezza, micro-segmentazione • Hardening di sistemi operativi: CIS Benchmarks, disabilitazione servizi non necessari, gestione patch

	• Hardening di applicazioni web: header di sicurezza HTTP, WAF, OWASP Top 10 remediation • Baseline di sicurezza: strumenti di audit (OpenSCAP, Lynis, CIS-CAT) • Sicurezza della supply chain software: SBOM, scansione delle dipendenze • Cenni al modello Zero Trust applicato alla protezione perimetrale
Laboratorio	• Configurazione di firewall perimetrale con iptables/nftables e pfSense • Configurazione di una DMZ in ambiente simulato: web server pubblico isolato dalla rete interna • Hardening di un server Linux con Lynis: analisi del report e applicazione delle raccomandazioni • Configurazione di un WAF (ModSecurity) su Nginx: protezione da SQL injection e XSS • Scansione della baseline di sicurezza con OpenSCAP e confronto con CIS Benchmark • Configurazione di WireGuard VPN tra due VM
Competenze in uscita	• Applicare tecniche di hardening a sistemi, reti e applicazioni web; • Configurare protezioni perimetrali di base (firewall, VPN, IDS/IPS, segmentazione, DMZ); • Verificare la conformità di un sistema con i CIS Benchmarks; • Riconoscere e mitigare le vulnerabilità OWASP Top 10.

UFC 22 – Sicurezza Reti Wireless e 5G – ore 40	
Teoria	• Fondamenti delle comunicazioni wireless e standard Wi-Fi: 802.11a/b/g/n/ac/ax; • Vulnerabilità delle reti Wi-Fi: WEP (obsoleto), WPA2/WPA3, attacchi di deautenticazione, evil twin, rogue AP; • Hardening delle reti wireless aziendali: autenticazione enterprise 802.1X, RADIUS, EAP-TLS; • Monitoraggio e rilevamento delle intrusioni su reti wireless: WIDS; • Sicurezza dei dispositivi IoT wireless: vulnerabilità comuni, firmware update, isolamento in VLAN; • Panoramica sul 5G: architettura di base, network slicing, edge computing, rischi di sicurezza specifici; • Minacce emergenti su reti mobili: IMSI catcher, SS7 vulnerabilities (cenni).
Laboratorio	• Analisi di una rete Wi-Fi con Wireshark e aircrack-ng (su rete propria autorizzata): cattura degli handshake; • Configurazione di autenticazione enterprise 802.1X con FreeRADIUS e certificati client EAP-TLS; • Rilevamento di un rogue access point con Kismet in ambiente laboratorio; • Configurazione di una VLAN dedicata per i dispositivi IoT: isolamento e regole firewall; • Hardening di un access point aziendale: disabilitazione WPS, SSID nascosto, aggiornamento firmware; • Simulazione di attacco deautenticazione (ambiente controllato) e configurazione delle contromisure.
Competenze in uscita	• Mettere in sicurezza una rete Wi-Fi aziendale riconoscendo le minacce più comuni; • Configurare un'autenticazione enterprise per reti wireless (802.1X/RADIUS); • Rilevare intrusioni wireless e configurare le contromisure; • Applicare politiche di sicurezza per dispositivi IoT wireless.

UFC 23 – Sandbox, Malware Analysis e Threat Detection – ore30	
Teoria	• Tassonomia del malware: virus, worm, trojan, ransomware, rootkit, fileless malware, spyware; • Ambienti sandbox: concetti, isolamento, analisi dinamica sicura (Cuckoo, Any.run); • Analisi statica di base: hash, stringhe, packer, PE header (Windows); • Analisi dinamica in ambiente controllato: monitoraggio processi, rete, file system, registry; • Strumenti di analisi: VirusTotal, Cuckoo Sandbox, Process Monitor, Process Hacker; • Indicatori di compromissione (IoC): hash, IP, domini, pattern — formati STIX/TAXII; • Tecniche di evasione del malware: anti-VM, anti-sandbox, obfuscation — contromisure; • Threat detection: signature-based, euristiche, anomaly detection, machine learning; • Integrazione dell'analisi malware nei processi di incident response.
Laboratorio	• Analisi statica di un sample malware (safe/inerte): hash con sha256sum, strings, analisi PE: • Analisi dinamica in Cuckoo Sandbox o Any.run: lancio del sample e lettura del report: • Utilizzo di VirusTotal per analisi di file sospetti e correlazione IoC: • Configurazione di regole YARA per il rilevamento di malware specifico: • Creazione di una regola di rilevamento personalizzata in Wazuh/OSSEC: • Caso studio: analisi di un ransomware noto (WannaCry, in ambiente isolato) — comportamento, IoC, remediation

Competenze in uscita	• Analizzare un file sospetto in ambiente sandbox; • Riconoscere gli indicatori di compromissione (IoC) di un attacco malware; • Configurare regole di rilevamento (YARA, SIEM) per minacce note; • Integrare l'analisi malware nei processi di incident response.

UFC 24 – Disaster Recovery e Business Continuity Management – ore 40	
Teoria	• Analisi del rischio e valutazione degli impatti sul business (BIA); • Framework e standard internazionali: ISO 22301, ISO 27031, NIST SP 800-34; • Pianificazione del Disaster Recovery: RTO, RPO, strategie (hot/warm/cold standby); • Business Continuity Planning (BCP): struttura del piano, team di crisi, comunicazione; • Continuità operativa in ambienti cloud: strategie di replica multi-region, failover automatico; • Soluzioni di backup e recovery: on-premise, cloud (DRaaS, BCaaS), backup 3-2-1; • Service Level Agreement (SLA): definizione, monitoraggio, penali; • Integrazione di infrastrutture on-premise e cloud in un piano di continuità; • Test e revisione del piano DR: tabletop exercise, full-scale test, simulazioni.
Laboratorio	• Redazione guidata di un Business Continuity Plan per un caso aziendale ICT assegnato; • Calcolo di RTO e RPO per scenari applicativi: database, web server, email; • Configurazione di backup automatici su cloud (AWS S3 + Glacier) con politiche di retention; • Simulazione di disaster recovery: ripristino di una VM da snapshot su cloud; • Tabletop exercise: simulazione guidata di un incidente ransomware con gestione della crisi; • Configurazione di un failover DNS e routing con AWS Route 53 o Azure Traffic Manager (demo).
Competenze in uscita	• Contribuire alla pianificazione di un piano di disaster recovery e business continuity; • Configurare soluzioni di backup in ambienti cloud; • Calcolare RTO e RPO e scegliere la strategia DR più adatta; • Condurre un tabletop exercise e documentare i risultati.

UFC 25 – SOC, SIEM/SOAR e Threat Intelligence – ore 40	
Teoria	• Ruolo e struttura di un Security Operations Center (SOC): livelli L1/L2/L3, workflow operativo • Concetti di SIEM: raccolta, normalizzazione, correlazione e analisi dei log • Configurazione di regole di correlazione e generazione di alert; tuning per ridurre i falsi positivi • Piattaforme SIEM: panoramica Splunk, Elastic SIEM, Microsoft Sentinel, Wazuh (open-source) • Concetti di SOAR: playbook, automazione della risposta, integrazione con ticketing • Threat Intelligence: fonti (OSINT, feed commerciali), formati STIX/TAXII, condivisione (MISP) • Ciclo di vita della Threat Intelligence: raccolta, elaborazione, analisi, diffusione, feedback • MITRE ATT&CK Framework: struttura, tattiche, tecniche, procedure (TTP) • Triage degli alert: gestione delle priorità, false positive vs incidenti reali • Metriche operative SOC: MTTD, MTTR; reportistica verso il management
Laboratorio	• Installazione di Wazuh (SIEM open-source): configurazione di agenti su Linux e Windows • Creazione di regole di correlazione personalizzate in Wazuh per rilevare attività sospette • Dashboard Wazuh: configurazione di panel per visualizzare alert, integrità file, policy compliance • Triage di un set di alert simulati: classificazione per priorità usando MITRE ATT&CK • Configurazione di un playbook di risposta automatica in Wazuh (active response) • Simulazione di integrazione Threat Intelligence: import di feed IoC in Wazuh e creazione di alert correlati • Esercizio: ricostruzione della kill chain di un attacco simulato con Wazuh
Competenze in uscita	• Operare all'interno di un SOC di primo livello utilizzando strumenti SIEM (Wazuh/Elastic) • Effettuare il triage degli alert e orientarsi con il framework MITRE ATT&CK • Configurare regole di correlazione e playbook di risposta automatica • Integrare feed di Threat Intelligence nel SIEM

UFC 26 – Gestione delle vulnerabilità nei sistemi AI e Incident Response – ore 30

Teoria	• Incident Response: ciclo di vita (preparazione, identificazione, contenimento, eradicazione, ripristino, lezioni apprese) • Pianificazione e preparazione: Incident Response Plan, team di risposta, runbook • Comunicazione e gestione della crisi: comunicazione interna, verso il management, verso le autorità • Gestione delle patch e delle vulnerabilità: patch management process, vulnerability scanning periodico • Vulnerabilità specifiche dei sistemi AI in contesti energetici: data poisoning su modelli predittivi, adversarial input su sistemi SCADA • Incident response per sistemi AI: rilevamento di anomalie nei modelli, rollback, retraining • Casi pratici guidati: simulazione (tabletop exercise) di risposta a un incidente ransomware
Laboratorio	• Redazione di un Incident Response Plan per un'organizzazione ICT assegnata • Simulazione di incident response su un caso ransomware (tabletop): dal rilevamento al ripristino • Documentazione di un incidente: redazione del post-mortem e della root cause analysis • Scansione periodica delle vulnerabilità con OpenVAS e prioritizzazione del patch management • Demo: anomaly detection su un modello AI in produzione (output anomali, concept drift) • Configurazione di un processo di vulnerability disclosure e patch management
Competenze in uscita	• Gestire un incidente di sicurezza seguendo un processo strutturato, dalla preparazione alla comunicazione • Applicare le procedure di risposta a scenari ransomware • Gestire il processo di patch management e vulnerability scanning periodico • Riconoscere le vulnerabilità specifiche dei sistemi AI in contesti industriali

UFC 27 – Sicurezza dell'AI e Security-for-AI – ore 20

Teoria	• Superficie d'attacco dei sistemi AI: dati di training, modello, pipeline di inferenza • Adversarial attack: adversarial examples, evasion attack — principi e difese • Data poisoning: attacchi alla fase di training, backdoor attack • Model extraction e model inversion: furto/ricostruzione di informazioni dal modello • Prompt injection e attacchi specifici ai Large Language Model (LLM) • Tecniche di difesa: adversarial training, input sanitization, robustezza del modello • Governance e sicurezza della supply chain AI: dataset, modelli pre-addestrati, dipendenze • Security-by-design nei sistemi che integrano componenti AI • Framework di riferimento: OWASP Top 10 for LLM, NIST AI RMF — panoramica
Laboratorio	• Demo di adversarial example: perturbazione di un'immagine per ingannare un classificatore • Tentativo di prompt injection su un'applicazione LLM in ambiente controllato • Analisi della superficie d'attacco di un sistema AI-based per il monitoraggio energetico • Verifica della supply chain AI: controllo dell'integrità di un modello pre-addestrato scaricato • Configurazione di input sanitization per un chatbot LLM aziendale
Competenze in uscita	• Riconoscere le principali minacce specifiche ai sistemi AI (adversarial, prompt injection, data poisoning) • Applicare i criteri base di un design sicuro per sistemi AI • Orientarsi nei framework OWASP Top 10 for LLM e NIST AI RMF • Verificare la sicurezza della supply chain AI

UFC 28 – Etica, normativa e responsabilità nella sicurezza (GDPR, NIS2, AI Act) – ore 20

Teoria	• Breve storia dell'etica nell'informatica e nell'intelligenza artificiale • Regolamento GDPR: principi, basi giuridiche del trattamento, diritti degli interessati (accesso, rettifica, cancellazione, portabilità) • GDPR applicato all'ICT: privacy by design, privacy by default, misure tecniche e organizzative • Direttiva NIS2: ambito di applicazione, obblighi per soggetti essenziali e importanti, sanzioni • Data Protection Impact Assessment (DPIA): quando è obbligatoria, metodologia, output • Notifica di data breach: tempistiche (72 ore), contenuti, comunicazione agli interessati • AI Act europeo: classificazione del rischio (inaccettabile, alto, limitato, minimo), obblighi per i sistemi ad alto rischio • Casi di studio: GDPR breach reali, sanzioni NIS2, controversie AI — analisi critica e buone pratiche

Laboratorio	• Analisi di una privacy policy aziendale: identificazione delle carenze rispetto al GDPR • Redazione di una DPIA semplificata per un sistema di monitoraggio energetico AI-based • Simulazione della notifica di un data breach all'autorità di controllo (Garante) • Classificazione di sistemi AI reali secondo il rischio AI Act (esercitazione a gruppi) • Caso studio: analisi di una sanzione GDPR reale e identificazione delle misure correttive
Competenze in uscita	• Orientarsi negli obblighi normativi in materia di sicurezza e protezione dei dati (GDPR, NIS2, AI Act) • Riconoscere quando è necessaria una DPIA e redigerla in forma semplificata • Gestire la notifica di un data breach nei tempi e nei modi previsti dalla normativa • Classificare i sistemi AI secondo il rischio AI Act

Ambito 5. Trasformazione Digitale AI-Based per l'Efficientamento Energetico

UFC 29 – Fondamenti di intelligenza artificiale ed AI generativa – ore 20	
Teoria	• Fondamenti di Intelligenza Artificiale: definizione, breve storia, distinzione IA debole/forte • Reti neurali: concetti di base (neuroni, strati, funzioni di attivazione, forward/backpropagation) • Agenti Intelligenti: concetto generale (percezione-decisione-azione) • Elaborazione del Linguaggio Naturale (NLP): concetti di base (tokenizzazione, embedding, transformer) • Modelli generativi: GAN, modelli diffusivi, architettura Transformer — concetti • Introduzione ai Large Language Model: training, fine-tuning, RLHF — senza formalismo matematico • Casi d'uso dell'AI generativa in ambito industriale ed energetico • Prompt engineering: principi base (chiarezza, contesto, esempi, step-by-step, few-shot) • Uso pratico e comparato di ChatGPT, Claude, Gemini: differenze, limiti, buone pratiche • Aspetti etici e sociali nell'IA (approfonditi in UFC 34)
Laboratorio	• Laboratorio pratico di prompt engineering su più strumenti (ChatGPT, Claude, Gemini): confronto risposte • Costruzione di prompt efficaci per casi d'uso tecnici ICT: generazione codice, debug, documentazione • Utilizzo dell'AI generativa per l'analisi e la sintesi di un documento tecnico (report di sicurezza) • Creazione di un assistente virtuale personalizzato con istruzioni di sistema (system prompt) • Prompt iterativo: raffinamento progressivo di un prompt per ottimizzare i risultati • Analisi critica di un caso di allucinazione dell'AI: identificazione e verifica delle fonti
Competenze in uscita	• Comprendere i concetti fondamentali di intelligenza artificiale e reti neurali • Utilizzare in modo efficace e consapevole i principali assistenti AI generativi (ChatGPT, Claude, Gemini) • Applicare tecniche di prompt engineering per uso professionale • Riconoscere i limiti e le allucinazioni dei modelli AI

UFC 30 – Machine Learning e Large Language Model – ore 30	
Teoria	• Concetti introduttivi del Machine Learning: panoramica e ambiti di applicazione • Apprendimento supervisionato: regressione lineare e logistica, alberi decisionali, random forest • Apprendimento non supervisionato: clustering (k-means), riduzione della dimensionalità (PCA — cenni) • Apprendimento per rinforzo: concetti (agente, ambiente, reward) — cenni • Overfitting, underfitting, regolarizzazione: concetti pratici; train/test split, cross-validation • Valutazione dei modelli: accuracy, precision, recall, F1-score, curva ROC • Architettura Transformer e meccanismi di attenzione: spiegazione concettuale • Large Language Model: addestramento, fine-tuning, RAG (Retrieval-Augmented Generation) • Valutazione e limiti degli LLM: allucinazioni, bias, contesto limitato • Integrazione di LLM in applicazioni tramite API (OpenAI, Anthropic, Mistral) • Orchestrazione di workflow AI: strumenti n8n e Claude Code — introduzione pratica
Laboratorio	• Addestramento di un modello di classificazione su Google Colab: regressione logistica su dataset energetico • Valutazione del modello: matrice di confusione, precision, recall, F1-score • Costruzione di un semplice flusso n8n che integra un LLM per un caso d'uso reale • Integrazione di un LLM via API: chiamata all'API Anthropic Claude per classificare anomalie energetiche • Utilizzo di Claude Code come assistente per lo sviluppo di script Python per l'analisi dati • Progetto: modello di anomaly detection su dati di consumo energetico simulati

Competenze in uscita	• Comprendere i concetti base del Machine Learning (supervisionato, non supervisionato, overfitting, validazione) • Addestrare e valutare un modello di classificazione su dati reali • Integrare un LLM in un'applicazione tramite API • Costruire un semplice flusso automatizzato con n8n o Claude Code

UFC 31 – Dispositivi intelligenti per l'automazione industriale e l'efficienza energetica - ore 40	
Teoria	• Tipologie di sensori per energia e ambiente: smart meter, TA/TV, sensori temperatura/umidità/luminosità/presenza/portata • Concetto di dispositivo intelligente: smart meter, prese smart, termostati smart, gateway IoT • Modalità di collegamento: filo (RS-485, Modbus RTU) e radio (Wi-Fi, ZigBee, LoRa, NB-IoT) • Nozione di campionamento: intervallo di misura, media, picco, risoluzione • Microcontrollori Arduino: programmazione pratica (lettura sensori, invio dati) • Raspberry Pi come gateway IoT: configurazione, Python, acquisizione e invio dati • Protocolli IoT: MQTT (broker, publish/subscribe, QoS), CoAP (cenni), HTTP REST • Architettura IoT: Edge Computing, Fog Computing, Cloud — scelta in funzione della latenza e del volume • Sicurezza e privacy in IoT: vulnerabilità comuni, firmware update, segmentazione VLAN • Piattaforma IoT pratica: AWS IoT Core o Azure IoT Hub — una a scelta del docente • Manutenzione predittiva basata su dati da sensori: concetti ed esempio guidato con ML
Laboratorio	• Collegamento di un sensore di temperatura/umidità (DHT22) ad Arduino: lettura e display seriale • Invio dati da Arduino via MQTT a un broker Mosquitto locale • Configurazione di un Raspberry Pi come gateway IoT: ricezione dati da Arduino, pre-processing, invio al cloud • Dashboard IoT: visualizzazione dei dati di consumo energetico su Node-RED o Grafana • Integrazione con AWS IoT Core o Azure IoT Hub: registrazione del dispositivo, invio telemetria, regole di routing • Progetto: sistema di monitoraggio energetico low-cost con Arduino/Raspberry Pi, MQTT e dashboard cloud • Esempio di manutenzione predittiva: addestramento di un modello ML su dati di vibrazione simulati
Competenze in uscita	• Collegare, configurare e leggere dati da sensori e dispositivi intelligenti (smart meter, Arduino, Raspberry Pi) • Comprendere l'architettura di un sistema IoT (Edge/Fog/Cloud) • Utilizzare i protocolli di comunicazione IoT più diffusi (MQTT, Modbus) • Implementare un sistema di monitoraggio energetico IoT end-to-end

UFC 32 – Sistemi SCADA, HMI e supervisione dei processi di efficienza energetica - ore 40	
Teoria	• Concetto di HMI: pannelli operatore, interfacce web di inverter, UPS, climatizzazione — ruolo del tecnico ITS • Differenza tra HMI locale e supervisione centralizzata SCADA/BEMS • Architettura di un sistema SCADA: livelli (campo, controllo, supervisione, MES) • Comunicazione SCADA-PLC-field devices: protocolli Modbus TCP, OPC UA, MQTT, IEC 61850 • Data logging, storicizzazione e trend analysis in sistemi SCADA • Applicazioni negli impianti energetici: fotovoltaico, cogenerazione, smart grid, edifici intelligenti • Creazione di un progetto SCADA con Ignition Community Edition o WinCC (uno a scelta del docente) • Implementazione di dashboard di monitoraggio e allarmi • Cybersecurity nei sistemi SCADA/OT: segmentazione IT/OT, protezione Modbus, anomaly detection
Laboratorio	• Connessione a un PLC simulato (Factory I/O o OpenPLC): configurazione della comunicazione Modbus TCP • Creazione di una schermata HMI in Ignition: sinottico, indicatori, grafici storici, allarmi • Configurazione di tag OPC UA in Ignition: lettura di variabili dal PLC simulato • Dashboard di monitoraggio energetico: visualizzazione dei consumi in tempo reale, KPI energetici • Configurazione di allarmi: soglie di consumo, fault detection, notifiche email/SMS • Integrazione con cloud: esportazione dei dati SCADA verso InfluxDB/Grafana o AWS IoT • Esercizio di cybersecurity OT: identificazione di traffico Modbus anomalo con Wireshark
Competenze in uscita	• Realizzare un'interfaccia HMI/SCADA di supervisione, leggendo dati da un PLC simulato • Configurare allarmi e dashboard di monitoraggio energetico • Comprendere i protocolli industriali (Modbus TCP, OPC UA, MQTT) e le architetture SCADA • Applicare i principi di cybersecurity OT alla protezione dei sistemi SCADA

UFC 33 – Sistemi di automazione e AI Agents per l'efficientamento energetico - ore 30	
Teoria	• Concetto di agente intelligente applicato a contesti industriali/energetici (percezione-decisione-azione) • Differenza tra automazione a regole (rule-based) e automazione basata su AI/agenti • Architetture di AI Agents: agenti reattivi, basati su obiettivi, multi-step, multi-agent • Integrazione di LLM come layer decisionale: function calling, tool use, orchestrazione • Orchestrazione di agenti con sistemi SCADA/BEMS esistenti: integrazione con API, Modbus, MQTT • Casi d'uso energetici: ottimizzazione set point, manutenzione predittiva, risposta automatica ad anomalie • Framework per agenti AI: LangChain, LangGraph, OpenAI Assistants, n8n — panoramica • Aspetti di sicurezza e supervisione umana (human-in-the-loop) nell'automazione basata su agenti • Valutazione dell'affidabilità e dei limiti degli AI Agents in contesti critici
Laboratorio	• Costruzione di un agente AI semplice con n8n: trigger → LLM → azione (es. alert su anomalia energetica) • Integrazione di un agente AI con un sistema SCADA simulato via API/Modbus • Progetto: agente di ottimizzazione energetica che legge dati IoT e suggerisce azioni al tecnico • Implementazione di human-in-the-loop: configurazione di un step di approvazione umana nel workflow • Test di affidabilità: simulazione di input anomali e verifica del comportamento dell'agente • Demo LangChain/LangGraph: costruzione di un agente multi-step per analisi di report energetici
Competenze in uscita	• Comprendere il concetto di agente intelligente applicato a contesti industriali/energetici • Costruire semplici agenti AI con strumenti no-code (n8n) e framework Python (LangChain) • Integrare un agente AI con sistemi SCADA e IoT • Applicare i principi di supervisione umana (human-in-the-loop) nei sistemi automatizzati

UFC 34 – Normativa, Etica e sicurezza dell'IA - ore 20	
Teoria	• Panoramica storica e importanza dell'etica nell'intelligenza artificiale applicata all'energia • Il Regolamento europeo AI Act: struttura, classificazione del rischio (inaccettabile/alto/limitato/minimo) • Obblighi per i sistemi AI ad alto rischio: trasparenza, documentazione, supervisione umana, accuracy • Trasparenza e spiegabilità (XAI): tecniche di base (LIME, SHAP — concetti) per modelli energetici • Bias ed equità negli algoritmi applicati alla gestione energetica: identificazione e mitigazione • Responsabilità e accountability nell'uso di sistemi AI per decisioni automatizzate su impianti • Standard e linee guida internazionali: UNESCO Recommendation on AI Ethics, NIST AI RMF, ISO/IEC 42001 • Casi di studio: errori, controversie e buone pratiche nell'AI applicata all'energia
Laboratorio	• Classificazione di sistemi AI energetici reali secondo il rischio AI Act (esercitazione a gruppi) • Analisi di bias in un dataset energetico: identificazione di disparità nei dati di consumo per fasce orarie • Redazione di una scheda di trasparenza (model card) per un modello di anomaly detection energetico • Caso studio critico: analisi di un fallimento di sistema AI in ambito industriale/energetico • Discussione guidata: governance AI in un'azienda energetica — ruoli, processi, strumenti
Competenze in uscita	• Orientarsi negli obblighi normativi ed etici legati all'uso dell'IA (AI Act, UNESCO, NIST AI RMF • Identificare bias e problemi di equità nei dataset e nei modelli AI • Applicare principi di trasparenza e spiegabilità ai sistemi AI in contesti energetici • Classificare i sistemi AI secondo il rischio AI Act e identificare gli obblighi applicabili