Syllabus

Release 4.0 - 2023

9 788869 911590

SICUREZZA DEI CALCOLATORI E DELLE RETI

Macrocompetenza

MA01 - INFORMATICA E SICUREZZA

Modulo

C01.2 SICUREZZA DEI CALCOLATORI E DELLE RETI

Unità Didattiche 9

Capacità Sviluppate 37

Conoscenza Abilità Attitudine

DigComp European e-Competence Framework

Unità didattica	Argomento	Capacità sviluppata	Competenza
C01.2.1 Fondamenti di Sicurezza e Privacy Digitale	C01.2.1.1 Introduzione alla sicurezza digitale	C01.2.1.1.1 Comprendere l'importanza della sicurezza digitale.	Concetti di sicurezza informatica, minacce cibernetiche. Riconoscere l'importanza di proteggere le risorse digitali. Valorizzare la sicurezza digitale come priorità
	C01.2.1.2 Protezione dei dati e privacy	C01.2.1.2.1 Salvaguardare i dati personali e la privacy online.	Natura dei dati sensibili, impatto della condivisione non autorizzata. Applicare il principio di minimizzazione dei dati, gestire autorizzazioni delle app. Rispettare le normative sulla protezione dei dati come il GDPR.
	C01.2.1.3 Riconoscimento delle minacce online	C01.2.1.3.1 Identificare e mitigare rischi digitali.	Tecniche di attacco come phishing, malware, ingegneria sociale. Identificare segni di attacchi, evitare azioni sospette. Mantenere una postura di sicurezza proattiva.
	C01.2.1.4 Comportamenti sicuri online	C01.2.1.4.1 Adottare abitudini di sicurezza digitale.	Pratiche per creare password robuste, aggiornare il software. Implementare prassi per prevenire intrusioni. Prendersi cura della propria sicurezza digitale.
	C01.2.2.5 Alfabetizzazione mediatica e valutazione delle fonti online	C01.2.2.5.1 Valutare criticamente le informazioni online.	Tecniche di verifica delle fonti, riconoscimento delle notizie false. Analizzare le fonti online per accuratezza e affidabilità. Coltivare uno spirito critico e inquisitivo nel confronto con le informazioni online, prima di accettarle come veritiere.
	C01.2.2.6 Etica digitale e comportamento online responsabile	C01.2.2.6.1 Comportarsi eticamente e responsabilmente online.	Principi di comportamento etico online, conseguenze delle azioni digitali. Prendere decisioni informate riguardo all'uso di dati personali e condivisione online. Promuovere comportamenti rispettosi e responsabili nella sfera digitale.

Unità didattica	Argomento	Capacità sviluppata	Competenza
C01.2.2 Privacy online e gestione dei dati personali	C01.2.2.1 Privacy online e gestione dei dati personali	C01.2.2.1.1 Preservare la riservatezza e controllare i dati personali.	Importanza della protezione dei dati, diritti degli interessati. Applicare i principi di consenso e finalità nell'elaborazione dei dati. Rispettare le normative sulla protezione dei dati come il GDPR.
	C01.2.2.2 Consapevolezza dell'ingegneria sociale e phishing	C01.2.2.2.1 Riconoscere e difendersi dalle tattiche di manipolazione.	Tattiche di phishing, ingegneria sociale e loro conseguenze. Identificare schemi di attacco. Coltivare un approccio di sospetto critico.
	C01.2.2.3 Diritto alla dimenticanza e rimozione dei dati	C01.2.2.3.1 Comprendere il concetto di diritto alla dimenticanza e le procedure per la rimozione dei dati.	Definizione di diritto alla dimenticanza, leggi sulla privacy e rimozione dei dati. Richiedere la rimozione dei dati personali, comprendere le implicazioni legali. Promuovere e rispettare il diritto alla dimenticanza come parte della privacy digitale.
C01.2.3 Cultura della sicurezza e consapevolezza	C01.2.3.1 Risposta agli incidenti e reporting	C01.2.3.1.1 Rispondere in modo adeguato agli eventi di sicurezza nel contesto aziendale.	Pianificazione di risposta agli incidenti, procedure di notifica Eseguire il piano di risposta, comunicare con l'equipe di sicurezza. Essere pronti a gestire situazioni di emergenza in conformità alla normativa.
	C01.2.3.1 Consapevolezza della sicurezza sul posto di lavoro	C01.2.3.1.1 Promuovere la consapevolezza della sicurezza tra i colleghi di lavoro.	Importanza della sicurezza sul posto di lavoro, minacce interne. Promuovere e partecipare a sessioni di sensibilizzazione, fornire informazioni sulla sicurezza. Contribuire a un ambiente di lavoro sicuro e consapevole della sicurezza.
	C01.2.3.3 Educazione alla sicurezza dei bambini e degli anziani	C01.2.3.3.1 Educare i bambini e gli anziani sulla sicurezza digitale.	Rischi online per bambini e anziani, consigli per un utilizzo sicuro. Comunicare in modo efficace le pratiche di sicurezza, supportare nell'uso dei dispositivi. Promuovere la sicurezza digitale intergenerazionale.

Unità didattica	Argomento	Capacità sviluppata	Competenza
C01.2.4 Sicurezza ambientale e benessere dell'utente	C01.2.4.1 Impatto ambientale delle tecnologie informatiche	C01.2.4.1.1 Comprendere l'impatto delle tecnologie informatiche sull'ambiente.	Consumo energetico dei dispositivi, impronta di carbonio dei data center. Calcolare e valutare l'impatto ambientale dell'utilizzo di dispositivi informatici. Integrare la sostenibilità nelle decisioni informatiche.
	C01.2.4.2 Salute e sicurezza durante l'uso dei dispositivi	C01.2.4.2.1 Salute e sicurezza durante l'uso dei dispositivi	Impatto posture sbagliate e uso prolungato dei dispositivi sulla salute. Applicare pratiche ergonomiche per ridurre rischi di affaticamento e danni fisici. Adottare comportamenti che favoriscano il benessere durante l'uso dei dispositivi.
	C01.2.4.3 Sicurezza dell'utilizzo dei dispositivi	C01.2.4.3.1 Conoscere e applicare buone pratiche per un uso sicuro dei dispositivi.	Minacce alla sicurezza legate all'uso di dispositivi e reti. Implementare misure di sicurezza, come aggiornamenti e utilizzo di reti sicure. Adottare comportamenti responsabili per prevenire rischi informatici.
C01.2.5 Impatto dell'Intelligenza Artificiale sulla sicurezza e sulla privacy	C01.2.5.1 IA e sicurezza digitale	C01.2.5.1.1 Comprendere il ruolo dell'IA nella sicurezza e nella privacy.	Concetti di base dell'intelligenza artificiale, applicazioni nella sicurezza. Identificare le sfide e le opportunità dell'IA nella protezione dei dati. Apprezzare il ruolo crescente dell'IA nel panorama della sicurezza informatica.
	C01.2.5.2 Rischi e benefici dell'IA per la sicurezza	C01.2.5.2.1 Valutare l'impatto positivo e negativo dell'IA sulla sicurezza.	Potenziali miglioramenti nella rilevazione delle minacce, rischi di attacchi basati sull'IA. Analizzare come l'IA possa essere sfruttata dai cybercriminali. Adottare un approccio equilibrato nella valutazione dell'IA come strumento di sicurezza.
	C01.2.5.3 Prevenzione e mitigazione delle minacce AI	C01.2.5.3.1 Sviluppare strategie per affrontare le minacce basate sull'IA.	Le minacce AI, come deepfakes e attacchi di generazione testuale. Implementare contromisure per rilevare e mitigare minacce basate sull'IA. Essere preparati ad affrontare nuovi tipi di attacchi basati sull'IA.

Unità didattica	Argomento	Capacità sviluppata	Competenza
	C01.2.5.4 Etica e regolamentazione dell'IA nella ricurezza	C01.2.5.4.1 Esplorare le implicazioni etiche e legali dell'IA nella sicurezza.	Impatto sociale dell'IA, dilemmi etici, regolamentazioni. Considerare le implicazioni etiche nell'uso dell'IA per la sicurezza. Promuovere un utilizzo etico e conforme dell'IA nella sicurezza.
	C01.2.5.5 Futuro dell'IA nella sicurezza e nella privacy	C01.2.5.5.1 Progettare una strategia per il futuro dell'IA e della sicurezza.	Tendenze emergenti nell'IA e nella sicurezza, impatto sull'evoluzione delle minacce. Sviluppare piani per affrontare le sfide future dell'IA nella sicurezza. Essere pronti ad adattarsi al cambiamento nel panorama dell'IA e della sicurezza.
	C01.2.5.6 Consapevolezza delle truffe basate sull'IA	C01.2.5.6.1 Riconoscere e difendersi dalle truffe basate sull'IA.	Tipi di truffe basate sull'IA come voice synthesis, truffe finanziarie. Identificare segni di truffe basate sull'IA, adottare pratiche per evitare inganni. Mantenere uno stato di vigilanza per proteggersi dalle minacce AI.
C01.2.6 Internet of Things (IoT)	C01.2.6.1 Sicurezza e privacy nell'Internet of Things	C01.2.6.1.1 Consapevolezza della sicurezza nell'Internet of Things	Le sfide legate alla sicurezza e alla privacy nell'IoT. Prendere precauzioni per proteggere i dispositivi IoT da minacce cibernetiche. Riconoscere l'importanza della sicurezza nella connettività IoT.
	C01.2.6.2 Consapevolezza dei rischi e delle vulnerabilità nell'IoT	C01.2.6.2.1 Identificare i rischi e le vulnerabilità legate all'IoT.	Tipi di rischi nell'IoT come l'accesso non autorizzato, il furto di dati personali. Valutare i potenziali punti deboli e le vulnerabilità nei dispositivi IoT. Mantenere un'attenzione costante sulla sicurezza nell'ambiente IoT.
	C01.2.6.3 Sicurezza nella configurazione e gestione dei dispositivi IoT	C01.2.6.3.1 Configurare e gestire dispositivi IoT in modo sicuro.	Processi di configurazione e gestione dei dispositivi IoT. Implementare misure di sicurezza come aggiornamenti regolari, autenticazione forte. Assumere un approccio proattivo nella protezione dei dispositivi IoT.

Unità didattica	Argomento	Capacità sviluppata	Competenza
	C01.2.6.4 Implicazioni etiche nell'Internet of Things	C01.2.6.4.1 Esplorare le questioni etiche legate all'IoT.	Dilemmi etici come la raccolta di dati personali, la sorveglianza invasiva. Riflettere sulle implicazioni etiche delle tecnologie IoT e sulla privacy degli utenti. Considerare gli aspetti etici nella progettazione e nell'uso di dispositivi IoT.
	C01.2.6.5 Privacy nell'Internet of Things	C01.2.6.5.1 Proteggere la privacy nell'ambiente IoT.	Rischio per la privacy nell'IoT, principi di protezione dei dati. Applicare misure di privacy come l'anonimizzazione dei dati, il controllo degli accessi. Approccio proattivo nella verifica delle policy di privacy adottate nella progettazione dell'IoT.
C01.2.7 Sicurezza delle applicazioni mobili	C01.2.7.1 Introduzione alla sicurezza delle applicazioni mobili	C01.2.7.1.1 Comprendere le minacce e le sfide legate alla sicurezza delle applicazioni mobili.	Le principali minacce alla sicurezza delle applicazioni mobili, come malware, vulnerabilità e attacchi di phishing. Analizzare le vulnerabilità comuni nelle app mobili e comprenderne gli effetti sulla privacy e la sicurezza dei dati. Interesse nella protezione delle informazioni personali e dei dati sensibili su dispositivi mobili.
	C01.2.7.2 Strumenti e tecniche per la sicurezza delle applicazioni mobili	C01.2.7.2.1 Utilizzare strumenti e tecniche per rafforzare la sicurezza delle applicazioni mobili.	L'uso di strumenti di analisi statica e dinamica per identificare vulnerabilità nelle app mobili. Applicare tecniche di codifica sicura e autenticazione per prevenire attacchi alle app mobili. Mostrare dedizione nell'adozione di buone pratiche di sviluppo per garantire la sicurezza delle app mobili.
	C01.2.7.3 Gestione delle minacce e sicurezza dei dati nelle app mobili	C01.2.7.3.1 Gestire le minacce alla sicurezza e garantire la protezione dei dati nelle app mobili.	Strategie per mitigare le minacce alla sicurezza delle app mobili, come l'implementazione di patch. Configurare funzionalità di sicurezza come la crittografia dei dati, l'autenticazione multifattoriale (MFA) e le autorizzazioni. Dimostrare un approccio proattivo alla gestione delle minacce e alla protezione dei dati sensibili nelle app mobili.
C01.2.8 Sicurezza nel Cloud Computing	C01.2.8.1 Introduzione alla sicurezza nel Cloud Computing	C01.2.8.1.1 Riconoscere le potenziali minacce e i vantaggi della sicurezza nel cloud.	Panoramica della sicurezza nel cloud, differenze principali rispetto alla sicurezza tradizionale. Identificare le principali minacce nel cloud. Adottare un approccio proattivo nella valutazione delle soluzioni cloud.

Unità didattica	Argomento	Capacità sviluppata	Competenza
	C01.2.8.2 Sicurezza personale e dei dati nel cloud	C01.2.8.2.1 Salvaguardare le proprie informazioni e risorse nel cloud.	Principali strategie di protezione personale nel cloud. Applicare misure di sicurezza di base come autenticazione a due fattori. Priorizzare la sicurezza personale nell'uso quotidiano del cloud.
	C01.2.8.3 Collaborazione sicura nel cloud	C01.2.8.3.1 Utilizzare strumenti di collaborazione nel cloud in modo sicuro.	Rischi comuni associati alla condivisione di dati nel cloud. Impostare correttamente i permessi di condivisione e utilizzare soluzioni di collaborazione protette. Essere consapevoli delle implicazioni di sicurezza durante la collaborazione online.
	C01.2.8.4 Protezione da minacce comuni nel cloud	C01.2.8.4.1 Riconoscere e proteggersi da minacce comuni come phishing e malware.	Overview delle minacce più comuni e come si manifestano. Adottare comportamenti sicuri e utilizzare strumenti di protezione. Mantenere un atteggiamento sempre vigile verso possibili minacce.
C01.2.9 Sicurezza nelle reti informatiche	C01.2.8.5 Strategie di intervento per incidenti nel cloud	C01.2.8.5.1 Creare una strategia personale per rispondere a eventuali incidenti di sicurezza nel cloud.	Panoramica degli incidenti comuni e delle loro conseguenze. Implementare backup regolari e conoscere i passi da seguire in caso di sospetti incidenti di sicurezza. Essere sempre preparati e sapere come agire in caso di emergenza.
	C01.2.9.1 Introduzione alla sicurezza nelle reti informatiche	C01.2.9.1.1 Comprendere le minacce e le sfide legate alla sicurezza nelle reti informatiche.	Principali minacce alla sicurezza nelle reti informatiche, come attacchi DDoS e sniffing. Analizzare i rischi associati all'uso delle reti informatiche e comprendere le misure di sicurezza necessarie. Mostrare interesse nella protezione delle reti e delle comunicazioni digitali da intrusioni malevole.
	C01.2.9.2. Protezione delle reti e sicurezza dei dispositivi	C01.2.9.2.1 Implementare misure di sicurezza per proteggere le reti informatiche e i dispositivi.	Le tecnologie di sicurezza come firewall, VPN e autenticazione per la protezione delle reti. Configurare misure di sicurezza a livello di rete e sui dispositivi, riconoscere dispositivi compromessi. Dimostrare dedizione nell'adozione di misure di sicurezza per garantire l'integrità delle reti e dei dati.

Unità didattica	Argomento	Capacità sviluppata	Competenza
	C01.2.9.3 Sicurezza delle reti wireless e crittografia	C01.2.9.3.1 Proteggere le reti wireless e utilizzare la crittografia per garantire la sicurezza delle comunicazioni.	Le minacce alla sicurezza delle reti wireless, come attacchi di spoofing e sniffing. Configurare reti wireless sicure, utilizzare protocolli di crittografia come WPA2 per proteggere le comunicazioni. Dimostrare impegno nella creazione e nel mantenimento di reti wireless sicure e protette.