EUCIP
European Certification of
Informatics Professionals

EUCIP IT Administrator - Modulo 1
PC Hardware

Syllabus Versione 3.1

La versione ufficiale in lingua inglese del syllabus *EUCIP IT Administrator – Modulo 1 - PC Hardware* è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo www.eucip.org. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di marzo 2019.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – PC Hardware

Questo documento presenta il syllabus di *EUCIP IT Administrator – PC Hardware*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato che affronti il test per *EUCIP IT Administrator – PC Hardware*. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Scopi del modulo

EUCIP IT Administrator – PC Hardware richiede che il candidato abbia un'ampia comprensione dei concetti relativi all'hardware di un PC e sia in grado di eseguire alcune installazioni e operazioni di manutenzione dell'hardware.

Il candidato dovrà essere in grado di:

- Comprendere gli elementi interni di un PC, incluse le schede madri, il BIOS, i microprocessori, la memoria e i bus.
- Comprendere e saper gestire le risorse del sistema, riconoscere e avere una buona conoscenza delle interfacce di un PC, incluse USB, schede di memoria e SATA.
- Installare e partizionare unità di memoria di massa, riconoscere le tecnologie video relative a monitor e schede video.
- Riconoscere i più comuni tipi di stampanti ed essere in grado di installare e gestire le stampanti.
- Conoscere i diversi tipi di alimentatori elettrici e i principi delle tecnologie UPS ed EPS.
- Installare e sostituire componenti hardware e diagnosticare problemi relativi all'hardware.

CATEGORIA	AREA	RIF.	ARGOMENTO
1.1 Schede madri	*1.1.1 Funzioni e tipi*	1.1.1.1	Comprendere il ruolo di una scheda madre.
		1.1.1.2	Comprendere le funzioni base integrate di una scheda madre.
		1.1.1.3	Comprendere il ruolo dei componenti di base di una scheda madre, quali: slot/socket per la CPU, chipset, memoria cache, bus, porte, slot di espansione, ecc.
		1.1.1.4	Identificare i componenti di base di una scheda madre.
		1.1.1.5	Identificare i diversi tipi di schede madri e saperle distinguere.
1.2 BIOS	*1.2.1 Caratteristiche di base*	1.2.1.1	Comprendere il termine BIOS, dove è memorizzato e quali sono le sue funzioni.

CATEGORIA	AREA	RIF.	ARGOMENTO
		1.2.1.2	Definire e comprendere la funzione dei termini legati al BIOS: POST, SETUP, CMOS, UEFI e Firmware.
		1.2.1.3	Identificare le impostazioni di base che possono essere regolate a partire dal BIOS, quali ora, password, dispositivi, gestione alimentazione, ordine di avvio.
	1.2.2 Aggiornamento	1.2.2.1	Descrivere come verificare la versione attuale del BIOS.
		1.2.2.2	Descrivere come aggiornare il BIOS quando necessario.
		1.2.2.3	Controllare, modificare le impostazioni del BIOS.
1.3 Microprocessori	*1.3.1 Caratteristiche e tipi*	1.3.1.1	Comprendere il ruolo della CPU.
		1.3.1.2	Definire i termini “velocità della CPU”, “overclock”, “fattore di moltiplicazione” (“multiply factor”).
		1.3.1.3	Descrivere i componenti di base di una CPU, quali core, registri, FPU, cache L1, bus.
		1.3.1.4	Identificare i fattori che determinano la velocità del processore.
		1.3.1.5	Elencare le diverse tensioni delle CPU e comprendere come possono essere impostate.
		1.3.1.6	Distinguere tra i diversi tipi di CPU relativamente alle loro capacità e limitazioni.
	1.3.2 Slot e socket	1.3.2.1	Identificare i tipi principali di zoccoli (socket) e contenitori (package) per le CPU.
		1.3.2.2	Identificare le corrette modalità per l’installazione di una CPU, quali inserimento corretto, collegamento corretto della ventola di raffreddamento.
		1.3.2.3	Comprendere la causa di problemi termici della CPU e sapere come risolverli.
1.4 Memoria	*1.4.1 RAM*	1.4.1.1	Distinguere tra memoria statica e dinamica.

CATEGORIA	AREA	RIF.	ARGOMENTO
		1.4.1.2	Distinguere tra i diversi tipi di DRAM in termini di velocità, capacità.
		1.4.1.3	Comprendere i termini “parità” e “memoria con ECC”, e la funzione di tali memorie.
		1.4.1.4	Comprendere il termine “divisione delle memoria in banchi” e il numero di bit usati da ciascun tipo di DRAM.
	1.4.2 ROM	1.4.2.1	Comprendere la funzione della ROM e le sue caratteristiche. Comprendere le differenze tra i diversi tipi di ROM, quali PROM, EPROM, EEPROM.
	1.4.3 Cache	1.4.3.1	Comprendere come opera la memoria cache e i relativi vantaggi.
		1.4.3.2	Identificare i diversi tipi di memoria cache e la loro posizione.
		1.4.3.3	Comprendere come opera la cache del disco e i relativi vantaggi.
1.5 Bus	*1.5.1 Struttura e ampiezza di banda*	1.5.1.1	Comprendere il termine “bus” e le sue funzioni.
		1.5.1.2	Descrivere la struttura di un bus.
		1.5.1.3	Comprendere la funzione di un bus indirizzi, di un bus dati e di un bus di controllo.
		1.5.1.4	Comprendere come l’ampiezza di banda può influenzare un bus.
	1.5.2 Tipi di bus	1.5.2.1	Definire i termini “front side bus” e “back side bus”.
		1.5.2.2	Comprendere la funzione dei bus di I/O.
		1.5.2.3	Distinguere tra i diversi tipi di bus di I/O, quali PCI, PCI-X, PCIe, USB.
1.6 Risorse di sistema	*1.6.1 Comprendere e gestire risorse di sistema*	1.6.1.1	Comprendere la funzione degli indirizzi delle porte di I/O.
		1.6.1.2	Comprendere la funzione di una richiesta di interrupt (IRQ).
		1.6.1.3	Comprendere la funzione del DMA.

CATEGORIA	AREA	RIF.	ARGOMENTO
		1.6.1.4	Delineare gli scopi, le tecniche e gli standard della gestione dell'alimentazione.
		1.6.1.5	Controllare le risorse di sistema usate e disponibili.
1.7 Interfacce	*1.7.1 Interfaccia parallel ATA*	1.7.1.1	Comprendere come opera un'interfaccia IDE, i suoi limiti e le sue capacità.
		1.7.1.2	Comprendere i termini "IDE primario", "IDE secondario", "Master" e "Slave".
		1.7.1.3	Sapere quante unità IDE possono essere gestite da un PC. Configurare le unità IDE usando le impostazioni del BIOS.
	1.7.2 Interfaccia SCSI	1.7.2.1	Comprendere come opera l'interfaccia SCSI e quali sono le differenze rispetto alle interfacce PATA.
		1.7.2.2	Comprendere i termini "Host adapter", "Identificativo SCSI" (SCSI ID), "LUN" e "terminatore".
		1.7.2.3	Descrivere i principali tipi di SCSI, le loro capacità e i loro limiti.
		1.7.2.4	Sapere quanti dispositivi SCSI possono essere gestiti da una catena SCSI. Configurare i dispositivi SCSI.
		1.7.2.5	Saper identificare diversi cavi e connettori SCSI.
	1.7.3 Interfaccia serial ATA	1.7.3.1	Comprendere lo scopo e la funzione di un'interfaccia SATA.
	1.7.4 Interfaccia USB	1.7.4.1	Distinguere tra le interfacce USB, le loro modalità operative, la loro capacità e i loro limiti.
		1.7.4.2	Identificare le connessioni USB fisiche e comprenderne i limiti.
		1.7.4.3	Sapere quanti dispositivi USB possono essere collegati a un PC.
	1.7.5 Interfaccia FireWire	1.7.5.1	Distinguere tra le interfacce FireWire, le loro modalità operative, la loro capacità e i loro limiti.

CATEGORIA	AREA	RIF.	ARGOMENTO
		1.7.5.2	Sapere quanti dispositivi FireWire possono essere usati. Comprendere i limiti del FireWire.
	1.7.6 Schede di memoria	1.7.6.1	Identificare diversi tipi di schede di memoria, quali Compact Flash (CF), Secure Digital (SD), microSSD, Memory Stick.
		1.7.6.2	Descrivere la funzione di un lettore di schede.
	1.7.7 Controller RAID	1.7.7.1	Identificare i tipi di configurazioni RAID in termini di prestazioni e sicurezza.
		1.7.7.2	Comprendere le capacità di “hot swap” delle unità RAID.
		1.7.7.3	Identificare la funzione della scheda SATA controller del RAID.
		1.7.7.4	Identificare la funzione della scheda SCSI controller del RAID.
1.8 Memoria di massa	*1.8.1 Principi*	1.8.1.1	Comprendere le modalità operative di un disco e come vengono immagazzinati i dati. Comprendere i termini “traccia”, “settore”, “cilindro”, “cluster”, “cilindro-testina-settore” (CHS), blocco.
		1.8.1.2	Partizionare un disco fisso. Comprendere i termini “unità logica” e “partizione attiva”.
		1.8.1.3	Installare un disco fisso,un drive ottico, un dispositivo SSD. Identificare i cavi necessari e come vanno collegati.
		1.8.1.4	Comprendere i termini relativi alla gestione dei dischi: formattazione a basso livello, partizione, formattazione ad alto livello.
		1.8.1.5	Distinguere tra le diverse tecnologie di dischi ottici, quali CD-R, CD-RW, DVD+/-R, DVD+/-RW, Blu-ray.
1.9 Dispositivi di visualizzazione	*1.9.1 Monitor*	1.9.1.1	Distinguere tra diversi tipi comuni di monitor, quali TFT, LED.
		1.9.1.2	Identificare i fattori che influenzano la qualità dell’immagine, quali risoluzione, frequenza di refresh, numero di colori.

CATEGORIA	AREA	RIF.	ARGOMENTO
	1.9.2 Scheda grafica	1.9.2.1	Identificare gli standard più comuni di risoluzione grafica, quali VGA, SVGA, XGA, HD, FULL HD, 720p, 1080p, 4K.
		1.9.2.2	Comprendere le funzioni dei componenti fondamentali di una scheda grafica, quali GPU, memoria, BIOS video, RAMDAC.
		1.9.2.3	Identificare la funzione di PCIe ed i suoi vantaggi.
		1.9.2.4	Identificare i problemi termici della GPU e le tecniche di raffreddamento, quali ventola e “heat pipes”.
		1.9.2.5	Identificare i diversi connettori e cavi usati per collegare le scheda grafica di tipo HDMI, DVI, VGA al monitor.
		1.9.2.6	Identificare le diverse configurazioni di schede grafiche multiple, quali SLI, crossfire.
	1.9.3 Libreria grafica	1.9.3.1	Comprendere la funzione delle specifiche usate per la definizione della grafica, quali DirectX, OpenGL.
1.10 Stampanti	*1.10.1 Tipi*	1.10.1.1	Distinguere tra le principali tecnologie di stampa, quali matrice di punti, getto d’inchiostro e laser.
		1.10.1.2	Comprendere le modalità operative di una stampante a matrice di punti, i suoi vantaggi e i suoi limiti.
		1.10.1.3	Comprendere le modalità operative di una stampante a getto d’inchiostro, i suoi vantaggi e i suoi limiti.
		1.10.1.4	Comprendere le modalità operative di una stampante laser, i suoi vantaggi e i suoi limiti.
		1.10.1.5	Comprendere le modalità operative delle stampanti a trasferimento termico e a sublimazione, i loro vantaggi e i loro limiti.
	1.10.2 Installazione e gestione	1.10.2.1	Riconoscere le diverse modalità di comunicazione tra un PC e una stampante, quali porta parallela, porta seriale, porta USB, rete wireless, LAN.

CATEGORIA	AREA	RIF.	ARGOMENTO
1.11 Alimentazione	*1.11.1 Tipi e funzione*	1.11.1.1	Comprendere i termini volt, ampere, ohm, watt, corrente alternata e corrente continua.
		1.11.1.2	Comprendere la funzione dell'alimentatore e riconoscere diversi tipi di alimentatori.
		1.11.1.3	Identificare diverse connessioni elettriche verso le periferiche.
		1.11.1.4	Comprendere i termini APM, ACPI.
	1.11.2 Scariche elettrostatiche	1.11.2.1	Comprendere il termine "surge protector" e quali sono le sue modalità operative. Comprendere il termine "scarica elettrostatica" ("ESD"), sapere quando si verifica e quali danni può provocare.
		1.11.2.2	Identificare i passi da compiere per proteggere l'hardware dai danni provocati dalle scariche elettrostatiche. Comprendere come le condizioni meteorologiche influenzino il verificarsi di scariche elettrostatiche.
	1.11.3 UPS	1.11.3.1	Comprendere lo scopo di un UPS, sapere come operano i diversi tipi di UPS e come comunicano con un PC.
		1.11.3.2	Comprendere il potenziale impatto del picco di corrente dovuto all'accensione degli alimentatori dei PC.
1.12 Installazione hardware	*1.12.1 Installare e sostituire l'hardware*	1.12.1.1	Installare e sostituire un componente di base, quale CPU, memoria, alimentatore, scheda madre, disco fisso, scheda grafica.
		1.12.1.2	Installare e configurare un secondo disco fisso o CD-ROM. Creare e gestire diverse partizioni.
		1.12.1.3	Installare schede di espansione, quali scheda audio, scheda di rete.
		1.12.1.4	Installare e configurare una normale scheda controller o un controller di tipo RAID.
1.13 Diagnosi e risoluzione dei problemi	*1.13.1 Problemi hardware*	1.13.1.1	Riconoscere i messaggi di errore più importanti al momento dell'avvio, quali "invalid system disk", "keyboard error". Identificare i passaggi necessari alla soluzione degli errori più comuni.

CATEGORIA	AREA	RIF.	ARGOMENTO
		1.13.1.2	Riconoscere un messaggio di errore proveniente da un componente di base, quale i segnali acustici all'avvio.
		1.13.1.3	Controllare nel BIOS l'hardware installato e le relative configurazioni.
		1.13.1.4	Controllare le risorse usate, quali indirizzi di I/O, IRQ e DMA.

EUCIP
European Certification of
Informatics Professionals

EUCIP IT Administrator - Modulo 2
Sistemi operativi

Syllabus Versione 3.1

La versione ufficiale in lingua inglese del syllabus *EUCIP IT Administrator – Modulo 2 – Sistemi operativi* è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo www.eucip.org. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di marzo 2019.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – Sistemi operativi

Questo documento presenta il syllabus di *EUCIP IT Administrator – Sistemi operativi*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato che affronti il test per *EUCIP IT Administrator – Sistemi operativi*. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Scopi del modulo

EUCIP IT Administrator – Sistemi operativi richiede che il candidato abbia un'ampia comprensione dei concetti relativi ai sistemi operative e sia in grado di configurare e gestire un sistema operativo.

Il candidato dovrà essere in grado di:

- Conoscere i fondamenti dei sistemi operativi (OS) e installare un sistema operativo.
- Configurare e aggiornare un sistema operativo, installare hardware e software.
- Installare schede di rete, programmi di navigazione web e di posta elettronica.
- Gestire le prestazioni e gli eventi di un sistema operativo, gestire gli account di utenti e di gruppi.
- Creare e gestire risorse condivise e permessi degli account, gestire stampanti di rete.
- Eseguire copie di sicurezza, usare strumenti di amministrazione e servizi di rete, installare e gestire servizi internet.
- Eseguire diagnosi e interventi per la risoluzione di problemi del sistema operativo, essere in grado di installare un DBMS.

CATEGORIA	AREA	RIF.	ARGOMENTO
2.1 Fondamenti dei sistemi operativi	*2.1.1 Funzioni di base*	2.1.1.1	Comprendere la funzione e le modalità d'uso di un sistema operativo.
		2.1.1.2	Conoscere i tipi principali di sistemi operativi, quali batch, time-sharing, real time.
		2.1.1.3	Definire i concetti principali dei sistemi operativi, quali multitasking, multiutente, processi, thread, contesto, commutazione di contesto (context switch) e protezione.
		2.1.1.4	Distinguere tra i più comuni sistemi operativi per i PC.
		2.1.1.5	Delineare le principali caratteristiche dei sistemi operativi, quali multitasking, multiutente, real time, interfaccia grafica.
	2.1.2 Processo di installazione	2.1.2.1	Installare un sistema operativo da CD-ROM, dispositivo USB, rete.

CATEGORIA	AREA	RIF.	ARGOMENTO
	2.1.3 Sistema operativo doppio	2.1.3.1	Installare più sistemi operativi su un PC.
		2.1.3.2	Conoscere i passaggi del processo di avvio quando sono installati più sistemi operativi. Identificare i file usati durante l'avvio e la loro funzione.
		2.1.3.3	Definire il termine “Menu di avvio” (“Boot menu”) e comprendere quando viene usato. Visualizzare e modificare le impostazioni del menu di avvio.
2.2 Organizzazione di un sistema operativo	*2.2.1 Processo di avvio*	2.2.1.1	Conoscere i file usati durante il processo di avvio e la loro funzione.
		2.2.1.2	Conoscere la cartella da cui vengono caricati i file di avvio.
		2.2.1.3	Conoscere i file di avvio necessari su un disco di avvio e le loro funzioni.
		2.2.1.4	Creare un disco di avvio.
2.3 Uso, configurazione e aggiornamento di un sistema operativo	*2.3.1 Interfaccia di un sistema operativo*	2.3.1.1	Descrivere l'interfaccia dei sistemi operativi. Definire il termine “application program interface” (API).
		2.3.1.2	Usare l'interfaccia del sistema operativo per aggiungere, eliminare, modificare collegamenti e icone.
	2.3.2 Configurare l'ambiente	2.3.2.1	Configurare e modificare le impostazioni dello schermo: colori, risoluzione, frequenza di refresh, driver della scheda video.
		2.3.2.2	Configurare e modificare le impostazioni della scrivania, quali sfondo, temi, barre delle applicazioni.
		2.3.2.3	Configurare e modificare le impostazioni di mouse e tastiera.
		2.3.2.4	Configurare e modificare le impostazioni internazionali.
		2.3.2.5	Aggiungere, modificare ed eliminare una stampante. Impostare una stampante come predefinita, controllare lo stato di una stampante e aggiornare i driver.

CATEGORIA	AREA	RIF.	ARGOMENTO
		2.3.2.6	Descrivere come sono organizzate le cartelle, directory di un sistema operativo. Sapere dove vengono salvati file particolari, quali file di sistema, file di applicazioni, file temporanei, file internet.
	2.3.3 File di configurazione	2.3.3.1	Conoscere i file contenenti informazioni di configurazione, quali registry, valori di avvio (startup default). Sapere dove vengono salvati.
		2.3.3.2	Controllare e modificare i file di configurazione mediante una utilità di sistema.
		2.3.3.3	Proteggere, eseguire copie di sicurezza e ripristinare i file di configurazione.
	2.3.4 Aggiornamento	2.3.4.1	Aggiornare il sistema operativo a una nuova versione.
		2.3.4.2	Comprendere l'importanza di mantenere aggiornato un sistema. Installare gli aggiornamenti di un sistema operativo.
		2.3.4.3	Configurare il sistema in modo che gli aggiornamenti vengano installati automaticamente.
	2.3.5 Documentazione	2.3.5.1	Controllare la configurazione attuale del server e preparare la documentazione relativa.
		2.3.5.2	Controllare la configurazione attuale di un client e preparare la documentazione relativa.
	2.3.6 File System	2.3.6.1	Riconoscere i file system comuni che possono essere usati dai sistemi operativi, quali FAT, NTFS, EXT2, EXT4.
		2.3.6.2	Conoscere le principali caratteristiche e funzionalità di diversi file system.
		2.3.6.3	Conoscere il file system adatto a ciascun sistema operativo.
		2.3.6.4	Conoscere i motivi per convertire da un file system a un altro. Convertire da un file system ad un altro se e quando risulta utile.

CATEGORIA	AREA	RIF.	ARGOMENTO
		2.3.6.5	Conoscere la funzione degli attributi di file e directory.
	2.3.7 Ottimizzare le prestazioni dei dischi	2.3.7.1	Verificare i dischi e risolvere i problemi usando un programma di utilità disponibile.
		2.3.7.2	Definire il termine “frammentazione” e indicare per quali motivi si verifica.
		2.3.7.3	Definire il termine “deframmentazione”. Usare un programma di utilità per eseguire la deframmentazione.
		2.3.7.4	Riconoscere i file indesiderati su un disco. Eliminare file indesiderati usando un programma di utilità disponibile.
	2.3.8 Utilità di amministrazione dischi	2.3.8.1	Usare l'utilità di amministrazione dischi disponibile per creare, formattare e attivare una partizione.
		2.3.8.2	Configurare e controllare i file system.
		2.3.8.3	Comprendere il termine RAID e i vantaggi derivanti dal suo uso. Identificare i tipi di RAID più comuni, quali RAID0, RAID1 e RAID5.
		2.3.8.4	Installare e gestire un sistema RAID.
2.4 Installare hardware e software	*2.4.1 Installazione di hardware*	2.4.1.1	Controllare l'hardware disponibile installato e la relativa configurazione. Preparare la documentazione necessaria.
		2.4.1.2	Definire i termini “dispositivi” e “driver” e descrivere i relativi ruoli nell'installazione e nella gestione dell'hardware.
		2.4.1.3	Controllare le risorse usate, quali indirizzi di I/O, IRQ, DMA.
		2.4.1.4	Verificare la presenza di conflitti di risorse e risolverli.
		2.4.1.5	Installare, eliminare e aggiornare driver di dispositivi hardware, usando fonti diverse.
	2.4.2 Installazione di software	2.4.2.1	Installare, aggiornare e disinstallare software applicativo.

CATEGORIA	AREA	RIF.	ARGOMENTO
2.5 Comunicazioni esterne	*2.5.1 Rete*	2.5.1.1	Installare una scheda di rete. Aggiornare i driver di una scheda di rete.
		2.5.1.2	Configurare una scheda di rete.
		2.5.1.3	Installare e configurare il protocollo TCP/IP.
		2.5.1.4	Comprendere il termine “firewall personale”. Configurare un firewall personale.
	2.5.2 Browser internet	2.5.2.1	Installare, configurare e usare un browser internet.
		2.5.2.2	Modificare le impostazioni di un browser internet, quali eliminare i file di navigazione temporanei, cancellare la cronologia di navigazione.
		2.5.2.3	Verificare e modificare il browser predefinito.
	2.5.3 Software di posta elettronica	2.5.3.1	Installare e usare software per la posta elettronica.
		2.5.3.2	Configurare protocolli per il software di posta elettronica, quali POP3, IMAP, SMTP.
2.6 Prestazioni ed eventi	*2.6.1 Prestazioni*	2.6.1.1	Riconoscere un programma di utilità disponibile per il tracciamento delle prestazioni di hardware e software.
		2.6.1.2	Riconoscere un programma di utilità disponibile per il controllo della memoria, e sapere come funziona.
		2.6.1.3	Controllare le prestazioni di un singolo dispositivo o attività.
		2.6.1.4	Controllare le informazioni di stato disponibili sulle prestazioni, quali memoria totale e libera, memoria virtuale in uso, risorse disponibili.
		2.6.1.5	Controllare le attività e i processi attivi.
	2.6.2 Eventi	2.6.2.1	Controllare gli eventi, il log di sistema.
2.7 Gestione di account utenti e account di gruppi	*2.7.1 Inserimento, eliminazione di utenti e gruppi*	2.7.1.1	Distinguere tra i diversi ruoli di utenti e gruppi.

CATEGORIA	AREA	RIF.	ARGOMENTO
		2.7.1.2	Aggiungere, eliminare un utente o un gruppo.
		2.7.1.3	Aggiungere, eliminare un utente da un gruppo.
	2.7.2 Impostazione proprietà	2.7.2.1	Visualizzare le proprietà di un utente, quali tempo di collegamento, profilo.
		2.7.2.2	Modificare le proprietà di un utente, quali password, tempo di collegamento, profilo.
		2.7.2.3	Visualizzare le proprietà di un gruppo, quali membri del gruppo.
	2.7.3 Strumenti di amministrazione	2.7.3.1	Usare un programma di utilità disponibile per gestire utenti e gruppi.
2.8 Risorse condivise e permessi account	*2.8.1 Creazione di risorse condivise*	2.8.1.1	Comprendere il termine “risorse condivise”, sapere quali sono i loro vantaggi e i loro rischi relativi a sicurezza e privacy.
		2.8.1.2	Creare risorse condivise, quali file, stampanti, modem.
		2.8.1.3	Verificare le risorse condivise disponibili su una rete. Controllare quali utenti stanno usando le risorse condivise e verificare i permessi delle risorse condivise.
	2.8.2 Eliminazione di risorse condivise	2.8.2.1	Eliminare risorse condivise, quali file, stampanti, modem.
		2.8.2.2	Scollegare utenti da una risorsa condivisa.
	2.8.3 Unità logiche di rete	2.8.3.1	Definire il termine “unità logica di rete”.
		2.8.3.2	Conoscere i passaggi da eseguire per collegare una unità logica di rete ad una risorsa condivisa.
		2.8.3.3	Conoscere i passaggi necessari per collegare un client ad una risorsa di stampa condivisa, usando una porta logica di stampa.
		2.8.3.4	Collegare un client a una risorsa condivisa su un server o su altri client.

CATEGORIA	AREA	RIF.	ARGOMENTO
	2.8.4 Gestione dei permessi degli account	2.8.4.1	Comprendere le opzioni dei permessi relativi alle risorse condivise che possono essere usate dal sistema operativo di rete.
		2.8.4.2	Impostare, eliminare e modificare i permessi di un utente o gruppo.
		2.8.4.3	Controllare quali utenti sono collegati. Scollegarli dalla rete.
2.9 Gestione delle stampanti di rete	*2.9.1 Installazione e gestione di stampanti*	2.9.1.1	Installare una stampante locale, di rete.
		2.9.1.2	Collegare e usare una stampante condivisa e controllarne i permessi.
		2.9.1.3	Verificare lo stato della stampante (stato della coda di stampa).
		2.9.1.4	Annullare, sospendere o riordinare un processo nella coda di stampa.
2.10 Sicurezza e protezione	*2.10.1 Copie di sicurezza*	2.10.1.1	Comprendere l'importanza di eseguire delle copie di sicurezza.
		2.10.1.2	Pianificare le copie di sicurezza usando i programmi di utilità disponibili e un dispositivo di memoria esterno.
		2.10.1.3	Ripristinare file da una copia di sicurezza.
2.11 Programmi di utilità	*2.11.1 Strumenti di amministrazione*	2.11.1.1	Tenere sotto controllo le prestazioni del server, quali utilizzo della CPU, utilizzo della memoria, utilizzo del disco, allineamenti memoria (page fault).
		2.11.1.2	Comprendere la funzione dei programmi di utilità per la gestione delle risorse condivise.
	2.11.2 Utilità di rete	2.11.2.1	Configurare una rete utilizzando dei programmi di utilità di rete.
		2.11.2.2	Tracciare l'uso della rete utilizzando dei programmi di utilità di rete.
2.12 Condivisione di servizi internet	*2.12.1 Installazione di servizi*	2.12.1.1	Installare, configurare e gestire un semplice server di posta elettronica.
		2.12.1.2	Installare, configurare e gestire un semplice servizio web.

CATEGORIA	AREA	RIF.	ARGOMENTO
2.13 Diagnosi e risoluzione dei problemi	*2.13.1 Diagnosi*	2.13.1.1	Utilizzare i programmi di diagnostica disponibili per analizzare le impostazioni hardware e software del sistema.
		2.13.1.2	Diagnosticare e risolvere i problemi che si possono verificare durante il processo di avvio.
		2.13.1.3	Diagnosticare e risolvere i problemi relativi ai file di configurazione del sistema.
		2.13.1.4	Diagnosticare e risolvere i problemi relativi alla stampa locale.
	2.13.2 Risoluzione dei problemi	2.13.2.1	Avviare un computer in modalità sicura.
		2.13.2.2	Comprendere la funzione di un disco di ripristino. Saper utilizzare un disco di ripristino per ripristinare il sistema.
		2.13.2.3	Identificare i motivi per cui un utente non riesce ad accedere alla rete. Localizzare la fonte del problema, quale server, cavo, scheda di rete, driver.
		2.13.2.4	Diagnosticare e risolvere i problemi relativi ai permessi di un utente, quali salvataggio file, uso di una risorsa condivisa.
		2.13.2.5	Diagnosticare e risolvere i problemi relativi agli account utente locali e di dominio, se un dominio è disponibile.
		2.13.2.6	Diagnosticare i problemi di stampa.
2.14 Database	*2.14.1 Gestione dei dati*	2.14.1.1	Comprendere la necessità di disporre sui server delle raccolte dati coerenti.
		2.14.1.2	Installare un DBMS su un server.
		2.14.1.3	Descrivere come vengono utilizzati DDL e DML per gestire un database.
		2.14.1.4	Comprendere l'importanza di atomicità, consistenza, isolamento e durabilità (ACID) per assicurare l'affidabilità delle transazioni su un database.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator - Modulo 3 Reti

Syllabus Version 3.1

La versione ufficiale in lingua inglese del syllabus EUCIP *IT Administrator – Modulo 3 - Reti* è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo www.eucip.org. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di marzo 2019.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – Reti

Questo documento presenta il syllabus di *EUCIP IT Administrator - Reti*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato che affronti il test per *EUCIP IT Administrator - Reti*. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Scopi del modulo

EUCIP IT Administrator - Reti richiede che il candidato abbia un'ampia comprensione dei concetti relativi alle reti e sia in grado di svolgere attività di configurazione e supporto sulle reti.

Il candidato dovrà essere in grado di:

- Descrivere le principali architetture di rete e i protocolli di comunicazione.
- Comprendere il modello di riferimento OSI e i diversi strati: fisico, collegamento dati, rete, trasporto, sessione, presentazione, applicazioni.
- Eseguire la configurazione a basso livello, quale collegamento a una rete, installazione di una scheda di rete, configurazione IP.
- Impostare servizi web e di posta elettronica, e saper usare FTP.
- Eseguire verifiche e interventi di base per la risoluzione di problemi sulla rete.
- Comprendere i principi legali fondamentali relativi all'uso e alla sicurezza della rete.
- Conoscere i problemi fondamentali di sicurezza della rete e dei browser.

CATEGORIA	AREA	RIF.	ARGOMENTO
3.1 Introduzione alle reti	*3.1.1 Architetture e protocolli di comunicazione*	3.1.1.1	Descrivere lo sviluppo dell'approccio client-server da un sistema gerarchico a sistemi distribuiti.
		3.1.1.2	Descrivere gli standard "de facto" e "de jure": la suite TCP/IP e il modello OSI; le organizzazioni di standardizzazione, quali CCITT, ITU-TS, IEEE, ISO e IAB.
3.2 Il modello di riferimento OSI	*3.2.1 Introduzione agli strati del modello di riferimento*	3.2.1.1	Descrivere lo scopo del modello di riferimento a strati (principio di incapsulamento e punti di accesso ai servizi nei modelli a strati).
		3.2.1.2	Descrivere il ruolo di ciascun livello del modello OSI: fisico, collegamento dati, rete, trasporto, sessione, presentazione, applicazione.
		3.2.1.3	Descrivere gli scopi principali dei protocolli, quali controllo di errore, gestione della sessione, controllo del flusso.
		3.2.1.4	Distinguere tra il modello ISO/OSI e il protocollo TCP/IP.

CATEGORIA	AREA	RIF.	ARGOMENTO
3.3 Livello fisico	*3.3.1 Tipi di dati e segnali*	3.3.1.1	Descrivere le proprietà dei segnali analogici e digitali.
		3.3.1.2	Distinguere tra bit, byte e pacchetti nei segnali digitali binari.
	3.3.2 Trasmissione dati	3.3.2.1	Riconoscere i principali mezzi trasmissivi confinati (cavi in rame e fibre ottiche) e non confinati (microonde, radio, infrarossi, laser, satellite).
		3.3.2.2	Descrivere i sistemi di cablaggio strutturato (comportamento, uso e vantaggi), componenti (spine, prese, cavi di raccordo, rack, ecc.), ed elementi aggiuntivi non certificati.
		3.3.2.3	Riconoscere le principali topologie di rete: bus lineare, stella, anello, albero.
		3.3.2.4	Distinguere tra le modalità di comunicazione (simplex, half-duplex, full duplex) e i tipi di trasmissione (asincrona, sincrona, seriale, parallela).
		3.3.2.5	Riconoscere i termini “bit di start”, “bit di stop”, parità, “bit di dati” e sapere dove vengono usati. Riconoscere i termini SYNC, STX, ETX, ACK e NACK e sapere dove vengono usati.
		3.3.2.6	Definire cosa si intende per canali e banda.
	3.3.3 Protocolli	3.3.3.1	Descrivere i sistemi Ethernet dal punto di vista della velocità di trasmissione dati, del mezzo trasmissivo, delle lunghezze massime e del numero massimo di nodi.
		3.3.3.2	Descrivere un sistema di rete FDDI dal punto di vista della struttura, della velocità di trasmissione dati e dai limiti di distanza.
		3.3.3.3	Conoscere le velocità di trasmissione dati disponibili nei sistemi ATM e Frame Relay.

CATEGORIA	AREA	RIF.	ARGOMENTO
	3.3.4 Dispositivi	3.3.4.1	Elencare i mezzi trasmissivi e le tecniche utilizzati per le comunicazioni non cablate (infrarossi, spread spectrum, microonde in banda stretta) e la loro gamma operativa. Riconoscere il problema della diffusione delle onde radio.
		3.3.4.2	Descrivere la funzione di un hub e di un repeater.
3.4 Livello collegamento dati	*3.4.1 Introduzione*	3.4.1.1	Definire i concetti di “commutazione di circuito” e “commutazione di pacchetto”. Definire il concetto di frame.
		3.4.1.2	Descrivere le operazioni CSMA/CD. Definire il concetto di indirizzo MAC.
		3.4.1.3	Definire i principi di base del controllo di accesso al mezzo trasmissivo in un sistema FDDI.
	3.4.2 Modalità di trasferimento asincrona (Asynchronous Transfer Mode - ATM) e Frame Relay.	3.4.2.1	Definire quali sono le connessioni logiche ATM: percorso di trasmissione, percorso virtuale, canale virtuale.
		3.4.2.2	Definire quali sono le connessioni logiche Frame Relay, quali circuito virtuale, circuito virtuale permanente, identificatore della connessione dati.
	3.4.3 Protocollo punto-punto (Point-to-Point Protocol - PPP)	3.4.3.1	Descrivere lo scopo e le operazioni del protocollo PPP; descrivere le differenze tra PPP e SLIP.
	3.4.4 LAN virtuale (Virtual LAN - VLAN)	3.4.4.1	Descrivere quali operazioni può eseguire una VLAN a livello di collegamento dati.
	3.4.5 Bridge e switch	3.4.5.1	Descrivere la funzione di uno switch e di un bridge.
3.5 Livello rete	*3.5.1 Protocolli di rete*	3.5.1.1	Descrivere lo scopo di un sistema di indirizzamento.
		3.5.1.2	Descrivere lo scopo del protocollo IP. Definire il termine “datagramma”.
	3.5.2 Protocolli di supporto	3.5.2.1	Conoscere le funzioni dei protocolli ICMP, DHCP e ARP.

CATEGORIA	AREA	RIF.	ARGOMENTO
	3.5.3 Indirizzamento IP	3.5.3.1	Descrivere lo schema di indirizzamento IP, la relazione tra gli indirizzi IP e le classi di rete, i concetti di sottorete e CIDR. Essere in grado di distinguere tra IPv4 e IPv6.
	3.5.4 Internetworking	3.5.4.1	Descrivere le necessità e le funzioni dell'instradamento.
	3.5.5 Dispositivi di rete: router e switch di livello 3	3.5.5.1	Essere in grado di distinguere tra indirizzi logici e fisici.
		3.5.5.2	Descrivere lo scopo di un router e la funzione di uno switch di livello 3.
3.6 Livello trasporto	*3.6.1 Fondamenti del livello trasporto*	3.6.1.1	Definire i termini "segmento", "porta", "porta ben nota" (well-known-port) e "connessione" nel contesto del livello trasporto.
	3.6.2 Protocolli del livello trasporto	3.6.2.1	Comprendere lo scopo del protocollo TCP e i suoi meccanismi principali: PAR, controllo di flusso, multiplexing, segnalazione di dati urgenti. Conoscere le caratteristiche del protocollo UDP e sapere quali sono le differenze rispetto al TCP.
	3.6.3 VLAN	3.6.3.1	Definire il termine VLAN. Conoscere i vantaggi e i rischi di una VLAN.
	3.6.4 Sicurezza del livello di trasporto	3.6.4.1	Descrivere lo scopo del NAT (Network Address Translation) e del PAT (Port Address Translation). Riconoscere diversi tipi di NAT, quali SNAT, DNAT.
		3.6.4.2	Comprendere lo scopo di un proxy di indirizzamento (address proxy).
		3.6.4.3	Comprendere lo scopo di un firewall e le sue funzioni principali.
3.7 Livello sessione	*3.7.1 Attivazione di una sessione: negoziazione dei parametri*	3.7.1.1	Descrivere i dettagli della fase di negoziazione RAS & PPP/SLIP.
		3.7.1.2	Descrivere le fasi di negoziazione del DHCP.

CATEGORIA	AREA	RIF.	ARGOMENTO
3.8 Livello presentazione	*3.8.1 Standard per la codifica dei dati*	3.8.1.1	Descrivere gli standard ASCII, ANSI e UNICODE, i limiti di ASCII relativamente alle lingue nazionali (concetto di insieme di caratteri), codifica dei dati interna al computer (file binari rispetto a file di testo, controllo della codifica del carattere di fine linea EOL nei sistemi DOS/Windows, Apple e Unix/Linux), codifica dei numeri interna al computer ("big-endian" rispetto a "little-endian", rappresentazione canonica).
	3.8.2 Protocollo MIME	3.8.2.1	Comprendere come è possibile usare il protocollo MIME nella gestione di diversi oggetti.
	3.8.3 Altri formati non binari	3.8.3.1	Descrivere lo scopo della compressione dei file e gli standard principali per le piattaforme note, quali ZIP, GZIP, TAR.
3.9 Applicazioni	*3.9.1 Applicazioni di rete*	3.9.1.1	Descrivere lo scopo del livello applicazione.
		3.9.1.2	Descrivere lo scopo di TELNET.
		3.9.1.3	Descrivere lo scopo del protocollo FTP.
		3.9.1.4	Descrivere lo scopo dei protocolli DHCP e TFTP.
	3.9.2 Risorse remote sul web	3.9.2.1	Definire il termine Uniform Resource Locator (URL).
		3.9.2.2	Descrivere l'impiego e le principali operazioni del DNS (Domain Name System).
		3.9.2.3	Descrivere lo scopo dei protocolli HTTP e HTTPS.
		3.9.2.4	Comprendere i principi di funzionamento di CGI e di applet.
		3.9.2.5	Definire il termine cookie. Riconoscere vantaggi e rischi dei cookie.
		3.9.2.6	Descrivere le intestazioni http "content-type" e lo standard MIME.
		3.9.2.7	Comprendere l'impiego dei principali linguaggi di markup e dei fogli di stile, quali HTML, SGML, XML, CSS, XSL.

CATEGORIA	AREA	RIF.	ARGOMENTO
		3.9.2.8	Descrivere lo scopo di un gateway.
	3.9.3 Posta elettronica	3.9.3.1	Descrivere l'impiego e i componenti del protocollo SMTP (Simple mail transfer protocol).
		3.9.3.2	Descrivere la struttura di un indirizzo di posta elettronica.
		3.9.3.3	Comprendere l'impiego dei protocolli POP3 e IMAP.
		3.9.3.4	Riconoscere i limiti di trasmissione dei dati di SMTP, quali messaggi di posta elettronica di grandi dimensioni, allegati sconosciuti.
		3.9.3.5	Comprendere lo scopo di MIME e la sua relazione con SMTP.
	3.9.4 Applicazioni di gruppo	3.9.4.1	Definire lo scopo e le caratteristiche dei sistemi di chat e di messaggistica istantanea.
		3.9.4.2	Descrivere lo scopo e le modalità d'impiego di un forum e dei social media.
		3.9.4.3	Comprendere il termine "netiquette".
	3.9.5 Controllo di accesso e condivisione	3.9.5.1	Descrivere le policy DAC, MAC, RBAC, lo scopo della condivisione di file, i diversi livelli autorizzativi e i concetti di login e di script di logon.
		3.9.5.2	Descrivere le finalità dei protocolli NetBIOS, NETBEUI, SMB e CIFS, principi di operazioni, caratteristiche principali e differenze.
		3.9.5.3	Descrivere l'operazione di server browsing, l'elezione e le operazioni del master browser, la condivisione di servizi (principali differenze tra di loro, livello di incapsulamento in Ethernet rispetto a IP).
	3.9.6 Controllo di rete	3.9.6.1	Descrivere lo scopo del protocollo SNMP (Simple Network Management Protocol), lo scopo di un gestore di rete e di un agente SNMP.
		3.9.6.2	Descrivere le funzionalità di SNMP e i principali strumenti a sua disposizione.

CATEGORIA	AREA	RIF.	ARGOMENTO
3.10 Configurazione a basso livello	*3.10.1 Connessione a una rete*	3.10.1.1	Connettere un computer a un segmento Ethernet, quale 10BaseT, 100BaseT, 100BaseF, Gbit Ethernet.
		3.10.1.2	Connettere hub o switch in cascata usando porte incrociate, cavi incrociati o cavi coassiali.
		3.10.1.3	Connettere un computer ad una rete wireless. Sapere come utilizzare un punto d'accesso. Sapere perché e come configurare il canale, la cifratura WAP, WPA2, EAP, PEAP, il DHCP.
	3.10.2 Installare una scheda di rete	3.10.2.1	Riconoscere i vincoli relativi all'installazione di una scheda di rete: sicurezza personale, sicurezza della scheda, garanzia, approvazione tecnica.
		3.10.2.2	Installare una scheda di rete. Riconoscere il tipo di bus per un PC, i tipi di bus presenti sulla scheda madre e le loro differenze.
		3.10.2.3	Conoscere i sistemi automatici di riconoscimento hardware, quali, ad esempio, PCMCIA, USB, FireWire.
		3.10.2.4	Inserire delle schede di rete in un computer.
	3.10.3 Driver	3.10.3.1	Installare i driver per la scheda di rete su diversi sistemi operativi.
	3.10.4 Configurazione IP	3.10.4.1	Definire i parametri IP fondamentali: numero IP, maschera IP, default gateway, server DNS.
		3.10.4.2	Configurare i parametri IP fondamentali su diversi sistemi operativi.
	3.10.5 Configurazione di NetBIOS, NETBEUI, SMB, CIFS	3.10.5.1	Installare servizi di condivisione incapsulati in Ethernet e IP sulle piattaforme Windows e Linux/Unix.
		3.10.5.2	Impostare il livello di autenticazione per utente, per condivisione.
3.11 Uso e configurazione dei servizi di rete	*3.11.1 Impostazione del browser internet*	3.11.1.1	Impostare un browser internet, inclusi proxy e plugin.

CATEGORIA	AREA	RIF.	ARGOMENTO
	3.11.2 Impostazione e uso della posta elettronica	3.11.2.1	Configurare account di posta elettronica ed elementi relativi, quali server POP o IMAP, server SMTP.
		3.11.2.2	Configurare le regole per la gestione automatica della posta elettronica.
		3.11.2.3	Impostare le regole di codifica della posta elettronica, quali HTML, testo.
		3.11.2.4	Sapere come accedere alle applicazioni di webmail e come usarle.
	3.11.3 Uso di FTP/SFTP	3.11.3.1	Usare un programma FTP e SFTP per eseguire dei semplici trasferimenti di file.
	3.11.4 Condivisione di oggetti	3.11.4.1	Accedere a oggetti condivisi, quali dischi, directory, modem e stampanti utilizzando sistemi Windows, Apple Macintosh, Linux/Unix; interrompere la stampa su rete.
		3.11.4.2	Attivare/disattivare il montaggio automatico di oggetti condivisi utilizzando sistemi Windows o Apple Macintosh.
		3.11.4.3	Condividere dischi, directory e stampanti utilizzando diversi sistemi operativi.
3.12 Diagnosi e risoluzione dei problemi	*3.12.1 Connessioni fisiche*	3.12.1.1	Usare l'heartbeat e i relativi indicatori led.
		3.12.1.2	Verificare una connessione WLAN di un PC.
	3.12.2 Verifica IP	3.12.2.1	Usare delle verifiche di rete, quali il protocollo ICMP o il comando ping per controllare la rete e il comportamento della rete sotto pressione.
		3.12.2.2	Verificare l'operatività corretta del DHCP ottenendo l'elenco dei valori IP (indirizzo host, gateway, DNS) e controllando il comportamento di richieste e risposte.
	3.12.3 Verifica dei servizi	3.12.3.1	Usare il comando ping per controllare la conversione DNS di un nome.
		3.12.3.2	Usare i programmi nslookup e dig per verificare le operazioni del DNS.

CATEGORIA	AREA	RIF.	ARGOMENTO
		3.12.3.3	Usare il comando route per verificare i pacchetti in uscita.
		3.12.3.4	Usare tcpdump per controllare i pacchetti.
		3.12.3.5	Usare i comandi traceroute/tracert per verificare come i pacchetti raggiungono un determinato server.
	3.12.4 Verifica dei protocolli	3.12.4.1	Usare la query MX di nslookup/dig per ottenere l'elenco dei server di posta di un dominio.
		3.12.4.2	Usare il programma Telnet per simulare manualmente una semplice sessione SMTP, verificare l'esistenza di un account e inviare un messaggio di posta elettronica.
		3.12.4.3	Usare il programma Telnet per simulare una sessione POP3 / IMAP e ottenere un elenco dei messaggi in attesa.
		3.12.4.4	Usare il programma Telnet per simulare una sessione HTTP e scaricare una pagina per verificare l'operatività di un server.
3.13 Aspetti legali	*3.13.1 Cablaggio*	3.13.1.1	Conoscere le norme per il cablaggio strutturato, quali standard di cablaggio industriale e garanzie che un installatore deve fornire ai propri clienti.
	3.13.2 Installazioni wireless	3.13.2.1	Conoscere le norme europee e nazionali relative al wireless.
	3.13.3 Sicurezza sul lavoro	3.13.3.1	Conoscere le principali norme di sicurezza sul lavoro vigenti nella propria nazione.
3.14 Problemi fondamentali di sicurezza	*3.14.1 Sicurezza di rete*	3.14.1.1	Comprendere gli aspetti fondamentali della sicurezza delle informazioni: confidenzialità, integrità e disponibilità.
	3.14.2 Crittografia	3.14.2.1	Conoscere i principi della crittografia a chiave privata e chiave pubblica.
	3.14.3 Sicurezza del browser internet	3.14.3.1	Saper distinguere tra una connessione sicura e una connessione non sicura. Sapere quando è necessario usare una transazione sicura.

CATEGORIA	AREA	RIF.	ARGOMENTO
		3.14.3.2	Attivare, disattivare cookie, ActiveX, Java e JavaScript.

EUCIP
European Certification of
Informatics Professionals

EUCIP IT Administrator - Modulo 4
IT Security

Syllabus Version 3.1

La versione ufficiale in lingua inglese del syllabus EUCIP *IT Administrator – Modulo 4 – IT Security* è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo www.eucip.org. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di marzo 2019.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – IT Security

Questo documento presenta il syllabus di *EUCIP IT Administrator – IT Security*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato che affronti il test per *EUCIP IT Administrator – IT Security*. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Scopi del modulo

EUCIP IT Administrator – IT Security richiede che il candidato abbia un'ampia comprensione dei concetti relativi alla sicurezza informatica e sia in grado di implementare le misure di sicurezza necessarie ad una rete.

Il candidato dovrà essere in grado di:

- Riconoscere i principali rischi e i principi di gestione della sicurezza; dovrà inoltre conoscere gli standard relativi.
- Riconoscere comuni metodi di cifratura ed essere in grado di applicare i relativi protocolli di crittografia.
- Comprendere i principi di autenticazione a chiave e di controllo di accesso.
- Conoscere i concetti di disponibilità legati alla resilienza e sapere come implementare procedure di copie di sicurezza.
- Comprendere i tipi principali di codice maligno e le minacce; dovrà inoltre essere in grado di proteggere un sistema dagli attacchi.
- Conoscere l'infrastruttura a chiave pubblica e saper applicare i relativi principi.
- Comprendere gli aspetti chiave della sicurezza di rete ed essere in grado di usare firewall, controlli di accesso e gestione dei log.
- Conoscere i principali aspetti sociali, etici e legali della sicurezza informatica.

CATEGORIA	AREA	RIF.	ARGOMENTO
4.1 Gestione della sicurezza	*4.1.1 Concetti fondamentali*	4.1.1.1	Descrivere i principali aspetti della sicurezza dell'informazione: confidenzialità, integrità, disponibilità.
		4.1.1.2	Definire i termini autenticazione e non ripudio.
	4.1.2 Gestione del rischio	4.1.2.1	Riconoscere i principali problemi nell'ambito della valutazione del rischio, quali valore dell'informazione, vulnerabilità, minacce, pericoli, violazioni, impatti, livello di rischio.
		4.1.2.2	Descrivere la relazione tra processi/obiettivi aziendali e gestione del rischio IT; sapere qual è il ruolo della sicurezza IT nella riduzione del rischio.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.1.2.3	Descrivere le funzioni più comuni della sicurezza ad alto livello, quali identificazione e autenticazione, controllo di accesso, responsabilità, ispezioni, riuso degli oggetti, accuratezza, affidabilità del servizio, scambio sicuro di dati.
		4.1.2.4	Saper distinguere tra funzionalità e garanzia, riconoscere l'importanza di raggiungerle entrambe per poter controllare i rischi di sicurezza IT.
	4.1.3 Gestione della sicurezza dell'informazione	4.1.3.1	Descrivere il ruolo di una policy di sicurezza nella conduzione della gestione della sicurezza IT.
		4.1.3.2	Conoscere i processi chiave da implementare in una organizzazione per migliorare la sicurezza dell'informazione, quali ISO/IEC 17799, BS 7799.
		4.1.3.3	Comprendere la necessità per un'organizzazione di pianificare soluzioni di disaster recovery e business continuity.
		4.1.3.4	Definire le responsabilità chiave del personale di un'organizzazione, quali responsabili della sicurezza, amministratori di sistema, normali utenti.
		4.1.3.5	Sapere come partecipare ad un Computer Security Incident Response Team (CSIRT).
	4.1.4 Standard ed enti di normazione	4.1.4.1	Riconoscere i principali enti di normalizzazione e comprendere qual è il loro ruolo.
		4.1.4.2	Riconoscere le metodologie che permettono di valutare i diversi livelli di garanzia (ITSEC, ISO/IEC 15408 - Common Criteria).
		4.1.4.3	Conoscere gli elementi chiave delle norme pubblicate relative all'infrastruttura per la gestione della sicurezza in un'organizzazione, quali ISO/IEC 17799, BS 7799 parte 2.
4.2 Crittografia	*4.2.1 Concetti generali*	4.2.1.1	Comprendere i concetti fondamentali della crittografia, quali testo in chiaro, testo cifrato, algoritmi crittografici.

CATEGORIA	AREA	RIF.	ARGOMENTO
	4.2.2 Cifratura simmetrica	4.2.2.1	Comprendere i principi fondamentali della cifratura simmetrica, quali chiave segreta comune, algoritmi.
		4.2.2.2	Saper distinguere tra i principali standard di cifratura simmetrica, quali DES, 3DES, AES, Blowfish, AES.
	4.2.3 Cifratura asimmetrica	4.2.3.1	Definire i principi fondamentali della cifratura asimmetrica.
		4.2.3.2	Conoscere i principali standard relativi alla chiave pubblica, quali Public Key Cryptography Standard (PKCS) #1, PKCS #7.
	4.2.4 Funzioni di hash e digest	4.2.4.1	Definire i principi fondamentali delle funzioni di hash e digest.
		4.2.4.2	Conoscere i principali standard relativi alle funzioni di hash, quali MD5, SHA1.
	4.2.5 Confronto tra metodi di cifratura	4.2.5.1	Conoscere i vantaggi e gli svantaggi della cifratura simmetrica e asimmetrica.
		4.2.5.2	Comprendere la forza dei diversi metodi di cifratura, sia asimmetrica che simmetrica. Essere consapevoli del concetto di “spazio delle chiavi”.
		4.2.5.3	Comprendere il problema della distribuzione delle chiavi nella crittografia simmetrica e asimmetrica.
		4.2.5.4	Descrivere il ruolo del principio di Kerckhoffs e dell’open source nell’applicazione della disponibilità e robustezza della crittografia.
	4.2.6 Uso	4.2.6.1	Descrivere l’uso dei meccanismi di cifratura, quali le firme digitali per risalire all’autenticità.
		4.2.6.2	Saper distinguere tra la sicurezza di un algoritmo e la sicurezza di un protocollo crittografico.
		4.2.6.3	Descrivere l’uso di hash e digest per ottenere integrità e autenticazione.
		4.2.6.4	Sapere come una firma elettronica implementa il non ripudio e l’autenticazione.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.2.6.5	Comprendere i principi e le caratteristiche fondamentali della cifratura necessari a ottenere la confidenzialità.
	4.2.7 Applicazioni	4.2.7.1	Saper descrivere come si usa la crittografia per proteggere i dati nelle transazioni online.
		4.2.7.2	Installare e impostare il software che gestisce il protocollo PGP.
		4.2.7.3	Comprendere i principi fondamentali di SSH.
		4.2.7.4	Installare e impostare il software che gestisce il protocollo SSH.
		4.2.7.5	Comprendere i principi fondamentali di S/MIME.
		4.2.7.6	Comprendere i principi fondamentali di TLS/SSL.
		4.2.7.7	Comprendere come vengono utilizzate le smartcard.
4.3 Autenticazione e controllo di accesso	*4.3.1 Concetti di autenticazione*	4.3.1.1	Descrivere differenti schemi di autenticazione, quali PAP, CHAP, Kerberos.
		4.3.1.2	Comprendere i principi fondamentali della gestione delle password, quali complessità, memorizzazione, modifiche periodiche.
		4.3.1.3	Descrivere il funzionamento principale dell'autenticazione mediante token.
		4.3.1.4	Saper riconoscere diversi schemi di autenticazione biometrica, quali impronte digitali, scansione dell'iride, riconoscimento vocale.
	4.3.2 Autenticazione di rete	4.3.2.1	Identificare i diversi requisiti per l'autenticazione di rete e su host.
		4.3.2.2	Identificare i diversi schemi di autenticazione via Wi-Fi, quali WEP, WPA, WPA2, EAP, PEAP e le relative limitazioni.
		4.3.2.3	Identificare diversi protocolli di rete per l'autenticazione di processi distribuiti, quali Kerberos.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.3.2.4	Descrivere la complessità delle architetture ad autenticazione centralizzata (“single sign-on”).
		4.3.2.5	Descrivere i principi fondamentali di funzionamento di Kerberos, quali lo scambio di ticket.
		4.3.2.6	Descrivere il protocollo WSS (Web services-security), lo standard XML-Encryption ed e-Signature.
	4.3.3 Controllo di accesso	4.3.3.1	Conoscere i principali approcci nel controllo di accesso: MAC, DAC, RBAC.
		4.3.3.2	Descrivere cosa sono una Lista di controllo degli accessi (ACL – Access Control List) e un elenco di capacità.
		4.3.3.3	Descrivere come gestire il controllo di accesso nei comuni file system.
		4.3.3.4	Descrivere come gestire il controllo di accesso in un RDBMS (Relational Database Management System).
4.4 Disponibilità	*4.4.1 Concetti di disponibilità*	4.4.1.1	Riconoscere diversi tipi di requisiti relativi alla disponibilità dell’informazione.
		4.4.1.2	Conoscere diversi tipi di requisiti necessari ad una infrastruttura ICT, quali UPS, aria condizionata, cablaggio.
	4.4.2 Resilienza	4.4.2.1	Conoscere diversi tipi di meccanismi di duplicazione di dischi fissi, quali RAID.
		4.4.2.2	Descrivere diversi tipi di duplicazione di host e meccanismi di distribuzione del carico.
		4.4.2.3	Conoscere diversi tipi di infrastrutture per la disponibilità di reti LAN, WAN, WLAN.
	4.4.3 Copie di sicurezza	4.4.3.1	Implementare procedure efficaci di copie di sicurezza locali e di rete.
		4.4.3.2	Verificare una copia di sicurezza e implementare un recupero.
4.5 Codice maligno	*4.5.1 Programmi*	4.5.1.1	Sapere come viene operato un computer: sistema operativo, programmi, shell, macro.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.5.1.2	Descrivere i requisiti di convalida dell'ingresso dal punto di vista della sicurezza.
		4.5.1.3	Conoscere diversi tipi di overflow e descrivere come possono essere sfruttati per eseguire del codice.
		4.5.1.4	Descrivere i diversi tipi di attacchi nell'interazione browser/webserver, quali cross site scripting.
		4.5.1.5	Descrivere l'attacco di tipo Denial of Service e le modalità con cui può influenzare ambienti e risorse.
		4.5.1.6	Descrivere i diversi metodi di attacco a un computer, quali CD-Rom, dispositivi USB, messaggi di posta elettronica, navigazione web, client di chat.
		4.5.1.7	Conoscere le modalità corrette per accedere a Internet.
		4.5.1.8	Descrivere i rischi di adware e spyware.
	4.5.2 Gestione automatica dei tipi di file	4.5.2.1	Descrivere come una GUI riconosce quale azione eseguire su un allegato di posta elettronica usando il tipo MIME e l'estensione.
		4.5.2.2	Descrivere come i programmi di posta elettronica riconoscono quale azione eseguire su un allegato di un messaggio usando il tipo MIME e l'estensione.
	4.5.3 Codice scaricabile	4.5.3.1	Descrivere come i tipi MIME possono essere usati in modo doloso e come è possibile difendere un PC da simili attacchi.
		4.5.3.2	Descrivere come le macro possono essere usate in modo doloso e come è possibile difendere un PC da simili attacchi.
		4.5.3.3	Descrivere come le applet possono essere usate in modo doloso e come è possibile difendere un PC da simili attacchi.
	4.5.4 Software virale, virus e malware	4.5.4.1	Riconoscere le principali categorie di codici virali, quali trojan, virus, worm.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.5.4.2	Comprendere come funziona un programma antivirus.
		4.5.4.3	Descrivere i diversi strumenti che possono essere usati per la protezione contro il malware: antispyware, firewall personali.
		4.5.4.4	Comprendere scopi e limitazioni dei programmi antivirus.
		4.5.4.5	Installare, impostare e aggiornare un programma anti-malware.
4.6 Infrastruttura a chiave pubblica	*4.6.1 Uso della PKI*	4.6.1.1	Essere consapevoli dei problemi di distribuzione della chiave pubblica, quali l'identificazione del proprietario.
		4.6.1.2	Comprendere lo scopo dei Certificati e delle Liste di revoca (CRL – Certificate Revocation Lists).
		4.6.1.3	Descrivere i certificati X.509.V3.
		4.6.1.4	Comprendere l'infrastruttura a chiave pubblica (PKI) e le sue componenti principali: Registration Authority e Certification Authority.
		4.6.1.5	Usare un browser per generare le chiavi e le richieste di certificazione nei confronti di una Certification Authority.
		4.6.1.6	Importare ed esportare un certificato in un browser.
		4.6.1.7	Accedere a una CRL e importarla in un browser.
		4.6.1.8	Usare il protocollo OCSP (Online Certificate Status Protocol).
		4.6.1.9	Saper riconoscere i diversi avvertimenti forniti dai browser quando devono mettere in guardia l'utente sulla validità di un certificato.
	4.6.2 Servizi di elenco (Directory)	4.6.2.1	Saper riconoscere il protocollo LDAP (Lightweight Directory Access Protocol).
		4.6.2.2	Usare un browser per interrogare un server LDAP per ottenere i dati relativi a un particolare Distinguished Name.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.6.2.3	Definire i termini “Common Name”, “Distinguished Name” e “Attributo”.
		4.6.2.4	Descrivere lo stardard X.509 in termini di Certification Authority, struttura del certificato ed estensioni del certificato.
		4.6.2.5	Descrivere come è possibile usare i server LDAP per supportare la gestione del profilo utente e l’autenticazione.
4.7 Sicurezza di rete	*4.7.1 Concetti di telecomunicazione*	4.7.1.1	Comprendere le modalità operative di Ethernet dal punto di vista dell’indirizzo MAC, CSMA/CD.
		4.7.1.2	Comprendere gli aspetti principali del TCP/IP: indirizzi, numeri di porta, flusso principale delle operazioni.
		4.7.1.3	Descrivere l’incapsulamento di TCP/IP in Ethernet.
		4.7.1.4	Descrivere i servizi di rete nell’ambiente TCP/IP.
		4.7.1.5	Installare e gestire un analizzatore di rete.
		4.7.1.6	Descrivere delle principali tipologie di attacco allo stack TCP/IP, quali “sniffing di pacchetti”, “IP spoofing”, “rerouting”, “connection hijacking”, “(distributed) denial of service”.
		4.7.1.7	Descrivere come si possono usare switch e VLAN per organizzare la sicurezza di una LAN.
	4.7.2 Reti wireless	4.7.2.1	Conoscere le principali tecnologie wireless, quali WiFi, Bluetooth, Home Wireless.
		4.7.2.2	Comprendere i problemi di sicurezza relativi alle reti wireless e quali possono essere le possibili soluzioni.
	4.7.3 Servizi	4.7.3.1	Comprendere il concetto di servizi quali punti di accesso ai server.
		4.7.3.2	Essere a conoscenza degli impieghi illeciti dei servizi, quali utilizzi abusivi, denial of service, contraffazione dei dati.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.3.3	Essere consapevoli dei rischi legati all'utilizzo fraudolento di DNS.
		4.7.3.4	Essere consapevoli dei principali schemi di autenticazione e delle rispettive vulnerabilità.
		4.7.3.5	Essere consapevoli che debolezze dei protocolli o vulnerabilità nel software possono essere sfruttate per attaccare un server in rete.
		4.7.3.6	Essere consapevoli che i client possono essere vulnerabili quanto i server.
		4.7.3.7	Essere consapevoli dei rischi associati alle tecnologie e ai programmi di tipo peer-to-peer.
	4.7.4 Controllo di accesso	4.7.4.1	Essere consapevoli di come opera l'autenticazione di rete e come viene gestita.
		4.7.4.2	Essere consapevoli di come opera l'autenticazione di rete basata su chiave crittografica e come viene gestita.
		4.7.4.3	Essere consapevoli di come opera l'autenticazione basata su dominio in sistemi di tipo Windows.
	4.7.5 Gestione dei log	4.7.5.1	Riconoscere le informazioni rilevanti per la sicurezza che possono essere ricavate dai log di sistema.
		4.7.5.2	Impostare la registrazione dei log delle applicazioni.
		4.7.5.3	Impostare un servizio centralizzato di registrazione dei log.
		4.7.5.4	Essere consapevoli di come proteggere i log dalle manomissioni.
	4.7.6 Controllo di accesso ai servizi HTTP	4.7.6.1	Comprendere la differenza fra siti web HTTP e HTTPS.
		4.7.6.2	Comprendere come l'interazione tra il servizio web e gli altri componenti del sistema possa influenzare la sicurezza.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.6.3	Implementare una versione sicura di un sito web non sicuro, generando chiavi e richieste di certificati; importare chiavi e certificati.
		4.7.6.4	Configurare un sito web in modo che l'identificazione e l'autorizzazione del client avvenga utilizzando password in testo normale.
		4.7.6.5	Configurare un sito web in modo che l'identificazione e l'autorizzazione del client avvenga utilizzando dei certificati, quali SSL V.3.
		4.7.6.6	Riconoscere quali tipi di accessi agli oggetti di una directory possono essere limitati nei siti web.
		4.7.6.7	Applicare le corrette limitazioni di accesso a una specifica directory di un sito web.
	4.7.7 Controllo di accesso ai servizi di posta elettronica	4.7.7.1	Comprendere che è possibile contraffare il mittente ed altre informazioni relative ad un messaggio di posta elettronica.
		4.7.7.2	Impostare un semplice accesso con autenticazione via password sui servizi POP e IMAP.
		4.7.7.3	Impostare un accesso con autenticazione via certificato crittografico sui servizi POP e IMAP.
		4.7.7.4	Impostare l'autenticazione basata su SASL (Simple Authentication and Security Layer) per il servizio SMTP.
		4.7.7.5	Impostare un accesso via tunnel cifrato ai servizi POP e IMAP.
		4.7.7.6	Definire il termine "spam". Illustrare le possibili contromisure.
	4.7.8 Firewall	4.7.8.1	Definire il termine "firewall". Conoscere i limiti e il potenziale di un firewall e saper riconoscere le diverse architetture di firewall, quali gateway, circuiti.
		4.7.8.2	Definire il termine DMZ (De-Militarized Zone).

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.8.3	Descrivere cosa è un proxy e quali sono le sue modalità operative.
		4.7.8.4	Comprendere come usare un proxy per ridurre il numero di indirizzi IP utilizzati e proteggere una rete interna.
		4.7.8.5	Descrivere cosa è un NAT (Network/Port Address Translation) e in quale modo contribuisce alla sicurezza.
		4.7.8.6	Comprendere i principi di funzionamento dei firewall IP per limitare l'accesso ai servizi IP.
		4.7.8.7	Comprendere i principi di funzionamento dei firewall proxy per limitare e rendere sicura la gestione dei protocolli.
		4.7.8.8	Installare un firewall e un server proxy; implementare una policy di sicurezza.
		4.7.8.9	Nascondere gli indirizzi IP utilizzando un firewall.
		4.7.8.10	Impostare NAT su un firewall.
		4.7.8.11	Impostare le regole di controllo degli accessi su un firewall.
	4.7.9 Intrusion detection	4.7.9.1	Conoscere le categorie fondamentali dei sistemi di rilevamento dei tentativi di intrusione (IDS – Intrusion detection systems) quali IDS di rete, IDS basati su host.
		4.7.9.2	Controllare i log e gli eventi relativi alla sicurezza.
		4.7.9.3	Conoscere i sistemi IPS (Intrusion Prevention Systems) quali IPS di rete, IPS wireless, IPS basati su host.
		4.7.9.4	Installare ed eseguire una configurazione di base di un IDS (Intrusion Detection System).
	4.7.10 Reti private virtuali (VPN)	4.7.10.1	Descrivere i principi dei protocolli IPSEC/IKE.
		4.7.10.2	Descrivere le proprietà di sicurezza della separazione del traffico in base a circuito (MPLS).

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.10.3	Descrivere quali livelli di sicurezza possono essere forniti da diverse tecnologie, quali SSL, IPSEC.
		4.7.10.4	Installare un client VPN.
4.8 Aspetti sociali, etici, legali della sicurezza informatica	*4.8.1 Concetti fondamentali*	4.8.1.1	Comprendere i termini “riservatezza” (privacy), “anonimato”, “uso di pseudonimi”.
	4.8.2 Tecnologie di rinforzo alla privacy	4.8.2.1	Riconoscere l’esistenza di un bilanciamento tra autenticazione e privacy.
		4.8.2.2	Comprendere le problematiche etiche legate a tracciamento e sorveglianza sui luoghi di lavoro.
		4.8.2.3	Descrivere gli aspetti principali dei codici deontologici ed etici.
		4.8.2.4	Descrivere gli aspetti principali dell’etica hacker.
		4.8.2.5	Riconoscere le principali forme di crimini informatici, quali cracking, furto d’identità, furto di dati, accessi fraudolenti.
		4.8.2.6	Comprendere i problemi etici e di privacy legati alla biometria.
	4.8.3 Legislazione europea	4.8.3.1	Essere a conoscenza degli aspetti legali della firma digitale e del framework Comunitario relativo alla firma elettronica.
		4.8.3.2	Essere a conoscenza della legge a tutela dei dati personali (GDPR) e comprenderne le implicazioni relative al trattamento dei dati personali.
		4.8.3.3	Essere a conoscenza delle principali considerazioni relative all’informatica forense e alla raccolta di prove.