Corso di formazione in real-time e in FAD

Amministratore di sistema

Descrizione del corso

Gli obiettivi del corso sono:

- riconoscere i principali elementi dell'hardware di un personal computer
- comprendere i fondamenti dei sistemi operativi (OS) e configurare e mantenere un sistema operativo
- comprendere il modello di riferimento OSI, come connettersi ad una rete e come funzionano i tipici servizi di rete, quali posta elettronica e software collaborativo (groupware)
- comprendere i concetti chiave della sicurezza informatica, essere consapevole del software malevolo e dei tipici concetti della sicurezza di rete, così come degli aspetti sociali, etici e legali della sicurezza informatica

Programma

- Amministratore di sistema: ruolo, responsabilità e rischi alla luce del GDPR
- Hardware del PC
 - Riconoscere i componenti hardware
 - Scheda madre (LPX, ATX, NLX)
 - Bios (POST, CMOS)
 - Microprocessore (CPU)
 - Bus e risorse di sistema (PCI, PCI-X, PCIe, USB)
 - Interfacce (IDE, SCSI, SATA)
 - Memorie di massa
 - Dispositivi di visualizzazione (VGA, SVGA, XVGa, HD, FullHD, 720p, 1080p, 4k)
 - Stampanti
- Sistemi Operativi
 - Caratteristiche Client e server
 - Configurazione del sistema
 - Gestione del disco (file system e BackUp)
 - Manutenzione del disco
 - Condivisione delle risorse e gestione delle autorizzazioni
 - Strumenti di amministrazione
 - Diagnosi e risoluzione dei problemi
 - Basi di dati (DBMS e ACID).
- Reti
 - Modello di riferimento OSI
 - Livelli fisico, dati e rete (segnali analogici e digitali).
 - Livelli trasporto, sessione e presentazione (TCP)
 - Livello applicazione (TELNET)
 - WWW (URL, DNS)
 - Posta elettronica (SMTP, POP3, IMAP)
 - Applicazioni e condivisione (Social Media, Forum, SMB, CIFS)
 - Connessione a una rete (10baseT, 100baseT, 100baseF...)
 - Configurazione e utilizzo servizi di rete (FTP, SFTP, ICMP)
- Sicurezza informatica
 - Principi di base (disaster recovery - hash - digest)
 - Autenticazione, disponibilità e controllo di accesso (MAC, DAC, RBAC)
 - Codice maligno (adware, spyware...)
 - Infrastruttura a chiave pubblica (PKI)

Corso di formazione in real-time e in FAD

- Sicurezza di rete (“sniffing di pacchetti”, “IP spoofing”, “rerouting”, “TCP”, “hijacking”, “(distributed) denial of service”)
- Firewall (DMZ, Proxy)
- Aspetti sociali, etici, legali

Destinatari

- amministratore di sistema
- amministratore di rete
- amministratore di database e banche dati
- amministratore di apparati di sicurezza informatica
- amministratore di software applicativo

Durata

Il corso che proponiamo ha una durata di 20 ore.

Materiale didattico

Slides.

Modalità di erogazione

I corsi possono essere seguiti in aula o in FAD su piattaforma dedicata.

Contatti

Responsabile della formazione

Mail: info@hedya.it | hedya@legalmail.it | formazione@hedya.it

Cell: + 39 3206307243