PROGRAMMA

Data Protection Officer | Modulo B

Area Data Security

Obiettivo

Il modulo B consente l'acquisizione delle necessarie conoscenze di carattere tecnico-informatico con particolare riferimento alla sicurezza informatica.

Inoltre il corso (Modulo B del per percorso completo per DPO Corso Cod. GDPO) risponde al requisito formativo per accedere all'esame di certificazione così come previsto dalla UNI 11697:2018 "*Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali- requisiti di conoscenza, abilità ed esperienza*".

Programma

Durante il corso verranno trattati i seguenti argomenti:

- I principi della sicurezza informatica: Riservatezza; Integrità; Disponibilità; Resilienza; Non ripudio; Tecniche di anonimizzazione; Tecniche crittografiche; Tecniche di pseudonimizzazione; Sistemi e tecniche di monitoraggio (KPI)
- Accountability e Governance IT: Policy; Regolamenti; Gestione del log, Gestione delle infrastrutture hardware; software e di telecomunicazione e rete; Gestione degli applicativi; Best practices.
- Cloud e privacy: Tipologie di Cloud e servizi; Problematiche Cloud; Cloud e privacy; Cloud e sicurezza; Contratti Cloud
- BYOD: Bring your own device: Vantaggi e svantaggi; Rischi; ; Misure di sicurezza; Policy interne.
- Data breach: strumenti per l'identificazione della violazione: IDS; Firewall; Threat Intelligence; Threat Analysis
- Incident Response e Digital Forensics: cosa fare in caso di incidente:
  - Introduzione alla Forensics: cosa è, Strumenti e Norme
- Incident response: Preservare; Acquisire; Analizzare
- Case study: Ramsonware in banca; Insider e furto dati; Sito PA bucato
- La valutazione di impatto in materia di protezione dei dati (aspetti tecnici)
- Valutazione preliminare
- Esecuzione DPIA
- Metodologia di valutazione di impatti e rischi
- Finalizzazione e decisione finale
- Consultazione preventiva
- Case study
- Test di fine modulo

Destinatari

Liberi professionisti e funzioni aziendali che rivestono, devono rivestire o valutano di rivestire il ruolo del DPO nell'ambito di aziende private e pubbliche.

Prerequisiti

E' preferibile possedere una delle seguenti opzioni:

- conoscenza generale del GDPR (es. corso cod. GEUP)
- basi per i sistemi di sicurezza informatica (es. corso cod. IBS27)
- la norma UNI 11697:2017 nei punti: D1 Sviluppo della Strategia per la Sicurezza Informatica, E8 Gestione della sicurezza dell'informazione e E9 Governance dei sistemi informativi

Materiale didattico

- Dispensa, contenente le slides e i materiali utilizzati durante il corso
- Norme ad uso didattico (da riconsegnare al termine del corso): Norma UNI 11697:2018

Durata del corso

24 ore + verifica dell'apprendimento

Docente

Il corso viene svolto da docenti qualificati TÜV Italia.

Attestati

Al termine verrà rilasciato:

- Attestato di Competenza (a fronte del superamento del test finale)
- Attestato di Frequenza (in caso di non superamento del test finale)