CertComp

Syllabus

DPO - PRIVACY

Introduzione alla Certificazione "DPO-Privacy"

Il Corso di Formazione e Certificazione **DPO-PRIVACY** affronta le normative, i compiti e le responsabilità in riferimento **GDPR** (General Data Protection Regulation) ovvero il **Modello Organizzativo di Gestione e Controllo Privacy Dati Personali** conforme al REGOLAMENTO (UE) 2016/679.
La normativa riguarda la protezione delle persone fisiche rispetto al trattamento dei dati personali, nonché la circolazione dei dati stessi.

Il Corso di Formazione e Certificazione **DPO-PRIVACY** ha una durata complessiva di **400 ore**.
Le ore di Corso di Formazione previste per il modulo didattico sono indicative, in quanto variano in funzione delle competenze, abilità e capacità che il Candidato possiede e delle specifiche aree di Skill previste dal relativo modulo didattico. Il totale tiene conto delle ore complessive di formazione date dalla lettura delle dispense, dall'esecuzione delle esercitazioni, dall'approfondimento sui link di riferimento, dall'integrazione delle eventuali richieste di chiarimenti/spiegazioni al Tutor/Docente e dal numero medio di ore necessarie a superare il TEST di Verifica Finale dell'apprendimento.

Al termine del Corso di formazione viene rilasciato al Candidato l'**Attestato di Frequenza al Corso di Formazione DPO-PRIVACY.**

Syllabus

- ### Definizione dei domini del Syllabus

In ambito informatico il "dominio" di un esame si riferisce all'insieme di competenze che identificano in modo univoco le conoscenze e competenze rispetto ad una particolare tecnologia, prodotto, logica di processo, attività intellettuale o pratica. Il dominio dell'esame TESI su **DPO-Privacy** è composto da vari elementi, differenti tra loro, che identificano parti specifiche per stabilire le conoscenze in modo globale. Per la costruzione della prova d'esame **"DPO-Privacy",** sono stati nel dettaglio identificati i seguenti **domini e sottodomini** per la composizione dell'Esame:

DPO-Privacy		
Domain	**Sub-Domain**	
1	**1.0 Origini e significato della protezione dei dati**	*1.0.1 Riservatezza e Privacy*
		1.0.2 Protezione dei dati
	2.0 Principi fondamentali riguardo i dati personali	*2.0.1 Principio di limitazione della raccolta dei dati*
		2.0.2 Principio della qualità dei dati
		2.0.3 Principio della specificità dello scopo
		2.0.4 Principio della limitazione d'uso
		2.0.5 Principio di salvaguardia della sicurezza
		2.0.6 Principio di apertura
		2.0.7 Principio di partecipazione individuale
		2.0.8 Principio di responsabilizzazione

	3.0 Il regolamento generale sulla protezione dei dati dell'UE	*3.0.1 La proposta di regolamento UE sulla e-privacy*
	4.0 Qualifiche, competenze e posizione del DPO/RPD	*4.0.1 Funzioni del DPO/RPD*
		4.0.2 Le mansioni del Responsabile della protezione dei dati
		4.0.3 I compiti del DPO/RPD
		4.0.4 Azioni preliminari
		4.0.5 Mappatura generale delle attività di trattamento
		4.0.6 La creazione di un registro delle attività
		4.0.7 Contenuti e struttura delle voci di registro del Titolare
		4.0.8 Contenuti e struttura delle voci di registro del Responsabile
		4.0.9 Contenuti e struttura del registro del DPO/RPD
		4.0.10 Riesame delle attività di trattamento dei dati personali
		4.0.11 Valutazione dei rischi posti dalle attività di trattamento di dati personali
2	**1.0 Gestione dei trattamenti a rischio elevato**	*1.0.1 I diversi ruoli e responsabilità del Titolare e del DPO/RPD*
		1.0.2 Trattamenti a rischio elevato
	2.0 Metodologie per la conduzione di una DPIA	*2.0.1 Criteri per una valutazione di impatto*
	3.0 Come gestire la documentazione della DPIA	*3.0.1 Ripetizione dei compiti su base continuativa*
	4.0 Gestione delle violazioni dei dati personali	*4.0.1 Le violazioni dei dati*
3	**1.0 Notifica alla competente autorità di protezione dei dati o DPA**	*1.0.1 Termini per la notifica*
		1.0.2 Documentazione e valutazione della violazione
		1.0.3 Comunicazioni all'interessato
		1.0.4 Informazioni da fornire
	2.0 Valutazioni dell'esistenza di un rischio	*2.0.1 Fattori da considerare nella valutazione del rischio*
		2.0.2 Facilità di identificazione delle persone fisiche
		2.0.3 Gravità delle conseguenze per le persone fisiche
		2.0.4 Caratteristiche particolari dell'interessato
		2.0.5 Caratteristiche particolari del titolare del trattamento
		2.0.6 Numero di persone fisiche interessate
	3.0 Compiti di indagine	*3.0.1 Monitoraggio della conformità*
		3.0.2 Poteri esecutivi
		3.0.3 Funzioni di consulenza

		3.0.4 Data protection by design e by default
		3.0.5 Consulenza e monitoraggio della conformità delle politiche di protezione
		3.0.6 Coinvolgimento nelle certificazioni e nei codici di condotta
	4.0 Cooperazione con l'Autorità di protezione dati	*4.0.1 Relazione DPO/RPD - DPA*
		4.0.2 Garantire il rispetto del regolamento
		4.0.3 Verifiche preliminari
		4.0.4 Esecuzione
		4.0.5 Misura dell'efficacia delle disposizioni adottate
		4.0.6 Gestione di reclami e richieste dell'interessato
		4.0.7 Compiti di informazione di sensibilizzazione interna ed esterna
		4.0.8 Pianificazione e riesame delle attività del DPO/RPD
4	**1.0 Che cos'è la sicurezza informatica**	*1.0.1 La scala delle minacce alla sicurezza informatica*
		1.0.2 Le sfide della sicurezza informatica
		1.0.3 Sicurezza dell'applicazione
		1.0.4 Sicurezza sul cloud
		1.0.5 Gestione dell'identità e sicurezza dei dati
		1.0.6 Sicurezza mobile
		1.0.7 Sicurezza della rete
		1.0.8 Disaster recovery e pianificazione della continuità operativa
		1.0.9 Formazione degli utenti
		1.0.10 Criminalità informatica
		1.0.11 I vantaggi della sicurezza informatica
		1.0.12 Triade della CIA
		1.0.13 Chi è un esperto di sicurezza informatica?
		1.0.14 Cosa fa un esperto di sicurezza informatica
	2.0 Gli attacchi informatici	*2.0.1 Principali tipi di attacchi*
		2.0.2 Ruoli IT all'interno dell'azienda
		2.0.3 Cos'è l'hacking etico
		2.0.4 Quali sono i diversi tipi di hacker
		2.0.5 White Hat Hacker vs Black Hat Hacker
		2.0.6 Quali sono i ruoli e le responsabilità di un hacker tecnico
		2.0.7 Principali vantaggi dell'hacking etico
		2.0.8 Cos'è il test di penetrazione
		2.0.9 Cos'è Kali Linux
		2.0.10 Aree di penetration test

		2.0.11 Cos'è SQL injection?
		2.0.12 Come funziona SQL in un sito web
	3.0 I firewall	*3.0.1 Perché i firewall sono importanti*
		3.0.2 Usi chiave dei firewall
		3.0.3 Funzioni del firewall
		3.0.4 Come funziona un firewall
		3.0.5 Tipi di firewall
		3.0.6 Livello applicazione e firewall proxy
		3.0.7 L'importanza di NAT e VPN
		3.0.8 VPN (Rete Privata Virtuale)
		3.0.9 Attacchi interni
	4.0 Vulnerabilità	*4.0.1 Cos'è un attacco ransomware*
		4.0.2 Come si svolge un attacco ransomware
		4.0.3 Tipi di ransomware
		4.0.4 Come prevenire gli attacchi ransomware
		4.0.5 Attacchi ransomware popolari nella storia
	5.0 Conoscere la rete	*5.0.1 Cosa sono le reti informatiche*
		5.0.2 Cos'è un indirizzo IP
		5.0.3 Perché utilizzare un indirizzo IP
		5.0.4 Funzionamento di un indirizzo IP
		5.0.5 Versioni dell'indirizzo IP
		5.0.6 Tipi di indirizzi IP
	6.0 Prevenzione degli attacchi informatici	*6.0.1 Tipi di attacchi informatici*
		6.0.2 Come prevenire gli attacchi informatici