PROGRAMMA ANALITICO D'ESAME

DPO/RPD

idcert Proficiency Level Specialised Framework DigComp *e-CF

EQF 4

Sommario

PRESUPPOSTI NORMATIVI

IDCERT per la produzione dei suoi corsi si ispira alle più recenti disposizioni europee nell'ambito della formazione con l'intento di fornire un'alta qualità formativa ed una corrispondente omogeneità di metodo tali da permettere a tutti coloro che seguono i suoi corsi e conseguono le sue certificazioni o attestazioni di poter spendere le competenze ed i titoli acquisiti con la certezza di spendibilità a livello europeo.

I sistemi di classificazione dei corsi

IDCERT in rispondenza ai più moderni e riconosciuti sistemi di valutazione delle competenze classifica i suoi corsi secondo i parametri espressi dal DigComp, dal quadro tecnico del sistema europeo di crediti per l'istruzione e la formazione professionale (ECVET). Riconosce, inoltre, come i valori della conoscenza e delle competenze possano avere un impatto positivo verso il raggiungimento degli obiettivi previsti dalla "Agenda 2030 per lo Sviluppo Sostenibile".

Il DigComp Framework

Il *DigComp*, nelle sue evoluzioni, rappresenta lo strumento attraverso il quale l'Europa intende fornire le linee guida per la formazione digitale per il cittadino, il lavoro e l'impresa.
Il *DigComp Framework* è stato sviluppato attraverso un ampio processo di analisi e confronto di quadri e modelli esistenti di competenze ICT, alfabetizzazione digitale, informazione e alfabetizzazione mediatica, per citarne solo alcuni.
Il *DigComp Framework* viene utilizzato per valutare, riconoscere e certificare i risultati di apprendimento delle competenze digitali.
Questo riconoscimento è importante sia per coloro che desiderano dimostrare già di avere competenze digitali sia per coloro che sono interessati a formarsi.

Per sintetizzare gli aspetti più salienti, il *DigComp* articola la sua strutturazione in 5 dimensioni:

Dimensione 1: Aree di competenze individuate come facenti parte delle competenze digitali.
Dimensione 2: Descrittori delle competenze e titoli pertinenti a ciascuna area.
Dimensione 3: Livelli di padronanza per ciascuna competenza.

Dimensione 4: Conoscenze, abilità e attitudini applicabili a ciascuna competenza.
Dimensione 5: Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Per maggiori approfondimenti sul *DigComp* riferirsi qui.

Secondo questo schema IDCERT costruisce i syllabus, l'articolazione ed il sistema di valutazione dei suoi corsi.

I livelli di padronanza

Ciascun livello rappresenta un gradino in più nell'acquisizione da parte dei cittadini delle competenze in base alla sfida cognitiva, alla complessità delle attività che possono gestire e alla loro autonomia nello svolgimento dell'attività.

Sulla base di questo metodo IDCERT classifica i suoi corsi secondo il seguente *Proficiency level*:

Livelli di apprendimento EQF

L'EQF è un quadro basato sui risultati dell'apprendimento articolato su 8 livelli per tutti i tipi di qualificazioni, che funge da strumento di "traduzione" tra i diversi quadri nazionali delle qualificazioni.
I valori espressi da 1 ad 8 sono la combinazione coerente dei risultati di apprendimento, che possono essere valutati e validati autonomamente. I risultati dell'apprendimento sono suddivisi in *conoscenze*, *abilità* e *competenze* che corrispondono ad azioni attraverso le quali l'individuo dimostra di padroneggiare le competenze acquisite, in base a determinati criteri di performance e condizioni contestuali.
IDCERT classifica i suoi corsi indicandone il valore EQF.

Rispondenza agli obiettivi dell'Agenda 2030

"Agenda 2030 per lo Sviluppo Sostenibile" è un programma d'azione per le persone, il pianeta e la prosperità sottoscritto nel settembre 2015 dai governi dei 193 Paesi membri dell'ONU. Essa ingloba 17 Obiettivi per lo Sviluppo Sostenibile – *Sustainable Development Goals, SDGs* – in un grande programma d'azione per un totale di 169 *target* o traguardi. I Paesi si sono impegnati a raggiungere gli obiettivi previsti entro il 2030.
IDCERT sposa pienamente la strategia europea per lo sviluppo sostenibile dando il suo contributo nell'ambito della formazione ed in particolare per quella digitale.
I percorsi formativi di IDCERT propongono l'acquisizione di conoscenze e competenze che possono contribuire ai processi di empowerment delle persone e quindi al potenziamento delle loro capacità di resilienza che, nei nuovi scenari disegnati dall'*Agenda 2030 per lo sviluppo sostenibile*, trovano una loro piena collocazione. La partecipazione e l'appoggio di IDCERT a progetti ed iniziative valoriali in ambito sociale, ambientale ed economico aggiungono e rafforzano la sua aderenza a quegli obiettivi previsti dall'*Agenda* con un particolare focus su alcuni di essi.

I CORSI IDCERT

La certificazione IDCERT, così come le sue attestazioni, diventano titoli da aggiungere sul proprio CV, su LinkedIn, su Facebook ecc. a dimostrazione di essere in possesso di determinate competenze richieste dal mercato del lavoro.

Corsi per le competenze digitali

I corsi che rilasciano la **certificazione IDCERT** sono in linea con il *DigComp Framework*.
Il Framework DigComp viene utilizzato in tre domini principali in cui la competenza digitale è sempre più importante:

- **Formazione scolastica e formazione in generale**.
  Il quadro normativo trova applicazione nell'istruzione a tutti i livelli, a partire dalla scuola, dove contribuisce ai risultati scolastici e al benessere dei bambini e i giovani.
- **Apprendimento permanente e inclusione**.
  La competenza digitale è importante nella vita di tutti i giorni e la mancanza di tale competenza può esacerbare la condizione di chi è già in posizione di svantaggio o addirittura può contribuire all'esclusione sociale.
- **Occupazione e lavoro**.
  La competenza digitale oggi è necessaria per un'ampia varietà di profili professionali e nel mondo del lavoro.

Corsi per altri tipi di competenze

Come già chiarito poc'anzi, IDCERT abbraccia in pieno la nuova filosofia europea sulla formazione che mira a fornire competenze classificabili e valutabili secondo criteri certi e condivisi. Alla luce di questo, IDCERT classifica tutti i suoi corsi non strettamente legati alle conoscenze digitali mutuando la medesima strutturazione prevista dal *DigComp*, rispettandone comunque i principi generali ove non fosse possibile una perfetta corrispondenza al framework a seguito della diversità delle materie trattate.

Obiettivi del corso

Il corso **DPO/RPD** fornisce ai partecipanti gli strumenti pratici, attraverso modelli interattivi ed esercitazioni, per divenire gestore per la protezione dei Dati Personali dell'Organizzazione.
Il percorso formativo ha una durata di 400 ore e si snoda nei vari aspetti normativi e legali legati alla protezione dei dati personali e la conoscenza di alcuni argomenti in ambito di sicurezza informatica. Il sempre maggiore impiego di sistemi di comunicazione e archiviazione digitale oggi impongono a questa figura professionale la comprensione di limiti e rischi legati alla digitalizzazione.
Il Data Protection Officer (DPO) è una figura di supporto al titolare o responsabile del trattamento dei dati personali nell'applicazione e per l'osservanza del Regolamento (UE) 2016/679, in conformità all' art. 37 (Designazione del Responsabile della protezione dei dati), art. 38 (Posizione del Responsabile della protezione dei dati) e art. 39 (Compiti del Responsabile della protezione dei dati).
Al Data Protection Officer (Responsabile della protezione dei dati personali), così come indicato nella Norma UNI 11697:2017 e nel Regolamento UE 2016/679, in particolare all'art. 39, è consentita l'assegnazione di compiti diversi e/o ulteriori inclusi in altri profili di livello manageriale nel rispetto del principio di assenza di conflitto di interessi.
Inoltre, il corso impartisce nozioni tese ad acquisire conoscenze legali sulla contrattualistica, competenze sulla sicurezza informatica (tecniche di attacco, crittografia, ecc.) e sui sistemi informatici e relativi database.

Su questi presupposti IDCERT può essere impiegata come standard nella definizione di programmi di certificazione .

Il percorso di certificazione è suddiviso in 2 moduli; per ciascuno di essi sono previsti:

- manuali PDF
- video lezioni
- esercitazioni
- esame finale.

Il percorso formativo può svolgersi interamente online sul sito *idcert.io* oppure offline presso le sedi dei *Competence Center* affiliati IDCERT.
La piattaforma web di proprietà è accessibile anche a persone con disabilità visiva e/o uditiva.

Ottenimento della certificazione

La certificazione si conclude con il superamento degli esami previsti alla fine di ogni modulo. L'esame si considera superato con il 75% di risposte corrette.

La certificazione IDCERT è l'unica certificazione italiana costruita interamente sul *DigComp Framework* e, quindi, l'unica in grado di attestare in maniera oggettiva le competenze digitali necessarie per operare correttamente come cittadini digitali con i dispositivi (computer, smartphone e tablet), sia per lavoro che per uso personale, così come richiesto dal *DigComp*.

Destinatari

Il corso è indirizzato a tutte le figure professionali coinvolte in attività in ambito Privacy: a coloro che vogliono qualificare le proprie competenze specifiche sulla protezione dei Dati Personali, mediante un valido attestato riconosciuto sia per il settore pubblico che privato; a coloro che vogliono maturare le competenze nell'ambito della protezione dei Dati Personali:

- Imprenditori
- Quadri aziendali
- Professionisti e consulenti d'impresa
- Studenti universitari e in materie giuridiche ed economiche
- Amministratori e dipendenti di Pubbliche Amministrazioni

IL PROGRAMMA ANALITICO

Esso è strutturato seguendo le impostazioni del *DigComp Framework*, rappresentando, per ogni **competenza** (colonna sinistra), i relativi **descrittori** (colonna centrale) e le **conoscenze, abilità e attitudini** applicabili ad ogni singola competenza (colonna destra).
In questo modo sono immediatamente identificabili le competenze previste, per ogni area di competenza, e le specifiche di raggiungimento di conoscenze, abilità e attitudini.

MODULO 1
Il ruolo del DPO/RPD

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. IL DATA PROTECTION OFFICER – RESPONSABILE PROTEZIONE DATI	1.1 Evoluzione della figura del Data Protection Officer (DPO)	1.1.1 Introduzione della figura
	1.2 Diritto del Consiglio d'Europa	1.2.1 La nomina del DPO all'interno della Convenzione n. 108 del 1981
	1.3 La Direttiva 95/46/CE	1.3.1 Il Considerando 49
	1.4 Regolamento CE 45/2001	1.4.1 Art. 24 del Regolamento CE 45/2001
	1.5 Il GDPR e il D.lgs 101/2018	1.5.1 Il D.Lgs 101/2018
2. NOMINA DEL DPO / RPD	2.1 L'obbligo di nomina di un DPO/RPD per le autorità pubbliche	2.1.1 Competenze specialistiche del DPO/RPD
	2.2 Compiti del DPO/RPD	2.2.1 Parere del DPO/RPD sulla valutazione d'impatto
	2.3 Linee guida dei Garanti Europei	2.3.1 Il principio di responsabilizzazione
	2.4 Concetto di Autorità Pubblica	2.4.1 Le raccomandazioni del WP29

3. LE ATTIVITA' DEL DPO/RPD	3.1 Attività principali	3.1.1 Considerando 97 del GDPR
	3.2 Il concetto di "Larga scala"	3.2.1 Modelli di trattamento su larga scala
	3.3 Monitoraggio regolare e sistematico	3.3.1 Modelli di monitoraggio regolare e sistematico
4. DESIGNAZIONE, COMPETENZE, MODALITA' CONTRATTUALI	4.1 Chi deve nominare il DPO/RPD	4.1.1 Criteri di nomina
	4.2 Competenze e capacità del DPO	4.2.1 Competenze richieste all'interno di organismi pubblici
	4.3 Contratto di servizi	4.3.1 Art. 37 paragrafo 7 del GDPR
5. POSIZIONE, AUTONOMIA E INDIPENDENZA DEL DPO/RPD	5.1 Necessità del coinvolgimento del DPO/RPD	5.1.1 Garanzie di coinvolgimento del DPO/RPD
	5.2 Necessità di risorse	5.2.1 Art. 38 paragrafo 2 del Regolamento UE 2016/679
	5.3 Autonomia e indipendenza del DPO/RPD	5.3.1 Le penalizzazioni 5.3.2 Clausole sull'indipendenza
6. CONFLITTI DI INTERESSE, RISCHI E RUOLI DEL DPO/RPD	6.1 Conflitto di interessi	6.1.1 Le buone prassi 6.1.2 Il Gruppo istituzionale UE sul conflitto d'interessi
	6.2 L'approccio basato sul rischio	6.2.1 Gli ordini di priorità
	6.3 Il ruolo del DPO/RPD nella tenuta del Registro delle attività di trattamento	6.3.1 La prassi consolidata in tema di tenuta registri

MODULO 2

Il regolamento privacy UE 2016/679 (GDPR)

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. DISPOSIZIONI GENERALI, PRINCIPI E DIRITTI DELL'INTERESSATO (artt. 1-23)	1.1 Capo I – Disposizioni generali	1.1.1 Ambito di applicazione materiale 1.1.2 Ambito di applicazione territoriale 1.1.3 Definizioni
	1.2 CAPO II – Principi	1.2.1 I principi applicati 1.2.2 La disciplina del consenso
	1.3 CAPO III – Diritti dell'interessato	1.3.1 L'informativa sui dati personali (Sezione 1-2) 1.3.2 Le modalità dell'informativa 1.3.2 "Rettifica e cancellazione" (Sezione 3) 1.3.3 Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche (Sezione 4)
2. TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO (artt. 24-43)	2.1 Obblighi generali	2.1.1 Privacy by design 2.1.2 La pseudonimizzazione 2.1.3 Privacy by default 2.1.4 Responsabile del Trattamento
	2.2 Sicurezza dei dati personali (sezione 2)	2.2.1 Misure tecniche e organizzative
	2.3 Valutazione d'impatto sulla protezione dei dati e consultazione	2.3.1 La valutazione d'impatto (art. 35 GDPR)
	2.4 Responsabile della protezione dei dati (sezi. 4)	2.4.1 DPO (Data Protection Officer)
	2.5 Codici di condotta e certificazione (Sezione 5)	2.5.1 I Codici di condotta 2.5.2 La certificazione

3. TRASFERIMENTO DATI VERSO PAESI TERZI E COMITATO EUROPEO PER LA PROTEZIONE DATI (artt. 44-76)	3.1 Trasferimento dei dati verso paesi terzi o organizzazioni internazionali.	3.1.1 Divieto di trasferimento 3.1.2 Ipotesi di trasferimento dati extra UE 3.1.3 Deroghe all'adeguatezza
	3.2 Il Comitato Europeo per la protezione dei dati	3.2.1 Art. 68 del GDPR 3.2.2 Linee guida del EDPB
4. SANZIONI, RESPONSABILITÀ E RIMEDI ARTT. 77 – 91	4.1 Le sanzioni	4.1.1 L'art. 83 del Regolamento UE 2016/679 4.1.2 L'art. 84 del GDPR 4.1.2 L'art. 84 del GDPR
	4.2 Responsabilità	4.2.1 L'art. 82 del GDPR 4.2.2 La responsabilità del DPO/RPD
	4.3 Rimedi	4.3.1 Tempi di decisione 4 .3.2 Rappresentanza degli interessati

MODULO 3

Il Codice dell'Amministrazione Digitale

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. IL CODICE DELL'AMMINISTRAZIONE DIGITALE - STRUTTURA	1.1 Assetto del CAD	1.1.1 La suddivisione in articoli
	1.2 Ambito di applicazione	1.2.1 Aspetti organizzativi delle PA
	1.3 I diritti dei cittadini e delle imprese (sezione II)	1.3.1 I gestori dei pubblici servizi
	1.4 Organizzazione dell'e-Government nelle pubbliche amministrazioni	1.4.1 La governance 10
2. FORMAZIONE E SOTTOSCRIZIONE DEL DOCUMENTO INFORMATICO	2.1. Formazione del documento informatico	2.1.1 Differenza tra documento scritto e sottoscritto

	2.2 La sottoscrizione (sezione 2)	2.2.1 Firma elettronica e firma digitale organizzative
	2.3 Le copie di documenti informatici	2.3.1 L'art. 23 del CAD
	2.4 I certificatori di firma	2.4.1 I certificatori accreditati
3. LA GESTIONE E LA CONSERVAZIONE DEI DOCUMENTI (CAPO III)	3.1 Protocollo informatico	3.1.1 Il c.d. nucleo minimo
	3.2 Gestione informatizzata	3.2.1 Utilizzo di strumenti tecnologici
	3.3 Cooperazione applicativa	3.3.1 I sistemi di cooperazione
	3.4 Fascicolo informatico	3.4.1 Conservazione documento informatico
4. TRASMISSIONE INFORMATICA DEI DOCUMENTI (CAPO IV)	4.1 La posta elettronica	4.1.1 L'art. 45 del CAD 4.1.2 Distinzione tra consegna e disponibilità 4.1.3 L'art. 47 del CAD
	4.2 La posta elettronica certificata	4.2.1 La pec per le aziende 4.2.2 Rapporti tra pec e firma digitale
5. DATI DELLE PUBBLICHE AMMINISTRAZIONI, IDENTITÀ DIGITALI, ISTANZE E SERVIZI ON-LINE	5.1 I dati delle pubbliche amministrazioni	5.1.1 La fruizione del dato
	5.2 L' erogazione dei servizi on line	5.2.1 I livelli europei di interazione 5.2.2 La Legge n. 241 del 1990 26 5.2.3 I servizi on line delle PA: fruibilità 5.2.4 Pubblicazione di atti normativi e amministrativi 5.2.5 L'art. 65 del CAD
6. SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI (CAPO VI)	6.1 Lo sviluppo e l'acquisizione dei sistemi informatici da parte delle Pubbliche Amministrazioni	6.1.1 L'istituto del concorso di idee
	6.2 Il riuso	6.2.1 Le regole del riuso nel nuovo CAD
7. LE REGOLE TECNICHE (CAPO VII)	7.1 L'Autorità Informatica nella Pubblica Amministrazione	7.1.1 L'articolo 71 del CAD
8. IL SISTEMA PUBBLICO DI	8.1 Il RUPA (Rete Unitaria della	8.1.1 Internet nelle PA

CONNETTIVITÀ – SPC	Pubblica Amministrazione)	
	8.2 SPC (Sistema Pubblico di Connettività)	8.2.1 L'articolo 76 del CAD
	8.3 Commissione di coordinamento	8.3.1 La governance del Sistema Pubblico di Connettività
	8.4 Rete internazionale delle pubbliche amministrazioni	8.4.1 Osmosi tra SPC e Rete Internazionale PA
9. DECRETO SEMPLIFICAZIONI E CODICE DELLA AMMINISTRAZIONE DIGITALE	9.1 Identità digitale, domicilio digitale e accesso ai servizi digitali	9.1.1 Il diritto di accesso
	9.2 SPID e CIE come unici strumenti di autenticazione	9.2.1 I livelli di sicurezza
	9.3 Diritto al domicilio digitale e relativi indici	9.3.1 Linee guida AgID
	9.4 Piattaforma per la notificazione digitale degli atti della Pubblica Amministrazione	9.4.1 Inclusione digitale delle persone con disabilità 9.4.2 Semplificazione anagrafica (ANPR) 9.4.3 Pagamenti digitali: PagoPA e biglietti elettronici dei Comuni
	9.5 Governance della trasformazione digitale	9.5.1 Strategia digitale: coordinamento e attuazione 9.5.2 Codice di condotta tecnologica ed esperti 9.5.3 Disponibilità dei dati della PA 9.5.4 Piattaforma Digitale Nazionale Dati (PDND) 9.5.5 CED delle PA e migrazione in cloud
10. LA TRANSIZIONE DIGITALE DELLA PUBBLICA AMMINISTRAZIONE	10.1 La digitalizzazione nella Pubblica Amministrazione	10.1.1 La strategia di transizione digitale
	10.2 Il D.L. 22/2021 di riordino dei ministeri	10.2.1 Art. 8 D.L. 22 del 2021
	10.3 Comitato interministeriale per la transizione digitale	10.3.1 La segreteria tecnico-amministrativa del Comitato
	10.4 La Riforma della PA	10.4.1 Il programma di riforme

	10.5 La digitalizzazione della P.A. nel Piano Nazionale di Ripresa e Resilienza (PNRR)	10.5.1 La missione n. 1 del PNRR
	10.6 Indicazioni europee	10.6.1 Il Country Report 2020
	10.7 Strategia nazionale per le competenze digitali	10.7.1 I quattro assi di intervento
	10.8 Piano triennale per l'informatica nella p.a. e Strategia 2025	10.8.1 Le azioni di intervento
	10.8.1 Le azioni di intervento	
	10.9 Le modifiche al Codice dell'amministrazione	10.9.1 Il nuovo CAD

MODULO 4

Trasferimento dati all'estero e privacy comparata

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. LA CIRCOLAZIONE DEI DATI NELLE SOCIETÀ MULTINAZIONALI	1.1 Il DPO nelle multinazionali: la normativa di riferimento	1.1.1 L'art. 37 par. 2 del Regolamento UE 2016/679
	1.2 Gli obblighi del titolare	1.2.1 Linee Guida e Garanti Europei
	1.3 I contatti con le autorità	1.3.1 La gestione della Data Protection
	1.4 Il DPO nelle multinazionali: un adempimento necessario	1.4.1 L'accountability del Titolare del trattamento
	1.5 Multinazionali e GDPR	1.5.1 Estensione dell'ambito di applicazione del GDPR 1.5.2 Clausole di protezione dei dati

		1.5.3 Deroghe
2. PRIVACY: PROFILI DI DIRITTO COMPARATO	2.1 Il concetto di privacy nel diritto americano	2.1.1 Pronunce giurisprudenziali statunitensi
	2.2 La nuova direttiva europea	2.2.1 Introduzione del GDPR 2.2.2 La Dichiarazione universale dei diritti dell'uomo 12 2.2.3 Le linee guida europee e la Convezione n. 108 2.2.4 Trattato di Lisbona e Carta di Nizza 2.2.5 La Legge n. 675 del 1996 2.2.6 Il Decreto Legislativo n. 196 del 30 giugno 2003 2.2.7 Evoluzione normativa post 2012
	2.3 Un confronto tra le diverse realtà ordinamentali	2.3.1 La situazione nei paesi europei 2.3.2 Il caso Cambridge Analytica
	2.4 Riflessioni finali	2.4.1 Le principali innovazioni apportate dal Protocollo
3. SISTEMA DI GESTIONE E CONTROLLO DEI DATI	3.1 Sistema di gestione privacy e accountability	3.1.1 Il principio di accountability
	3.2 Sistema di gestione privacy: strutturare il modello organizzativo	3.2.1 I nuovi modelli di gestione
	3.3 La logica di un sistema di gestione privacy	3.3.1 Gli standard internazionali
	3.4 Sistema di gestione privacy: il metodo	3.4.1 Il ciclo di Deming
	3.5 Sistema di gestione privacy: il risk-based thinking	3.5.1 La valutazione del rischio
	3.6 Il sistema di gestione privacy: a cosa serve	3.6.1 Scopo del sistema di gestione privacy
	3.7 Struttura del sistema di gestione privacy	3.7.1 Il "contenitore" privacy
	3.8 Integrazione dei sistemi	3.8.1 I Sistemi di Gestione dell'azienda

	3.9 Intellegibilità dei modelli organizzativi	3.9.1 Orizzonte internazionale dei requisiti
4. LE MISURE DI SICUREZZA TRA GDPR E ISO 27001	4.1 GDPR e sicurezza dei dati personali	4.3 ISO 27001:2017 e sicurezza
	4.2 Responsabilità	4.2.1 L'art. 82 del GDPR 4.2.2 La responsabilità del DPO/RPD
	4.3 ISO 27001:2017 e sicurezza delle informazioni	4.3.1 Il raggio di operatività
	4.4 GDPR E ISO 27001: una relazione imprescindibile?	4.4.1 Il Considerando 100 del GDPR
5. LA PRIVACY BY DESIGN IN UN CONTESTO DI COMPLIANCE CON LA ISO 9001	5.1 Privacy by design e ISO 9001: il quadro di riferimento	5.1.1 La UNI EN ISO 9001:2015 (Sistema gestione qualità)
	5.2 Privacy by design e ISO 9001:il giusto approccio	5.2.1 La compliant
6. L'AUDIT IN AMBITO PRIVACY	6.1 Approfondimenti tecnici negli audit privacy: a cosa servono	6.1.1 La UNI EN ISO 19011:2018
	6.2 La struttura di un'attività di audit di tipo tecnico	6.2.1 Le best practice
	6.3 Considerazioni	6.3.1 I piani di miglioramento

MODULO 5
Profili di responsabilità

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. IL DIRITTO DELL'ERA DIGITALE	1.1 Internet e la responsabilità civile	1.1.1 La dottrina italiana
	1.2 Individuazione del soggetto agente	1.2.1 La "delocalizzazione" e la "dematerializzazione" 1.2.2 L'identità nel fatto illecito in rete 1.2.3 Il gestore o titolare del sito web
	1.3 L'inadeguatezza del criterio del locus commissi delicti	1.3.1 La competenza territoriale 1.3.2 Le pronunce giurisprudenziali 1.3.3 Le probabili soluzioni
2. FATTISPECIE DI REATO IN RETE	2.1 La diffamazione on-line	2.1.1 La lesione dei diritti della personalità
	2.2 La violazione della privacy	2.2.1 Normativa di collegamento
	2.3 La responsabilità dei certificatori	2.3.1 La responsabilità aquiliana
	2.4 La responsabilità degli "Istituti di Moneta Elettronica"	2.4.1 I tre profili specifici di responsabilità
	2.5 Il cybersquatting (domain name grabbing)	2.5.1 Orientamenti giurisprudenziali difformi
	2.6 Il deep-linking e il surface-linking	2.6.1 Il web-linking agreement
	2.7 Il framing	2.7.1 La violazione dell'art. 2598 c.c.
	2.8 I meta-tag	2.8.1 La violazione dell'art. 4 c.1 D.lgs n. 72 del 1992
	2.9 Lo spamming	2.9.1 La fattispecie di reato in

		Europa
3. IL REGIME DI RESPONSABILITÀ DEI SOCIAL NETWORK PROVIDER	3.1 Quadro normativo ed evoluzione giurisprudenziale	3.1.1 Le categorie di intermediari digitali
	3.2 Gli orientamenti della giurisprudenza italiana: la figura dell'hosting provider "attivo"	3.2.1 Provvedimenti cautelari applicati 3.2.2 I ruoli attivi dei provider
	3.3 Il regime di responsabilità oggettiva o per colpa	3.3.1 La teoria del rischio di impresa
	3.4 Il caso specifico dei social network	3.4.1 Gli instant articles di Facebook 3.4.2 Il problema del bilanciamento 3.4.3 Strategia per il mercato unico digitale in Europa
	3.5 Il regime di responsabilità per la diffusione di contenuti illeciti nei sistemi di Blockchain	3.5.1 Le tipologie di blockchain 3.5.2 Il soggetto responsabile 3.5.3 Lo pseudoanonimato
	3.6 Lotta agli illeciti	3.6.1 La direttiva 2000/31/CE
	3.7 Conclusioni	3.7.1 Obblighi del provider

MODULO 6

I Concetti base della sicurezza

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. LE MINACCE INFORMATICHE	1.1 Vari tipi di minacce	1.1.1 Distinzione tra informazione e dati 1.1.2 Il crimine informatico 1.1.3 I rischi del cloud computing e violazione della privacy 1.1.4 Differenza tra eventi accidentali ed eventi indesiderati
2. IL CORRETTO USO DELLE INFORMAZIONI	2.1 Tutela e gestione delle informazioni	2.1.1 Le caratteristiche delle informazioni: integrità

		confidenzialità, disponibilità 2.1.2 Il furto di identità 2.1.3 Prevenire la Perdita di dati 2.1.4 Comprensione delle linee guida e politiche per l'uso dell'ICT
3. COME PROTEGGERSI A LIVELLO INDIVIDUALE	3.1 Sicurezza della persona	3.1.1 Conoscere e saper prevenire accessi non autorizzati, frodi, raccolta impropria di dati 3.1.2 Comprendere e conoscere le metodologie di ingegneria sociale come: Phishing, Spear phishing e Shoulder surfing 3.1.3 Come prevenire il furto di identità 3.1.4 Le varie metodologie legate al furto di identità come: Skimming
4. LA PROTEZIONE DEI DATI	4.1 Protezione dei file	4.1.1 Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza delle macro 4.1.2 La cifratura: vantaggi e limiti 4.1.3 Cifrare un file, una cartella, un'unità disco 4.1.4 Proteggere i file di Office (Word, Excel, PowerPoint ecc.)

MODULO 7

Sicurezza delle reti

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. GESTIRE CONNESSIONI SICURE	1.1 Le connessioni	1.1.1 Conoscere le reti come: Lan, Wlan, Man, Wan e Gan 1.1.2 Conoscere il ruolo di amministratore della rete 1.1.3 Configurazione di un firewall a casa o a lavoro
2. LA SICUREZZA DELLE RETI WIRELESS	2.1 Protezione	1.2.1 Saper riconoscere i vari tipi di rete e i protocolli di sicurezza come: Wpa, Wep 1.2.2 Conoscere il termine hotspot personale 1.2.3 Configurare un hotspot personale

MODULO 8

La sicurezza in rete

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. PRESERVARE I DATI	1.1 Backup dei dati	1.1.1 Le caratteristiche di una procedura di backup 1.1.2 Impostare backup su supporti di memoria come: unità esterna, Cloud
2. ELIMINAZIONE DEFINITIVA DEI DATI	2.1 Rimozione o distruzione dei dati	2.1.1 Comprendere l'importanza di eliminare in permanenza i dati da supporti di memoria di massa, interni o esterni 2.1.2 Saper identificare i metodi di distruzione permanente dei dati

ChangeLog

versione 1.1

NOVITÀ

- Inserimento dell'indicazione del valore del corso secondo il quadro EQF basato sui risultati dell'apprendimento articolato su 8 livelli.
- Inserimento della rispondenza ai punti dell'Agenda per lo Sviluppo sostenibile.

AGGIORNAMENTI

- Adeguamento dei testi per una maggiore rispondenza a quanto previsto dal DigComp Framework.

idcert srl

Ufficio Italia - Europa
Via G. Pugnani 1
Andria - BT
T. 0883 885287

Numero Verde 800-108090

P.iva 08020870724
info@idcert.io

Ufficio California - Stati Uniti
2372 Morse Ave, Irvine,
CA 92614, United States