EUROPEAN INFORMATICS PASSPORT

EIPASS DPO

Programma analitico d'esame

Disclaimer

CERTIPASS ha predisposto questo documento per l'approfondimento delle materie relative alla Cultura Digitale e al migliore utilizzo del personal computer, in base agli standard e ai riferimenti Comunitari vigenti in materia; data la complessità e la vastità dell'argomento, peraltro, come editore, CERTIPASS non fornisce garanzie riguardo la completezza delle informazioni contenute; non potrà, inoltre, essere considerata responsabile per eventuali errori, omissioni, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione ed eventualmente utilizzate anche da terzi.

CERTIPASS si riserva di effettuare ogni modifica o correzione che a propria discrezione riterrà sia necessaria, in qualsiasi momento e senza dovere nessuna notifica.

L' Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del portale eipass.com dedicate al Programma.

Premessa

Il Regolamento Europeo sulla protezione dei dati personali n. 2016/679 (GDPR) ha previsto in determinati casi, sia per gli enti pubblici sia per le aziende private, la designazione del Responsabile per la protezione dei dati personali, anche detto Data Protection Officer.

Il Data Protection Officer è una figura di alto livello professionale che deve essere coinvolta in tutte le questioni inerenti alla protezione dei dati personali. Gode di ampia autonomia ed è designato in funzione delle proprie qualità professionali, soprattutto in relazione alla conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai propri compiti; deve, inoltre, possedere delle qualità manageriali , oltre che una buona conoscenza delle nuove tecnologie.

Il programma di certificazione EIPASS DPO è stato realizzato per consentire di operare come Data Protection Officer, sia nella Pubblica Amministrazione sia nel privato, acquisendo le competenze necessarie al ruolo.

Centro Studi EIPASS

Programma analitico d'esame

EIPASS DPO

Metodo

La prima parte del programma è dedicata specificamente al DPO, definendone come viene designato, qual è la sua posizione all'interno della struttura pubblica o privata nella quale opera, e i compiti previsti dall'incarico.

La seconda parte fornisce un ampio e dettagliato quadro sulla relazione tra le nuove tecnologie, e quindi il loro utilizzo, e i danni che ne possono scaturire da un uso improprio, ma anche i diritti dell'individuo che si appresta a utilizzarle.

Seguono un'agile trattazione del Codice dell'Amministrazione Digitale, di cui si approfondiscono principi e aggiornamenti, e la trattazione sul Regolamento UE 679/2016 e le nuove norme sulla protezione dei dati personali, ultimo riferimento normativo in materia di trattamento dei dati personali.

Un ampio spazio è riservato alla PEC (Posta Elettronica Certificata) e a tutte le implicazioni tecnico-pratiche che derivano dalla sua introduzione massiva nella PA.

Argomento correlato è quello relativo ai documenti informatici e alla loro archiviazione; si affronta a 360°, fino a chiarire finalità e funzionamento della firma elettronica o digitale.

Infine, l'ultima parte consente l'acquisizione di competenze indispensabili per operare in sicurezza, sia in relazione alla creazione e alla conservazione dei dati che al loro scambio in rete.

Tutti gli argomenti sono trattati da esperti di settore, che hanno realizzato strumenti didattici e-learning di facile consultazione che facilitano l'apprendimento.

Moduli d'esame

Modulo 1 | Il DPO: designazione, posizione e compiti

Modulo 2 | Nuove tecnologie: diritti e danni

Modulo 3 | Il Codice dell'Amministrazione Digitale

Modulo 4 | La protezione dei dati personali: il GDPR

Modulo 5 | PEC, firma elettronica e archiviazione dei documenti digitali

Modulo 6 | IT Security

Prova d'esame e valutazione

Il rilascio della certificazione avverrà previo sostenimento e superamento di esami online (1 per modulo), tramite piattaforma DIDASKO. Per superare ogni esame, il Candidato dovrà rispondere correttamente ad almeno il 75% delle 30 domande previste, in un tempo massimo di 30 minuti.

Sono previste domande con risposta a scelta multipla, quesiti vero/falso o simulazioni operative.

Ogni esame è unico, essendo le domande e l'ordine delle risposte scelto casualmente dal sistema all'avvio. Lo stesso sistema calcolerà la percentuale di risposte esatte fornite, decretando istantaneamente il superamento o meno dell'esame: non essendovi, quindi, alcun intervento da parte di un Docente/Esaminatore, viene garantita l'obiettività dell'esito conseguito.

Il Supervisore, figura autorizzata da CERTIPASS previo conseguimento di apposita abilitazione, si limita al controllo del rispetto delle previste procedure.

L'eventuale, mancato superamento di uno o più dei previsti moduli comporterà la ripetizione degli stessi attraverso una prova suppletiva.

Modulo 1

IL DPO: DESIGNAZIONE, POSIZIONE E COMPITI

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato possiede le competenze necessarie per operare come Data Protection Officer, conoscendone la definizione del ruolo e i compiti. Conosce le procedure di nomina, quindi i requisiti e l'atto. Ha acquisito il concetto dell'operare in autonomia, senza conflitti di interessi. Il candidato possiede conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati.

Contenuti del modulo

Introduzione

- La riservatezza e la protezione dei dati personali
- Il Regolamento (UE) 2016/679

Il Data Protection Officer

- La nascita del Data Protection Officer
- Il Data Protection Officer in Italia
- Il Data Protection Officer nel Regolamento europeo sulla privacy

Nomina obbligatoria del RPD

- Definizione di «autorità pubblica o di organismo pubblico»
- Definizione di «monitoraggio regolare e sistematico»
- Definizione di «larga scala»
- Definizione di «attività principali»
- Soggetti a cui spetta nominare il RPD
- Nomina di un unico RPD
- Requisiti particolari del RPD
- L'atto di designazione del RPD

Posizione del RPD

- Coinvolgimento del RPD
- Sostegno del RPD
- L'autonomia del RPD
- Il conflitto di interessi

Compiti del RPD

- Gli ulteriori compiti e funzioni del RPD
- Conoscenze e caratteristiche personali del RPD

La privacy by design e la privacy by default

- La privacy «by design»
- La pseudonimizzazione
- La privacy «by default»

Fonti giuridiche

1	DATA PROTECTION OFFICER		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	La nascita del Data Protection Officer	**1.1**	Riconoscere e definire la nascita della figura del DPO
1.2	Il Data Protection Officer in Italia	**1.2**	Riconoscere e definire l'introduzione della figura del DPO con riferimento all'Italia
1.3	Il Data Protection Officer nel Regolamento europeo sulla privacy	**1.3**	Riconoscere e definire il ruolo del DPO come attribuito dal Regolamento

2	NOMINA OBBLIGATORIA DEL RPD		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	Definizione di «autorità pubblica o di organismo pubblico»	**2.1**	Riconoscere e definire il concetto di «autorità pubblica o di organismo pubblico»
2.2	Definizione di «monitoraggio regolare e sistematico»	**2.2**	Riconoscere e definire il concetto di «monitoraggio regolare e sistematico»
2.3	Definizione di «larga scala»	**2.3**	Riconoscere e definire il concetto di «larga scala»
2.4	Definizione di «attività principali»	**2.4**	Riconoscere e definire il concetto di «attività principali»
2.5	Soggetti a cui spetta nominare il RPD	**2.5**	Identificare i soggetti a cui spetta nominare il RPD
2.6	Nomina di un unico RPD	**2.6**	Descrivere le procedure di nomina del RPD
2.7	Requisiti particolari del RPD	**2.7**	Definire i requisiti particolari che deve possedere il RPD
2.8	L'atto di designazione del RPD	**2.8**	Definire come avviene la designazione del RPD

3 | POSIZIONE DEL RPD			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
3.1	Coinvolgimento del RPD	**3.1**	Identificare quando e come deve essere coinvolto il RPD nelle questioni riguardanti la protezione dei dati personali
3.2	Sostegno del RPD	**3.2**	Riconoscere come il titolare e il responsabile del trattamento devono sostenere il RPD nell'esecuzione dei suoi compiti
3.3	L'autonomia del RPD	**3.3**	Definire l'indipendenza nello svolgimento del ruolo
3.4	Il conflitto di interessi	**3.4**	Definire il conflitto di interessi che può incorrere nello svolgimento del ruolo

4 | COMPITI DEL RPD			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
4.1	Gli ulteriori compiti e funzioni del RPD	**4.1**	Descrivere in che misura al RPD possono essere attribuiti ulteriori compiti e funzioni
4.2	Conoscenze e caratteristiche personali del RPD	**4.2**	Definire quali conoscenze e caratteristiche deve possedere il RPD per operare

5 | LA PRIVACY BY DESIGN E LA PRIVACY BY DEFAULT			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
5.1	La privacy by design	**5.1**	Definire il principio della privacy by design e descrivere la sua applicazione
5.2	La pseudonimizzazione	**5.2**	Identificare e descrivere la metodologia della pseudonimizzazione
5.3	La privacy by default	**5.3**	Definire il principio della privacy by default e descrivere la sua applicazione

Modulo 2

NUOVE TECNOLOGIE: DIRITTI E DANNI

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato possiede le competenze necessarie per conoscere i danni delle tecnologie ma anche per riconoscere i diritti dell'individuo che si appresta a utilizzarle. Sa distinguere le conseguenze di carattere patrimoniale e non patrimoniale. Comprende il concetto di società dell'informazione e di errore d'informazione. Il Candidato conosce i diritti della personalità, il concetto di privacy e sa applicare le misure minime di sicurezza in internet.

Contenuti del modulo

Le nuove tecnologie e i nuovi danni

- Il danno patrimoniale: danno emergente e lucro cessante
- La risarcibilità del danno non patrimoniale
- Danno alla persona e danno alla lezione dei diritti della personalità

Il risarcimento del danno non patrimoniale

- Le categorie di danno non patrimoniale: biologico, morale, esistenziale
- I danni bagatellari
- Il danno non patrimoniale delle persone giuridiche

Gli interessi tutelati

- La lesione all'integrità psico-fisica
- La violazione dell'identità personale
- Il diritto all'immagine
- La libertà di espressione in internet
- La tutela dell'onore e della reputazione
- Il diritto d'autore in internet
- Il diritto all'oblio

Il diritto alla riservatezza: evoluzione e tutela giuridica

- Le origini del diritto alla riservatezza
- La legislazione europea in materi di tutela della riservatezza
- Il ruolo delle informazioni e il nuovo concetto di privacy
- Le fonti normative di rango internazionale e comunitario in materia di privacy
- Il Codice della privacy

Le misure di sicurezza informatica

- Le misure di sicurezza informatica: profili generali
- Le misure di sicurezza nel Regolamento UE n. 679/2016
- Privacy by design
- Privacy by default
- Valutazione di impatto sulla protezione dei dati
- Le violazioni delle misure di sicurezza informatica: profili di responsabilità

1	LE NUOVE TECNOLOGIE E I NUOVI DANNI		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	Il danno patrimoniale: danno emergente e lucro cessante	**1.1**	Riconoscere e definire il danno patrimoniale, identificando le due componenti del danno emergente e del lucro cessante
1.2	La risarcibilità del danno non patrimoniale	**1.2**	Riconoscere e definire il danno non patrimoniale, anche in relazione alla risarcibilità
1.3	Danno alla persona e danno alla lesione dei diritti della personalità	**1.3**	Riconoscere e definire il danno alla persona e il danno alla lesione dei diritti della personalità; Conoscere la tutela prevista dal Codice Civile

2	IL RISARCIMENTO DEL DANNO NON PATRIMONIALE		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	Le categorie di danno non patrimoniale: biologico, morale, esistenziale	**2.1**	Aprire e chiudere il browser; descriverne l'interfaccia, riconoscendone ogni elemento
2.2	I danni bagatellari	**2.2**	Riconoscere e definire i danni bagatellari
2.3	Il danno non patrimoniale delle persone giuridiche	**2.3**	Identificare la tutela dalle lesioni a carattere non patrimoniale delle persone giuridiche

3	GLI INTERESSI TUTELATI		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
3.1	La lesione all'integrità psico-fisica	**3.1**	Riconoscere la lesione dell'integrità fisica, identificandola come ipotesi più frequente di danno alla persona
3.2	La violazione dell'identità personale	**3.2**	Riconoscere e definire l'interesse a non vedere alterato o travisato il proprio patrimonio ideologico, in relazione alla violazione dell'identità personale

3.3	Il diritto all'immagine	**3.3**	Definire il diritto all'immagine e riconoscere il danno patrimoniale per la violazione del diritto stesso, anche specificamente in internet
3.4	La libertà di espressione in internet	**3.4**	Definire il diritto alla manifestazione del pensiero e riconoscere la tutela della libertà di manifestazione del pensiero
3.5	La tutela dell'onore e della reputazione	**3.5**	Riconoscere, in tema di potenzialità lesive della libera manifestazione del pensiero, i beni maggiormente in pericolo, cioè l'onore, la reputazione, la riservatezza e l'identità
3.6	Il diritto d'autore in internet	**3.6**	Definire il diritto d'autore, specificamente rispetto a internet
3.7	Il diritto all'oblio	**3.7**	Definire il diritto all'oblio e identificare le sue applicazioni, con riferimento alle recenti sentenze in materia

4 | IL DIRITTO ALLA RISERVATEZZA: EVOLUZIONE E TUTELA GIURIDICA

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
4.1	Le origini del diritto alla riservatezza	**4.1**	Descrivere le origini del diritto alla riservatezza
4.2	La legislazione europea in materia di tutela della riservatezza	**4.2**	Descrivere la legislazione europea in materia di tutela della riservatezza
4.3	Il ruolo delle informazioni e il nuovo concetto di privacy	**4.3**	Descrivere la condizione dei nuovi pericoli che possono colpire il privato, in relazione alle nuove tecnologie e alla Rete
4.4	Le fonti normative di rango internazionale e comunitario in materia di privacy	**4.4**	Definire le fonti normative in materia di privacy, nello specifico conosce la Convenzione di Strasburgo del 1981, la Direttiva 46/95/CE, la L. 675/96 e la Dir. 2002/58/CE
4.5	Il Codice della privacy	**4.5**	Definire i principi fondamentali del Codice della privacy, anche in relazione al Regolamento Europeo 679/2016

5 | LE MISURE DI SICUREZZA INFORMATICA

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
5.1	Le misure di sicurezza in Internet	**5.1**	Identificare le misure di sicurezza in relazione alla privacy
5.2	Le misure di sicurezza nel Regolamento UE 679/2016	**5.2**	Adottare le misure di sicurezza connesse alla protezione dei dati e alla riservatezza secondo le disposizioni del Regolamento UE 679/2016
5.3	Privacy by design	**5.3**	Adottare misure tecniche e organizzative "fin dalla progettazione" del trattamento per garantire la sicurezza dei dati personali

5.4	Privacy by default	**5.4**	Adottare misure tecniche e organizzative "come impostazione predefinita" del trattamento per garantire la sicurezza dei dati personali
5.5	Valutazione di impatto sulla protezione dei dati	**5.5**	Eseguire l'analisi di rischio connessa all'utilizzo dei dati personali, secondo le disposizioni del Regolamento UE 679/2016
5.6	Le violazioni delle misure di sicurezza informatica: profili di responsabilità	**5.6**	Riconoscere i profili di responsabilità connessi alla violazione delle norme in materia di trattamento dei dati personali

Modulo 3

IL CODICE DELL'AMMINISTRAZIONE DIGITALE

Cosa sa fare il Candidato che si certifica con EIPASS DPO

III Candidato certificato conoscere le norme più importanti del Codice dell'Amministrazione Digitale (CAD), ai fini di un corretto e consapevole utilizzo dei dispositivi digitali impiegati nei contesti operativi delle Pubbliche Amministrazioni.

In particolare, il Candidato conosce:

- Le principali normative in materia di informatizzazione della PA
- Gli aggiornamenti più rilevanti introdotti con la riforma del CAD
- I diritti dei cittadini e delle imprese sanciti dal CAD
- Le normative riguardanti la trasparenza e gli obblighi delle PA

Contenuti del modulo

Il rinnovamento della Pubblica Amministrazione

- Informatizzazione - Dematerializzazione - Digitalizzazione - E-Government
- L'Amministrazione nell'era digitale
- Il CAD e le recenti modifiche

L'analisi del Codice dell'Amministrazione Digitale: obiettivi, strategie, effetti

- Principi generali
- La qualità dei servizi resi e soddisfazione dell'utenza
- L'organizzazione delle Pubbliche Amministrazioni

Gli strumenti dell'informatizzazione: documento informatico e firme elettroniche

- Le novità del D.Lgs 179/2016
- Formazione, gestione e conservazione dei documenti informatici
- La comunicazione e l'accesso ai dati
- Sviluppo, acquisizione e riuso dei sistemi informatici nelle Pubbliche Amministrazioni

L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni

- La pubblicazione dei dati e la trasparenza
- L'Agenda Digitale

1	IL RINNOVAMENTO DELLA PUBBLICA AMMINISTRAZIONE		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	Informatizzazione - Dematerializzazione - Digitalizzazione - E-Government	**1.1.1**	La dematerializzazione
		1.1.2	La digitalizzazione
1.2	L'Amministrazione nell'era digitale	**1.2.1**	Cenni sulle tappe evolutive dei processi di informatizzazione
		1.2.2	Il DLgs 12 febbraio 1993
1.3	Il CAD e le recenti modifiche	**1.3.1**	Il Dlgs 7 marzo 2005, n. 82
		1.3.2	I principi della Legge 7 agosto 2015, n. 124
		1.3.3	Le modifiche del Dlgs 26 agosto 2016, n. 179

2	STRUMENTI DI COLLABORAZIONE ONLINE		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	Principi generali	**2.1.1**	Il domicilio digitale delle persone fisiche
		2.1.2	I pagamenti con modalità informatiche (art. 5 del CAD)
		2.1.3	L'identità digitale
		2.1.4	L'utilizzo della PEC
2.2	La qualità dei servizi resi e soddisfazione dell'utenza	**2.2.1**	L'art. 7 del CAD
		2.2.2	L'alfabetizzazione informatica
		2.2.3	Connetività alla rete Internet negli uffici e luoghi pubblici
		2.2.4	Partecipazione democratica ele ronica (art. 9 del CAD)
2.3	L'organizzazione delle Pubbliche Amministrazioni	**2.3.1**	L'Art.12 del CAD
		2.3.2	Rapporti tra Stato, Regioni e autonomie locali (art. 14)
		2.3.3	L'Agenzia per l'Italia Digitale
		2.3.4	L'Art. 15: Digitalizzazione e riorganizzazione
		2.3.5	Strutture per l'organizzazione, l'innovazione e le tecnologie (art.17)
		2.3.6	La Conferenza permanente per l'innovazione tecnologica

3 | GLI STRUMENTI DELL'INFORMATIZZAZIONE: DOCUMENTO INFORMATICO E FIRME ELETTRONICHE

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
3.1	Le novità del Dlgs 179/2016	**3.1.1**	Il documento informatico
		3.1.2	La firma elettronica
		3.1.3	La firma elettronica e l'efficacia probatoria dei documenti informatici
3.2	Formazione, gestione e conservazione dei documenti informatici	**3.2.1**	La trasmissione informatica dei documenti: la PEC e la cooperazione applicativa
		3.2.2	Il Sistema pubblico di connettività
3.3	La comunicazione e l'accesso ai dati	**3.3.1**	Trasmissione dei documenti tra le pubbliche amministrazioni
		3.3.2	Disponibilità e fruibilità dei dati delle pubbliche amministrazioni
		3.3.3	Siti Internet delle pubbliche amministrazioni (art. 53 CAD)
		3.3.4	Identità Digitale e Regolamento eIDAS
		3.3.5	L'accesso telematico ai servizi della Pubblica Amministrazione
		3.3.6	Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica
		3.3.7	Carta d'identità elettronica e carta nazionale dei servizi
3.4	Sviluppo, acquisizione e riuso dei sistemi informatici nelle Pubbliche Amministrazioni	**3.4.1**	Il Cloud computing

4 | L'INFORMATIZZAZIONE E LA TRASPARENZA NELLE PUBBLICHE AMMINISTRAZIONI

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
4.1	La pubblicazione dei dati e la trasparenza	**4.1.1**	Il diritto di accesso
		4.1.2	I titolari del diritto di accesso
		4.1.3	L'art. 5 D.Lgs 33/2013: l'accesso civico
		4.1.4	I limiti al diritto di accesso
		4.1.5	L'oggetto della richiesta: gli atti accessibili
		4.1.6	Il diritto di accesso della L. 241/1990, il diritto di accesso civico e il diritto di accesso del "FOIA"
		4.1.7	La pubblicazione dei dati e la trasparenza dopo il D.Lgs 97/2019

4.2	L'Agenda Digitale	**4.2.1**	L'Agenda Digitale Italiana
		4.2.2	L'Agenzia per l'Italia digitale
		4.2.3	L'atto amministrativo telematico
		4.2.4	Le criticità della digitalizzazione

Modulo 4

LA PROTEZIONE DEI DATI PERSONALI: IL GDPR

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato conoscere le novità più importanti del Regolamento UE 679/2016 (il General Data Protection Regulation — DPR), come quella sull'accountability.

Sa che il GDPR non contiene la distinzione tra condizioni di liceità previste per i soggetti privati e quelle valide per le amministrazioni pubbliche. Sa esaminare e comprendere, quindi, tutte le disposizioni del GDPR, utili a valutare quali saranno le reali prospettive di cambiamento all'interno delle amministrazioni.

Contenuti del modulo

Il General Data Protection Regulation (GDPR)

- I tratti distintivi del GDPR
- Il campo di applicazione del GDPR
- La definizione di dato personale del GDPR
- Il principio di responsabilizzazione
- I principi applicabili al trattamento dei dati personali
- L'informativa sui dati personali

I diritti dell'interessato al trattamento dei dati personali

- La proliferazione
- Il diritto di accesso
- Il diritto all'oblio
- Il diritto alla portabilità dei dati
- Il diritto di opposizione

I titolari e i responsabili del trattamento

- Gli obblighi del titolare e del resposabile del trattamento
- Il resposabile della protezione dei dati

Sanzioni e rimedi in caso di violazione del GDPR

- Il Comitato europeo per la protezione dei dati
- Il principio dello sportello unico: one stop shop
- Le sanzioni
- La violazione dei dati personali
- Le autorità nazionali di controllo
- I rimedi per la violazione dei dati personali

1 | IL GENERAL DATA PROTECTION REGULATION (GDPR)

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	I tratti distintivi del GDPR	**1.1**	Riconoscere i tratti distinti del Regolamento UE 679/2016 (il General Data Protection Regulation — GDPR) in materia di trattamento dei dati personali
1.2	Il campo di applicazione territoriale del GDPR	**1.2**	Descrivere l'ambito di applicazione territoriale del GDPR
1.3	La definizione di dato personale nel GDPR	**1.3**	Definire il "dato personale" secondo le disposizioni del GDPR
1.4	Il principio di responsabilizzazione	**1.4**	Riconoscere il principio secondo cui il titolare del trattamento dei dati personali è tenuto a osservare ed essere in grado di comprovare il rispetto del GDPR
1.5	I principi applicabili al trattamento dei dati personali	**1.5**	Riconoscere gli altri principi alla base delle nuove norme in materia di trattamento dei dati personali
1.6	L'informativa sui dati personali	**1.6**	Riconoscere le norme da rispettare per redigere le "informative" sul trattamento dei dati personali

2 | I DIRITTI DELL'INTERESSATO AL TRATTAMENTO DEI DATI

Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	La proliferazione	**2.1**	Riconoscere le norme da seguire per la "profilazione", un tipo di trattamento dei dati personali al quale il GDPR dedica particolare attenzione
2.2	Il diritto di accesso	**2.2**	Definire il diritto di accesso ai propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
2.3	Il diritto all'oblio	**2.3**	Definire il diritto alla cancellazione dei propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
2.4	Il diritto alla portabilità dei dati	**2.4**	Definire il diritto alla portabilità dei propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
2.5	Il diritto di opposizione	**2.5**	Definire il diritto di opposizione al trattamento dei dati personali, riconosciuto dal GDPR agli interessati del trattamento

3	I TITOLARI E I RESPONSABILI DEL TRATTAMENTO		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
3.1	Gli obblighi del titolare e del responsabile del trattamento	**3.1**	La valutazione di impatto sulla protezione dei dati personali Il registro delle attività di trattamento dei dati personali
3.2	Il Resposabile della protezione dei Dati (RPD)	**3.2**	I compiti e le funzioni del RPD

4	SANZIONI E RIMEDI IN CASO DI VIOLAZIONE DEL GDPR		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
4.1	Il Comitato europeo per la protezione dei dati	**4.1**	Riconoscere le norme da seguire per la "profilazione", un tipo di trattamento dei dati personali al quale il GDPR dedica particolare attenzione
4.2	Il principio dello sportello unico: one stop shop	**4.2**	Definire il diritto di accesso ai propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
4.3	Le sanzioni	**4.3**	Definire il diritto alla cancellazione dei propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
4.4	La violazione dei dati personali (Data breach)	**4.4**	Definire il diritto alla portabilità dei propri dati personali, riconosciuto dal GDPR agli interessati del trattamento
4.5	Le autorità nazionali garanti della protezione dei dati personali	**4.5**	Definire il diritto di opposizione al trattamento dei dati personali, riconosciuto dal GDPR agli interessati del trattamento
4.6	I rimedi per la violazione dei dati personali	**4.6**	I diritti che il danneggiato può far valere avverso il trattamento dei dati personali

Modulo 5

PEC, FIRMA ELETTRONICA E ARCHIVIAZIONE DEI DOCUMENTI DIGITALI

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato sa cos'è e come funziona la Posta Elettronica Certificata (PEC).

Sa perché e quando la PEC ha valore legale.

Sa cos'è la firma elettronica, conoscendone le diverse tipologie. Sa inoltre cos'è il sigillo elettronico.

Conosce il sistema di archiviazione dei documenti digitali.

Contenuti del modulo

La Posta Elettronica Certificata

- Cos'è la PEC
- La procedura di invio di un messaggio tramite PEC
- Il registro generale degli indirizzi elettronici
- Il Dominio digitale

I documenti informatici e le firme elettroniche

- La firma digitale
- Firma elettronica ed efficacia probatoria dei documenti informatici
- Il sigillo elettronico

L'archiviazione dei documenti digitali

- La digitalizzazione della Pubblica amministrazione.
- L'informatizzazione
- La dematerializzazione
- La digitalizzazione
- Il documento informatico
- La conservazione dei documenti della Pubblica amministrazione

1 I LA POSTA ELETTRONICA CERTIFICATA (PEC)			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	La PEC	**1.1**	Che cos'è la Posta Elettronica Certificata (PEC)
1.2	La procedura di invio di un messaggio tramite PEC	**1.2**	La procedura per inviare un messaggio di Posta elettronica certificata
1.3	Il Registro generale degli indirizzi elettronici	**1.3**	Come reperire gli indirizzi PEC nel Registro generale degli indirizzi elettronici
1.4	Il Dominio digitale	**1.4**	Che cos'è il Dominio digitale, l'istituto più significativo della digitalizzazione dei rapporti tra i cittadini e la Pubblica amministrazione

2 I LA FIRMA ELETTRONICA E IL SIGILLO ELETTRONICO			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	La firma elettronica	**2.1**	Che cosa sono la firma elettronica, la firma elettronica avanzata e la firma elettronica qualificata. Le disposizioni sono contenute nel Regolamaneto eIDAS
2.2	Firma elettronica ed efficacia probatoria dei documenti informatici	**2.2**	Il valore giuridico delle firme elettroniche
2.3	Il sigillo elettronico	**2.3**	Che cos'è il sigillo elettronico. Le disposizioni sono contenute nel Regolamento eIDAS

3 I ARCHIVIAZIONE DEI DOCUMENTI DIGITALI			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
3.1	La digitalizzazione della Pubblica amministrazione	**3.1**	Che cos'è l'e-government
3.2	L'informatizzazione	**3.2**	Che cosa si intende per informatizzazione dei processi amministrativi
3.3	La dematerializzazione	**3.3**	Che cosa si intende per dematerializzazione dei documenti
3.4	La digitalizzazione	**3.4**	Che cosa si intende per digitalizzazione della Pubblica amministrazione
3.5	Il Documento informatico	**3.5**	Che cos'è il Documento informatico
3.6	La conservazione dei documenti della Pubblica amministrazione	**3.6**	Le norme in materia di archiviazione di documenti elettronici
3.7	Le copie, i duplicati, gli estratti analogici e informatici	**3.7**	Il valore giuridico delle copie digitali dei documenti
3.8	Le copie informatiche di documenti analogici	**3.8**	Come riprodurre un documento analogico su suppporto informatico
3.9	Le copie analogiche di documenti informatici	**3.9**	Come riprodurre un documento informatico

Modulo 6

IT SECURITY

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato conosce il concetto di sicurezza informatica, comprende la differenza tra sicurezza attiva e passiva e sa come rilevare un attacco hacker.

Conosce i maleware più diffusi e sa come attivarsi per proteggere i propri dispositivi ed i propri dati. Comprende quanto sia importante che i dati siano autentici, affidabili, integri e riservati. Sa backupparli e recuperarli.

Utilizza in sicurezza la posta elettronica e gli altri strumenti di comunicazione online. Conosce e utilizza in maniera corretta la tecnologia P2P.

Sa come navigare in sicurezza, utilizzando tutte le accortezze necessarie per salvaguardare i propri dati.

Contenuti del modulo

Definizioni

- Le finalità dell'IT Security
- Il concetto di privacy
- Misure per la sicurezza dei file

Maleware

- Gli strumenti di difesa
- L'euristica

La sicurezza delle reti

- La rete e le connessioni
- Navigare sicuri con le reti wireless

Navigare in sicurezza

- Il browser e la sicurezza online
- Gli strumenti messi a disposizione da Google Chrome
- Strumenti di filtraggio dei contenuti

Sicurezza nella comunicazione online

- La vulnerabilità della posta elettronica
- Come gestire gli strumenti di comunicazione online
- La tecnologia peer to peer

Sicurezza dei dati

- Gestire i dati sul PC in maniera sicura
- Il ripristino di sistema
- Eliminare i dati in modo permanente

1 | DEFINIZIONI			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
1.1	Le finalità dell'IT Security	**1.1.1**	Definire il concetto di IT Security, comprendendo la differenza tra dato e informazione e sapendo cosa siano gli standard di sicurezza e come certificarli (ISO)
		1.1.2	Definire il rischio come la risultante dell'equazione tra minaccia/vulnerabilità e contromisure; definire gli aspetti centrali dell'IT Security: integrità, confidenzialità, disponibilità, non ripudio e autenticazione
		1.1.3	Conoscere le minacce e distinguere tra eventi accidentali e indesiderati
		1.1.4	Comprendere il significato di crimine informatico e riconoscere le diverse tipologia di hacker
		1.1.5	Distinguere tra misure di protezione passive e attive
		1.1.6	Riconoscere e attuare misure di sicurezza, quali l'autenticazione e l'utilizzo di password adeguate per ogni account, l'utilizzo dell'OTP, l'autenticazione a due fattori (tramite sms e e-mail, applicazione e one button authentication), la cancellazione della cronologia del browser; comprendere e definire la biometria applicata alla sicurezza informatica; definire il concetto di accountability
1.2	Il concetto di privacy	**1.2.1**	Riconoscere i problemi connessi alla sicurezza dei propri dati personali
		1.2.2	Comprendere e definire il concetto di *social engineering*
		1.2.3	Comprendere cosa sia e cosa comporta il furto d'identità; mettere in pratica buone prassi per limitare al massimo i pericoli connessi; verificare se la propria identità è stata rubata e, se è necessario, sapere a chi rivolgersi e cosa fare per limitare i danni
		1.2.4	Come difendersi dagli attacchi di ingegneria sociale
1.3	Misure per la sicurezza dei file	**1.3.1**	Definire una macro e comprenderne le implicazioni, in tema di sicurezza
		1.3.2	Cambiare le impostazioni delle macro in Centro protezione
		1.3.3	Impostare una password per i file di Office

2	MALWARE		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
2.1	I maleware	**2.1.1**	Definire il concetto di maleware, distinguendo quelli di tipo parassitario da quelli del settore di avvio
		2.1.2	Definire e riconoscere il funzionamento dei maleware più diffusi: virus, worm, trojan horse, dialer, hijacking, zip bomb, spyware; riconoscere gli spyware più pericolosi (phishing, vishing, pharming, sniffing); riconoscere le modalità di diffusione di uno spyware; comprendere se il proprio PC è infettato da uno spyware; evitare che il proprio PC venga infettato da uno spyware e, eventualmente, rimuoverlo
		2.1.3	Definire e riconoscere il funzionamento dei maleware della categoria attacchi login: thiefing e keylogger
2.2	Gli strumenti di difesa	**2.2.1**	A cosa serve il firewall; come funziona tecnicamente; quali sono i diversi tipi
		2.2.2	A cosa serve l'antivirus
		2.2.3	Come funziona e quali sono le diverse componenti di un antivirus
		2.2.4	Definire le diverse opzioni disponibili per programmare una scansione del sistema; comprendere il concetto di avanzamento e analisi dei risultati di una scansione; definire il tipo real-time e il concetto di analisi comportamentale; riconoscere i diversi tipi di riparazione
		2.2.5	Valutare l'importanza di un costante aggiornamento dell'antivirus; definire il concetto di euristica applicata a questo contesto; definire il CERT (Computer Emergency Response Team)
2.3	L'euristica	**2.3.1**	Cos'è l'euristica e come funzionano i maleware creati secondo questo principio, detti poliformi

3	LA SICUREZZA DELLE RETI		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
3.1	La rete e le connessioni	**3.1.1**	Definire il concetto di rete in informatica e di networking
		3.1.2	Distinguere le diverse tipologie di reti informatiche (LAN, WAN, MAN)
		3.1.3	Distinguere i vari tipi di reti LAN (star, bus, ring, mesh)
		3.1.4	Comprendere il principio di vulnerabilità delle reti, riconoscendone le diverse tipologie
		3.1.5	Riconoscere il ruolo e gli oneri che un amministratore di sistema ha in relazione alla sicurezza della rete
		3.1.6	A cosa è utile il firewall e come funziona tecnicamente; distinguere i firewall dal funzionamento interno (a filtraggio di pacchetti e a livello di circuito)
3.2	Navigare sicuri con le reti wireless	**3.2.1**	Comprendere l'importanza di un utilizzo ragionato della password nei sistemi Wi-Fi
		3.2.2	Riconoscere i diversi protocolli utilizzati per proteggere questo tipo di rete: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPA 2 (con standard di criptazione AES, Advanced Encryption Standard)
		3.2.3	Cos'è e come funziona l'hotspot; come attivare l'hotspot personale o tethering; come connettersi e disconnettersi da una connessione tramite hotspot; cos'è e come funziona l'hotspot 2.0 e come attivarlo su Windows 10; riconoscere le differenze tra l'hotspot e l'hotspot 2.0; cos'è il roaming
		3.2.4	Riconoscere i pericoli connessi alla navigazione su reti wireless pubbliche
		3.2.5	I diversi tipi di attacchi portati tramite reti wireless pubbliche: intercettazione o eavesdropping, jamming e MITM (man-in-the-middle attack)

4	NAVIGARE IN SICUREZZA		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
4.1	Il browser e la sicurezza online	**4.1.1**	Cosa sono e come si gestiscono i file temporanei di Internet
		4.1.2	Come salvare le password dei diversi account; comprendere i vantaggi e gli svantaggi di salvare le password sul PC; cancellare le password memorizzate
		4.1.3	Come impostare, utilizzare e eliminare la funzione di compilazione automatica dei form online
		4.1.4	Cosa sono e come si gestiscono i codici attivi
		4.1.5	Qual è la differenza tra coockie di sessione e persistenti e quale sia il loro impatto sulla sicurezza dei dati
4.2	Gli strumenti messi a disposizione da Google Chrome	**4.2.1**	Riconoscere le icone relative al protocollo SSL (Secure Socket); comprende cos'è il certificato di sicurezza e a cosa serve
		4.2.2	Gestire gli avvisi per siti non sicuri
		4.2.3	Cos'è e come funziona Sandboxing
		4.2.4	Cosa sono gli aggiornamenti automatici
		4.2.5	Cos'è e come funziona Smart Lock
		4.2.6	Come navigazione in incognito e settare le preferenze
		4.2.7	Come proteggere la privacy, navigando in incognito e gestendo le apposite preferenze

5 | SICUREZZA NELLA COMUNICAZIONI ONLINE			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
5.1	La vulnerabilità della posta elettronica	**5.1.1**	Comprendere e distinguere le diverse minacce; comprendere il funzionamento e la finalità della cifratura delle e-mail; riconoscere, definire e utilizzare software per crittografare i messaggi di posta elettronica: Virtru, ProntonMail, Sbwave Enkryptor, Lockbin, Encipher.it, Secure Gmail
		5.1.2	Cos'è la firma digitale; comprendere la differenza di funzionamento tra la firma digitale e la cifratura dei messaggi di posta elettronica
		5.1.3	Definire le caratteristiche del phishing e riconoscere le e-mail fraudolenti finalizzate al furto dei dati; come comportarsi nel caso in cui si è vittima di tentativi di phishing
		5.1.4	Come gestire la posta indesiderata e lo spam; cosa fare per ridurre al minimo il rischio di essere spammato
		5.1.5	Gestire in sicurezza una casella di posta su Gmail: creare e aggiornare la password, verificare gli accessi non autorizzati, segnalare mail come phishing o spam, segnalare come normale una mail precedentemente segnalata come spam, aggiungere e aggiornare il filtro antispam
5.2	Come gestire gli strumenti di comunicazione online	**5.2.1**	Riconoscere e gestire i possibili rischi che derivano dall'utilizzo di blog, messaggistica istantanea e social network (Facebook e Twitter), quali adescamento e divulgazione dolosa di immagini altrui
		5.2.2	Riconoscere i casi di social network poisoning e comprendere i potenziali e gravi pericoli derivanti da un uso non etico dei social network, come il cyberbullismo
		5.2.3	Utilizzare software che consentono una condivisione sicura di messaggi e contenuti (ChatSecure, Silent Circle, Signal Messenger, Telegram, Wickr); comprendere e descrivere il funzionamento della crittografia end to end
5.3	La tecnologia peer to peer	**5.3.1**	Comprendere e definire il funzionamento e le applicazioni del P2P, avendo consapevolezza delle implicazioni che ne derivano sul piano della sicurezza e del copyright
		5.3.2	Comprendere e valutare i rischi pratici che derivano dal P2P: maleware, software piratato, rallentamento delle prestazioni del PC

6	SICUREZZA DEI DATI		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
6.1	Gestire i dati sul PC in maniera sicura	**6.1.1**	Riconoscere e definire lo storage; distinguere tra vantaggi e svantaggi dei tipi principali: NAS (Network Attached Storage), DAS (Direct Attached Storage) e SAN (Storage Area Network)
		6.1.2	Cos'è il backup, a cosa serve; come fare il backup manuale; comprendere il vantaggio di fare un backup utilizzando *Cronologia file di Windows 10*; ripristinare i file salvati
		6.1.3	Come ripristinare i file salvati e come escludere dal backup i file che non vogliamo copiare
		6.1.4	Come fare il backup su Mac, usando Time Machine
		6.1.5	Cos'è il cloud e come funziona OneDrive; riconoscere e utilizzare software specifici dedicati al backup
6.2	La procedura per stampare fogli di calcolo	**6.2.1**	Cos'è il ripristino di sistema e come farlo su Windows 10
		6.2.2	Come fare il ripristino di sistema su Mac
6.3	Eliminare i dati in modo permanente	**6.3.1**	Cos'è e come funziona il cestino
		6.3.2	Conoscere software specifici che consentono di eliminare definitivamente file

www.certipass.org

- ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE DELLE COMPETENZE DIGITALI EIPASS
- ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA – DIRETTIVA 170/2016
- ENTE ISCRITTO AL WORKSHOP ICT SKILLS, ORGANIZZATO DAL CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION)
- ENTE ADERENTE ALLA COALIZIONE PER LE COMPETENZE DIGITALI – AGID
- ENTE ISCRITTO AL PORTALE DEGLI ACQUISTI IN RETE DELLA PUBBLICA AMMINISTRAZIONE, MINISTERO DELL'ECONOMIA E DELLE FINANZE, CONSIP (L. 135 7 AGOSTO 2012) | MEPA
- ENTE PRESENTE SU PIATTAFORMA SOFIA E CARTA DEL DOCENTE

PER INFORMAZIONI SULLE CERTIFICAZIONI INFORMATICHE **VISITA IL SITO**

www.eipass.com