EUROPEAN INFORMATICS PASSPORT

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 al fine di acquisire le competenze informatiche per operare come Data Protection Officer, sia nella Pubblica Amministrazione sia nel privato.

Certipass

Centro Studi

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, 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 | Nuove tecnologie e tutela della personalità

Modulo 2 | La protezione dei dati personali: il GDPR

Modulo 3 | Il DPO: designazione, posizione e compiti

Modulo 4 | Il Codice dell'Amministrazione Digitale

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.

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

Modulo 1

NUOVE TECNOLOGIE E TUTELA DELLA PERSONALITÀ

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato sa definire i cambiamenti portati dalla società della tecnica e dell'informazione, conoscendone le implicazioni sul diritto.

Sa definire il diritto dell'informatica e l'informatica giuridica. Conosce e identifica gli interessi tutelati in relazione alle nuove tecnologie.

Il Candidato certificato conosce i diritti in relazione all'identità digitale, in particolare il diritto alla riservatezza e la sua evoluzione nel tempo in Europa. Inoltre sa definire il concetto di privacy e conosce il codice della privacy in relazione alla protezione dei dati e allo sviluppo tecnologico.

Contenuti del modulo

Le nuove tecnologie e i diritti della personalità

- Introduzione
- Diritto dell'informatica e informatica giuridica
- Nuove tecnologie e interessi tutelati
- L'identità al vaglio delle nuove tecnologie informatiche
- Il diritto all'oblio

Il diritto alla riservatezza

- Le origini del diritto alla riservatezza
- La legislazione europeo in materia di tutela della riservatezza
- Il ruolo delle informazioni e il nuovo concetto di privacy
- Il codice della privacy

1 | LE NUOVE TECNOLOGIE E I DIRITTI DELLA PERSONALITÀ

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
1.1	Introduzione	**1.1.1**	La società della tecnica e dell'informazione
		1.1.2	Tecnologia e diritto
1.2	Diritto dell'informatica e informatica giuridica	**1.2.1**	Diritto dell'informatica
		1.2.2	Informatica giuridica
1.3	Diritto dell'informatica e informatica giuridica	**1.3.1**	La libertà di espressione in internet
		1.3.2	La tutela dell'onore e della reputazione
		1.3.3	La violazione dell'identità personale
1.4	Diritto dell'informatica e informatica giuridica	**1.4.1**	Il diritto all'immagine
		1.4.2	La violazione del diritto all'immagine in internet
		1.4.3	Il diritto d'autore in internet
		1.4.4	L'eredità digitale
1.5	Diritto dell'informatica e informatica giuridica	**1.5.1**	La decisione di Google Spain
		1.5.2	Le sentenze in materia di diritto all'oblio

2 | IL DIRITTO ALLA RISERVATEZZA

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
2.1	Le origini dei diritto alla riservatezza	**2.1.1**	Ordinamento europeo
2.2	La legislazione europea in materia di tutela della riservatezza	**2.2.1**	Interventi legislativi precedenti al Reg. Eu. 679/2016
2.3	Il ruolo delle informazioni e il nuovo concetto di privacy	**2.3.1**	Le fonti normative di rango internazionale e europeo in materia di privacy
		2.3.2	La Convenzione di Strasburgo del 1981 e la Direttiva 46/95/CE
		2.3.3	La Legge n. 675 del 1996
		2.3.4	La direttiva 2002/58 CE
2.4	Il codice della privacy	**2.4.1**	La protezione dei dati e lo sviluppo tecnologico nel Regolamento Europeo 679 del 2016

Modulo 2

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
- 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 profilazione
- 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 responsabile del trattamento
- Il responsabile 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 garanti della protezione dei dati personali
- I rimedi per la violazione dei dati personali

1 | IL GENERAL DATA PROTECTION REGULATION (GDPR)

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
1.1	I tratti distintivi del GDPR	**1.1.1**	Il campo di applicazione territoriale del GDPR
1.2	La definizione di dato personale nel GDPR	**1.2.1**	Dato personale della persona fisica
		1.2.2	Dati personali sensibili e giudiziari
1.3	Il principio di responsabilizzazione	**1.3.1**	Approccio applicativo
1.4	I principi applicabili al trattamento dei dati personali	**1.4.1**	Ulteriori principi sanciti dal GDPR
1.5	L'informativa sui dati personali	**1.5.1**	Le modalità dell'informativa
		1.5.2	Le ipotesi di esonero dell'informativa

2 | I DIRITTI DELL'INTERESSATO AL TRATTAMENTO DEI DATI

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
2.1	La profilazione	**2.1.1**	Garanzie per la profilazione
2.2	Il diritto di accesso	**2.2.1**	Tipo di dati a cui si ha accesso
2.3	Il diritto all'oblio	**2.3.1**	Casi in cui è possibile esercitare il diritto all'oblio
2.4	Il diritto alla portabilità dei dati	**2.4.1**	Obiettivi
		2.4.2	Condizioni
2.5	Il diritto di opposizione	**2.5.1**	Definizione

3 | I TITOLARI E I RESPONSABILI DEL TRATTAMENTO

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
3.1	Gli obblighi del titolare e del responsabile del trattamento	**3.1.1**	La Valutazione di impatto sulla protezione dei dati personali
		3.1.2	Il Registro delle attività di trattamento dei dati personali
3.2	Il Responsabile della protezione dei Dati (RPD)	**3.2.1**	Designazione del Responsabile della protezione dei dati
		3.2.2	I compiti del Responsabile della protezione dei dati

4 | SANZIONI E RIMEDI IN CASO DI VIOLAZIONE DEL GDPR			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
4.1	Il Comitato europeo per la protezione dei dati	**4.1.1**	La Valutazione di impatto sulla protezione dei dati personali
4.2	Il principio dello sportello unico: one stop shop	**4.2.1**	Lead authority
4.3	Le sanzioni	**4.3.1**	Criteri
		4.3.2	Entità
4.4	La violazione dei dati personali (Data breach)	**4.4.1**	La notifica
4.5	Le autorità nazionali garanti della protezione dei dati personali	**4.5.1**	Ruolo e compiti
4.6	I rimedi per la violazione dei dati personali	**4.6.1**	Diritti

Modulo 3

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 *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
1.1	La nascita del Data Protection Officer	**1.1.1**	Riconoscere e definire la nascita della figura del DPO
2.1	Il Data Protection Officer in Italia	**2.1.1**	Riconoscere e definire l'introduzione della figura del DPO con riferimento all'Italia
3.1	Il Data Protection Officer nel Regolamento europeo sulla privacy	**3.1.1**	Riconoscere e definire il ruolo del DPO come attribuito dal Regolamento

2 | NOMINA OBBLIGATORIA DEL RPD			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
2.1	Definizione di «autorità pubblica o di organismo pubblico»	**2.1.1**	Riconoscere e definire il concetto di «autorità pubblica o di organismo pubblico»
2.2	Definizione di «monitoraggio regolare e sistematico»	**2.2.1**	Riconoscere e definire il concetto di «monitoraggio regolare e sistematico»
2.3	Definizione di «larga scala»	**2.3.1**	Riconoscere e definire il concetto di «larga scala»
2.4	Definizione di «attività principali»	**2.4.1**	Riconoscere e definire il concetto di «attività principali»
2.5	Soggetti a cui spetta nominare il RPD	**2.5.1**	Identificare i soggetti a cui spetta nominare il RPD
2.6	Nomina di un unico RPD	**2.6.1**	Descrivere le procedure di nomina del RPD
2.7	Requisiti particolari del RPD	**2.7.1**	Definire i requisiti particolari che deve possedere il RPD
2.8	L'atto di designazione del RPD	**2.8.1**	Definire come avviene la designazione del RPD

3 | POSIZIONE DEL RPD			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
3.1	Coinvolgimento del RPD	**3.1.1**	Identificare quando e come deve essere coinvolto il RPD nelle questioni riguardanti la protezione dei dati personali
3.2	Sostegno del RPD	**3.2.1**	Riconoscere come il titolare e il responsabile del trattamento devono sostenere il RPD nell'esecuzione dei suoi compiti
3.3	L'autonomia del RPD	**3.3.1**	Definire l'indipendenza nello svolgimento del ruolo
3.4	Il conflitto di interessi	**3.4.1**	Definire il conflitto di interessi che può incorrere nello svolgimento del ruolo

4 | COMPITI DEL RPD			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
4.1	Gli ulteriori compiti e funzioni del RPD	**4.1.1**	Descrivere in che misura al RPD possono essere attribuiti ulteriori compiti e funzioni
4.2	Conoscenze e caratteristiche personali del RPD	**4.2.1**	Definire quali conoscenze e caratteristiche deve possedere il RPD per operare

5 | COMPITI DEL RPD			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
5.1	Gli ulteriori compiti e funzioni del RPD	**5.1.1**	Descrivere in che misura al RPD possono essere attribuiti ulteriori compiti e funzioni
5.2	Conoscenze e caratteristiche personali del RPD	**5.2.1**	Definire quali conoscenze e caratteristiche deve possedere il RPD per operare

6 | LA PRIVACY BY DESIGN E LA PRIVACY BY DEFAULT			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
6.1	La privacy by design	**6.1.1**	Definire il principio della privacy by design e descrivere la sua applicazione
6.2	La pseudonimizzazione	**6.2.1**	Identificare e descrivere la metodologia della pseudonimizzazione
6.3	La privacy by default	**6.3.1**	Definire il principio della privacy by default e descrivere la sua applicazione

Modulo 4

IL CODICE DELL 'A MMINISTRAZIONE DIGITALE

Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato conosce 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
- Il Decreto semplificazioni

Il Codice dell'Amministrazione Digitale

- Gli obiettivi e le strategie
- I diritti di cittadinanza digitale
- I principi generali
- Organizzazione delle Pubbliche Amministrazioni. Rapporti fra Stato, Regioni e autonomie locali

Gli strumenti dell'informatizzazione: firme elettroniche e documento informatico

- La Firma Elettronica
- Il documento informatico

L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni

- Formazione, gestione e conservazione dei documenti informatici
- I dati pubblici
- La piattaforma digitale nazionale dati
- L'accesso telematico ai servizi della Pubblica Amministrazione
- Il sistema pubblico di connettività

Sviluppo, acquisizione e riuso di sistemi informatici nelle Pubbliche Amministrazioni

- Criteri di scelta
- L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni
- Il diritto di accesso
- La pubblicazione dei dati e la trasparenza
- L'Agenda Digitale
- Le criticità della digitalizzazione della amministrazione: la sicurezza e il digital divide

1 | IL RINNOVAMENTO DELLA PUBBLICA AMMINISTRAZIONE

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
1.1	Informatizzazione - Dematerializzazione - Digitalizzazione - E-Government	**1.1.1**	Informatizzazione
		1.1.2	E-Government
		1.1.3	La dematerializzazione
		1.1.4	La digitalizzazione
1.2	L'Amministrazione nell'era digitale	**1.2.1**	Cenni alle tappe evolutive dei processi di informatizzazione
		1.2.2	Il d.lgs. 12 febbraio 1993
		1.2.3	Il d.lgs. 196/2003
1.3	Il Codice dell'amministrazione digitale e le recenti modifiche	**1.3.1**	La Legge Madia
1.4	Il Decreto semplificazioni	**1.4.1**	Definizioni

2 | IL CODICE DELL'AMMINISTRAZIONE DIGITALE

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
2.1	Gli obiettivi e le strategie	**2.1.1**	Strumenti di cittadinanza digitale
2.2	I diritti di cittadinanza digitale	**2.2.1**	Il Domicilio digitale
		2.2.2	L'identità digitale
		2.2.3	Il Sistema Pubblico di Identità Digitale (SPID)
		2.2.4	La Carta d'Identità Elettronica
2.3	I principi generali	**2.3.1**	Pagamenti con modalità informatiche
		2.3.2	Comunicazioni tra imprese e amministrazioni pubbliche
		2.3.3	Diritto a servizi online semplici e integrati
		2.3.4	L'alfabetizzazione informatica

2.4	Organizzazione delle Pubbliche Amministrazioni. Rapporti fra Stato, Regioni e autonomie locali	**2.4.1**	Codice di condotta tecnologica
		2.4.2	Rapporti tra Stato, Regioni e autonomie locali
		2.4.3	L'Agenzia per l'Italia Digitale
		2.4.4	Digitalizzazione e riorganizzazione
		2.4.5	Responsabile per la transizione digitale e difensore civico digitale
		2.4.6	Piattaforma nazionale per la governance della trasformazione digitale

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

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
3.1	La Firma Elettronica	**3.1.1**	Indicazioni normative
3.2	Il documento informatico	**3.2.1**	Definizione

4 | L'INFORMATIZZAZIONE E LA TRASPARENZA NELLE PUBBLICHE AMMINISTRAZIONI

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
4.1	Formazione, gestione e conservazione dei documenti informatici	**4.1.1**	La trasmissione dei documenti informatici
		4.1.2	Valore giuridico della trasmissione
		4.1.3	Trasmissione dei documenti tra le pubbliche amministrazioni
		4.1.4	La trasmissione via PEC e la cooperazione applicativa
4.2	I dati pubblici	**4.2.1**	La disponibilità dei dati pubblici
4.3	La piattaforma digitale nazionale dati	**4.3.1**	Definizione
		4.3.2	Disponibilità dei dati generati nella fornitura di servizi in concessione
		4.3.3	Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni
		4.3.4	Siti internet delle pubbliche amministrazioni

		4.3.5	Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni
4.4	L'accesso telematico ai servizi della Pubblica Amministrazione	**4.4.1**	Istanza e dichiarazioni presentate alle pubbliche amministrazioni per via telematica
		4.4.2	Anagrafe nazionale della popolazione residente - ANPR
4.5	Il sistema pubblico di connettività	**4.5.1**	Obiettivi e modalità

5 | SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
5.1	Criteri di scelta	**5.1.1**	Il Cloud computing
5.2	L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni	**5.2.1**	Il Responsabile per la trasparenza
		5.2.2	La pubblicazione dei dati e la trasparenza
5.3	Il diritto di accesso	**5.3.1**	I titolari del diritto di accesso
		5.3.2	Art. 5 d.lgs. 33/2013: l'Accesso civico
		5.3.3	I limiti al diritto di accesso
		5.3.4	L'obbligo di motivazione dei rifiuto
		5.3.5	L'oggetto della richiesta: gli atti accessibili
		5.3.6	Il diritto di accesso previsto dalla L. 241/1990, il diritto di accesso civico e il diritto di accesso del "FOIA"
5.4	La pubblicazione dei dati e la trasparenza	**5.4.1**	Documenti e informazioni da pubblicare
5.5	L'Agenda Digitale	**5.5.1**	L'Agenza Digitale italiana
		5.5.2	L'Agenzia per l'Italia Digitale
5.6	Le criticità della digitalizzazione della amministrazione: la sicurezza e il digital divide	**5.6.1**	Il c.d. "digital divide" (divario digitale)

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 cittadinanza digitale e i nuovi diritti

- Gli strumenti

La posta elettronica certificata (PEC)

- Invio di un messaggio tramite PEC
- La procedura di invio di un messaggio tramite PEC
- Il sigillo elettronico

L'archiviazione dei documenti digitali

- Il Documenti informatico
- Le copie, i duplicati, gli estratti analogici e informatici e il loro valore

1 | LA CITTADINANZA DIGITALE E I NUOVI DIRITTI

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
1.1	Gli strumenti	**1.1.1**	Il domicilio digitale
		1.1.2	La firma elettronica
		1.1.3	Il sigillo elettronico

2 | LA POSTA ELETTRONICA CERTIFICATA (PEC)

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
2.1	Invio di un messaggio tramite PEC	**2.1.1**	Fasi
2.2	La procedura di invio di un messaggio tramite PEC	**2.2.1**	Il Registro generale degli indirizzi elettronici
		2.2.1	La trasmissione via PEC
2.3	Il sigillo elettronico	**2.3.1**	Che cos'è il sigillo elettronico. Le disposizioni sono contenute nel Regolamento eIDAS

3 | L'ARCHIVIAZIONE DEI DOCUMENTI DIGITALI

Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *L'utente certificato sa...*	
3.1	Il Documento informatico	**3.1.1**	Fasi
3.2	Le copie, i duplicati, gli estratti analogici e informatici e il loro valore	**3.2.1**	Le copie informatiche di documenti analogici
		3.2.2	Le copie analogiche di documenti informatici

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. Cono- sce 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 *L'utente certificato conosce...*		Skills/Capacità pratiche *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	**2.1.1**	Riconoscere i problemi connessi alla sicurezza dei propri dati personali
		2.1.2	Comprendere e definire il concetto di social engineering
		2.1.3	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
		2.1.4	Come difendersi dagli attacchi di ingegneria sociale
1.3	Misure per la sicurezza dei file	**3.1.1**	Definire una macro e comprenderne le implicazioni, in tema di sicurezza
		3.1.2	Cambiare le impostazioni delle macro in Centro protezione
		3.1.3	Impostare una password per i file di Office

2 | MALWARE			
Knowledge/Conoscenze *L'utente certificato conosce...*		Skills/Capacità pratiche *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 *L'utente certificato conosce...*		Skills/Capacità pratiche *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 *L'utente certificato conosce...*		Skills/Capacità pratiche *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 *L'utente certificato conosce...*		Skills/Capacità pratiche *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 *L'utente certificato conosce...*		Skills/Capacità pratiche *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

- 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