EIPASS Pubblica Amministrazione

Programma analitico d'esame

Premessa

L'acquisizione di competenze digitali è un fattore vitale per chi è impegnato nelle Pubbliche Amministrazioni. Proprio per questo, gli interventi legislativi in favore della digitalizzazione si moltiplicano con l'intenzione di creare un sistema integrato ed efficiente al servizio dei cittadini. Non si può dunque prescindere da una formazione attualizzata di chi è chiamato a creare e attivare questo sistema: i dipendenti pubblici.

Il programma di digitalizzazione delle PA, basato sugli obiettivi di crescita dettati dall'Agenda Digitale Europea e definiti dall'Agenda Digitale Italiana, prevede il suo completamento entro il 2020 e, naturalmente, presenta numerose tappe intermedie che dovranno essere raggiunte molto prima: questo significa che le amministrazioni pubbliche devono essere nelle condizioni di fornire quanto prima servizi digitalizzati efficaci, per allinearsi alle prerogative indicate e raggiungere gli obiettivi prefissati.

Le attuali disposizioni legislative presenti nel Codice dell'Amministrazione Digitale (CAD) stabiliscono "che i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni" (CAD I, Art. 3.1) al fine di ottimizzare la produttività del lavoro, e l'efficienza e trasparenza degli uffici che servono il pubblico. Nel Codice dell'Amministrazione Digitale (CAD), sono chiaramente stabiliti gli standard moderni ed innovativi per imprese e Pubblica Amministrazione.

Il sistema produttivo e sociale non può più attendere: le Pubbliche Amministrazioni devono evolvere digitalmente, seguendo il percorso tracciato dall'Agenda Digitale. Per completarlo con successo, è imprescindibile investire nell'aggiornamento continuo del personale addetto e nell'introduzione delle nuove tecnologie per conseguire, in tempi rapidi, un livello adeguato di efficienza e trasparenza.

Molte sono le novità nel settore digitale nell'ambito delle Pubbliche Amministrazioni, sia a livello pratico che normativo.

Spesso gli operatori sono in difficoltà nel seguire le rapide trasformazioni e le repentine implementazioni che caratterizzano la pratica e i servizi offerti dalle PA, per cui necessitano di un solido ed efficace supporto formativo che permetta loro di rispondere al meglio alla nuova realtà digitale, per sfruttarne le potenzialità e le opportunità di controllo e immediatezza, in vista del continuo innalzamento delle perfomance e, quindi, della qualità dei servizi offerti ai cittadini.

Le Pubbliche Amministrazioni, peraltro, sono già quotidianamente alla prese con numerose attività informatizzate, per cui è indispensabile possedere competenze digitali specifiche:

- gestione dei procedimenti amministrativi;
- archiviazione dei documenti;
- pagamenti elettronici;

- fatturazione elettronica;
- accessibilità;
- giustizia digitale;
- circolazione e scambio dati.

Perché tutti questi servizi possano essere avviati e forniti nei modi e nei tempi prospettati dall'Agenda Digitale, è necessario un forte impegno di istituzioni e persone.

Ma è chiaro che gli obiettivi prefissati non saranno mai raggiunti se non si terrà nella dovuta considerazione la centralità dell'informatica e delle relative competenze che, in prima battuta, gli operatori stessi devono possedere ed impiegare giorno per giorno.

Certipass

Comitato Tecnico-Scientifico

Disclaimer

Certipass ha redatto il presente documento programmatico in base agli standard e ai riferimenti Comunitari vigenti in materia di competenze a carattere digitale. Il documento riporta le informazioni riguardanti il Programma di certificazione "EIPASS® Pubblica Amministrazione". Certipass non si assume alcuna responsabilità derivante dall'applicazione in ambito diverso dallo stesso, neanche da informazioni elaborate da terzi in base ai contenuti del presente Programma.

Certipass si riserva di aggiornare il presente documento a propria discrezione, in ogni momento e senza darne preavviso, pubblicando le modifiche effettuate. L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

Copyright

Programma analitico d'esame EIPASS Pubblica Amministrazione

Il percorso di certificazione EIPASS Pubblica Amministrazione si struttura a partire dalle basi normative per comprendere le implicazioni che queste comportano nella pratica operativa.

Dopo l'essenziale modulo sull'informatica di base, segue un'agile trattazione sulle innovazioni introdotte dall'Agenda Digitale in cui verranno descritti ed analizzati i principali lineamenti normativi introdotti dal CAD (Codice dell'Amministrazione Digitale).

Il terzo modulo è dedicato ai documenti informatici e alla loro archiviazione. Comprende, inoltre, un'esauriente analisi delle normative e delle disposizioni pratiche riferite all'impiego della firma elettronica o digitale.

Un ampio e dettagliato spazio è riservato alla PEC (Posta Elettronica Certificata), essenziale strumento teso a sostituire la tradizionale posta raccomandata AR, con tutte le implicazioni pratiche e normative che ne derivano.

L'ultimo modulo si occupa delle problematiche relative alla privacy, chiarisce gli elementi normativi connessi alla protezione dei dati personali e affronta le implicazioni riguardanti la sicurezza informatica.

Tutte le lezioni sono illustrate da esempi che permettono di comprendere a fondo le varie tematiche, chiarendo gli aspetti più complessi inerenti le trasformazioni che stanno interessando lo strategico settore delle Pubbliche Amministrazioni.

Si indicano di seguito gli argomenti oggetto di analisi e di verifica dei cinque moduli previsti:

Modulo 1: Informatica di base e www

Modulo 2: Codice dell'Amministrazione Digitale

Modulo 3: Documento informatico, conservazione sostitutiva ed archiviazione

Modulo 4: Posta Elettronica Certificata - CEC-PAC, PEC-ID

Modulo 5: La Protezione dei dati personali

Modalità di certificazione e valutazione

Il rilascio della certificazione avverrà previo sostenimento e superamento di esami online (1 per modulo). Ciascuna sessione avrà una durata di 30 minuti.

Nel corso della sessione il Candidato dovrà effettuare 30 test inerenti il modulo interessato, consistenti in domande a scelta multipla, quesiti vero/falso o simulazioni operative. I test saranno selezionati dal Sistema di rete in modalità casuale. Sarà sempre il sistema che calcolerà la percentuale di risposte esatte fornite decretando il superamento o meno dell'esame ed esprimendo in merito la valutazione dello stesso: non essendovi alcun intervento da parte di un Docente/Esaminatore, viene garantita l'obiettività dell'esito conseguito.

L'Esaminatore, figura autorizzata da Certipass previo conseguimento di apposita qualifica, si limiterà quindi al controllo del rispetto delle previste procedure.

La valutazione finale sarà espressa in percentuale. Ciascun esame si riterrà superato previa l'attribuzione al Candidato di una percentuale minima di risposte esatte pari o superiore al 75% del totale. L'eventuale, mancato superamento di uno o più dei previsti moduli comporterà la ripetizione degli stessi attraverso una prova suppletiva.

1 Informatica di base e www

Obiettivo del modulo

Il modulo intende accertare nel candidato il possesso delle competenze digitali relative sia ai fondamenti dell'hardware, posti alla base dell'Information Technology, che all'utilizzo delle più comuni funzioni di un Sistema Operativo ad interfaccia grafica, con particolare attenzione alla gestione ed alla organizzazione dei file e delle cartelle.

In particolare, il candidato dovrà mostrarsi in grado di:

- Descrivere i concetti generali della Tecnologia dell'Informazione;
- Classificare i computer;
- Descrivere la principali componenti costituenti un computer;
- Descrivere le periferiche di input e di output;
- Descrivere le varie tipologie di memoria e di dispositivi per la memorizzazione;
- Gestire adeguatamente le risorse laboratoriali;
- Misurare le informazioni utilizzando le più comuni unità di misura;
- Descrivere ed applicare all'utilizzo pratico i concetti generali per la gestione di un sistema operativo ad interfaccia grafica (GUI);
- Installare e disinstallare un programma applicativo;
- Gestire autonomamente file e cartelle.

Secondariamente, si certificano le competenze possedute in ordine all'utilizzo di servizi di rete.

In particolare, il candidato dovrà mostrarsi in grado di:

- Utilizzare un Browser per la navigazione in rete
- Utilizzare efficacemente un motore di ricerca
- Utilizzare servizi di posta elettronica
- Utilizzare aree riservate per la condivisione e la trasmissione di dati e documenti

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
1.0 Conoscere i concetti generali della Tecnologia dell'Informazione	1.0.1 Analisi di base componenti hardware	a. Indicare la corretta accezione di base del termine "hardware" b. Indicare i principali componenti hardware di un computer
	1.0.2 Classificazione dei computer	a. Descrivere un computer, definendo le differenze caratterizzanti le varie tipologie disponibili (PC, notebook, laptop, smartphone, mainframe, ecc.)
	1.0.3 Analisi e gestione dei dispositivi di memoria	a. Distinguere e denominare i diversi tipi di memoria centrale presenti nel computer (RAM, ROM, EPROM, CACHE) in relazione alla loro tipologia e funzione b. Riconoscere i principali tipi di dispositivi di archiviazione (memorie di massa), quali: CD, DVD, "pendrive", dischi fissi, archivi remoti, unità di rete
	1.0.4 Porte di input/output	a. Descrivere caratteristiche e differenze fra le porte di input disponibili su un computer (USB, seriale, parallela) b. Descrivere caratteristiche e differenze fra le porte di output disponibili su un computer (VGA, audio, ecc.)
	1.0.5 Le periferiche di Input/Output	a. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di output b. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di output c. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di sia di input che di output
1.1 Ottimizzare le risorse	1.1.1 Gestione delle risorse	a. Classificare le risorse di laboratorio in base alle caratteristiche delle stesse b. Individuare ed applicare i migliori criteri di ergonomia c. Individuare corretti principi di condivisione delle risorse disponibili in base ai vari possibili contesti operativi

1.2 Comprendere i concetti generali per la gestione di un sistema operativo ad interfaccia grafica	1.2.1 Impostazione e personalizzazione di un Sistema Operativo ad interfaccia grafica	a. Descrivere le principali procedure per modificare la configurazione dell'interfaccia grafica e delle impostazioni di "default" (impostazioni audio, impostazioni risoluzioni schermo, ecc.) b. Indicare la corretta procedura di installazione di un "software applicativo" c. Indicare la corretta procedura di disinstallazione di un "software applicativo"
1.3 Comprendere le modalità e le funzionalità di gestione di file e cartelle	1.3.1 Concettualizzazione di base	a. Indicare e denominare i supporti hardware utili alla archiviazione di file e cartelle b. Indicare come un Sistema Operativo ad interfaccia grafica (GUI) visualizza le unità disco, le cartelle, i file e la struttura nidificata di questi ultimi (funzione dei segni + e – accanto alle cartelle) c. Descrivere e differenziare le più diffuse modalità di misurazione dei file e delle cartelle (KByte, MByte, GByte) d. Indicare la procedura utile alla creazione di copie di backup di file e cartelle su dispositivi remoti; viceversa, indicare le modalità di ripristino di copie di backup precedentemente create
	1.3.2 Gestione di cartelle	a. Creare, eliminare, denominare e rinominare, aprire, chiudere, comprimere una cartella b. Organizzare il contenuto di una cartella secondo criteri differenti c. Accedere alle proprietà di una cartella per analizzarle e modificarle

	1.3.3 Gestione di file	a. Indicare l'uso dell'estensione di un file, e riconoscere in base alla loro estensione i file di tipo più comune b. Archiviare un file attribuendogli un nome, una destinazione, un formato c. Rinominare un file precedentemente creato d. Modificare l'ordine dei file visualizzati in una cartella, scegliendo tra le opzioni disponibili e. Dalle proprietà di un file, riconoscere e possibilmente modificare le sue impostazioni sorgenti
1.4 Utilizzare un Browser per la navigazione in rete	1.4.1 Definire caratteristiche e funzionalità del Browser	a. Definire cosa è un Browser b. Discriminare funzioni e strumenti impiegabili in un Browser c. Orientarsi fra le opzioni disponibili per la gestione del Browser
	1.4.2 Utilizzare un Browser	a. Impostare la pagina iniziale del Browser utilizzando le opzioni disponibili b. Gestire le funzioni di cronologia delle esplorazioni c. Gestire le funzioni di eliminazione d. Gestire le funzioni di protezione e. Modificare opportunamente le impostazioni di visualizzazione f. Modificare la barra strumenti del Browser g. Chiudere una scheda/tutte le schede precedentemente aperte h. Gestire le preferenze i. Gestire le opzioni di visualizzazione j. Gestire la barra strumenti k. Impostare un criterio di protezione

1.5 Utilizzare efficacemente un motore di ricerca	1.5.1	Gestire le funzioni di un motore di ricerca	a. Definire il concetto di indicizzazione b. Ricercare un argomento di interesse utilizzando parole, simboli, stringhe frasali a seconda dei casi c. Salvare pagine contenenti le informazioni desiderate d. Traslare, quando possibile, il contenuto di pagine in documenti di testo e. Utilizzare un motore di ricerca per il reperimento di immagini f. Utilizzare un motore di ricerca per il reperimento di eventi g. Utilizzare funzioni di traduzione contestuali al motore di ricerca h. Utilizzare opportune protezioni nei confronti di siti non certificati i. Bloccare siti non adeguati all'Utenza
1.6 Utilizzare servizi di posta elettronica	1.6.1	Caratteristiche e funzionalità dei servizi di posta elettronica	a. Definire cosa è un Client b. Definire cosa è un Account c. Definire cosa è un Server di Posta elettronica d. Definire i concetti di Userid e Password e. Discriminare le caratteristiche dei servizi di posta elettronica rispetto a quelle di altri servizi di comunicazione in rete

	1.6.2	Utilizzare un servizio di posta elettronica	a. Impostare un account di posta elettronica in base a criteri di invio e ricezione messaggi b. Impostare un client di posta elettronica c. Impostare correttamente le opzioni di invio e ricezione rese disponibili dal client o dal server impiegato d. Impostare un criterio di priorità e. Impostare un criterio di invio f. Impostare un criterio di lettura del messaggio da parte del destinatario g. Allegare al messaggio un file, una cartella h. Ricercare un messaggio all'interno della posta inviata o ricevuta i. Impostare un elenco di posta indesiderata j. Bloccare un mittente k. Impostare un criterio di protezione alla posta ricevuta l. Discriminare messaggi di posta elettronica pericolosi per la propria privacy
1.7 Utilizzare aree riservate per la condivisione e la trasmissione di dati e documenti	1.7.1	Accedere ad un'area riservata	a. Registrarsi in un'area riservata b. Identificarsi in un'area riservata c. Modificare i dati relativi all'Account Utente d. Effettuare il download di documenti

2 Codice dell'Amministrazione Digitale: Principi Generali alla luce delle modifiche apportate dall'Agenda Digitale. Trasparenza Amministrativa

Obiettivo del modulo

Il Codice dell'Amministrazione Digitale (CAD), varato con decreto legislativo 7 marzo 2005 n. 82, rappresenta la codificazione del duplice obbiettivo di riassetto e semplificazione delle normative e dei lineamenti istituzionali relativi alla Pubblica Amministrazione.

Ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando al meglio le tecnologie dell'informazione e della comunicazione nei rapporti interni tra le diverse amministrazioni, e tra queste e i privati.

Il modulo presente intende accertare nel candidato il livello di conoscenza 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 dovrà conoscere:

- 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

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
2.0 Le principali leggi in materia di informatizzazione della pubblica amministrazione	2.0.1 Dal D.lgs. n.39/1993 al Codice dell'Amministrazione digitale (CAD)	d. Prima definizione di un documento digitale e. D. Lgs. n. 39/1993 f. Codice dell'Amministrazione Digitale (CAD)
	2.0.2 Principi ispiratori, finalità e ambito di applicazione del nuovo CAD	l. Principio di responsabilità m. Principio di legalità n. Principio di imparzialità o. Diritto dei cittadini e delle imprese all'uso delle tecnologie verso amministrazioni e gestori di servizi pubblici (art.3) p. Opportunità per le amministrazioni di capitalizzare il "dividendo dell'efficienza" consentito dall'innovazione digitale (art.15) q. Obbligo di coordinarsi, di lavorare insieme, di fare sistema (art.14)
	2.0.3 Il governo dell'informatizzazione nella PA: dall'Aipa a DigitPA	a. Aipa b. Cnipa c. D.P.C.M. 27 settembre 2001 d. Da DigitPA a AgID
2.1 I principali cambiamenti introdotti dalla riforma del CAD	2.1.1 Aspetti normativi e tematiche affrontate dal CAD	j. Validità dei documenti indipendente dal supporto k. Formazione, gestione e conservazione digitale dei documenti; protocollo informatico e fascicolo elettronico l. Pagamenti elettronici m. Comunicazioni elettroniche tra imprese e amministrazioni n. Disponibilità e fruibilità dei dati delle pubbliche amministrazioni o. Continuità operativa, disaster recovery e sicurezza digitale p. Siti pubblici e trasparenza, moduli online e trasmissione delle informazioni via web

		q. Patrimonio informativo delle amministrazioni e basi di dati di interesse nazionale r. Servizi in rete e Customer satisfaction dei cittadini s. Accesso ai servizi in rete t. Sfida agli open data
2.2 I diritti dei cittadini e delle imprese sanciti dal CAD	2.2.1 Il diritto all'uso delle tecnologie (Art.3)	f. Le autorità di riferimento g. Posizioni rilevanti in merito h. Ipotesi in cui la PA deve far ricorso alle tecnologie telematiche
	2.2.2 La partecipazione al procedimento amministrativo informatico (Artt. 4 e 9)	m. Obbligo di gestione informatica dei procedimenti amministrativi n. Obbligo di informare sulle modalità di visione dei documenti elettronici di proprio e personale interesse o. Obbligo di pubblicazione dell'indirizzo istituzionale di Posta elettronica certificata della PA di riferimento
	2.2.3 Le comunicazioni elettroniche con la pubblica amministrazione	a. Qualità dei servizi resi e soddisfazione dell'utenza (Art.7)
2.3 Trasparenza e obblighi di pubblicità delle Pubbliche Amministrazioni	2.3.1 Pubblicità legale e Albo pretorio on-line	e. Obbligo di pubblicazione di atti e provvedimenti nei siti pertinenti delle PA f. Albo pretorio online g. Modalità di pubblicazione dei documenti nell'Albo online
	2.3.2 Caratteristiche e contenuto dei siti istituzionali	a. Accessibilità b. Contenuti minimi c. Linee guida per i siti web della PA d. Interoperabilità
	2.3.3 Le banche dati delle pubbliche amministrazioni	a. Informazione geograficamente localizzata b. Anagrafe Nazionale della Popolazione Residente

3 Documento informatico, conservazione sostitutiva ed archiviazione

Obiettivo del modulo

Il modulo intende accertare nel candidato il possesso di competenze relative alle modalità di archiviazione dei documenti digitali e alla disciplina legata alla pratica di conservazione dei documenti elettronici. In successione saranno affrontate le tematiche relative alla dematerializzazione degli archivi informatici, alle copie digitali dei documenti e in generale alla conservazione degli stessi.

Ogni aspetto sarà considerato sempre facendo riferimento al quadro normativo più aggiornato, l'azione di verifica valuterà la comprensione anche di quest'ultimo, insieme all'acquisizione particolareggiata delle pratiche e degli elementi normativi che riguardano la firma digitale ed elettronica.

In particolare, il candidato dovrà mostrare la propria preparazione in ordine ai seguenti argomenti:

- Digitalizzazione e archiviazione documentale
- Dematerializzazione degli archivi
- Disciplina probatoria dei documenti elettronici
- Copie digitali
- Conservazione dei documenti elettronici
- Firme elettroniche e digitali

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
3.0 Digitalizzazione e archiviazione documentale	3.0.1 L'archivio e i flussi documentali	a. Concetto di archivio b. Classificazione c. Fascicolo d. Flussi documentali
	3.0.2 Gli "oggetti" dell'archivio digitale	a. Regole per l'archiviazione e conservazione dei documenti in formato digitale b. Documenti analogici obbligatori
3.1 Documenti informatici	3.1.1 La dematerializzazione degli archivi	a. Definizioni introdotte dal Codice dell'Amministrazione Digitale (CAD)
	3.1.2 La disciplina probatoria dei documenti informatici	a. Validità dei documenti informatici b. Apposizione di firma digitale
	3.1.3 Le copie	a. Art. 22 del CAD b. Copie di documenti informatici e loro validità c. Procedure di validazione
3.2 Conservazione dei documenti informatici	3.2.1 Il sistema e i requisiti per la conservazione	a. Caratteristiche del sistema di conservazione b. Differenza tra sistema analogico e sistema digitale di conservazione c. Formati di conservazione d. Pacchetti informativi e. Soggetti coinvolti nel sistema di conservazione
	3.2.2 Il Responsabile della conservazione	a. Funzioni b. Conformità del processo
	3.2.3 Il Manuale della conservazione	a. Elementi essenziali b. Fasi del processo di conservazione sostitutiva
	3.2.4 Nuove regole tecniche per i sistemi di conservazione	a. Regime transitorio

3.3 Firma elettronica	3.3.1 Evoluzione	a. Introduzione b. Primi certificatori accreditati c. Gli organi di vigilanza
	3.3.2 La situazione giuridica oggi	a. Codice civile e firma elettronica b. Efficacia della scrittura privata c. Sottoscrizione autenticata d. Copie di atti pubblici e scritture private e. Codice penale e firma elettronica
	3.3.3 Le firme elettroniche nell'Unione Europea	a. Direttive comunitarie b. Divergenze con la normativa nazionale c. Le Decisioni più recenti
	3.3.4 Legislazione nazionale	a. Tipologie definite dal CAD
	3.3.5 Firma elettronica	a. Firme elettroniche non verificabili b. SSCD c. Firma elettronica avanzata
	3.3.6 Firma digitale	a. Definizione b. Caratteristiche c. Firma elettronica qualificata
	3.3.7 Differenza tra firma digitale e firma elettronica qualificata	a. Certificato qualificato b. Crittografia asimmetrica c. Controllo esclusivo del dispositivo di firma d. Dispositivo sicuro per la generazione della firma e. Requisiti per i dispositivi sicuri per la generazione della firma elettronica qualificata f. Requisiti dei dispositivi per la generazione della firma digitale
	3.3.8 Base tecnologica	a. Crittografia b. Crittografia e firma digitale
	3.3.9 Processo di generazione	a. Fasi della generazione di una firma digitale
	3.3.10 Verifica della firma digitale	a. Fasi del processo di verifica

4 Posta Elettronica Certificata - CEC-PAC, PEC-ID

Obiettivo del modulo

Il modulo intende verificare nel candidato il possesso delle competenze relative all'utilizzo corretto della Posta Elettronica Certificata. Il nuovo sistema di invio e ricezione documenti è uno strumento strategico per le PA e il rapporto con i suoi utenti, può essere utilizzata in qualsiasi contesto nel quale sia necessario avere prova opponibile dell'invio e della consegna di un determinato documento. In altri termini consente di disporre di una prova legalmente valida, con preciso riferimento temporale, dell'avvenuta spedizione di un determinato messaggio, con l'eventuale documentazione allegata, nonché della sua consegna ai destinatari designati.

La Posta Elettronica Certificata sostituisce quindi efficacemente la Posta Raccomandata AR cartacea, rappresentando una notevole semplificazione e un evidente risparmio economico sia per i cittadini e le imprese che per le stesse PA, comprendendo inoltre un minor spreco di tempo e risorse.

Saranno tema di analisi e oggetto di verifica il quadro normativo di riferimento, il regolamento e il funzionamento della PEC, la disciplina di accreditamento e di vigilanza, i decreti succedutisi nel tempo che disciplinano i procedimenti

In particolare il candidato dovrà mostrare la propria preparazione in ordine ai seguenti argomenti.

- Vantaggi e svantaggi dell'utilizzo della PEC
- Quadro normativo di riferimento
- Regolamento e funzionamento della PEC
- Regole tecniche della PEC
- Circolare Cnipa /49 del 24.11.2005 su Accreditamento
- Riferimenti normativi sulla PEC nel Codice dell'Amministrazione Digitale
- Circolare Cnipa /51 del 07.12.2006 su Vigilanza
- Decreto Legge del 29.11.2008 sull'istituzione dell'obbligo di uso della PEC per le PA
- Disposizioni in materia di rilascio e di uso della casella di Pec assegnata ai cittadini
- Decreto Ministeriale 19.03.2013 che individua le regole per l'identificazione del titolare di una PEC
- Elenco gestori PEC

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
4.0 Introduzione alla PEC	4.0.1 Vantaggi e svantaggi	a. Garanzie offerte dalla PEC b. Validazione della PEC c. Identità del mittente d. PEC/FAX
4.1 Il quadro normativo di riferimento	4.1.1 Il quadro normativo di riferimento	a. D. P.R. 11 febbraio 2005 n. 68
4.2 Funzionamento della PEC	4.2.1 Regolamento d'uso della PEC	a. Trasmissione del documento informatico b. Soggetti del servizio c. Obblighi
	4.2.2 Funzionamento della PEC	a. Gli attori b. Controlli c. Schema funzionale d. Funzionalità e. Dati di certificazione f. Ricevute g. Avvisi h. Dominio
4.3 Circolari CNIPA	4.3.1 Accreditamento	a. Modalità di accreditamento b. Documentazione richiesta
	4.3.2 Vigilanza	a. Modalità
4.4 Normative sulla PEC	4.4.1 Contenuti del Codice dell'Amministrazione Digitale	a. Contenuti relativi alla PEC b. Obbligo di registrazione protocollo
	4.4.2 Decreto Legge del 29 novembre 2008 n. 185	a. Obbligo di dotarsi di PEC per tutte le imprese e i professionisti
	4.4.3 Disposizioni in materia di rilascio e di uso della casella di Pec assegnata ai cittadini - CEC-PAC	a. Servizio PostaCertificat@ b. Caratteristiche della CEC-PAC c. Procedura di attivazione
	4.4.4 Regole per l'identificazione, anche in via telematica, del titolare della PEC	a. Criteri di validità e identificazione b. Il servizio PEC-ID

	4.4.5 Decreto Ministeriale 19.03.2013	a. Istituzione dell'Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti b. Caratteristiche dell'INI-PEC c. Modalità di accesso d. Elenco gestori PEC

5 La Protezione dei dati personali

Obiettivo del modulo

Il modulo intende fornire al candidato le necessarie competenze per occuparsi della gestione dei dati personali senza violare le normative sulla privacy e affrontare in modo adeguato le problematiche legate al tema della sicurezza informatica. Il punto di partenza è il Codice per la protezione dei dati personali che trova fondamento nella Carta dei diritti fondamentali dell'Unione europea in cui si colloca il diritto alla riservatezza o privacy. In esso si stabilisce che i dati personali siano trattati solo dietro esplicito consenso; un diritto che afferma la libertà e la dignità della persona, preservandola da quello che può essere definito "potere informatico".

Le nuove tecnologie digitali pongono infatti numerosi interrogativi rispetto alla privacy, in quanto l'utilizzo dei servizi internet, della mail o degli acquisti su internet, e naturalmente anche i rapporti con la PA digitale richiedono continuamente il trattamento dei dati personali che non può essere lasciato ad un uso privo di limitazioni e procedimenti definiti e condivisi.

L'avvento del web 2.0 ha reso ancor più urgente la regolamentazione della privacy e le normative sulla sicurezza informatica in quanto ha reso ancora più diffusa e frequente la pratica della comunicazione sul web con la condivisione di file multimediali di ogni tipologia: dalle foto, ai video, ai messaggi testuali o audio.

Nella trattazione presente nel modulo 5 troverà spazio la normativa sul Garante della privacy e quella relativa ai diritti dell'interessato e alle modalità di fornire il consenso.

Qui in dettaglio gli aspetti affrontati nel modulo:

- Privacy: definizione ed evoluzione
- Codice in materia di protezione dei dati personali
- I diritti dell'interessato
- Le regole in materia di protezione dei dati personali
- Le regole specifiche dei soggetti pubblici
- Privacy e diritto di accesso
- Le misure di sicurezza
- Il *disaster recovery*

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
5.0 Privacy: definizione ed evoluzione	5.0.1 Privacy come diritto alla riservatezza	a. Origini b. Carta dei diritti fondamentali dell'Unione europea
	5.0.2 Nuova dimensione della Privacy	a. Incremento dei dati scambiati b. Necessità di accordi internazionali c. Rischi d. D.L. n.196 del 30.06.2003
5.1 Codice in materia di protezione dei dati personali	5.1.1 Caratteristiche principali	a. Le suddivisioni principali b. La definizione di dato personale e comunicazione c. Ambito di applicazione del Codice d. Finalità e necessità del trattamento dei dati personali
	5.1.2 Figure connesse alla protezione dei dati personali	a. Il garante b. Il titolare c. L'interessato d. Il responsabile e. L'incaricato
5.2 I diritti dell'interessato		a. Diritto a ottenere informazioni sul trattamento dei propri dati b. Diritto alla modifica e alla cancellazione dei propri dati.
5.3 Le regole in materia di protezione dei dati personali	5.3.1 Limiti e obbligazioni delle P.A. in merito al trattamento dati	a. Individuare gli attori coinvolti b. Art.5 della Convenzione di Strasburgo c. La Direttiva Europea 95/46/CE
	5.3.2 Criticità	a. Responsabilità civile b. Danni e risarcimenti c. Cessazione del trattamento
5.4 Le regole specifiche per i soggetti pubblici	5.4.1 Comunicazioni e accessi	a. Limiti e obblighi della PA relativi al trattamento dati dei suoi utenti b. D.P.R. 14 novembre 2002, n. 313

	5.4.2 Dati sensibili	a. Normativa b. Autorizzazioni c. Raccomandazioni del Garante
	5.4.3 Banche dati	a. Visibilità e riservatezza b. Big data c. Open data
5.5 Privacy e diritto di accesso	5.5.1 Esigenze in conflitto: trasparenza e imparzialità contro riservatezza	a. Diritto di accesso b. Condizioni in cui il diritto alla privacy non risulta prioritario
5.6 Il consenso al trattamento dei dati personali	5.6.1 Consenso in forma scritta	a. Art.23 Codice della Privacy
	5.6.2 Validità e modalità del consenso	a. Esplicitazione delle modalità di utilizzo dati b. Casi in cui il trattamento dati è consentito anche in assenza di esplicito consenso
5.7 Le misure di sicurezza	5.7.1 Adozione misure per la protezione dati	a. Art.34 del Codice Privacy b. Art.35 del Codice Privacy c. Misure minime
	5.7.2 Aggiornamento periodico e controllo	a. Novità in materia di sicurezza nel Codice della Privacy b. Decreto semplificazioni c. Reato di frode informatica
	5.7.3 Documento programmatico sulla sicurezza e misure minime	a. Strumenti di autenticazione b. Procedure di aggiornamento c. Sistemi di autorizzazione e protezione da accessi non autorizzati d. Adozione di procedure di backup e. Obbligo di adozione di protezioni crittografiche f. Documento programmatico sulla sicurezza

5.8 Il disaster recovery	5.8.1 Continuità operativa	a. Cause: malfunzionamenti, attacchi esterni, virus b. Priorità applicative c. Protezioni: backup dei dati, ridondanza dei dati, software anti-virus, gruppi di continuità, firewall, centri data alternativi.