PROGRAMMA ANALITICO D'ESAME

EIPASS PUBBLICA AMMINISTRAZIONE

La prima parte del programma è dedicata all'acquisizione di competenze indispensabili per navigare efficacemente in rete e operare in sicurezza, sia in relazione alla creazione e alla conservazione dei dati che al loro scambio in rete.

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.

Segue un'agile trattazione del Codice dell'Amministrazione Digitale, di cui si approfondiscono principi e aggiornamenti.

L' ultimo modulo si occupa delle problematiche relative alla privacy, introducendo il *Regolamento UE 679/2016 e le nuove norme sulla protezione dei dati personali*, ultimo riferimento normativo in materia di trattamento dei dati personali.

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 | Navigazione e cercare informazioni sul Web

Modulo 2 | IT Security

Modulo 3 | PEC, firma digitale e archiviazione dei documenti digitali

Modulo 4 | Il Codice dell'Amministrazione Digitale

Modulo 5 | La protezione dei dati personali: il GDPR

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'Esaminatore, 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

NAVIGARE E CERCARE INFORMAZIONI SUL WEB

Cosa sa fare il Candidato che si certifica con EIPASS Pubblica Amministrazione

Il Candidato certificato possiede le competenze digitali necessarie per utilizzare la rete Internet per la ricerca di informazioni e per un uso consapevole dei servizi online.

Sa distinguere un certificato digitale e sa cosa sia un sito sicuro.

È in grado mettere in atto tutte le azioni necessarie per ridurre al minimo i rischi per la sicurezza del computer, durante la navigazione.

È consapevole del fatto che in rete ci sono molte informazioni non affidabili; sa compararle con altre disponibili, per scegliere quelle più attendibili. Di conseguenza, riconosce i servizi online più adeguati alle proprie esigenze.

Contenuti del modulo

Concetti fondamentali del browsing

- Internet e il Web
- Come gestire la sicurezza

Uso del browser

- Operazioni iniziali
- Schede e finestre
- Configurazione

Strumenti del browser

- Usare la cronologia
- Gestire i *Preferiti*
- Strumenti di interazione con il Web

Eseguire ricerche sul Web

- I motori di ricerca
- Valutazione dell'informazione

Scambio delle informazioni via email

- La casella di posta elettronica
- Le applicazioni per gestire le email
- Creazione e invio dei messaggi
- La gestione dei messaggi

1	CONCETTI FONDAMENTALI DEL BROWSING		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
1.1	Internet e il Web	**1.1.1**	Definire il concetto di *rete informatica* e descrivere il processo storico che ha portato all'attuale struttura di Internet; cosa significa ISP, server e hosting
		1.1.2	Cos'è il browser e a cosa serve; quali sono le caratteristiche principali dei browser più diffusi; perché è importante aggiornare il browser
		1.1.3	Descrivere la composizione dell'URL (Uniform Resource Locator); comprendere il sistema dei livelli del dominio e identificare quelli più diffusi
		1.1.4	Descrivere e riconoscere i collegamenti tra pagine (link)
		1.1.5	Cosa è possibile fare tramite Internet: cercare informazioni tramite i motori di ricerca, fare acquisti, studiare, usufruire dei servizi della propria banca, comunicare con amici, colleghi, enti e istituzioni
1.2	Come gestire la sicurezza	**1.2.1**	Cos'è e a cosa serve la crittografia in informatica
		1.2.2	Riconoscere un sito sicuro, tramite la comprensione del protocollo

2	USO DEL BROWSER		
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
2.1	Le operazioni iniziali	**2.1.1**	Aprire e chiudere il browser; descriverne l'interfaccia, riconoscendone ogni elemento
		2.1.2	Inserire l'URL nella barra degli indirizzi; scegliere l'indirizzo tra quelli suggeriti automaticamente durante la digitazione
		2.1.3	Spostarsi tra pagine web, utilizzando i pulsanti *Avanti*, *Indietro*, *Ricarica*, *Interrompi*
2.2	Schede e finestre	**2.2.1**	Riconoscere l'utilità e comprendere il funzionamento di schede e finestre. Aprire e chiudere più schede, anche usando combinazione di tasti
		2.2.2	Aprire e chiudere le finestre, anche usando combinazione di tasti
		2.2.3	Aprire un link in un'altra scheda o finestra
		2.2.4	Spostare schede nella stessa finestra o in un'altra finestra
		2.2.5	Bloccare una scheda nella finestra del browser

2.3	Configurazione	**2.3.1**	Impostare la pagina iniziale del browser
		2.3.2	Riconoscere, definire e gestire i pop-up
		2.3.3	Riconoscere, definire e gestire i cookie

3 | STRUMENTI DEL BROWSER			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
3.1	La cronologia	**3.1.1**	Visualizzare una pagina web selezionandola nella cronologia
		3.1.2	Cancellare dati di navigazione dalla cronologia
		3.1.3	Cos'è, cosa comporta e come attivare la navigazione in incognito
3.2	I Preferiti	**3.2.1**	Aggiungere un segnalibro ai Preferiti; gestire la barra dei Preferiti; aggiungerne utilizzando combinazione di testi
		3.2.2	Organizzare, modificare, eliminare segnalibri dai Preferiti
		3.2.3	Importare e esportare i Preferiti
3.3	Gli strumenti di interazione con il Web	**3.3.1**	Scaricare file dal Web in unità definite, tenendo in considerazione i pericoli che possono derivare per l'integrità del sistema; definire la funzionalità della barra dei download
		3.3.2	Salvare testi e immagini dal Web
		3.3.3	Stampare una pagina web
		3.3.4	Definire il funzionamento dei plug-in; riconoscere i più diffusi; come eseguirli

4 | ESEGUIRE RICERCHE SUL WEB			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce...		L' utente certificato sa...	
4.1	I motori di ricerca	**4.1.1**	Cosa sono e come funzionano i motori di ricerca; riconoscere e utilizzare i più diffusi motori di ricerca; eseguire una ricerca di informazioni utilizzando parole chiave; definire una *query*
		4.1.2	Eseguire una ricerca di immagini utilizzando parole chiave
		4.1.3	Eseguire una ricerca avanzata; utilizzare Google Advance Search
		4.1.4	Eseguire una ricerca avanzata di contenuti liberamente utilizzabili, utilizzando Google

4.2	La valutazione dell'informazione	**4.2.1**	Come valutare la veridicità delle informazioni di una ricerca sul Web
		4.2.2	Come valutare le informazioni riportate in una pagina Web
		4.2.3	Comprendere quali siano le conseguenze di un utilizzo e una diffusione non corretta delle informazioni tramite Internet: diffamazione e violazione di diritti altrui

5 | LA POSTA ELETTRONICA			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L' utente certificato conosce…		L' utente certificato sa…	
5.1	La casella di posta elettronica	**5.1.1**	Come accedere ad un account di posta elettronica; comprendere la funzione delle cartelle standard di posta elettronica: Posta in arrivo, Posta inviata, Bozze, Posta Indesiderata/Spam, Cestino; Inserire uno o più indirizzi destinatari, nei campi *A*, *Copia conoscenza (Cc)*, *Copia nascosta (Ccn)*; inserire una descrizione adeguata nel capo *oggetto*; compilare il messaggio e aggiungere allegati; inviare il messaggio
		5.1.2	Riconoscere e descrivere la struttura di un indirizzo email
5.2	Le applicazioni tramite cui gestire le email	**5.2.1**	Riconoscere e descrivere l'interfaccia utente di Outlook 2016
		5.2.2	Aggiungere e configurare un account Microsoft, utile per gestire Outlook 2016
		5.2.3	Configurare il protocollo di rete necessario per ricevere le email: quali sono le differenze tra POP3 e IMAP
5.3	Creare e inviare messaggi	**5.3.1**	Quali sono i diversi metodi per creare un nuovo messaggio
		5.3.2	Come creare e inviare un messaggio con Outlook 2016
		5.3.3	Come gestire gli allegati con Outlook 2016
		5.3.4	Creare una rubrica e selezionare i destinatari del messaggio
		5.3.5	Utilizzare il controllo ortografico per verificare la correttezza del contenuto testuale del messaggio
5.4	Come gestire i messaggi	**5.4.1**	Rispondere e inoltrare messaggi
		5.4.2	Eliminare, organizzare e archiviare i messaggi ricevuti, utilizzando anche le regole previste da Outlook 2016
		5.4.3	Utilizzare le notifiche di riferimento
		5.4.4	Creare e inserire una firma

MODULO 2

IT SECURITY

Cosa sa fare il Candidato che si certifica con EIPASS Pubblica Amministrazione

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
4.3	Strumenti di filtraggio dei contenuti	**4.3.1**	Comprendere la funzione e definire i sistemi di filtraggio dei browser; come gestire SafeSearch di Google Chrome: attivare, disattivare e bloccare il filtro
		4.3.2	Segnalare i siti e le immagini inappropriate
		4.3.3	Riconoscere le funzionalità del centro per la sicurezza online di Google
		4.3.4	Riconoscere e definire il funzionamento del Safety Family di Windows
		4.3.5	Come funziona Homeguard Activity Monitor e gli altri software specializzati nel filtraggio dei contenuti (K9 Web Protection, Qustodio Free, SocialShield e così via)

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	Il ripristino di sistema	**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	

MODULO 3

PEC, FIRMA ELETTRONICA E ARCHIVIAZIONE DEI DOCUMENTI DIGITALI

Cosa sa fare il Candidato che si certifica con EIPASS Pubblica Amministrazione

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 elttronica 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 | LA POSTA ELETTRONICA CERTIFICATA			
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 | 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 | L'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 4

IL CODICE DELL'AMMINISTRAZIONE DIGITALE

Cosa sa fare il Candidato che si certifica con EIPASS Pubblica Amministrazione

Il 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 PA

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
- Il D.Lgs 217/2017

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 D. lgs 12 febbraio 1993
1.3	Il CAD e le recenti modifiche	**1.3.1**	Il D. lgs 7 marzo 2005, n. 82
		1.3.2	I principi della legge 7 agosto 2015, n.124
		1.3.3	Le modifiche del D.lgs 26 agosto 2016, n.179

2 | L' ANALISI DEL CODICE DELL' AMMINISTRAZIONE DIGITALE: OBIETTIVI, STRATEGIE, EFFETTI

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
2.2	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 elettronica (art. 9 del CAD)
2.3	L' organizzazione delle PA	**2.3.1**	L' art.12 del CAD. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa
		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 D. lgs 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	Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni
		3.3.4	Siti Internet delle pubbliche amministrazioni (art.53)
		3.3.5	Identità Digitale e regolamento eIDAS
		3.3.6	Accesso telematico ai servizi della pubblica amministrazione
		3.3.7	Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica
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'obbligo di motivazione del rifiuto
		4.1.6	L' oggetto della richiesta: gli atti accessibili
		4.1.7	Il diritto di accesso della L. 241/1990, il diritto di accesso civico e il diritto di accesso del "FOIA"
		4.1.8	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 dell'amministrazione
		4.2.5	Il c.d. "digital divide" (divario digitale)
4.3	Il D.Lgs 217/2017	**4.3.1**	Le novità più importanti

MODULO 5

LA PROTEZIONE DEI DATI PERSONALI: IL GDPR

Cosa sa fare il Candidato che si certifica con EIPASS Pubblica Amministrazione

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 REGOLAMENTO UE 679/2016 E LA DIRETTIVA UE 2016/680			
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**	La composizione e le funzioni del Comitato europeo per la protezione dei dati, un organo sovranazionale che ha il compito di armonizzare l'applicazione del GDPR negli Stati membri
4.2	Il principio dello sportello unico: one stop shop	**4.2**	Le norme da osservare quando i titolari del trattamento dei dati operano in più Paesi dell'Unione europea. Fortemente auspicato dalle imprese, questo principio semplifica le procedure e garantisce più coerenza nelle decisioni
4.3	Le sanzioni	**4.3**	Le sanzioni amministrative per la violazione del GDPR. Come ogni altro codice, anche il GDPR prevede infatti un sistema sanzionatorio
4.4	La violazione dei dati personali (Data breach)	**4.4**	Gli obblighi del titolare del trattamento dei dati personali; in partcolare, l'obbligo del titolare di notificare la violazione del trattamento al Garante
4.5	Le autorità nazionali garanti della protezione dei dati personali	**4.5**	Le funzioni del Garante, l'organo italiano di controllo in materia di violazione dei dati personali
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