EUROPEAN INFORMATICS PASSPORT

# PUBBLICA AMMINISTRAZIONE

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

L'acquisizione di competenze digitali è un fattore vitale per chi è impegnato nelle Pubbliche Amministrazioni. Gli interventi legislativi in favore della digitalizzazione si moltiplicano con l'intenzione di creare un sistema integrato ed efficiente al servizio dei cittadini.

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: le amministrazioni pubbliche devono allinearsi alle prerogative indicate e raggiungere gli obiettivi prefissati.

Primo e ineludibile passo è quello di far acquisire skills trasversali a tutti gli operatori e, soprattutto, a coloro che operano a contatto con il pubblico.

Il Codice dell'Amministrazione Digitale (CAD) stabilisce 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.

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 di tutto il personale.

Le novità tecniche e normative nel settore digitale sono continue: servono strumenti che consentano agli operatori di aggiornarsi con metodologia tarata sulle esigenze di chi lavora quotidianamente; necessitano di un solido ed efficace supporto formativo che permetta loro di sfruttare le potenzialità dell'ICT, per rispondere con sempre maggiore efficacia alle istanze dei cittadini.

Ogni attività necessita di competenze digitali:

- gestione dei procedimenti amministrativi;
- archiviazione dei documenti;
- pagamenti e fatturazione elettronici;
- accessibilità;
- circolazione e scambio dati.

Perché 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.

È necessario che tutti gli operati acquisiscano quelle skills digitali trasversali in ambito informatico indispensabili per poter operare, ogni giorno.

*Certipass*

Centro Studi

*Programma analitico d'esame*

# EIPASS PUBBLICA AMMINISTRAZIONE

## Metodo

Superando il vecchio schema "argomento", "ambito di intervento" e "testing di competenza", proponiamo un nuovo modo di elencare e descrivere i contenuti dei moduli previsti, basato su quello utilizzato nell'*e-Competence Framework for ICT Users – Part 2: User Guidelines*.

È un sistema intellegibile e immediato per chi deve affrontare il percorso di certificazione e, soprattutto, per chi deve valutare la congruenza delle competenze possedute dall'Utente certificato. Per ognuno degli argomenti previsti, quindi, troverete un quadro di riferimento che indica:

- la definizione sintetica della competenza di cui si tratta;
- tutto ciò che l'Utente certificato conosce di quell'argomento (*conoscenza teorica/knowledge*);
- tutto ciò che l'Utente certificato sa fare concretamente, in relazione alle conoscenze teoriche possedute (*conoscenze pratiche/Skills*);

## Procedure e strumenti

Per prepararsi alla prova d'esame, il candidato usufruisce dei servizi e del supporto formativo online.

Per superare la prova d'esame, è necessario rispondere correttamente ad almeno il 75% delle 30 domande previste per ogni modulo. Si precisa, infine, che ciascun modulo rappresenta uno specifico ambito di competenze e che, quindi, aldilà delle interconnessioni esistenti tra i vari settori, il candidato può stabilire autonomamente l'ordine con cui affrontarli.

## Moduli d'esame

**Modulo 1** | Navigare e cercare informazioni sul Web

**Modulo 2** | IT Security

**Modulo 3** | PEC, firma elettronica e archiviazione dei documenti digitali

**Modulo 4** | Il Codice dell'Amministrazione Digitale

**Modulo 5** | La protezione dei dati personali: il GDPR

*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 | I CONCETTI FONDAMENTALI DEL BROWSING

Comprendere i principi tecnici e sociali di Internet. Riconoscere e utilizzare gli elementi principali di una pagina web. Sapere cosa sia possibile fare in rete. In relazione alla sicurezza, conoscere il significato dei protocolli e definire il concetto di crittografia, applicato all'informatica.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Usare in modo efficace l'interfaccia utente del browser per navigare sul Web, scegliendo e selezionando i collegamenti più adeguati. Selezionare e configurare le preferenze del browser e le opzioni di rete, secondo lo proprie necessità. Usare gli strumenti comuni e i metodi più rapidi per massimizzare l'efficienza della navigazione.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Usare in modo efficace alcune funzionalità che permettono di sfruttare al meglio il browser, garantendo la sicurezza della navigazione. Gestire i Preferiti. Utilizzare il browser per acquisire informazioni e documenti e scambiarli con amici e colleghi.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Comprendere e assimilare il concetto di ricerca ed essere consapevole dei media disponibili online. Condurre le ricerche usando adeguate parole chiave. Identificare le relazioni logiche tra parole chiave; raffinare la ricerca quando necessario. Valutare la fondatezza e la credibilità delle informazioni rinvenute.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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** | L'e-commerce e la tutela della privacy | **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 | ESEGUIRE RICERCHE SUL WEB

Comprendere e assimilare il concetto di ricerca ed essere consapevole dei media disponibili online. Condurre le ricerche usando adeguate parole chiave. Identificare le relazioni logiche tra parole chiave; raffinare la ricerca quando necessario. Valutare la fondatezza e la credibilità delle informazioni rinvenute.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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 conoscenza 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

Comprendere il ruolo e l'importanza dell'IT Security nella vita digitale di tutti i giorni. Riconoscere i diversi pro- fili degli hacker e comprendere il significato di crimine informatico. Distinguere tra misure di sicurezza attive e passive. Definire il concetto di ingegneria sociale, connesso alle questioni attinenti la privacy. Applicare misure di sicurezza ai file di Office.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Conoscere i malware più diffusi e gli ultimi, costruiti secondo il principio dell'euristica. Conoscere i più popolari ed utili strumenti di difesa (prima di tutti, l'antivirus) e saperli attivare in maniera idonea, per proteggere effica- cemente dispositivi e dati da attacchi esterni.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Gestire dati autentici, affidabili, integri e riservati. Saperli backappare, recuperarli e trasmetterli, utilizzan- do tutti gli strumenti idonei per garantirne la sicurezza. Conoscere il funzionamento delle reti wireless e i protocolli più usati per proteggere questo tipo di reti. Riconoscere i pericoli connessi alla navigazione su reti pubbliche.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Conoscere e applicare gli strumenti messi a disposizione dai browser per navigare sicuri. Attivare le funzionalità per la sicurezza di Google Chrome. Conoscere il funzionamento di software specifici per il filtraggio dei contenuti e la sicurezza della nevigazione.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Utilizzare in sicurezza la posta elettronica, la chat, la messaggistica istantanea e i social network. Conoscere e utilizzare in maniera corretta la tecnologia P2P.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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

Gestire i dati sul PC in modo che non siano fonte di bug. Comprendere il concetto di storage e riconoscere i principali tipi (NAS, DAS, SAN). Comprendere il concetto di backup e come farlo sui sistemi Windows e Mac; capire come sia possibile farlo tramite cloud. Saper ripristinare il sistema. Eliminare i file dal PC in modo definitivo.

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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 |

*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 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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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 | CYBERCRIME E DIRITTO PENALE

| Knowledge/Conoscenze<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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 |
| | | **2.2.2** | 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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*L'utente certificato sa...* | |
|---|---|---|---|
| **3.1** | Il Documento informatico | **3.1.1** | Definire la struttura dei reati informatici |
| **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 4*

# IL CODICE DELL 'A MMINISTRAZIONE DIGITALE

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

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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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*

# 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
- 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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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<br>*L'utente certificato conosce...* | | Skills/Capacità pratiche<br>*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 |


- 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