



# EIPASS PRIVACY E SICUREZZA DEI DATI

*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](http://eipass.com) dedicate al Programma.

## Copyright © 2018

Tutti i diritti sono riservati a norma di legge e in osservanza delle convenzioni internazionali.

Nessuna parte di questo Programma può essere riprodotta con sistemi elettronici, meccanici o altri, senza apposita autorizzazione scritta da parte di CERTIPASS.

Nomi e marchi citati nel testo sono depositati o registrati dalle rispettive case produttrici.

Il logo EIPASS® è di proprietà esclusiva di CERTIPASS. Tutti i diritti riservati.

## Premessa

Il rapido evolversi delle tecnologie dell'informazione ha preteso una costante definizione di nuovi parametri di tutela della persona, anche in riferimento all'adattamento degli istituti giuridici già esistenti.

L'evoluzione tecnologica recente ha, dunque, innegabilmente modificato le modalità con cui i soggetti percepiscono la propria identità, l'immagine e le relazioni sociali, o più in generale, i vari aspetti della personalità.

La più recente capillare diffusione di internet, con i relativi strumenti di comunicazione, quali per esempio i social network, ha peraltro comportato l'ulteriore esigenza di coinvolgere anche la realtà virtuale nel modello di tutela tradizionalmente apprestato alla personalità.

La sfera della riservatezza si presta a essere la più vulnerata dai moderni mezzi di comunicazione e, pertanto, la definizione di privacy si arricchisce di nuovi significati partendo dal diritto a essere lasciati soli tipico del diciannovesimo secolo, sino alle più recenti istanze di tutela dei dati e dei mezzi tecnologici di protezione.

La prospettiva di lavoro tiene conto, pertanto, dell'evoluzione dei diritti della personalità generalmente intesi e declinati nella tutela della riservatezza, immagine, identità, manifestazione del pensiero e diritto d'autore, alla luce delle più moderne tesi di indagine.

*Centro Studi EIPASS*

## MODULO 1

### PRIVACY E SICUREZZA DATI

#### Obiettivo del modulo

Il modulo intende fornire 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 concetto di privacy, con le regole in materia di protezione di dati personali, anche per i soggetti pubblici.

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.

#### Contenuti del modulo

##### La protezione e la sicurezza dei dati

- La protezione dei dati in internet: aspetti giuridici
- Le misure di sicurezza informatica
- La protezione dei dati in internet: aspetti tecnici

## 1 | LA PROTEZIONE E LA SICUREZZA DEI DATI

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
<b>1.1</b>	La protezione dei dati in internet: aspetti giuridici	1.1.1	Il concetto di privacy
		1.1.2	Regole generali in materia di protezione di dati personali
		1.1.3	Regole per i soggetti pubblici
		1.1.4	La protezione dei dati nel Regolamento (UE) 2016/679
		1.1.5	La tutela dei dati in internet
<b>1.2</b>	Le misure di sicurezza informatica	1.2.1	Le misure di sicurezza informatica: profili generali
		1.2.2	Le misure minime di sicurezza
		1.2.3	Il trattamento dei dati mediante l'ausilio di sistemi elettronici
		1.2.4	Misure di sicurezza in materia di trattamento dei dati sensibili e giudiziari
		1.2.5	Le violazioni delle misure di sicurezza informatica
		1.2.6	Il disaster recovery
<b>1.3</b>	La protezione dei dati in internet: aspetti tecnici	1.3.1	Tecniche di protezione dei dati
		1.3.2	IT Security

## MODULO 2

# IL REGOLAMENTO UE 679/2016 E LE NUOVE NORME SULLA PROTEZIONE DEI DATI PERSONALI

### Obiettivi del modulo

L'utente conosce le novità più importanti del nuovo Regolamento, come quella sull'accountability.

Sa che il regolamento 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 regolamento utili a valutare quali saranno le reali prospettive di cambiamento.

Sa che si prevede l'aggiunta di un'apposita figura, referente: il Data Protection Officer.

### Contenuti del modulo

#### Il Regolamento UE 679/2016

- I principi
- I diritti dell'interessato
- I titolari e i responsabili del trattamento
- Sanzioni e rimedi
- Conclusioni

## 1 | LE NUOVE TECNOLOGIE E I NUOVI DANNI

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
1.1	I principi	1.1.1	Il regolamento UE 679/2016 e la direttiva UE 2016/680
		1.1.2	La definizione di dato personale nel Reg. UE 679/2016
		1.1.3	Il principio di responsabilizzazione (accountability)
		1.1.4	I principi di liceità e correttezza nel trattamento dei dati (Art. 5 del Regolamento)
		1.1.5	La "nuova informativa": le modalità e le ipotesi di esonero
1.2	I diritti dell'interessato	1.2.1	Il diritto di accesso
		1.2.2	La profilazione
		1.2.3	I nuovi diritti all'oblio e alla portabilità dei dati
		1.2.4	Il diritto di opposizione
1.3	I titolari e i responsabili del trattamento	1.3.1	La proceduralizzazione degli obblighi di titolari e responsabili
		1.3.2	Il responsabile della protezione dei dati: il Data Protection Officer (art.37)
		1.3.3	Il responsabile del trattamento: nuovi obblighi e responsabilità
		1.3.4	Data Breach e comunicazioni obbligatorie
1.4	Sanzioni e rimedi	1.4.1	Il Comitato Europeo per la protezione dei dati
		1.4.2	One-stop-shop
		1.4.3	Le sanzioni
		1.4.4	Le autorità nazionali garanti della protezione dei dati personali
		1.4.5	I rimedi per le violazioni dei dati; il trasferimento dei dati
1.5	Conclusioni	1.5.1	L'applicazione del Regolamento e le indicazioni del Garante per la protezione dei dati

## MODULO 3

### IL CODICE DELL'AMMINISTRAZIONE DIGITALE

#### Cosa sa fare il Candidato che si certifica con EIPASS DPO

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 Pubbliche Amministrazioni



### **Gli strumenti dell'informatizzazione: documento informatico e firme elettroniche**

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

### **L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni**

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

## 1 | IL RINNOVAMENTO DELLA PUBBLICA AMMINISTRAZIONE

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

## 2 | STRUMENTI DI COLLABORAZIONE ONLINE

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

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

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

### 4 | L'INFORMATIZZAZIONE E LA TRASPARENZA NELLE PUBBLICHE AMMINISTRAZIONI

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

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

## MODULO 4

# IL REGOLAMENTO UE 679/2016 E LE NUOVE NORME SULLA PRETEZIONE DEI DATI PERSONALI

### Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato conoscere le novità più importanti del nuovo Regolamento, come quella sull'accountability.

Sa che il regolamento 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 regolamento utili a valutare quale saranno le reali prospettive di cambiamento all'interno delle amministrazioni.

Sa che si prevede l'aggiunta di un'apposita figura, referente: il Data Protection Officer.

### Contenuti del modulo

#### Il Regolamento UE 679/2016

- I principi
- I diritti dell'interessato
- I titolari e i responsabili del trattamento
- Sanzioni e rimedi
- Conclusioni

## 1 | IL REGOLAMENTO UE 679/2016

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
<b>1.1</b>	I principi	<b>1.1.1</b>	Il regolamento UE 679/2016 e la direttiva UE 2016/680
		<b>1.1.2</b>	La definizione di dato personale nel Reg. UE 679/2016
		<b>1.1.3</b>	Il principio di responsabilizzazione (accountability)
		<b>1.1.4</b>	I principi di liceità e correttezza nel trattamento dei dati (Art. 5 del Regolamento)
		<b>1.1.5</b>	La "nuova informativa": le modalità e le ipotesi di esonero
<b>1.2</b>	I diritti dell'interessato	<b>1.2.1</b>	Il diritto di accesso
		<b>1.2.2</b>	La profilazione
		<b>1.2.3</b>	I nuovi diritti all'oblio e alla portabilità dei dati
		<b>1.2.4</b>	Il diritto di opposizione
<b>1.3</b>	I titolari e i responsabili del trattamento	<b>1.3.1</b>	La proceduralizzazione degli obblighi di titolari e responsabili
		<b>1.3.2</b>	Il responsabile della protezione dei dati: il Data Protection Officer (art.37)
		<b>1.3.3</b>	Il responsabile del trattamento: nuovi obblighi e responsabilità
		<b>1.3.4</b>	Data Breach e comunicazioni obbligatorie
<b>1.4</b>	Sanzioni e rimedi	<b>1.4.1</b>	Il Comitato Europeo per la protezione dei dati
		<b>1.4.2</b>	One-stop-shop
		<b>1.4.3</b>	Le sanzioni
		<b>1.4.4</b>	Le autorità nazionali garanti della protezione dei dati personali
		<b>1.4.5</b>	I rimedi per le violazioni dei dati; il trasferimento dei dati
<b>1.5</b>	Conclusioni	<b>1.5.1</b>	L'applicazione del Regolamento e le indicazioni del Garante per la protezione dei dati

## MODULO 5

# PEC, DOCUMENTI DIGITALI E DEMATERIALIZAZIONE DEGLI ARCHIVI CARTACEI

### Cosa sa fare il Candidato che si certifica con EIPASS DPO

Il Candidato certificato sa cos'è e come funziona la Posta Elettronica Certificata (PEC). Conosce cos'è e come funziona il log e quale è l'incidenza dei malware.

Sa perché e quando la PEC ha valore legale.

Sa cos'è la firma digitale, conoscendone le diverse tipologie.

Sa definire il sistema di funzionamento delle chiavi crittografiche asimmetriche.

Conosce la differenza tra contrassegno elettronico e foglio elettronico

Conosce il sistema di archiviazione dei documenti digitali, così come descritti nel manuale di conservazione.

### Contenuti del modulo

#### La Posta Elettronica Certificata

- Cos'è la PEC
- Il registro di log
- Messaggi di PEC con virus informatici

#### La firma digitale

- Cos'è la firma digitale
- Il contrassegno elettronico e il sigillo elettronico

#### Archiviazione dei documenti digitali

- La digitalizzazione della PA
- Le copie
- Il sistema e i requisiti per la conservazione dei documenti informatici

## 1 | LA POSTA ELETTRONICA CERTIFICATA

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
1.1	La PEC	1.1.1	Che cos'è la PEC
		1.1.2	La procedura di invio di un messaggio tramite PEC
1.2	Il registro di log	1.2.1	L'obbligo di registrazione
		1.2.2	Cosa deve contenere il registro di log
		1.2.3	Cosa deve garantire il registro di log
		1.2.4	I metadati del registro di log
1.3	Messaggi di PEC con virus informatici	1.3.1	Il DPR 11 febbraio 2005, n. 68
		1.3.2	L'art. 4 c. 2 del DPCM del 3 dicembre 2013
		1.3.3	Il valore legale della PEC

## 2 | LA FIRMA DIGITALE

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
2.1	La firma digitale	2.1.1	Cos'è la firma digitale
		2.1.2	Il token USB o la smart card
		2.1.3	Regolamento (UE) n. 910/2014
		2.1.4	Il servizio di marcatura temporale
		2.1.5	Le diverse tipologie: la firma elettronica semplice, la firma elettronica qualificata, la firma elettronica avanzata; il formato PAdES (PDF Advanced Electronic Signatures) e il formato CADES (CMS Advanced Electronic Signatures)
		2.1.6	Il sistema a chiavi crittografiche asimmetriche
2.2	Il contrassegno elettronico e il sigillo elettronico	2.2.1	L'art. 23-ter dal CAD
		2.2.2	Il Regolamento n. 910 del 2014, meglio noto come Regolamento eIDAS, in vigore dal 1° luglio 2016
		2.2.3	I sigilli elettronici avanzati

## 3 | ARCHIVIAZIONE DEI DOCUMENTI DIGITALI

Knowledge/Conoscenze	Skills/Capacità pratiche
----------------------	--------------------------



L'utente certificato conosce...		L'utente certificato sa...	
3.1	La digitalizzazione dei documenti	3.1.1	La digitalizzazione della PA
		3.1.2	Gli archivi: il fascicolo, l'archivio corrente, l'archivio di deposito, l'archivio storico
		3.1.3	La gestione dei flussi documentali
3.2	Le copie	3.2.1	Copie informatiche di documenti analogici
		3.2.2	Copie analogiche di documenti informatici
3.3	Il sistema e i requisiti per la conservazione dei documenti informatici	3.3.1	Il responsabile della conservazione
		3.3.2	Il manuale di conservazione
		3.3.3	Il processo di conservazione

## MODULO 6

### IT SECURITY

#### Cosa sa fare il Candidato che si certifica con EIPASS DPO

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

Conosce i malware 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 tipologie 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 <i>social engineering</i>
		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 malware	2.1.1	Definire il concetto di malware, distinguendo quelli di tipo parassitario da quelli del settore di avvio
		2.1.2	Definire e riconoscere il funzionamento dei malware 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 malware 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 malware creati secondo questo principio, detti poliformi

### 3 | LA SICUREZZA DELLE RETI

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
<b>3.1</b>	La rete e le connessioni	<b>3.1.1</b>	Definire il concetto di rete in informatica e di networking
		<b>3.1.2</b>	Distinguere le diverse tipologie di reti informatiche (LAN, WAN, MAN)
		<b>3.1.3</b>	Distinguere i vari tipi di reti LAN (star, bus, ring, mesh)
		<b>3.1.4</b>	Comprendere il principio di vulnerabilità delle reti, riconoscendone le diverse tipologie
		<b>3.1.5</b>	Riconoscere il ruolo e gli oneri che un amministratore di sistema ha in relazione alla sicurezza della rete
		<b>3.1.6</b>	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)
<b>3.2</b>	Navigare sicuri con le reti wireless	<b>3.2.1</b>	Comprendere l'importanza di un utilizzo ragionato della password nei sistemi Wi-Fi
		<b>3.2.2</b>	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 crittazione AES, Advanced Encryption Standard)
		<b>3.2.3</b>	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
		<b>3.2.4</b>	Riconoscere i pericoli connessi alla navigazione su reti wireless pubbliche
		<b>3.2.5</b>	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 cookie 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 fraudolente 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: malware, 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 <i>Cronologia file di Windows 10</i> ; ripristinare i file salvati
		6.1.3	Come ripristinare i file salvati e come escludere dal backup i file che non vogliamo copiare
		6.1.4	Come fare il backup su Mac, usando Time Machine
		6.1.5	Cos'è il cloud e come funziona OneDrive; riconoscere e utilizzare software specifici dedicati al backup
6.2	La procedura per stampare fogli di calcolo	6.2.1	Cos'è il ripristino di sistema e come farlo su Windows 10
		6.2.2	Come fare il ripristino di sistema su Mac
6.3	Eliminare i dati in modo permanente	6.3.1	Cos'è e come funziona il cestino
		6.3.2	Conoscere software specifici che consentono di eliminare definitivamente file











[www.certipass.org](http://www.certipass.org)

- > ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE DELLE COMPETENZE DIGITALI EIPASS
- > 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](http://www.eipass.com)