# IT Security

## 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 ter- zi.

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

Nella società attuale, gran parte delle attività che si svolgono quotidianamente sono affidate a computer e internet, per fare solo qualche esempio: la comunicazione tramite email o social network, l'intrattenimento tramite film digitali o la musica mp3, il trasporto tramite navigatore, gli acquisti online, la medicina, l'informazione.

Le informazioni personali e i dati sensibili sono memorizzati sul proprio computer o su sistemi altrui.

La sicurezza informatica deve proteggere questi sistemi e le informazioni in essi contenute, rilevando, prevenendo e rispondendo a eventuali attacchi.

Per minimizzare le probabilità di attacco o le conseguenze è fondamentale conoscere i rischi e le misure da attuare.

Inoltre è importante conoscere quelli che sono i propri diritti in rete e le regole di privacy da rispettare per non ledere i diritti degli altri.

*Certipass*

Centro Studi

*Programma analitico d'esame*

# EIPASS IT SECURITY

## 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** | Sicurezza informatica

**Modulo 2** | Privacy e sicurezza dei dati

*Modulo 1*

# SICUREZZA INFORMATICA

## Cosa sa fare il Candidato che si certifica con EIPASS IT Security

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

**L'IT Security**

- Concetti di base
- Le principali misure di sicurezza online
- Le principali tecniche di violazioni dei dati personali
- Misure per la sicurezza dei file

**Attacchi e minacce informatiche**

- I diversi tipi di malware
- Gli strumenti per difendersi dai malware

**Le reti informatiche e la loro sicurezza**

- I diversi tipi di reti informatiche
- La sicurezza delle reti informatiche
- La sicurezza nelle reti wireless
- Gli hotspot

**Misure per navigare sicure in Internet**

- Il browser e la sicurezza online
- Navigare in sicurezza

**Sicurezza nelle comunicazioni online**

- Posta elettronica
- Reti sociali
- Messaggistica istantanea
- Dispositivi mobili

**Mettere al sicuro i propri dati**

- Il backup dei dati
- Eliminare i dati

| 1 \| L'IT SECURITY | | | |
|---|---|---|---|
| Comprendere il ruolo e l'importanza dell'IT Security nella vita digitale di tutti i giorni. Riconoscere i diversi profili 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 alla privacy. Applicare misure di sicurezza ai file di Office. | | | |
| Knowledge / Conoscenze | | Skills / Capacità pratiche | |
| 1.1 | Concetti di base | 1.1.1 | Obiettivi dell'IT Security |
| | | 1.1.2 | I diversi tipi di minacce |
| | | 1.1.3 | Crimini informatici e hacker |
| | | 1.1.4 | Le linee guida e gli standard di sicurezza informatica |
| 1.2 | Le principali misure di sicurezza online | 1.2.1 | Definizione del Programme for International Student Assesment |
| | | 1.2.2 | L'autenticazione a più fattori |
| | | 1.2.3 | Riconoscimento dei dati biometrici |
| 1.3 | Le principali tecniche di violazioni dei dati personali | 1.3.1 | Le tecniche di ingegneria sociale |
| | | 1.3.2 | Difendersi dagli attacchi di ingegneria sociale |
| | | 1.3.3 | Il furto di identità |
| | | 1.3.4 | Prevenire il furto di identità |
| | | 1.3.5 | Capire se la propria identità è stata rubata |
| 1.4 | Misure per la sicurezza dei file | 1.4.1 | Registrare ed eseguire una macro |
| | | 1.4.2 | Cambiare le impostazioni delle macro |
| | | 1.4.3 | Proteggere i file con una password |

## 2 | ATTACCHI E MINACCE INFORMATICHE

Conoscere i malware più diffusi e recenti, 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 efficacemente dispositivi e dati da attacchi esterni.

| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
|---|---|---|---|
| 2.1 | I diversi tipi di malware | 2.1.1 | Virus informatici, Trojan e Worm |
| | | 2.1.2 | Spyware, adware e ransomware |
| | | 2.1.3 | Rootkit, backdoor e keylogger |
| | | 2.1.4 | Phishing, smishing, vishing, pharming e sniffing |
| 2.2 | Gli strumenti per difendersi dai malware | 2.2.1 | Utilizzare un antivirus |
| | | 2.2.2 | Avviare una scansione dei sistema con Windows Defender |
| | | 2.2.3 | Accedere alla cronologia della protezione con Windows Defender |
| | | 2.2.4 | Pianificare la scansione del sistema con Windows Defender |
| | | 2.2.5 | Verificare la disponibilità di aggiornamenti per Windows Defender |
| | | 2.2.6 | Avviare Windows Update |

| 3 \| LE RETI INFORMATICHE E LA LORO SICUREZZA<br>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 | | Skills/Capacità pratiche | |
| 3.1 | I diversi tipi di reti informatiche | 3.1.1 | Le reti LAN e WLAN |
| | | 3.1.2 | Le reti MAN, WAN e VPN |
| | | 3.1.3 | Le reti P2P e client/server |
| 3.2 | La sicurezza delle reti informatiche | 3.2.1 | Vulnerabilità delle reti informatiche |
| | | 3.2.2 | Il ruolo dell'amministratore di rete |
| | | 3.2.3 | Utilizzare un firewall per proteggere i dispositivi connessi a una rete |
| 3.3 | La sicurezza nelle reti wireless | 3.3.1 | I diversi tipi di attacchi alle reti wireless |
| | | 3.3.2 | L'importanza delle password per accedere alle reti wireless |
| | | 3.3.3 | I protocollo di sicurezza per le reti wireless |
| 3.4 | Gli hotspot | 3.4.1 | Cos'è e come funziona un hotspot |
| | | 3.4.2 | Configurare un hotspot personale: il tethering |

| 4 \| MISURE PER NAVIGARE SICURI IN INTERNET<br>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 navigazione. | | | |
|---|---|---|---|
| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
| 4.1 | Il browser e la sicurezza online | 4.1.1 | Gestire le password |
| | | 4.1.2 | Compilare automaticamente i moduli online |
| | | 4.1.3 | Cancellare la cronologia del browser |
| 4.2 | Navigare in sicurezza | 4.2.1 | Capire quando un sito web è sicuro |
| | | 4.2.2 | Verificare la sicurezza delle reti wireless |
| | | 4.2.3 | Utilizzare gli strumenti di filtraggio dei contenuti |

| 5 \| SICUREZZA NELLE COMUNICAZIONI ONLINE<br>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 | | Skills/Capacità pratiche | |
| 5.1 | Posta elettronica | 5.1.1 | La cifratura come argine alle infiltrazioni malware |
| | | 5.1.2 | La firma digitale come sistema per identificare il mittente delle email |
| | | 5.1.3 | Riconoscere lo spam |
| | | 5.1.4 | Riconoscere il phishing |
| | | 5.1.5 | Che cosa fare in caso di phishing |
| 5.2 | Reti sociali | 5.2.1 | Capire quando un sito web è sicuro |
| | | 5.2.2 | Verificare la sicurezza delle reti wireless |
| | | 5.2.3 | Utilizzare gli strumenti di filtraggio dei contenuti |
| | | 5.2.4 | I rischi della comunicazione sulle reti sociali |
| 5.3 | Messaggistica istantanea | 5.3.1 | I rischi per la sicurezza sui sistemi di messaggistica istantanea |
| | | 5.3.2 | La crittografia end-to-end (E2E) |
| 5.4 | Dispositivi mobili | 5.4.1 | Cosa sono le autorizzazioni |
| | | 5.4.2 | Controllare le autorizzazioni richieste delle app |
| | | 5.4.3 | Cosa fare se perdiamo il nostro dispositivo |

| 6 \| METTERE AL SICURO I PROPRI DATI<br>Gestire i dati sul PC in modo che non siano fonte di bug. Comprendere il concetto di backup e come farlo sul sistema Windows e su OneDrive, e sui dispositivi esterni. Saper ripristinare il sistema. Eliminare i file dal PC in modo definitivo. | | | |
|---|---|---|---|
| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
| 6.1 | Il backup dei dati | 6.1.1 | Creare copie di backup dei dati su un supporto esterno |
| | | 6.1.2 | Archiviare file su OneDrive |
| | | 6.1.3 | Eseguire copie di backup dei dati su OneDrive |
| | | 6.1.4 | Pianificare il backup dei dati su un supporto esterno |
| | | 6.1.5 | Ripristinare dati da una copia di backup |
| 6.2 | Eliminare i dati | 6.2.1 | Eliminare i dati dal computer e dai supporti esterni |
| | | 6.2.2 | Eliminare definitivamente i dati |

*Modulo 2*

# PRIVACY E SICUREZZA DEI DATI

## Cosa sa fare il Candidato che si certifica con EIPASS IT Security

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

**Il diritto alla riservatezza: evoluzione e tutela giuridica**

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

**Le misure di sicurezza informatica**

- Le misure di sicurezza in Internet: profili generali
- Le misure di sicurezza nel Regolamento UE n. 679/2016
- Le violazioni delle misure di sicurezza di informatica

**Sicurezza dei dati**

- La gestione sicura dei dati
- I diversi sistemi di storage
- Il ripristino di sistema
- Eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

| 1 \| IL DIRITTO ALLA RISERVATEZZA: EVOLUZIONE E TUTELA GIURIDICA | | | |
|---|---|---|---|
| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
| **1.1** | Le origini del diritto alla riservatezza | **1.1.1** | Pronunce della giurisprudenza |
| **1.2** | La legislazione europea in materia di tutela della riservatezza | **1.2.1** | Ordinamenti europei |
| **1.3** | Il ruolo delle informazioni e il nuovo concetto di privacy | **1.3.1** | Raccoglitore e fornitore di dati |
| **1.4** | La legislazione europea in materia di tutela della riservatezza | **1.4.1** | La Convenzione di Strasburgo del 1981 e la Direttiva 46/95/CE |
| | | **1.4.2** | La legge n. 675 del 1996 |
| | | **1.4.3** | La direttiva 2002/58 CE |
| **1.5** | Il Codice della privacy | **1.5.1** | La protezione dei dati e lo sviluppo tecnologico nel Regolamento Europeo 679 del 2016 |

| 2 \| LE MISURE DI SICUREZZA INFORMATICA | | | |
|---|---|---|---|
| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
| **2.1** | Le misure di sicurezza in Internet: profili generali | **2.1.1** | Requisito di sicurezza |
| **2.2** | Le misure di sicurezza nel Regolamento UE 679/2016 | **2.2.1** | Principio di responsabilizzazione |
| | | **2.2.2** | Privacy by design |
| | | **2.2.3** | Privacy by default |
| | | **2.2.4** | Valutazione d'impatto sulla protezione dei dati |
| **2.3** | Le violazioni delle misure di sicurezza informatica | **2.3.1** | Profili di responsabilità |

| 3 \| SICUREZZA DEI DATI | | | |
|---|---|---|---|
| Knowledge/Conoscenze | | Skills/Capacità pratiche | |
| **3.1** | La gestione sicura dei dati | **3.1.1** | Le tecniche di protezione dei dati |
| **3.2** | I diversi sistemi di storage | **3.2.1** | Il backup dei dati |
| | | **3.2.2** | Ripristinare i file salvati |
| | | **3.2.3** | Il backup su Mac |
| | | **3.2.4** | Il Cloud |
| **3.3** | Il ripristino di sistema | **3.3.1** | Il ripristino su Windows 10 |
| | | **3.3.2** | Il ripristino del sistema su Mac |
| **3.4** | Eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi | **3.3.1** | Il cestino |
| | | **3.3.2** | Eliminazione definitiva dei file |