

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 disponibile nell'[Aula Didattica 3.0](#).

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, al di là 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 3 | Strumenti informatici per la tutela in Rete



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 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

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 la privacy. Applicare misure di sicurezza ai file di Office.

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 <i>IT Security</i> , comprendendo la differenza tra <i>dato</i> e <i>informazione</i> 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' <i>IT Security</i> : 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 <i>crimine informatico</i> e riconoscere le diverse tipologia di <i>hacker</i>
		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 <i>Centro protezione</i>
		1.3.3	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 efficacemente dispositivi e dati da attacchi esterni.

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 <i>attacchi login</i> : <i>thiefing</i> e <i>keylogger</i>
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

Gestire dati autentici, affidabili, integri e riservati. Saperli backappare, recuperarli e trasmetterli, utilizzando 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		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

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	
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

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	
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	Strumenti di filtraggio dei contenuti	5.3.1	Comprendere la funzione e definire i sistemi di filtraggio dei browser; come gestire SafeSearch di Google Chrome: attivare, disattivare e bloccare il filtro
		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

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		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	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 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
- Le misure di sicurezza informatica
- Sicurezza dati



1 | IL DIRITTO ALLA RISERVATEZZA

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
1.1	Le origini del diritto alla riservatezza	1.1	Descrivere le origini del diritto alla riservatezza
1.2	La legislazione europea in materia di tutela della riservatezza	1.2	Descrivere la legislazione europea in materia di tutela della riservatezza
1.3	Il ruolo delle informazioni e il nuovo concetto di privacy	1.3	Descrivere la condizione dei nuovi pericoli che possono colpire il privato, in relazione alle nuove tecnologie e alla Rete
1.4	Le fonti normative di rango internazionale e comunitario in materia di privacy	1.4	Definire le fonti normative in materia di privacy, nello specifico conosce la Convenzione di Strasburgo del 1981, la Direttiva 46/95/CE, la L. 675/96 e la Dir. 2002/58/CE
1.5	Il Codice della privacy	1.5	Definire i principi fondamentali del Codice della privacy, anche in relazione al Regolamento Europeo 679/2016

2 | LE MISURE DI SICUREZZA INFORMATICA

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
2.1	Le misure di sicurezza in Internet	2.1	Identificare le misure di sicurezza in relazione alla privacy
2.2	Le misure di sicurezza nel Regolamento UE 679/2016	2.2	Adottare le misure di sicurezza connesse alla protezione dei dati e alla riservatezza secondo le disposizioni del Regolamento UE 679/2016
2.3	Privacy by design	2.3	Adottare misure tecniche e organizzative "fin dalla progettazione" del trattamento per garantire la sicurezza dei dati personali
2.4	Privacy by default	2.4	Adottare misure tecniche e organizzative "come impostazione predefinita" del trattamento per garantire la sicurezza dei dati personali
2.5	Valutazione di impatto sulla protezione dei dati	2.5	Eseguire l'analisi di rischio connessa all'utilizzo dei dati personali, secondo le disposizioni del Regolamento UE 679/2016



2.6	Le violazioni delle misure di sicurezza informatica: profili di responsabilità	2.6	Riconoscere i profili di responsabilità connessi alla violazione delle norme in materia di trattamento dei dati personali
-----	--	-----	---

3 SICUREZZA DEI DATI			
Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
3.1	Gestire i dati sul PC in maniera sicura	3.1.1	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)
		3.1.2	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
		3.1.3	Come ripristinare i file salvati e come escludere dal backup i file che non vogliamo copiare
		3.1.4	Come fare il backup su Mac, usando Time Machine
		3.1.5	Cos'è il cloud e come funziona OneDrive; riconoscere e utilizzare software specifici dedicati al backup
3.2	Il ripristino di sistema	3.2.1	Cos'è il ripristino di sistema e come farlo su Windows 10
		3.2.2	Come fare il ripristino di sistema su Mac
3.3	Eliminare i dati in modo permanente	3.3.1	Cos'è e come funziona il cestino
		3.3.2	Conoscere software specifici che consentono di eliminare definitivamente file



Modulo 3

STRUMENTI INFORMATICI PER LA TUTELA IN RETE

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

Il candidato certificato conosce gli strumenti pratici per attivare una tutela minima durante le attività di comunicazione e navigazione online.

Conosce il filtro Parental Control e lo utilizza sia per filtrare e bloccare gli accessi ad alcuni siti, sia per monitorare il comportamento online di bambini e ragazzi. Sa attivare il Parental Control su dispositivi Windows e Mac; sui browser e sulle app di Google; su Youtube.

Il candidato certificato sa definire quali sono le iniziative e gli strumenti per la tutela della privacy e della sicurezza in rete.

Conosce i filtri dei social network più utilizzati, quali Twitter e Facebook, ha acquisito le competenze per segnalare comportamenti scorretti o violazioni dei diritti sui social network. Ha dimestichezza con il concetto di pubblicare contenuti visibili a tutti o ad alcuni, e con le parole filtro per bloccare alcuni contenuti secondo la fascia d'età.

Contenuti del modulo

Strumenti pratici

- Parental Control

I social network; iniziative e strumenti per la tutela della privacy e della sicurezza in rete

- Twitter, filtri potenziati contro il cyberbullismo
- Come tutela i minori Facebook?



1 | STRUMENTI PRATICI

I più giovani, i cosiddetti nativi digitali, sono nati con il cellulare in mano e sono molto abili nel navigare in Internet e utilizzare i vari dispositivi per accedervi. Nonostante ciò è importante ricordare che la capacità d'uso e la consapevolezza delle minacce correlate è proporzionata all'età e al loro sviluppo cognitivo. Per tale motivo è fondamentale conoscere gli strumenti per controllare e/o prevenire azioni che, sul web, possano sfociare in situazioni sconvenienti per bambini e ragazzi.

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
1.1	Parental Control	1.1.1	Impostare il Parental Control di Windows
		1.1.2	Impostare il Parental Control di Mac OS Apple
		1.1.3	Applicare restrizioni sui tablet
		1.1.4	Impostare il Parental Control sui browser
		1.1.5	Impostare il Parental Control sull'App di Google
		1.1.6	Impostare il Parental Control su YouTube

2 | I SOCIAL NETWORK: INIZIATIVE E STRUMENTI PER LA TUTELA DELLA PRIVACY E DELLA SICUREZZA

I social network più diffusi e utilizzati prevedono delle misure di tutela minime che si possono attuare per prevenire e contrastare i pericoli della Rete.

Knowledge/Conoscenze		Skills/Capacità pratiche	
L'utente certificato conosce...		L'utente certificato sa...	
2.1	Twitter, filtri potenziati contro il cyberbullismo	2.1.1	Riconoscere i filtri di Twitter contro il cyberbullismo
2.2	Come tutela i minori Facebook?	2.2.1	Effettuare una segnalazione di un minore di età inferiore a 13 anni
		2.2.2	Effettuare una segnalazione di violazione dei diritti di privacy
		2.2.3	Effettuare una segnalazione di un messaggio minaccioso
		2.2.4	Pubblicare correttamente post
		2.2.5	Identificare le parole da utilizzare come filtro, sia in inglese sia in italiano

