MODULO 1

Sicurezza informatica

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

Il candidato certificato ha dimestichezza con i principi basilari e le problematiche inerenti la sicurezza informatica, con particolare riguardo agli aspetti legali e sociali connessi all'utilizzo diffuso del computer e della Rete.

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, recuperarli e trasmetterli in sicurezza tramite la tecnologia Bluetooh.

Utilizza in sicurezza la posta elettronica, la chat, la messaggistica istantanea ed i social network. Conosce e utilizza in maniera corretta anche la tecnologia P2P.

Sa come navigare in sicurezza, utilizzando tutte le accortezze necessarie per evitare i rischi e le minacce connesse ad Intenet.

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 durante la navigazione.

Contenuti del modulo

Introduzione alla sicurezza informatica

- protezione del sistema e degli utenti
- la sicurezza dei dati e la privacy
- proprietà intellettuale e copyright

IT Security: concetti di base

- il problema della sicurezza nel settore IT
- i vari tipi di attacchi

Malware

- i diversi tipi di malware
- gli strumenti di difesa

Sicurezza dei dati

- la gestione sicura dei dati
- la trasmissione dei dati tramite bluetooh

Sicurezza della comunicazione

- la posta elettronica
- le chat, la messaggistica istantanea e i social network
- la tecnologia P2P

Sicurezza delle reti

- le connessioni di rete
- i firewall
- le minacce su internet

Sicurezza della navigazione

- i filtri e le impostazioni per navigare in sicurezzai firewall

Sicurezza nelle comunicazioni online

- i rischi derivanti dall'uso degli strumenti di comunicazione

ARGOMENTO 1

INTRODUZIONE ALLA SICUREZZA INFORMATICA

e-Competence Framework | e-CF intermediate

Essere consapevole del tema cruciale della protezione dei dati e della privacy in ambito informatico. Riconoscere le misure di sicurezza più comuni. Descrivere i principali aspetti legali e sociali legati all'ICT, non solo in relazione ai tema di "proprietà intellettuale" e "copyright" ma anche rispetto alla libera circolazione delle informazioni.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K1.1	**I concetti di protezione del sistema e degli utenti** K1.1.1 Conoscere le principali operazioni di manutenzione e protezione del sistema. K1.1.2 Conoscere gli aspetti di vulnerabilità di un sistema informatico. K1.1.3 Conoscere gli antivirus.	**S1.1**	**Proteggere il sistema e gli utenti** S1.1.1 Mettere in atto le attività di rutine necessarie per tenere manutenuto ed in sicurezza il PC. S1.1.2 Riconoscere i virus più diffusi. S1.1.3 Comprendere l'importanza dell'aggiornamento dell'antivirus.
K1.2	**La sicurezza dei dati e la Privacy** K1.2.1 Gestire i dati personali. K1.2.2 Sapere cos'è il firewall.	**S1.2**	**Adottare misure che garantiscono la sicurezza** S1.2.1 Comprendere l'importanza di usare credenziali complesse e non lasciarle nelle libera disponibilità di terzi non autorizzati. (lunghezza adeguata delle password, utilizzo di cifre alfanumeriche, estrema riservatezza, modifica frequente). S1.2.1 Descrivere il funzionamento del firewall.
K1.3	**I concetti di proprietà intellettuale e copyright** K1.3.1 Conoscere le diverse licenze.	**S1.3**	**Identificare i problemi etici e sociali sorti con l'avvento dell'ICT** S1.3.1 Descrivere le problematiche inerenti il diritto d'autore e il plagio: proprietà intellettuale e copyright.

ARGOMENTO 2

IT SECURITY: CONCETTI BASE

e-Competence Framework | e-CF intermediate

Comprendere le questioni più importanti e basilari relativi alla sicurezza informatica, con particolare attenzione ai dispositivi da proteggere ed ai vari livelli di sicurezza applicabili. Conoscere quali siano i diversi tipi di attacchi possibili, avendo ben chiara la figura dell'hackeraggio e le differenze che ci sono tra quello immorale e quello etico.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con...*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K2.1	**IT Security** K2.1.1 Gli standard di sicurezza informatica. K2.1.2 Cosa proteggere (sistemi, dati, informazioni e reti). K2.1.3 Sicurezza attiva e sicurezza passiva. K2.1.4 I diversi livelli di protezione.	**S2.1**	**Gestire il problema della sicurezza informatica** S2.1.1 Applicare le linee guida e le politiche. S2.1.2 Proteggere le varie le risorse. S2.1.3 Utilizzare tecniche di sicurezza attiva e passiva. S2.1.4 Adottare le varie tecniche di autenticazione: scegliere in maniera opportuna le password, proteggere la propria password, utilizzare la One-time password.
K2.2	**Gli attacchi informatici** K2.2.1 Conoscere il significato del termine hacker.	**S2.2**	**Riconoscere gli attacchi informatici** S2.2.1 Riconoscere le diverse categorie di hacker.

ARGOMENTO 3

MALWARE

e-Competence Framework | e-CF intermediate

Conoscere i malware più diffusi. 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.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con...*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K3.1	**Attacchi e minacce informatiche** K3.1.1 Comprendere il termine malware, comprendere la differenza tra virus di tipo parassita e virus del settore d'avvio. K3.1.2 Comprendere la differenza tra i vari attacchi login.	**S3.1**	**Identificare i diversi tipi di malware** S3.1.1 Riconoscere virus, macro virus, worm e cavalli di troia. S3.1.2 Identificare e bloccare i meccanismi di propagazione.
K3.2	**Gli strumenti di difesa** K3.2.1 Conoscere i vari strumenti di difesa: antivirus e firewall.	**S3.2**	**Utilizzare i vari strumenti di difesa** S3.2.1 Eseguire scansioni antivirus e attivare il Firewall.
K3.3	**L'antivirus** K3.3.1 Conoscere che cosa è un antivirus e come funziona. K3.3.2 Comprendere l'importanza di una buona configurazione dell'antivirus della scansione. K3.3.3 Comprendere l'importanza dell'aggiornamento dell'antivirus. K3.3.4 Comprendere il ruolo dei sistemi operativi e dei programmi per la protezione.	**S3.3**	**Riconoscere le funzionalità dell'antivirus** S3.3.1 Descrivere come funziona un antivirus. S3.3.2 Descrivere le differenti modalità di scansione. S3.3.3 Descrivere cosa si intenda per *euristica* e *virus polimorfo*. S3.3.4 Comprendere quali siano i software più esposti agli attacchi malevoli.

ARGOMENTO 4

SICUREZZA DEI DATI

e-Competence Framework | e-CF intermediate

Gestire dati autentici, affidabili, integri e riservati. Saperli backappare, recuperarli e trasmetterli tramite bluetooth, utilizzando tutti gli strumenti idonei per garantirne la sicurezza.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K4.1	**La gestione sicura dei dati** K4.1.1 Comprendere l'importanza di gestire i dati in sicurezza. K4.1.2 Conoscere le tecniche di protezione dei dati. K4.1.3 Conoscere le tecniche di ripristino dei dati. K4.1.4 Comprendere l'importanza di eliminare in modo permanente i dati.	**S4.1**	**Gestire i dati in maniera sicura** S4.1.1 Riconoscere i principi alla base dell'IT Security (autenticità, affidabilità, integrità…). S4.1.2 Salvare efficacemente i dati disponibili. S4.1.3 Preparare un disco di ripristino dei dati. S4.1.4 Eliminare i dati in modo permanente.
K4.2	**La trasmissione dati tramite Bluetooth** K4.2.1 Conoscere come funziona la tecnologia bluetooth. K4.2.2 Comprendere quali sono i rischi per la sicurezza utilizzando il bluetooth.	**S4.2**	**Trasmettere in maniera sicura dati tramite Bluetooth** S4.2.1 Utilizzare la tecnologia Bluetooth. S4.2.2 Utilizzare in maniera sicura la tecnologia bluetooth.

ARGOMENTO 5

LA SICUREZZA DELLE COMUNICAZIONI

e-Competence Framework | e-CF intermediate

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

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K5.1	**La posta elettronica** K5.1.1 Conoscere le vulnerabilità derivanti dall'uso della posta elettronica. K5.1.2 Conoscere come funziona un client email. K5.1.3 Conoscere che cosa è lo spam. K5.1.4 Conoscere il significato di Hoaxes e Urban legend. K5.1.5 Conoscere i vantaggi dell'utilizzo della posta elettronica certificata.	**S5.1**	**Utilizzare in sicurezza la posta elettronica** S5.1.1 Mettere in atto i comportamenti più adeguati per minimizzare i problemi derivanti dall'utilizzo dell'e-mail. S5.1.2 Scegliere un programma e-mail client e impostare un account email. S5.1.3 Riconoscere ed evitare lo spam e gli attacchi phishing. S5.1.4 Riconoscere Hoaxes e Urban legend. S5.1.5 Sapere utilizzare la PEC.
K5.2	**Comunication tecnologies** K5.2.1 Conoscere i differenti strumenti di comunicazione istantanea. K5.2.2 Comprendere vantaggi e svantaggi derivanti da loro utilizzo. K5.2.3 Comprendere il significato del termine Social Engineering e Social Network Poisoning.	**S5.2**	**Utilizzare in sicurezza le chat, la messaggistica istantanea e i social network** S5.2.1 Utilizzare le chat, la messaggistica istantanea e i social network in sicurezza. S5.2.2 Ragionare sull'utilità e le conseguenze di un utilizzo massiggio di questi strumenti. S5.2.3 Riconoscere ed evitare il fenomeno del Social Engineering.
K5.3	**La tecnologia P2P** K5.3.1 Conoscere il significato del termine Peer to Peer. K5.3.2 Comprendere quali sono i rischi introdotti dalla tecnologia P2P.	**S5.3**	**Utilizzare in sicurezza la tecnologia P2P** S5.3.1 La tecnologia Peer to Peer. S5.3.2 I rischi introdotti dalla tecnologia P2P.

ARGOMENTO 6

LA SICUREZZA DELLE RETI

e-Competence Framework | e-CF intermediate

Conoscere quali siano le caratteristiche e i rischi connessi alle reti e alla navigazione su internet. Configurare ed utilizzare quotidianamente un firewall, in considerazione delle minacce più diffuse.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K6.1	**Le connessioni di rete** K6.1.1 Conoscere i vari tipi di connessione LAN.	**S6.1**	**Utilizzare in sicurezza una rete** S6.1.1 Riconoscere e valutare le caratteristiche delle diverse tipologie di rete.
K6.2	**Il Firewall** K6.2.1 Attivare un firewall e sapere come funziona.	**S6.2**	**Utilizzare in maniera efficace un firewall** S6.2.1 Configurare in maniera corretta un firewall.
K6.3	**Le minacce su Internet** K6.3.1 Comprendere il rischio del furto d'identità. K6.3.2 Conoscere il significato del termine spyware. K6.3.3 Comprendere la pericolosità di cookies e codici attivi.	**S6.3**	**Identificare le varie minacce su internet** S6.3.1 Comportarsi in maniera tale da non farsi rubare l'identità online. S6.3.2 Riconoscere ed evitare gli spyware. S6.3.3 Gestire in maniera opportuna codici attivi e cookies.

ARGOMENTO 7

SICUREZZA E PROTEZIONE

e-Competence Framework | e-CF intermediate

Agire proattivamente per la sicurezza dei dati personali e dei dispositivi. Approntare azioni preventive per ridurre i rischi per la sicurezza. Configurare le impostazioni del browser per ottenere il livello ottimale di sicurezza. Configurare in modo appropriato filtri e impostazioni delle applicazioni di sicurezza per proteggere i dati personali e i dispositivi, e navigare malus.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K7.1	**Il principio di "navigazione sicura"** K7.1.1 Conoscere i rischi derivanti dalla navigazione in Rete. K7.1.2 Conoscere i rischi derivanti dall'impiego dei dati personali e sensibili.	**S7.1**	**Ridurre al minimo i rischi per la sicurezza del computer** S7.1.1 Riconoscere le minacce presenti sul Web. S7.1.2 Sapere come difendersi dal *furto di identità* sul Web.
K7.2	**La navigazione sul Web** K7.2.1 Conoscere il funzionamento di cookie e K7.2.2 autorizzazioni. Conoscere il protocollo SSL.	**S7.2**	**Regolare le impostazioni per una navigazione sicura** S7.2.1 Gestire cookie e autorizzazioni. S7.2.2 Conoscere i motivi per cui vengono visualizzati gli avvisi SSL.
K7.3	**Il principio di "protezione"** K7.3.1 Conoscere il sistema di *filtro* previsto dal browser. K7.3.2 Interagire attivamente quando si verificano disservizi o abusi. K7.3.3 Conoscere le applicazioni di Google Chrome. K7.3.4 Sincronizzare i dati sul browser.	**S7.3**	**Filtrare i risultati delle proprie ricerche** S7.3.1 Attivare e tenere attivo il filtro del browser. S7.3.2 Segnalare i contenuti inappropriati. S7.3.3 Modificare le impostazioni di Google Chrome. S7.3.4 Modificare le impostazioni di crittografia e gestire le password.

ARGOMENTO 7

SICUREZZA NELLE COMUNICAZIONI ONLINE

e-Competence Framework | e-CF intermediate

Agire preventivamente per garantire la sicurezza dei dati personali e dei dispositivi. Configurare le impostazioni delle applicazioni per ottenere un livello di sicurezza ottimale. Usare consapevolmente i servizi di comunicazione, impostando filtri appropriati e impostazioni di sicurezza adeguati alla delicatezza dei dati personali e di quelli generici conservati nei dispositivi.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K8.1	**I rischi derivanti dall'uso degli strumenti di comunicazione** K8.1.1 Riconoscere i rischi per la sicurezza associati alle email, ai messaggi istantanei. K8.1.2 Sa cosa sono i sistemi crittografici. K8.1.3 Riconoscere possibili rischi associati alle informazioni pubblicate sui blog o sui social network: divulgazione di informazioni personali, problemi di sicurezza personale, divulgazione pubblica delle proprie idee politiche o religiose.	**S8.1**	**Prevenire i rischi derivanti dall'uso degli strumenti di comunicazione** S8.1.1 Impostare un filtro antispam per le email. S8.1.2 Generare e impiegare una chiave di criptazione per criptare file. S8.1.3 Configurare impostazioni di privacy e sicurezza per messaggi istantanei, blog, social network.

MODULO 2

Privacy e misure di sicurezza in Rete

Cosa sa fare il candidato che si certifica con EIPASS IT SECURITY

Il candidato certificato conosce il concetto di Privacy, il diritto alla riservatezza e gli interessi tutelati. In particolare conosce il diritto all'immagine e i danni provocati dalla violazione di tale diritto in internet. Ha dimestichezza con il diritto d'autore in internet, la libertà di espressione e la tutela dell'onore e della reputazione.

Il candidato acquisisce le nozioni base della legislazione in materia di Codice della privacy e delle fonti normative di rango internazionale e comunitario.

Infine sa applicare le misure minime di sicurezza informatica, soprattutto in materia di trattamento dei dati mediante l'ausilio di sistemi elettronici e in materia di trattamento dei dati sensibili.

Contenuti del modulo

Gli interessi tutelati

- Il diritto all'immagine
- La libertà di espressione in internet
- La tutela dell'onore e della reputazione
- Il diritto d'autore in internet
- Il diritto all'oblio

Il diritto alla riservatezza: evoluzione e tutela giuridica

- Le origini del diritto alla riservatezza
- La legislazione europea in materia di tutela della riservatezza
- Il ruolo delle informazioni e il nuovo concetto di privacy
- Le fonti normative di rango internazionale e comunitario in materi di privacy
- Il Codice della privacy

Le misure di sicurezza informatica

- Profili generali
- Le misure minime di sicurezza
- Il trattamento dei dati mediante l'ausilio di sistemi elettronici
- Misure di sicurezza in materia di trattamento dei dati sensibili e giudiziari

ARGOMENTO 1

GLI INTERESSI TUTELATI

e-Competence Framework | e-CF intermediate

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. 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 più diffusi, 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.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K1.1	**Il diritto all'immagine** K1.1.1 Il danno patrimoniale per la violazione del diritto K1.1.2 all'immagine. La violazione del diritto all'immagine in internet	**S1.1**	**Conoscere le possibilità consentite dalla legge per la pubblicazione delle immagini** S1.1.1 Riconoscere i risvolti patrimoniali dello sfruttamento del diritto all'immagine. S1.1.2 Definire i casi di violazione in internet del diritto all'immagine.
K1.2	**La libertà di espressione in internet**	**S1.2**	**Conoscere i diritti e i doveri intrinseci alla libertà di espressione in internet**
K1.3	**La tutela dell'onore e della reputazione**	**S1.3**	**Riconoscere la potenzialità lesiva della libera manifestazione del pensiero a riguardo dell'onore e della reputazione**
K1.4	**Il diritto d'autore in internet**	**S1.4**	**Conoscere il diritto d'autore in internet e la sua violazione**
K1.5	**Il diritto all'oblio** K1.5.1 La decisione Google Spain K1.5.2 Le recenti sentenze in materia di diritto all'oblio	**S1.5**	**Definire il diritto all'oblio, la sua rilevanza e applicabilità** S1.5.1 Conoscere il caso Google Spain. S1.5.2 Conoscere le più recenti sentenze in materia di diritto all'oblio.

ARGOMENTO 2

IL DIRITTO ALLA RISERVATEZZA

e-Competence Framework | e-CF intermediate

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. Parallelamente, anche le definizioni di diritto all'identità si arricchisce del paradigma digitale, e l'immagine conosce violazioni e sfruttamenti strettamente connessi alle tecnologie informatiche.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K2.1	**Le origini del diritto alla riservatezza**	**S2.1**	**Conoscere le origini del diritto alla riservatezza**
K2.2	**La legislazione europea in materia di tutela della riservatezza**	**S2.2**	**Definire il diritto alla riservatezza nell'ordinamento europeo**
K2.3	**Il ruolo delle informazioni e il nuovo concetto di privacy**	**S2.3**	**Riconoscere i nuovi pericoli e le tutele in relazione all'avvento delle nuove tecnologie e alla loro interazione con la sfera privata**
K2.4	**Le fonti normative di rango internazionale e comunitario in materia di privacy** K2.4.1 La convenzione di Strasburgo del 1981 e la Direttiva K2.4.2 46/95/CE K2.4.3 La legge n. 675 del 1996 K2.4.4 La direttiva 2002/58/CE	**S2.4**	**Conoscere le fonti normative di rango internazionale e comunitario in materia di privacy** S2.4.1 Conoscere la convenzione sulla protezione rispetto al trattamento automatizzato dei dati di carattere personale S2.4.2 Conoscere la legge sulla Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali S2.4.3 Conoscere la Direttiva sul consenso informato
K2.4	**Il Codice della privacy** K2.5.1 La protezione dei dati e lo sviluppo tecnologico nel Regolamento Europeo 679 del 2016	**S2.4**	**Conoscere le disposizioni in materia di trattamento dei dati personali** S2.5.1 Conoscere la disciplina per la protezione dei dati in materia di comunicazione online

ARGOMENTO 3

LE MISURE DI SICUREZZA INFORMATICA

e-Competence Framework | e-CF intermediate

Il tema della sicurezza informatica si intreccia indissolubilmente con il problema della privacy laddove si guardi alle nuove frontiere digitali nella tutela dei dati relativi alle nostre informazioni (genetiche, personali, finanziarie, ecc..) che comportano la ridefinizione dei rapporti tra pubblico e privato, interno ed esterno, stante la complessità dei sistemi giuridici disposti in rete.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K3.1	**Profili generali**	S3.1	**Conoscere i requisiti di sicurezza di rete: disponibilità, autenticazione, integrità e riservatezza**
K3.2	**Le misure minime di sicurezza**	S3.2	**Definire le misure minime di sicurezza**
K3.3	**Il trattamento dei dati mediante l'ausilio di sistemi elettronici**	S3.3	**Conoscere il Sistema di autenticazione informatica**
K3.4	**Misure di sicurezza in materia di trattamento dei dati sensibili e giudiziari**	S3.4	**Conoscere le misure specifiche per il trattamento dei dati sensibili e giudiziari**

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

ARGOMENTO 1

STRUMENTI PRATICI

e-Competence Framework | e-CF intermediate

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.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K1.1	**Parental Control** K1.1.1 Parental Control di Windows. K1.1.2 Parental Control Mac OS di Apple K1.1.3 Restrizione sui Tablet K1.1.4 Parental Control sui browser K1.1.5 Parental Control sull'App di Google K1.1.6 YouTube	**S1.1**	**Conoscere le funzioni del Parental Control** S1.1.1 Attivare il Parental Control sui dispositivi Windows. S1.1.2 Attivare il Parental Control sui dispositivi Mac OS. S1.1.3 Inserire restrizioni nell'utilizzo dell'iPad S1.1.4 Attivare il Parental Control sui browser, in particolare Google Chrome S1.1.5 Attivare il Parental Control sull'App di Google del tablet o dello smartphone S1.1.6 Impostare i filtri su YouTube

ARGOMENTO 2

I SOCIAL NETWORK; INIZIATIVE E STRUMENTI PER LA TUTELA DELLA PRIVACY E DELLA SICUREZZA

e-Competence Framework | e-CF intermediate

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.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K2.1	**Twitter, filtri potenziati contro il cyberbullismo**	**S2.1**	**Conoscere i filtri di Twitter pensati contro il cyberbullismo**
K2.2	**Come tutela i minori Facebook?** K2.2.1 Segnalazione di un minore di età inferiore a 13 anni K2.2.2 Segnalazione di violazione dei diritti di privacy K2.2.3 Segnalazione di un messaggio minaccioso K2.2.4 Pubblicare post K2.2.5 Suggerimenti per parole/filtri (in italiano e inglese)	**S2.12**	**Conoscere le novità di Facebook sulla tutela dei minori** S2.2.1 Conoscere le procedure per segnalare un minore di età inferiore ai 13 anni S2.2.2 Conoscere le procedure per segnalare una violazione dei diritti di privacy S2.2.3 Conoscere le procedure per segnalare un messaggio ritenuto minaccioso S2.2.4 Conoscere le procedure per impostare il pubblico dei post S2.2.5 Individuare le parole, italiane e inglesi, utili per impostare i filtri parentali