



Struttura e sicurezza dei sistemi informatici

Fondamenti ICT e IT Security

Premessa

La competitività, l'innovazione, l'occupazione e la coesione sociale dipendono sempre più da un uso strategico ed efficace delle nuove tecnologie dell'informazione e della comunicazione, che passa soprattutto dalle conoscenze, le capacità, le competenze e l'inventiva dei giovani, dei lavoratori e dei cittadini che utilizzano, tutti i giorni, gli strumenti ICT.



Possedere e certificare le proprie competenze informatiche tramite un sistema riconosciuto e oggettivo facilita la mobilità delle persone. Un "linguaggio" comunemente accettato in questo settore dà la possibilità a tutti di riflettere sulle proprie competenze ICT e, soprattutto, di inserirle sul proprio curriculum, in maniera che possano essere facilmente giudicabili, per esempio, da possibili datori di lavoro che, quindi, avrebbero uno strumento in più per scegliere un nuovo dipendente piuttosto che un altro. Infatti, il quadro descritto in questo documento potrebbe essere utilizzato come "struttura" per rappresentare le e-competence nel Curriculum Europass.

Tratto dall'introduzione di e-Competence Framework for ICT User



L'e-Competence Framework for ICT Users è stato elaborato dal CEN, la Commissione Europea per la standardizzazione, sulla base di una serie di normative e politiche UE, tra cui:

- European e-Skills Summit Declaration:
- Decision 2318/2003/EC per l'adozione di un programma pluriennale finalizzato all'integrazione delle tecnologie dell'informazione e della comunicazione (TIC) nei sistemi di istruzione e formazione in Europa (e-Learning Programme);
- e-Skills in Europe: Towards 2010 and Beyond. Una relazione di sintesi della European e-Skills Forum presentato alla European Conference e-Skills;
- comunicazione della Commissione Europea sull'e-Skills in the 21st Century: Fostering Competitiveness, Growth and Jobs;
- Agenda digitale per l'Europa.

L'e-Competence Framework fornisce un quadro complessivo delle competenze digitali che deve possedere un utilizzatore medio del computer, di Internet e delle nuove tecnologie dell'informazione e della comunicazione; l'uso di un linguaggio condiviso per descrivere competenze, skill e livelli di proficiency lo rende facilmente comprensibile in Europa e nel mondo.

Tale strumento è stato creato per rendere immediatamente verificabili le competenze digitali di studenti e lavoratori alla prese con aziende, manager e dipartimenti delle risorse umane, istituti d'istruzione e organismi di formazione, osservatori di mercato e policy maker, organizzazioni del settore pubblico e privato.

Abbiamo organizzato il programma User facendo diretto riferimento alla classificazione fornita dall'e-Competence Framework for ICT Users (e-CF), per renderlo immediatamente riconoscibile ed utilizzabile in ogni settore: è il primo programma che ne utilizza compiutamente anche la struttura, non limitandosi a recepirne semplicemente i principi ispiratori.

I programmi Pocket Skills, più precisamente, attestano le competenze intermedie nell'utilizzo degli strumenti dell'ICT, così come descritte nella tabella sintetica dell'e-Competence Framework for ICT Users – Part 2: User Guidelines.

I programmi Pocket Skills sono lo strumento migliore per dimostrare oggettivamente il possesso di specifiche competenze nell'utilizzo corretto e maturo degli strumento ICT, nell'ambito della Scuola e dell'Università, in ambienti lavorativi e nella vita di relazione.

Considerata l'indipendenza da ogni specifica casa produttrice di software e/o hardware, il programma rispecchia appieno i criteri di interoperabilità e neutralità richiesti dalla Pubblica Amministrazione.

Centro studi EIPASS

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 sito dedicate al Programma.

Copyright © 2016

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

Nessuna parte di questo documento può essere riprodotta con sistemi elettronici, meccanici o altri, senza l'autorizzazione scritta da Certipass.

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

Struttura e sicurezza dei sistemi informatici - Fondamenti ICT e IT Security

Cosa sa fare il candidato che si certifica con questo Pocket Skills

Il candidato certificato sa descrivere i concetti di software e hardware, conosce le logiche che sovrintendono al funzionamento di un computer, alla gestione/organizzazione dei file e delle cartelle, all'installazione di driver e all'uso di utility di sistema. 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. Sa quanto è importante utilizzare il computer ed i dispositivi in maniera salutare e quali siano le parti riutilizzabili e/o riciclabili, promuovendo un approccio ed una visione ecologica della tecnologia e delle sue applicazioni.

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, recuperarli e trasmetterli in sicurezza tramite la tecnologia Bluetooth. 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 Internet.

Contenuti del modulo

Concetti e definizioni

- la parte hardware e la parte software del pc
- i sistemi operativi più conosciuti
- le applicazioni di base del computer

Organizzare dati e informazioni

- l'organizzazione di file e cartelle
- i diversi sistemi di conservazione dei dati

Internet e le Reti

- come accedere ad Internet
- LAN, Internet, www

Introduzione alla sicurezza informatica

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

Informatica "verde" e sicura

- l'utilizzo sicuro del sistema ICT
- lavorare al pc in maniera sana
- il principio di "Green ICT"

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 bluetooth

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

ARGOMENTO 1

INTRODUZIONE ALL'ICT: CONCETTI E DEFINIZIONI

e-Competence Framework | e-CF intermediate

Riconoscere e descrivere le componenti software ed hardware del computer, nel contesto più generale della Tecnologia dell'Informazione e della Comunicazione. Conoscere ed utilizzare con dimestichezza l'interfaccia grafica e gli strumenti disponibili sul Desktop e le applicazioni di base del computer.

TESTING

Conoscenza teorica/Knowledge (K) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K1.1	La Tecnologia dell'Informazione e della Comunicazione	S1.1	Riconoscere le diverse applicazione dell'ICT
K1.2	La parte hardware del computer	S1.2	Descrivere l'architettura e le componenti hardware di un computer
K1.3	La parte software del computer K1.3.1 Definire il termine sistema operativo K1.3.2 Distinguere i principali tipi di software applicativo. K1.3.3 Conoscere i diversi tipi di licenze per utilizzo dei software.	S1.3	Descrivere le componenti software di un computer S1.3.1 Descrivere i dispositivi per la memorizzazione e trasmissione dell'informazione. S1.3.2 Descrivere/simulare il processo di codifica dell'informazione S1.3.3 Settare e operare sui sistemi più diffusi.
K1.4	Gli strumenti e le utilità del sistema operativo K1.4.1 Conoscere il funzionamento del desktop e delle icone. K1.4.1 Utilizzare le finestre.	S1.4	Utilizzare con sicurezza gli strumenti del sistema operativo S1.4.1 Avviare, arrestare e/o riavviare correttamente il computer. Collegarsi in modo sicuro utilizzando un nome utente. Muoversi efficacemente sul Desktop. Utilizzare, creare, spostare, rinominare ed eliminare icone e collegamenti. Riconoscere le icone più comuni. Utilizzare la barra delle applicazioni. S1.4.1 Aprire e chiudere una finestra, riconoscerne le varie parti, ridurla ad icona, ridimensionarla, chiuderla, passare da finestra ad un'altra. Reperire le informazioni di base del computer. Modificare le configurazione del Desktop. Modificare, aggiungere ed eliminare una lingua dalla tastiera. Chiudere l'applicazione che non risponde. ISTALLARE/disinstallare un'applicazione. Collegare e scollegare in maniera corretta un dispositivo. Catturare l'immagine dello schermo o della finestra attiva.
K1.5	Le operazioni di base del computer K1.5.1 Conoscere i programmi base del sistema operativo.	S1.5	Riconoscere e utilizzare gli strumenti di base del computer S1.5.1 Ottimizzazione la funzionalità del sistema operativo.

ARGOMENTO 2

ORGANIZZARE DATI E INFORMAZIONI

e-Competence Framework | e-CF intermediate

Gestire accuratamente ed in maniera autonoma file e cartelle, riconoscendone gli elementi distintivi e categorizzanti, per tenere sempre in ordine il Desktop e le risorse disponibili nell'Unità.

TESTING

Conoscenza teorica/Knowledge (K) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K2.1	L'organizzazione di file e cartelle K2.1.1 Riconoscere le componenti e l'organizzazione nidificata delle cartelle e dei file	S2.1	Gestire correntemente file e cartelle S2.1.1 Conoscere la gerarchia ad albero. Identificare e differenziare i tipi di file in base all'estensione, indicando la funzione di una estensione. Cercare un file in base all'estensione.
K2.2	La gestione di file e cartelle K2.2.1 Conoscere la modalità tramite cui organizzare in maniera logica le risorse su un PC.	S2.2	Gestire con prontezza e velocità i file e le cartelle S2.1.2 Creare, selezionare, rinominare, salvare, spostare, eliminare, denominare, rinominare e condividere un file o una cartella. Modificare l'ordine dei file contenuti in una cartella, scegliendo fra le opzioni disponibili.

ARGOMENTO 3

INTERNET E LE RETI

e-Competence Framework | e-CF intermediate

Conoscere e definire i principi e gli strumenti più diffusi della Rete, per connettersi autonomamente e in sicurezza, scegliendo la modalità e le condizioni più confacenti ai propri bisogni e alle proprie finalità.

TESTING

Conoscenza teorica/Knowledge (K) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K3.1	L'accesso a internet K3.1.1 Conoscere alcuni dei metodi più diffusi per connettersi a Internet. K3.1.2 Conoscere il significato del termine "provider internet" (Internet Service Provider – ISP).	S3.1	Accedere e navigare S3.1.1 Utilizzare la linea telefonica, la telefonia mobile, il cavo, il wi-fi, il wi-max e il satellite per connettersi. S3.1.2 Scegliere un abbonamento a internet in base alle caratteristiche più importanti (costo, velocità di upload/download).
K3.2	LAN, MAN, WAN K3.2.1 Definire il concetto di "rete". K3.2.2 Definire il concetto di velocità di trasferimento, scaricamento e caricamento.	S3.2	Riconoscere e operare in rete e con le reti S3.2.2 Condividere, accedere a dati e dispositivi. S3.2.3 Distinguere tra World Wide Web, VoIP, posta elettronica, IM.

ARGOMENTO 4

LA SICUREZZA INFORMATICA

e-Competence Framework | e-CF intermedie

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 temi di "proprietà intellettuale" e "copyright" ma anche rispetto alla libera circolazione delle informazioni.

TESTING

Conoscenza teorica/Knowledge (K) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K4.1	La protezione del sistema e degli utenti K4.1.1 Conoscere le principali operazioni di manutenzione e protezione del sistema. K4.1.2 Conoscere gli aspetti di vulnerabilità di un sistema informatico. K4.1.3 Conoscere gli antivirus.	S4.1	Proteggere il sistema e gli utenti S4.1.1 Mettere in atto le attività di routine necessarie per tenere mantenuto ed in sicurezza il PC. S4.1.2 Riconoscere i virus più diffusi. S4.1.3 Comprendere l'importanza dell'aggiornamento dell'antivirus.
K4.2	La sicurezza dei dati e la Privacy K4.2.1 Gestire i dati personali. K4.2.2 Sapere cos'è il firewall.	S4.2	Adottare misure che garantiscono la sicurezza S4.2.1 Comprendere l'importanza di usare credenziali complesse e non lasciarle nelle libera disponibilità di terzi non autorizzati. S4.2.2 Descrivere il funzionamento del firewall.
K4.3	L'ICT e la tutela della proprietà intellettuale K4.3.1 Conoscere le diverse licenze.	S4.3	Identificare i problemi etici e sociali sorti con l'avvento dell'ICT S4.3.1 Descrivere le problematiche inerenti il diritto d'autore: proprietà intellettuale e copyright.

ARGOMENTO 5

INFORMATICA “VERDE” E SICURA

e-Competence Framework | e-CF intermediate

Conoscere i modi per utilizzare il computer e i dispositivi in maniera sana e senza controindicazioni per la propria salute e quella di chi lavora con noi, curando anche postura ed ergonomia. Sapere come attivare le opzioni che consentono di non sprecare energia e/o di riciclare il computer, i dispositivi o parti di essi.

TESTING

Conoscenza teorica/Knowledge (K) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K5.1	L'utilizzo sicuro del computer K5.1.1 Conoscere le precauzioni più diffuse per un utilizzo sicuro del computer.	S5.1	Utilizzare gli strumenti che consentono un utilizzo sicuro del computer S5.1.1 Aggiornare il sistema operativo.
K5.2	Lavorare al computer in maniera sana Conoscere le norme di base per la tutela della salute K5.2.1 nell'utilizzo del computer. Identificare alcune delle opzioni disponibili per K5.2.2 migliorare l'accessibilità.	S5.2	Organizzare la postazione di lavoro in maniere ergonomica e salutare S5.2.1 Illuminare correttamente il monitor e/o il dispositivo e l'ambiente. S5.2.2 Sapere quando effettuare pause, assumere la corretta postura, etc.
K5.3	L'informatica “verde” Conoscere le opzioni di risparmio energetico che si applicano ai computer e ai dispositivi elettronici. Riciclare anche in ambito ICT.	S5.3	Lavorare in maniera “Green” S5.3.1 Impostare lo spegnimento automatico, l'illuminazione dello schermo, la modalità di sospensione. S5.3.2 Sapere quali sono le componenti dei computer e dei dispositivi elettronici che è possibile riciclare e come farlo.

ARGOMENTO 6

IT SECURITY

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) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K6.1	Il problema della sicurezza informatica K6.1.1 Gli standard di sicurezza informatica. K6.1.2 Cosa proteggere (sistemi, dati, informazioni e reti). K6.1.3 Sicurezza attiva e sicurezza passiva. K6.1.4 I diversi livelli di protezione.	S6.1	Gestire il problema della sicurezza informatica K6.1.1 Applicare le linee guida e le politiche. K6.1.2 Proteggere le varie le risorse. K6.1.3 Utilizzare tecniche di sicurezza attiva e passiva. K6.1.4 Adottare le varie tecniche di autenticazione: scegliere in maniera opportuna le password, proteggere la propria password, utilizzare la One-time password.
K6.2	Gli attacchi informatici K6.2.1 Conoscere il significato del termine hacker.	S6.2	Riconoscere gli attacchi informatici K6.2.1 Riconoscere le diverse categorie di hacker.

ARGOMENTO 7 MALWARE

e-Competence Framework | e-CF intermedie

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) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K7.1	Attacchi e minacce informatiche K7.1.1 Comprendere il termine malware, comprendere la differenza tra virus di tipo parassita e virus del settore d'avvio. K7.1.2 Comprendere la differenza tra i vari attacchi login.	S7.1	Identificare i diversi tipi di malware S7.1.1 Riconoscere virus, macro virus, worm e cavalli di troia. S7.1.2 Identificare e bloccare i meccanismi di propagazione.
K7.2	Gli strumenti di difesa K7.2.1 Conoscere i vari strumenti di difesa: antivirus e firewall.	S7.2	Utilizzare i vari strumenti di difesa S7.2.1 Eseguire scansioni antivirus e attivare il Firewall.
K7.3	L'antivirus K7.3.1 Conoscere che cosa è un antivirus e come funziona. K7.3.2 Comprendere l'importanza di una buona configurazione dell'antivirus della scansione. K7.3.3 Comprendere l'importanza dell'aggiornamento dell'antivirus. K7.3.4 Comprendere il ruolo dei sistemi operativi e dei programmi per la protezione.	S7.3	Riconoscere le funzionalità dell'antivirus S7.3.1 Descrivere come funziona un antivirus. S7.3.2 Descrivere le differenti modalità di scansione. S7.3.3 Descrivere cosa si intenda per euristica e virus polimorfo. S7.3.4 Comprendere quali siano i software più esposti agli attacchi malevoli

ARGOMENTO 8

SICUREZZA DEI DATI

e-Competence Framework | e-CF intermedie

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) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K8.1	La gestione sicura dei dati K8.1.1 Comprendere l'importanza di gestire i dati in sicurezza. K8.1.2 Conoscere le tecniche di protezione dei dati. K8.1.3 Conoscere le tecniche di ripristino dei dati. K8.1.4 Comprendere l'importanza di eliminare in modo permanente i dati.	S8.1	Gestire i dati in maniera sicura S8.1.1 Riconoscere i principi alla base dell'IT Security (autenticità, affidabilità, integrità...) S8.1.2 Salvare efficacemente i dati disponibili. S8.1.3 Preparare un disco di ripristino dei dati. S8.1.4 Eliminare i dati in modo permanente.
K8.2	La trasmissione dati tramite Bluetooth K8.2.1 Conoscere come funziona la tecnologia bluetooth. K8.2.2 Comprendere quali sono i rischi per la sicurezza utilizzando il bluetooth.	S8.2	Trasmettere in maniera sicura dati tramite Bluetooth S8.2.1 Utilizzare la tecnologia Bluetooth. S8.2.2 Utilizzare in maniera sicura la tecnologia bluetooth.

ARGOMENTO 9

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) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K9.1	La posta elettronica K9.1.1 Conoscere le vulnerabilità derivanti dall'uso della posta elettronica. K9.1.2 Conoscere come funziona un client email. K9.1.3 Conoscere che cosa è lo spam. K9.1.4 Conoscere il significato di Hoaxes e Urban legend. K9.1.5 Conoscere i vantaggi dell'utilizzo della posta elettronica certificata.	S9.1	Utilizzare in sicurezza la posta elettronica S9.1.1 Mettere in atto i comportamenti più adeguati per minimizzare i problemi derivanti dall'utilizzo dell'e-mail. S9.1.2 Scegliere un programma e-mail client. S9.1.3 Riconoscere ed evitare lo spam e gli attacchi phishing. S9.1.4 Riconoscere Hoaxes e Urban legend. S9.1.5 Sapere utilizzare la PEC.
K9.2	Comunicazione tecnologie K9.2.1 Conoscere i differenti strumenti di comunicazione istantanea. K9.2.2 Comprendere vantaggi e svantaggi derivanti da loro utilizzo. K9.2.3 Comprendere il significato del termine Social Engineering e Social Network Poisoning.	S9.2	Utilizzare in sicurezza le chat, la messaggistica istantanea e i social network S9.2.1 Utilizzare le chat, la messaggistica istantanea e i social network in sicurezza. S9.2.2 Valutare ed eventualmente cambiare le impostazioni di default. S9.2.3 Riconoscere ed evitare il fenomeno del Social Engineering.
K9.3	La tecnologia peer to peer (P2P) K9.3.1 Conoscere il significato del termine Peer to Peer. K9.3.2 Comprendere quali sono i rischi introdotti dalla tecnologia P2P.	S9.3	Utilizzare in sicurezza la tecnologia P2P S9.3.1 La tecnologia Peer to Peer. S9.3.2 I rischi introdotti dalla tecnologia P2P.

ARGOMENTO 10

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) <i>Il Candidato conosce, è informato, ha familiarità con...</i>		Competenze pratiche / Skills (S) <i>Il Candidato è capace di</i>	
K10.1	Le connessioni di rete K10.1.1 Conoscere i vari tipi di connessione LAN.	S10.1	Utilizzare in sicurezza una rete S10.1.1 Riconoscere ed applicare le diverse tipologie di rete.
K10.2	Il Firewall K10.2.1 Attivare un firewall e sapere come funziona.	S10.2	Utilizzare in maniera efficace un firewall S10.2.1 Configurare in maniera corretta un firewall.
K10.3	Le minacce su Internet K10.3.1 Comprendere il rischio del furto d'identità. K10.3.2 Conoscere il significato del termine spyware. K10.3.3 Comprendere la pericolosità di cookies e codici attivi.	S10.3	Identificare le varie minacce su internet S10.3.1 Riconoscere i vari tipi di attacchi su internet. S10.3.2 Riconoscere ed evitare gli spyware. S10.3.3 Gestire in maniera opportuna codici attivi e cookies.

www eipass com

info@eipass.com



NUMERO VERDE
800.088.331