ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL' UNIVERSITÀ E DELLA RICERCA
PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA – DIRETTIVA 170/2016

FEDER CONSULTING
Centro di Formazione

ECDL epass®
european informatics passport

Programma analitico d'esame

INFORMATICA GIURIDICA

Premessa

La società occidentale attuale può essere definita società dell'informazione, in essa si scambiano quotidianamente milioni di informazioni e si condividono immagini e filmati. In questo scenario va considerata la possibilità di cadere nell'errore d'informazione, con la conseguente facilità di screditamento del singolo, sopprimendo la sua libertà di pensiero e attaccando i diritti della personalità. Insomma, l'altra faccia della medaglia delle possibilità offerte dalla Rete è rappresentata dai rischi legati a un uso improprio di questo strumento.

Inoltre le moderne tecnologie hanno reso possibile il commercio elettronico e la net-economy, che vanno però disciplinati da regole precise che tutelino sia il venditore che l'acquirente, in modo da rendere l'economia in internet quanto più pulita e trasparente.

Il corso insegna a cogliere le nuove prospettive offerte e a utilizzarle, a conoscere i danni delle tecnologie e a saper riconoscere i diritti dell'individuo che si appresta a utilizzarle.

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.

Destinatari

Il corso online EIPASS Informatica giuridica è rivolto a tutti coloro i quali vogliano approfondire i diritti, i danni, le normative e i reati connessi all'utilizzo delle nuove tecnologie, in particolare in materia di privacy e trattamento dei dati, di commercio elettronico e di cybercrimes.

Moduli d'esame

1. Nuove tecnologie: diritti e danni
2. Il commercio elettronico
3. PEC, firma digitale e archiviazione di documenti digitali
4. Cybercrimes: criminologia e reati informatici

MODULO 1

Nuove tecnologie: diritti e danni

Cosa sa fare il candidato che si certifica con EIPASS Informatica Giuridica

La società occidentale attuale può essere definita società dell'informazione, in essa si scambiano quotidianamente milioni di informazioni e si condividono immagini e filmati.

In questo scenario va considerata la possibilità di cadere nell'errore d'informazione, con la conseguente facilità di screditamento del singolo, sopprimendo la sua libertà di pensiero e attaccando i diritti della personalità.

Dalla menomazione totale o parziale dell'integrità fisica o, in ogni caso, dalla lesione della salute o dei valori inerenti la persona, possono scaturire conseguenze di carattere patrimoniale e non patrimoniale; lo studio di tali fattispecie è uno strumento necessario di conoscenza per tutti gli esperti di diritto, ma anche per docenti, educatori e professionisti del campo.

Tale conoscenza diventa strumento utile anche a definire nuovi parametri di tutela della persona, parametri che non rispettano più le tradizionali categorie ma vanno riadattati alle nuove attitudini lesive.

Argomento - Moduli	Ambiti di intervento - Capitoli	Conoscenze e competenze - Paragrafi
Nuove tecnologie: diritti e danni	1. Le nuove tecnologie e i nuovi danni	1.1 Il danno patrimoniale: danno emergente e lucro cessante 1.2 La risarcibilità del danno non patrimoniale 1.3 Danno alla persona e danno alla lesione dei diritti della personalità
	2. Il risarcimento del danno non patrimoniale	2.1 Le categorie di danno non patrimoniale: biologico, morale, esistenziale 2.2 I danni bagatellari 2.3 Il danno non patrimoniale delle persone giuridiche
	3. Gli interessi tutelati	3.1 La lesione all'integrità psico-fisica 3.2 La violazione dell'identità personale 3.3 Il diritto all'immagine 3.4 La libertà di espressione in internet 3.5 La tutela dell'onore e della reputazione 3.6 Il diritto d'autore in internet 3.7 Il diritto all'oblio
	4. Il diritto alla riservatezza: evoluzione e tutela giuridica	4.1 Le origini del diritto alla riservatezza 4.2 La legislazione europea in materi di tutela della riservatezza 4.3 Il ruolo delle informazioni e il nuovo concetto di privacy 4.4 Le fonti normative di rango internazionale e comunitario in materia di privacy 4.5 Il Codice della privacy

5. Le misure di sicurezza informatica	5.1 Le misure di sicurezza informatica: profili generali 5.2 Le misure di sicurezza nel Regolamaneto UE n. 679/2016 5.3 Privacy by design 5.4 Privacy by default 5.5 La valutazione di impatto sulla protezione die dati 5.6 Le violazioni delle misure di sicurezza informatica: profili di responsabilità

MODULO 2

Il commercio elettronico

Cosa sa fare il candidato che si certifica con EIPASS Informatica Giuridica

La Comunicazione della Commissione UE 97/157 fornisce una delle definizioni che meglio delinea le caratteristiche e le potenzialità del commercio elettronico, definendolo come «lo svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse quali la commercializzazione di beni e servizi per via elettronica, la distribuzione on- line di contenuti digitali, l'effettuazione per via elettronica di operazioni finanziarie e di borsa, gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo della Pubblica Amministrazione».

Le moderne tecnologie hanno reso possibile ciò che sembrava impossibile: il corso insegna a cogliere le nuove prospettive offerte dalla *net-economy* e a utilizzarle. Particolare rilevanza in questo contesto assume quindi il concetto di *point and click*: oggi un semplice click funge da consenso e diventa manifestazione di volontà, anche quando le clausole negoziali siano nascoste in altre pagine dei siti.

L'e-commerce va perciò disciplinato da precise regole che tutelino sia il venditore che l'acquirente, in modo da rendere l'economia in internet quanto più pulita e trasparente.

Argomento - Moduli	Ambiti di intervento - Capitoli	Conoscenze e competenze - Paragrafi
Il commercio elettronico	1. Il commercio elettronico	1.1 Le questioni giuridiche legate all'e-commerce 1.2 La definizione di e-commerce 1.3 Le tipologie di e-commerce 1.4 La normativa europea in materi di commercio elettronico 1.5 La normativa italiana in materia di commercio elettronico 1.6 Comunicazioni commerciali e spamming
	2. I contratti nel commercio elettronico	2.1 Le modalità di conclusione del contratto telematico 2.2 I contratti del commercio elettronico: il momento del perfezionamento 2.3 Il luogo di conclusione dei contratti telematici 2.4 La revoca nel contratto telematico 2.5 I contraenti. La legge applicabile e la giurisdizione competenze 2.6 La forma del contratto telematico
	3. Gli strumenti di pagamento	3.1 La carta di credito 3.2 La moneta elettronica 3.3 Il bonifico bancario 3.4 Il contrassegno 3.5 Il sistema Paypal 3.6 Square e Google Check-out
	4. Le altre questioni connesse al commercio elettronico	4.1 La tutela del consumatore 4.2 L'e-commerce e la tutela della privacy 4.3 Le misure di sicurezza 4.4 Il trattamento dei dati mediante l'ausilio di sistemi elettronici 4.5 Le comunicazioni commerciali non desiderate

5. I segni distintivi del commercio elettronico	5.1 I nomi a dominio 5.2 I contratti conclusi con i provider 5.3 Le responsabilità dell'Internet Service Provider
6. Le tipologie di e-commerce	6.1 Le tipologie di e-commerce 6.2 Il commercio elettronico indiretto 6.3 Il commercio elettronico diretto 6.4 Il momento impositivo
7. Il concetto di stabile organizzazione	7.1 La stabile organizzazione e il commercio elettronico 7.2 I potenziali profili elusivi legati alla nozione di stabile organizzazione nelle attività di commercio elettronico 7.3 Le novità introdotte dalla Legge n.208 del 28 Dicembre 2015 (legge di stabilità per il 2016)
8. L'attività di e-commerce	8.1 Come avviare e esercitare un'attività di e-commerce

MODULO 3

PEC, firma digitale e archiviazione

Cosa sa fare il candidato che si certifica con EIPASS Informatica Giuridica

Il nuovo sistema di invio e ricezione documenti è uno strumento strategico per le PA e il rapporto con i suoi utenti, può essere utilizzata in qualsiasi contesto nel quale sia necessario avere prova opponibile dell'invio e della consegna di un determinato documento. In altri termini consente di disporre di una prova legalmente valida, con preciso riferimento temporale, dell'avvenuta spedizione di un determinato messaggio, con l'eventuale documentazione allegata, nonché della sua consegna ai destinatari designati.

La firma digitale è un particolare tipo di firma elettronica avanzata che consente al titolare e al destinatario, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico. La firma digitale consente, infatti, di scambiare in rete documenti con piena validità legale, e può essere rilasciata a tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni.

Le Pubbliche amministrazioni, comprese le Istituzioni scolastiche, hanno ormai l'obbligo di gestire i flussi documentali integrati con il protocollo informatico ed elaborare i relativi piani di conservazione. La gestione dei flussi documentali è «l'insieme delle attività che consentono di organizzare la documentazione delle amministrazioni».

Argomento - Moduli	Ambiti di intervento - Capitoli	Conoscenze e competenze - Paragrafi
PEC, firma elettronica e archiviazione di documenti digitali	1. La Posta Elettronica Certificata (PEC)	1.1 Che cos'è la PEC 1.2 La procedura di invio di un messaggio tramite PEC 1.3 Il registro generale degli indirizzi elettronici 1.4 Il dominio digitale
	2. I documenti informatici e le firme elettroniche	2.1 La firma digitale 2.2 Firma elttronica ed efficacia probatoria dei documenti informatici 2.3 Il sigillo elettronico
	3. L'archiviazione dei documenti digitali	3.1 La digitalizzazione della Pubblica Amministrazione 3.2 L'informatizzazione 3.3 La dematerializzazione 3.4 La digitalizzazione 3.5 Il documento informatico 3.6 La conservazione dei documenti della Pubblica amministrazione

MODULO 4

Cybercrimes: Criminologia e reati informatici

Cosa sa fare il candidato che si certifica con EIPASS Informatica Giuridica

Internet offre a tutti nuove possibilità, abbattendo le distanze, permettendo l'informazione gratuita e favorendo la condivisione. L'altra faccia della medaglia è però rappresentata dai rischi legati a un uso improprio di questo strumento.

Tra i reati informatici che più spesso si nominano vi sono virus e malware, furto di identità, cyberstalking e pedofilia, reati le cui dinamiche sono difficilmente riconoscibili. Difatti, tanti utenti del web non sanno riconoscere episodi criminali né possono da questi difendersi.

Attraverso il corso *Cybercrimes*: criminologia e reati informatici si forniscono competenze basilari in materia di diritto penale, si presentano i reati in internet, approfondendo gli aspetti più significativi dal punto di vista criminologico. Obiettivo centrale è di ridimensionare il profilo del Cybercriminale, il suo modus operandi, la firma, la vittimologia e i fattori di rischio. I reati informatici previsti dall'ordinamento italiano sono diversi e per questo è fondamentale per adulti e ragazzi conoscerli, affinché l'ambiente del web non diventi un posto ad alto rischio di criminalità.

Argomento - Moduli	Ambiti di intervento - Capitoli	Conoscenze e competenze - Paragrafi
Cybercrimes: criminologia e reati informatici	1. Introduzione alla criminologia	1.1 Evoluzione storica 1.2 Criminologie, criminalistica e investigazione criminale 1.3 Studio del fenomeno criminale 1.4 Autori del crimine e criminal profiling 1.5 Vittimologie 1.6 Crime mapping
	2. Cybercrimes e aspetti criminologici	2.1 Autori e cybercrime: criminal profiling 2.2 Le vittime 2.3 Computer forensics
	3. Alcune fattispecie delittuose	3.1 Cyberstalking 3.2 Cyberbullismo 3.3 Cyberpedofilia 3.4 Cyberterrorismo
	4. Lineamenti di diritto penale	4.1 I principi del diritto penale 4.2 Il reato 4.3 Il tentativo 4.4 Le circostanze del reato 4.5 Il concorso di reati 4.6 Il concorso di persone nel reato 4.7 La punibilità, la pena e le misure di sicurezza
	5. I reati informatici	5.1 I principi del diritto penale 5.2 La Legge n. 547 del 1993 5.3 La legislazione europea 5.4 I reati informatici

6. I reati a mezzo internet	6.1 Ingiuria e diffamazione (artt. 594, 595 c.p.)
	6.2 Sostituzione di persona (art. 494 c.p.)
	6.3 Molestia o disturbo alle persone (art. 660 c.p.)
	6.4 Atti persecutori (art. 612-bi c.p.) e cyberstalking
	6.5 Cyberbullismo
	6.6 Pedopornografia (artt. 600-ter, 600-quater, 600- quater.1 c.p.)
	6.7 Estorsione
	6.8 Art. 167 cod. privacy
	6.9 Cyberterrorismo

www eipass com

info@eipass.com

NUMERO VERDE
800.088.331