

## Programma analitico d'esame

### EIPASS CYBERCRIMES

#### 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 il modulo.

#### Destinatari

Avvocati, docenti, studenti, impiegati, formatori, professionisti e chiunque voglia approfondire l'utilizzo degli strumenti ICT dal punto di vista giuridico, in particolare gli aspetti criminologici delle fattispecie delittuose perpetuate tramite internet.

#### Modulo d'esame

**Modulo 1** | Cybercrimes: reati informatici



## Modulo 1

# MODULO CYBERCRIMES: REATI INFORMATICI

## Cosa sa fare il Candidato che si certifica con EIPASS Cybercrimes

L'evoluzione della tecnologia ha portato al progressivo mutamento della normativa penale per adeguarla alla cybersecurity: l'avvento del cybercrime, con l'introduzione dei reati informatici, ha condotto il legislatore a rendere sempre più specifiche le fattispecie.

Un crimine informatico è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica sia hardware che software, per la commissione di uno o più crimini.

La casistica e la tipologia sono piuttosto ampie.

L'obiettivo in questa sede è fornire competenze basilari in materia di diritto penale: si presentano i reati in internet, approfondendone gli aspetti più significativi.

## Contenuti del modulo

- Introduzione
- Cybercrime: una guerra globale
- Cybercrime e diritto penale
- Struttura e classificazione del computer crimes
- Le frodi informatiche
- Le falsità informatiche
- I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici
- I reati contro la riservatezza informatica



Ambiti di intervento		Conoscenze e competenze	
Capitoli		Paragrafi	
1	Cybercrime: una guerra globale	1.1	La rilevanza del fenomeno dei reati informatici
		1.2	Le fonti sovranazionali del diritto penale dell'informatica
		1.3	I reati informatici nell'ordinamento italiano
2	Cybercrime e diritto penale	2.1	Il cybercrime nella cornice del diritto penale
		2.2	I principali principi del diritto penale: il principio di legalità e i suoi corollari
		2.3	I principi di determinatezza e tassatività
		2.4	Il principio di irretroattività della legge penale
		2.5	Il principio di materialità
		2.6	Il principio di offensività
3	Struttura e classificazione dei computer crimes	3.1	Definizioni e struttura dei reati informatici
		3.2	Il problema del bene giuridico protetto dai reati informatici
		3.3	La classificazione degli illeciti informatici: dai reati informatici ai reati cibernetici
		3.4	Le categorie dei reati informatici (in senso stretto)
4	Le frodi informatiche	4.1	Il fenomeno delle frodi informatiche
		4.2	Il delitto di frode informatica (art. 640 <i>ter</i> c.p.)
		4.3	Le condotte del reato di frode informatica
		4.4	Elemento soggettivo, consumazione ed evento
		4.5	Le circostanze aggravanti e il cd. phishing
		4.6	Rapporti con altri reati
		4.7	Il delitto di frode informatica del certificatore di firma digitale (art. 640 <i>quinqies</i> c.p.)
5	Le falsità informatiche	5.1	La natura dell'art. 491 <i>bis</i> c.p.
		5.2	La nozione di documento informatico
		5.3	Il bene giuridico protetto e le condotte di falsificazione informatica
		5.4	Condotta ed elemento soggettivo del reato
		5.5	Falsificazione o alterazione di carte di pagamento
		5.6	La struttura del reato di falsificazione o alterazione di carte di credito e pagamento
		5.7	Il reato di sostituzione di persona nell'era digitale



6	I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici	6.1	Introduzione
		6.2	Il microsistema dei danneggiamenti informatici
		6.3	Le condotte di danneggiamento informatico
		6.4	L'elemento soggettivo
		6.5	Le circostanze aggravanti
		6.6	Il reato di diffusione di apparecchiatura, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 <i>quinquies</i> c.p.)
		6.7	La nuova nozione di «violenza sulle cose» prevista dall'art. 392, co. 3, c.p.
7	I reati contro la riservatezza informatica	7.1	Introduzione
		7.2	L'accesso abusivo ad un sistema informatico o telematico (art. 615 <i>ter</i> c.p.)
		7.3	Detenzione e diffusione abusive di codici di accesso a sistemi informatici o telematici (art. 615 <i>quater</i> c.p.)
		7.4	Diffusione di apparecchiature dirette a danneggiare un sistema informatico o telematico (art. 615 <i>quinquies</i> c.p.)
		7.5	Le intercettazioni informatiche e telematiche
		7.6	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 <i>sexies</i> c.p.)
		7.7	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 <i>sexies</i> c.p.)

