



# Cybercrimes

Programma analitico d'esame

## 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 portale [eipass.com](http://eipass.com) dedicate al Programma.

### Copyright © 2026

Tutti i diritti sono riservati a norma di legge e in osservanza delle convenzioni internazionali. Nessuna parte di questo Programma può essere riprodotta con sistemi elettronici, meccanici o altri, senza apposita autorizzazione scritta da parte di CERTIPASS. Nomi e marchi citati nel testo sono depositati o registrati dalle rispettive case produttrici.

Il logo EIPASS® è di proprietà esclusiva di CERTIPASS. Tutti i diritti riservati.

## Premessa

Il cybercrime è un fenomeno complesso che abbraccia una gamma molto ampia di condotte criminali. Così come accade per il crimine tradizionale, quello informatico può assumere forme diverse e può essere perpetrato in qualsiasi momento e luogo, sfruttando le stesse infrastrutture digitali che connettono il mondo moderno.

Nel delineare i confini di questa materia, il quadro internazionale offre diversi punti di riferimento. Il trattato del Consiglio d'Europa riconduce il cybercrime ai reati contro i dati riservati e alla violazione del diritto d'autore. La Convenzione di Budapest sul Cybercrime (2001) offre la definizione tecnica di riferimento: sono computer crimes tutte le violazioni penali commesse per mezzo di un sistema informatico o che hanno il sistema stesso come obiettivo dell'attacco.

Un fenomeno in continua trasformazione, che non conosce confini geografici e colpisce indiscriminatamente cittadini, imprese e istituzioni. La sua capacità di evolversi rapidamente impone una risposta coordinata sul piano normativo e investigativo.

Questo modulo accompagna il lettore attraverso il diritto penale dell'informatica: dalle fonti internazionali alla normativa italiana, dalle principali fattispecie di reato fino alle novità della Riforma Nordio del 2024.

*Certipass*  
Centro Studi

## *Programma analitico d'esame*

### **Cybercrimes**

#### **Metodo**

Il corso online EIPASS Cybercrimes è rivolto ad avvocati, docenti, studenti, impiegati, formatori e professionisti, nonché a chiunque desideri approfondire uno dei temi più attuali e complessi del diritto penale contemporaneo: il *cybercrime*, ovvero l'insieme dei reati commessi mediante o contro sistemi informatici e telematici.

#### **Prova d'esame e valutazione**

Il rilascio della certificazione avverrà previo sostenimento e superamento di esami (uno per ciascun modulo), tramite piattaforma DIDASKO. Per superare ogni esame, il candidato dovrà rispondere correttamente ad almeno il 75% delle 30 domande previste, in un tempo massimo di 30 minuti.

Sono previste domande con risposta a scelta multipla.

Ogni esame è unico, essendo le domande e l'ordine delle risposte scelto casualmente dal sistema. Lo stesso sistema calcolerà la percentuale di risposte esatte fornite, decretando istantaneamente il superamento o meno dell'esame: non essendovi, quindi, alcun intervento da parte di un Docente/Esaminatore, viene garantita l'obiettività dell'esito conseguito. L'eventuale mancato superamento di uno o più dei previsti moduli comporterà la ripetizione degli stessi attraverso prova suppletiva.

#### **Moduli d'esame**

**Modulo 1** | Cybercrimes

## **Modulo 1**

# **CYBERCRIMES: REATI INFORMATICI**

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

Il candidato certificato conosce il fenomeno del cybercrime nella sua dimensione globale e transnazionale e sa orientarsi tra le principali fonti normative, internazionali e nazionali, che disciplinano i reati informatici.

Conosce i principi fondamentali del diritto penale applicati al contesto digitale: il concetto di reato, la distinzione tra crimini informatici e reati tradizionali, i beni giuridici tutelati e i principi di legalità, determinatezza, tassatività, irretroattività, materialità e offensività.

È inoltre in grado di riconoscere le principali fattispecie previste dal codice penale italiano, dalle frodi e falsità informatiche al danneggiamento di dati e sistemi, fino ai reati contro la riservatezza informatica e alle intercettazioni telematiche. Conosce, infine, le novità introdotte dalla riforma Nordio (legge n. 90/2024), inclusa l'estorsione informatica

## **Contenuti del modulo**

### **Cybercrimes e reati informatici**

- Cybercrime: una guerra globale

### **Cybercrime e diritto penale**

- Il cybercrime nella cornice del diritto penale
- I principali principi del diritto penale: il principio di legalità e i suoi corollari

### **Struttura e classificazione dei computer crimes**

- Definizione e struttura dei reati informatici

### **Le frodi informatiche**

- Il fenomeno delle frodi informatiche

### **Le falsità informatiche**

- La natura dell'art. 491 bis c.p.
- Falsificazione o alterazione di carte di pagamento

### **I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici**

- Introduzione

### **I reati contro la riservatezza informatica**

- Introduzione

### **I reati informatici a seguito della riforma Nordio legge 28 giugno 2024, n. 90**

- Reati informatici

## 1 | CYBERCRIMES E REATI INFORMATICI

| Knowledge/Conoscenze |                                | Skills/Capacità pratiche |   |
|----------------------|--------------------------------|--------------------------|---|
| 1.1                  | Cybercrime: una guerra globale | 1.1.1                    | La rilevanza del fenomeno dei reati informatici             |
|                      |                                | 1.1.2                    | Le fonti sovranazionali del diritto penale dell'informatica |
|                      |                                | 1.1.3                    | I reati informatici nell'ordinamento italiano               |

## 2 | CYBERCRIME E DIRITTO PENALE

| Knowledge/Conoscenze |   | Skills/Capacità pratiche |  |
|----------------------|---|--------------------------|--|
| 2.1                  | Il cybercrime nella cornice del diritto penale  | 2.1.1                    | Il diritto penale: reati, sanzioni e soggetti      |
| 2.2                  | I principali principi del diritto penale: il principio di legalità e i suoi corollari | 2.2.1                    | I principi di determinatezza e tassatività         |
|                      |   | 2.2.2                    | Il principio di irretroattività della legge penale |
|                      |   | 2.2.3                    | Il principio di materialità                        |
|                      |   | 2.2.4                    | Il principio di offensività                        |

## 3 | STRUTTURA E CLASSIFICAZIONE DEI COMPUTER CRIMES

| Knowledge/Conoscenze |   | Skills/Capacità pratiche |   |
|----------------------|---|--------------------------|---|
| 3.1                  | Definizioni e struttura dei reati informatici | 3.1.1                    | Tecnica di normazione e definizioni operative   |
|                      |   | 3.1.2                    | Il problema del bene giuridico protetto dei reati informatici                             |
|                      |   | 3.1.3                    | La classificazione degli illeciti informatici: dai reati informatici ai reati cibernetici |
|                      |   | 3.1.4                    | Le categorie dei reati informatici (in senso stretto)                                     |

#### 4 | LE FRODI INFORMATICHE

| Knowledge / Conoscenze |                                      | Skills / Capacità pratiche |   |
|------------------------|--------------------------------------|----------------------------|---|
| 4.1                    | Il fenomeno delle frodi informatiche | 4.1.1                      | Il delitto di frode informatica (art. 640 ter c.p.)   |
|                        |                                      | 4.1.2                      | Le condotte del reato di frode informatica  |
|                        |                                      | 4.1.3                      | Elemento soggettivo, consumazione ed evento   |
|                        |                                      | 4.1.4                      | Le circostanze aggravanti e il cd. phishing   |
|                        |                                      | 4.1.5                      | Rapporti con altri reati  |
|                        |                                      | 4.1.6                      | Il delitto di frode informatica del certificatore di firma digitale (art. 640 quinquies c.p.) |

#### 5 | LE FALSITÀ INFORMATICHE

| Knowledge / Conoscenze |  | Skills / Capacità pratiche |  |
|------------------------|--|----------------------------|--|
| 5.1                    | La natura della norma dell'art. 491 bis c.p.       | 5.1.1                      | Struttura e natura giuridica della norma   |
|                        |  | 5.1.2                      | La nozione di documento informatico  |
|                        |  | 5.1.3                      | Il bene giuridico protetto e le condotte di falsificazione informatica                 |
|                        |  | 5.1.4                      | Condotta ed elemento soggettivo del reato  |
| 5.2                    | Falsificazione o alterazione di carte di pagamento | 5.2.1                      | Art. 493 ter c.p.  |
|                        |  | 5.2.2                      | La struttura del reato di falsificazione o alterazione di carte di credito e pagamento |
|                        |  | 5.2.3                      | Il reato di sostituzione di persona nell'era digitale                                  |

#### 6 | I DELITTI CONTRO L'INTEGRITÀ DEI DATI, DEI PROGRAMMI E DEI SISTEMI INFORMATICI

| Knowledge / Conoscenze |              | Skills / Capacità pratiche |   |
|------------------------|--------------|----------------------------|---|
| 6.1                    | Introduzione | 6.1.1                      | Il microsistema dei danneggiamenti informatici  |
|                        |              | 6.1.2                      | Le condotte di danneggiamento informatico   |
|                        |              | 6.1.3                      | L'elemento soggettivo   |
|                        |              | 6.1.4                      | Le circostanze aggravanti   |
|                        |              | 6.1.5                      | Il reato di diffusione di apparecchiatura, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.) |
|                        |              | 6.1.6                      | La nuova nozione di «violenza sulle cose» prevista dall'art. 392, co. 3, c.p.   |

## 7 | I REATI CONTRO LA RISERVATEZZA INFORMATICA

| Knowledge/Conoscenze |              | Skills/Capacità pratiche |   |
|----------------------|--------------|--------------------------|---|
| 7.1                  | Introduzione | 7.1.1                    | L'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)  |
|                      |              | 7.1.2                    | Detenzione e diffusione abusive di codici di accesso a sistemi informatico o telematici (art. 615 quater c.p.)                                    |
|                      |              | 7.1.3                    | Diffusione di apparecchiature dirette a danneggiare un sistema informatico o telematico (art. 615 quinquies c.p.)                                 |
|                      |              | 7.1.4                    | Le intercettazioni informatiche e telematiche   |
|                      |              | 7.1.5                    | Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) |
|                      |              | 7.1.6                    | Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.)                       |

## 8 | I REATI INFORMATICA SEGUITO DELLA RIFORMA NORDIO LEGGE 28 GIUGNO 2024, N. 90

| Knowledge/Conoscenze |                   | Skills/Capacità pratiche |  |
|----------------------|-------------------|--------------------------|--|
| 8.1                  | Reati informatici | 8.1.1                    | La legge Nordio e i reati informatici  |
|                      |                   | 8.1.2                    | Il nuovo delitto di accesso abusivo a un sistema informatico o telematico (art. 615- ter c.p.)   |
|                      |                   | 8.1.3                    | Il delitto di detenzione e diffusione abusiva di apparecchiature, codice e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 – quater c.p.)  |
|                      |                   | 8.1.4                    | Il delitto di detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-bis c.p.) |
|                      |                   | 8.1.5                    | Il delitto di intercettazione, impedimento o interruzione illecita di comunicazione informatiche o telematiche (art. 617 -quater c.p.)   |
|                      |                   | 8.1.6                    | Il delitto di falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 -sexies c.p.)   |
|                      |                   | 8.1.7                    | Le disposizioni comuni: circostanze attenuanti   |

|  |  |        |   |
|--|--|--------|---|
|  |  | 8.1.8  | Il nuovo delitto di estorsione informatica  |
|  |  | 8.1.9  | Le modifiche alle fattispecie di danneggiamento   |
|  |  | 8.1.10 | Le modifiche al codice di procedura penale alle norme sui collaboratori di giustizia e in tema di responsabilità amministrativa degli enti (d. lgs 231/20019) |