Professioni & Concorsi

MANUALE
E QUESITI

CONCORSO

980 POSTI
AGENZIA DOGANE e MONOPOLI

100 Periti informatici (ADM/PINF)
32 Informatici (ADM/INF)

PROVA SCRITTA e ORALE

MANUALE e **QUESITI**
per la **prova scritta** e **orale**

IN OMAGGIO

ESTENSIONI **ONLINE**
TEST DI **VERIFICA**
SOFTWARE DI **ESERCITAZIONE**

EdiSES edizioni

MANUALE
E QUESITI

CONCORSO

980 POSTI
AGENZIA DOGANE e MONOPOLI

100 **Periti informatici** (ADM/PINF)
32 **Informatici** (ADM/INF)

PROVA SCRITTA e ORALE

MANUALE e **QUESITI** per la **prova scritta** e **orale**

Accedi ai servizi riservati

Il codice personale contenuto nel riquadro dà diritto a servizi riservati ai clienti. Registrandosi al sito, dalla propria area riservata si potrà accedere a:

MATERIALI DI INTERESSE
E CONTENUTI AGGIUNTIVI

CODICE PERSONALE

Grattare delicatamente la superficie per visualizzare il codice personale.
Le **istruzioni per la registrazione** sono riportate nella pagina seguente.
Il volume NON può essere venduto né restituito se il codice personale risulta visibile.
L'**accesso ai servizi riservati** ha la **durata di 18 mesi** dall'attivazione del codice e viene garantito esclusivamente sulle edizioni in corso.

Istruzioni per accedere ai contenuti e ai servizi riservati

SEGUI QUESTE SEMPLICI ISTRUZIONI

SE SEI REGISTRATO AL SITO

clicca su **Accedi al materiale didattico**

inserisci email e password

inserisci le ultime 4 cifre del codice ISBN, riportato in basso a destra sul retro di copertina

inserisci il tuo **codice personale** per essere reindirizzato automaticamente all'area riservata

SE NON SEI GIÀ REGISTRATO AL SITO

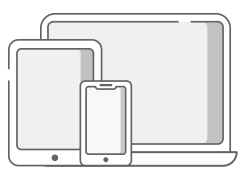
clicca su **Accedi al materiale didattico**

registrati al sito **edises.it**

attendi l'email di conferma per perfezionare la registrazione

torna sul sito **edises.it** e segui la procedura già descritta per utenti registrati

CONTENUTI AGGIUNTIVI



Per problemi tecnici connessi all'utilizzo dei supporti multimediali e per informazioni sui nostri servizi puoi contattarci sulla piattaforma **assistenza.edises.it**

Concorso

980 POSTI

AGENZIA DOGANE e MONOPOLI

100 PERITI INFORMATICI (ADM/PINF)
32 INFORMATICI (ADM/INF)

PROVA SCRITTA e ORALE

MANUALE e **QUESITI**
per la **prova scritta** e **orale**

EdiSES edizioni

Concorso 980 posti Agenzia Dogane e Monopoli - 100 periti informatici (ADM/PINF)
e 32 Informatici (ADM/INF)

9 8 7 6 5 4 3 2 1 0
2026 2025 2024 2023 2022

Le cifre sulla destra indicano il numero e l'anno dell'ultima ristampa effettuata

Andrea Monaco, laureato in Astrofisica, ha svolto incarichi presso i servizi informativi di organizzazioni operanti in ambito nazionale ed internazionale. Lavora dal 2010 nella Pubblica Amministrazione come funzionario informatico presso l'Inps. Con il ruolo di capo progetto, si occupa attualmente di attività legate al contesto delle entrate contributive e ad obiettivi strategici in ambito ICT definiti nel PNRR e nel Piano Strategico Digitale dell'Ente.

Cover Design and Front Cover Illustration: Digital Followers S.r.l.
Progetto grafico: ProMediaStudio di A. Leano – Napoli
Fotocomposizione: EdiSES edizioni S.r.l. – Napoli
Stampato presso: Print Sprint S.r.l. – Napoli
per conto della EdiSES edizioni S.r.l. – Napoli

www.edises.it
ISBN 978 88 3622 766 2 **assistenza.edises.it**

Sommario

Premessa

La Pubblica amministrazione italiana sta vivendo una fase in cui è chiamata a cogliere tutte le opportunità che le tecnologie digitali possono abilitare, per migliorare i processi interni ed i rapporti con cittadini e imprese.

Già con la legge di bilancio 2020 e il D.L. n. 162/2019 sono state previste diverse misure volte a promuovere e valorizzare l'informatizzazione della Pubblica amministrazione. L'opera di diffusione dell'amministrazione digitale è proseguita con il D.L. n. 76/2020 recante misure urgenti per la semplificazione e l'innovazione digitale. La digitalizzazione delle Pubbliche amministrazioni ha un ruolo centrale nel Piano nazionale di ripresa e resilienza ed è una delle componenti della Missione n. 1 del Piano denominata *Digitalizzazione, innovazione, competitività, cultura e turismo*. Si tratta di nuove tappe di un percorso che vuole favorire lo sviluppo di una società digitale, in cui i servizi della Pubblica amministrazione mettono al centro i cittadini e le imprese, costituendo un fattore di sviluppo per tutto il Paese.

L'attuale processo di modernizzazione e di riorganizzazione della Pubblica amministrazione prevede e incentiva il ricorso all'*outsourcing*, l'esternalizzazione di servizi o di specifiche funzioni, al fine di ottimizzare l'uso di risorse umane ed economiche a disposizione, nonché di velocizzare i tempi d'erogazione dei servizi e delle informazioni al cittadino. Tali obiettivi richiedono che vi sia un bilanciamento tra i costi sostenuti per realizzare i servizi e la qualità degli stessi: è necessario che l'amministrazione cliente abbia al suo interno competenze e strumenti per la gestione dei contratti tali da interloquire con efficacia coi fornitori, precisare i requisiti e verificarne il rispetto, monitorare gli SLA (*Service Level Agreement*, accordi sul livello del servizio), minimi definiti a livello contrattuale o migliorativi proposti in sede di offerta.

Riveste quindi un'importanza vitale la figura del funzionario informatico operante nella Pubblica amministrazione, cui è affidato il compito, e su cui grava la responsabilità (condivisa con gli altri ruoli istituzionali preposti), di fornire un apporto su tutti questi fronti, in virtù di capacità e competenze che spaziano dalle più ampie nozioni sulle principali tecnologie informatiche alla gestione di strumenti e risorse, alla pianificazione e gestione dei progetti e capacità relazionali e di lavoro in team.

Adeguati criteri di selezione in fase di concorso pubblico possono valutare le competenze e l'esperienza pregressa, ma non possono garantire che le nuove risorse acquisite siano già pronte per gestire la situazione in maniera ottimale in un contesto nuovo. Anche il personale già in servizio da anni deve far fronte ai cambiamenti che caratterizzano le tecnologie ICT e nel contempo portare avanti l'attività ordinaria e straordinaria, da cui dipendono livelli di servizio importanti per i riflessi sul valore erogato e percepito dal cittadino. Per questi motivi, nelle diverse Pubbliche amministrazioni, da una parte sta assumendo sempre maggiore importanza l'attività di formazione del personale interno e dall'altra è stata riconosciuta l'importanza di consolidare con personale nuovo, adeguatamente selezionato, la struttura di un reparto, come quello ICT, di importanza cruciale per questo tipo di organizzazioni.

Il volume è indirizzato a quanti intendono prepararsi alla prova scritta e a quella orale dei **profili informatici** (**100 Periti informatici ADM/PINF** e **32 Informatici ADM/IN**F) del concorso per complessivi 980 posti nell'Agenzia delle Dogane e dei Monopoli. Senza ripro-

porre gli argomenti già oggetto della prova preselettiva, il volume offre una sintesi, completa e aggiornata, delle materie specialistiche dell'area informatica.

Il manuale è strutturato in diverse sezioni.

I primi due capitoli trattano più genericamente del funzionario pubblico, focalizzando l'attenzione sulle caratteristiche dell'attività che questi svolge nell'ambito di una Pubblica amministrazione. In questa sezione è trattata in maniera ampia la questione delle responsabilità sotto i vari profili (penale, civile, amministrativo, disciplinare e gestionale).

Viene poi messo a fuoco (capitolo 3) il ruolo specifico del funzionario informatico, per quanto riguarda le responsabilità strettamente connesse alle attività che gli competono.

Per introdurre le sezioni relative alle competenze informatiche, viene effettuata (capitolo 4) una panoramica sull'informatizzazione nella Pubblica amministrazione, fornendo elementi essenziali legati alla normativa ed alle linee strategiche delineate dal Piano triennale.

Seguono capitoli più strettamente legati alle competenze tecniche e informatiche, che comprendono le nozioni di base (capitolo 5) e quelle più avanzate (capitolo 6), oltre alle competenze legate alle metodologie lavorative ed organizzative (capitolo 7).

Le ultime sezioni fanno riferimento all'attività concreta del funzionario informatico e sono basate su esperienze pratiche, approfondendo i servizi contrattuali e le metriche utilizzate per misurarne la qualità e stimarne i costi (capitolo 8), le attività connesse al ciclo di sviluppo del software (capitolo 9) ed una serie di *best practices* inerenti situazioni reali, con suggerimenti ed approfondimenti per interpretare al meglio questo ruolo (capitolo 10). Sono poi riportate le materie comuni ai due profili (ADM/PINF e ADM/INF) che non sono già state oggetto della prova preselettiva: Fini istituzionali, ordinamento e attribuzioni dell'ADM, Norme in materia di dogane, accise e giochi, Elementi di diritto penale con specifico riferimento ai reati contro la P.A., Lingua inglese.

Per ogni materia trattata sono disponibili dei **test a risposta multipla** (tra le estensioni online).

In **omaggio** il software di simulazione della prova scritta, strutturato secondo le indicazioni del bando per quanto riguarda il numero di domande, il tempo e il punteggio e che riporta tutte le materie della prova scritta (*anche quelle non esaminate in questo volume*).

Ulteriori materiali didattici sono disponibili nell'area riservata a cui si accede mediante la registrazione al sito *edises.it* secondo la procedura indicata nelle prime pagine del volume.

Eventuali errata-corrige saranno pubblicati sul sito *edises.it* secondo la procedura indicata nel frontespizio.

Altri aggiornamenti sulle procedure concorsuali saranno disponibili sui nostri profili social.

blog.edises.it
facebook.com/infoConcorsi
infoconcorsi.edises.it

Abbreviazioni

Tipo di atto normativo	Abbreviazioni, acronimi, sigle impiegate
Articolo di codici, leggi, decreti, ecc.	art., artt.
Circolare	Circ.
Codice civile	c.c.
Codice penale	c.p.
Costituzione della Repubblica italiana	Cost.
Decreto del Presidente del consiglio dei ministri	D.P.C.M.
Decreto del Presidente della Repubblica	D.P.R.
Decreto legge	D.L.
Decreto legislativo	D.Lgs.
Decreto ministeriale	D.M.
Direttiva UE	dir.UE
Legge statale	L.
Regio decreto	R.D.
Regolamento UE	reg.UE
Sentenza	sent.
Sentenza della Corte costituzionale	Corte cost., sent.
Sentenza della Suprema Corte di cassazione	Cass. sez. …, sent.
Testo unico	T.U.

Indice

Capitolo 3 Responsabilità e normativa in ambito ICT

Capitolo 4 La transizione digitale della Pubblica Amministrazione

Capitolo 3
Responsabilità e normativa in ambito ICT

3.1 Introduzione

Nell'ambito dell'ICT (*Information and Communication Technologies*) il concetto di responsabilità viene declinato generalmente secondo una prospettiva in cui è il professionista responsabile sui sistemi ed i servizi (l'*admin*) a dover agire affinché determinati crimini non si verifichino, senza invece che venga approfondita allo stesso modo la questione della responsabilità del professionista stesso.
Avendo delineato le diverse categorie della responsabilità in cui può incorrere un funzionario nella Pubblica amministrazione, si possono considerare ora alcune situazioni in cui le nozioni giuridiche richiamate nei paragrafi precedenti potrebbero chiamare in causa l'operato di un funzionario informatico.
Cominciamo con il fare chiarezza distinguendo fra Informatica giuridica e Diritto dell'Informatica. In linea generale, a dispetto di varie e contrastanti definizioni, ci si può riferire all'**informatica giuridica** come al complesso delle attività ed applicazioni dell'informatica in ambito giuridico; essa si concentra sugli strumenti informatici a disposizione del giurista, sulla redazione di ipertesti giuridici e, più in generale, sulle applicazioni utili per la documentazione e la consultazione nell'ambito della giurisprudenza[1]. Si può poi distinguere l'informatica giuridica *documentale*[2] o *metadocumentale* (o decisionale), *giudiziaria* (o giuridico-gestionale).
Il **diritto dell'informatica** è più attinente al tema trattato in questo volume e comprende:

- tutela giuridica del software;
- tutela della riservatezza rispetto alle banche dati personali;
- responsabilità per danni cagionati dall'uso del computer (*computer crimes*);
- contratti conclusi a mezzo di strumenti elettronici (comprende l'argomento della firma elettronica);
- contratti nei quali il mezzo elettronico (es. computer, software, pagine web) costituisce oggetto dell'attività negoziale;
- il cd. documento informatico[3].

Nel corso degli ultimi decenni, il diritto dell'informatica ha acquisito una sostanziale autonomia, cessando di essere una mera branca dell'informatica giuridica.

---

[1] Losano, M.G., *Informatica Giuridica*, in Dig. civ., IX, Torino, 1993, 417-420.

[2] Si può definire l'informatica giuridica documentale come quella disciplina che studia la classificazione, l'immagazzinamento e il reperimento a mezzo strumenti elettronici (hardware e software) di quei documenti che sono propri del campo normativo, giurisprudenziale, dottrinale e bibliografico.

[3] Nell'art. 1 del CAD il "documento informatico" è definito come: "documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

L'associazione tra le attività specifiche del funzionario informatico e le categorie di responsabilità in cui può incorrere, può essere effettuata sulla base del seguente schema concettuale, dove si distinguono:

- **reati** in cui può incorrere un generico **funzionario pubblico** (non solo informatico) di cui si cerca una corrispondenza rispetto le attività specifiche in ambito ITC;
- **reati connessi all'informatica** (*computer crimes*) rispetto ai quali la responsabilità dello specifico funzionario informatico può assumere una connotazione:
  - *attiva*: attraverso un'azione che porta a compiere uno dei suddetti reati;
  - *passiva*: avendo omesso di intervenire in maniera adeguata per prevenirli o avendo compiuto atti che hanno avuto il risultato di favorirli, direttamente o indirettamente.

A riguardo è necessaria una prima distinzione a monte tra responsabilità penale ed altre tipologie, motivata dal fatto che i cd. *computer crimes* hanno una valenza penale. Questi reati informatici devono prima essere introdotti, per poi approfondire la questione della responsabilità.

3.2 Crimini informatici

3.2.1 Premessa storica

La legislazione italiana nel settore informatico si è venuta sviluppando a partire dai primi anni '90, prendendo in considerazione i comportamenti e le condotte che incidono su sistemi informatici e telematici, dati e programmi.
La prospettiva legislativa adottata è stata in un primo momento quella di sanzionare aggressioni provenienti dall'esterno, eventualmente con la complicità di un operatore interno al sistema la cui azione, quindi, rientrerebbe nelle fattispecie dolose. Non è stata invece introdotta alcuna norma che punisse fatti dannosi a titolo di "colpa", richiedendo sempre la necessità del dolo (non esiste, ad esempio, un reato per la diffusione colposa di un virus a causa di un comportamento superficiale di un soggetto).

Il Gruppo dei 414

Le prime condanne per reati informatici, o per hacking, sono iniziate già nel 1983 con il caso dei *414s* di Milwaukee, in cui sei adolescenti fecero irruzione in sistemi informatici di prestigiose istituzioni, tra cui il *Los Alamos National Laboratory*, il *Memorial Sloan-Kettering Cancer Center* e la *Security Pacific Bank*. Nel maggio 1983 Gerald Wondra fu condannato a due anni di libertà vigilata.
In Europa l'esigenza di punire i crimini informatici emerse già alla fine degli anni Ottanta, tanto che, il 13/9/1989, il Consiglio d'Europa ha emanato una *Raccomandazione sulla Criminalità Informatica* dove venivano discusse le condotte informatiche abusive.

È con la **L. n. 547 del 1993** che, in Italia, si pongono le basi per una reale lotta al crimine informatico, punendo penalmente le più diffuse condotte criminose nel settore informatico come l'accesso abusivo, il danneggiamento, la frode informatica, il falso informatico, lo spionaggio, l'attentato ad impianti di pubblica utilità, la detenzione e la diffusione abusiva di codici d'accesso e la violenza sui beni informatici.

Il **D.Lgs. n. 231/2001**, in particolare all'24-*bis*, contempla una serie di fattispecie di reati posti sia a tutela dell'integrità:

- della sicurezza;
- della libera disponibilità di sistemi, reti, programmi e dati informatici e telematici;
- della riservatezza delle informazioni che vengono trattate e archiviate mediante l'utilizzo di sistemi informativi aziendali.

Oltre a apportare al Codice di procedura penale alcune modifiche finalizzate a regolamentare le indagini e le operazioni di perquisizione e sequestro dei dati informatici, il decreto ha previsto, con l'art. 24-*bis* introdotto dal D.L. 92/2008, nuove fattispecie di illecito amministrativo, commesse in relazione di delitti informatici e trattamento illecito dei dati.
Con la **L. n. 48/2008,** l'Italia ha proceduto a ratificare la **Convenzione internazionale del Consiglio di Europa sulla criminalità informatica**, tenuta a **Budapest il 23 novembre 2001**, che ha rappresentato il primo accordo internazionale specifico su questa tematica e che:

- ha introdotto nel codice penale nuove tipologie di reati informatici;
- ha riformulato alcune fattispecie già esistenti;
- ha provveduto a modificare il codice di procedura penale allo scopo di agevolare le indagini delle autorità preposte;
- ha integrato il Codice della privacy (art. 132 dell'allora vigente D.Lgs. n. 196/2003), consentendo all'Authority di ordinare ai fornitori e agli amministratori di servizi informatici o telematici di conservare per un periodo non superiore a sei mesi i dati relativi al traffico telematico.

Alcuni riferimenti normativi

- D.Lgs. n. 50/1992: "Attuazione della direttiva 85/577/CEE in materia di contratti negoziati fuori dei locali commerciali";
- D.Lgs. n. 518/1992: "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore";
- L. n. 547/1993: "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Direttiva UE 95/46/CE del 24/10/1995: relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- L. n. 185/1996: "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali";
- D.Lgs. n. 185/1999: "Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza";
- D.Lgs. n. 231/2001: disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;
- L. n. 48/2008: "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno";
- Codice civile, artt. dal 1469-bis al 1469-sexies del c.c. riguardo alla normativa sulle clausole vessatorie nei contratti dei consumatori.

3.2.2 Ambiti di applicazione

Tra i principali reati informatici previsti nel codice penale si possono citare:

- ***cyberstalking***: ossia la persecuzione di una persona condotta attraverso la rete;
- ***phishing***: truffe online attraverso le quali la vittima è portata a comunicare i propri dati sensibili;
- ***spam***: invio con frequenza elevata di messaggi pubblicitari di posta elettronica non richiesti o autorizzati;
- diffusione di ***malware***: software dannosi progettati per compromettere o sfruttare qualsiasi tipo di dispositivo o rete programmabile.

Le aree di intervento originariamente toccate dalla **L. 547/1993**, che rappresenta il primo intervento organico in materia, riguardano le seguenti categorie:

- frodi informatiche;
- falsificazioni;
- integrità dei dati e dei sistemi informatici;
- riservatezza dei dati e delle comunicazioni informatiche.

Con la L. n. 48/2008 il legislatore, oltre a sostituire l'originario art. 635-*bis* c.p., introduce ulteriori tre fattispecie (art. 635-*ter*, 635-*quater*, 635-*quinquies* c.p.), i ***digital crimes***, che sono divisibili idealmente in tre gruppi:

- danneggiamento di *hardware* e software;
- detenzione e diffusione di software o hardware allo scopo di compiere reati;
- violazione dell'integrità di dati.

Queste diverse categorie si possono sintetizzare nei seguenti ambiti:

Ambito	Norma	Argomento	Esempio
Frodi informatiche	Art. 640-*ter* c.p.	Estensione del reato di truffa descritto all'art. 640 c.p.	*Phishing*
	Art. 640-*quinquies* c.p.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	
Falsificazioni documento informatico	Art. 491-*bis* c.p.	Documenti informatici	
Integrità dei sistemi informatici	Art. 635-*bis* c.p.	Danneggiamento di sistemi informatici e telematici	
	Art. 635-*ter* c.p.	Danneggiamento di informazioni, dati programmi informatici utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità	
	Art. 635-*quater* c.p.	Danneggiamento di sistemi informatici o telematici	
	Art. 635-*quinquies* c.p.	Danneggiamento di sistemi informatici o telematici di pubblica utilità	
	Art. 420 c.p.	Attentato a impianti di pubblica utilità	

segue

Ambito	Norma	Argomento	Esempio
	Art. 615-*quinquies* c.p.	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	*Malware*
	Art. 392 c.p.	Esercizio arbitrario delle proprie ragioni con violenza sulle cose, esteso ai sistemi informatici (comma 3)	
Riservatezza di dati e comunicazioni	Art. 621 c.p.	Rivelazione del contenuto di documenti segreti	
	Art. 615-*ter* c.p.	Accesso abusivo ad un sistema informatico e telematico	*Hacking*
	Art. 615-*quater* c.p.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	
	Art. 617-*quater* c.p.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	*Sniffing*
	Art. 617-*quinquies* c.p.	Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	
	Art. 617-*sexies* c.p.	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche	
	Art. 130 del Codice in materia di protezione dei dati personali	Comunicazioni indesiderate	*Spamming*
Obblighi e responsabilità di enti-aziende	Art. 24-*bis* del D.Lgs. n. 231/2001	Responsabilità penale/amministrativa per i reati informatici più gravi, qualora ricorrano i requisiti soggettivi (commissione del reato da parte dei vertici aziendali o dei sottoposti) e oggettivi (interesse o vantaggio dell'Ente) richiesti.	
	Integrazione dell'art. 132 del Codice della Privacy operata dal D.Lgs. n. 231/2001	Consente alle autorità di ordinare ai fornitori e agli operatori dei servizi informatici e telematici di conservare (max sei mesi), i dati relativi al traffico telematico.	
	Decisione quadro M 2005/222/ GAI33 del 24/2/2005, art. 8	Punibilità penale dell'azienda che non attua una corretta sorveglianza e non applica idonee misure di sicurezza e, da tal superficialità, ne derivi un vantaggio per la stessa.	

3.2.3 Frodi informatiche

La categoria delle **frodi informatiche** è regolamentata dall'art. 640-*ter* c.p., in cui si legge che chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La reclusione è da uno a cinque anni e la multa da euro 309 a euro 1.549 se ricorrono circostanze aggravanti, tra cui è la circostanza che chi compie l'abuso è un operatore del sistema.
Si tratta perciò di un'estensione del reato di truffa descritto all'art. 640 c.p. in quanto trattasi di un reato consistente *nell'effettuare un intervento su un sistema informatico al fine di ricavarne un guadagno economico a danno di un soggetto terzo*.
Tra i reati che ricadono in questa categoria, vi sono le cd. pratiche di ***phishing***, la truffa realizzata sulla rete Internet ingannando gli utenti (in genere attraverso messaggi di posta elettronica ingannevoli).

3.2.4 Falsificazioni

La categoria delle **falsificazioni** è regolamentata dal Codice penale attraverso l'art. 491-*bis*, il quale dispone che in caso di **falsificazione di documenti informatici** pubblici, sottoscritti con firma digitale o altro tipo di firma elettronica qualificata, si applichi la medesima disciplina prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei (artt. da 476 a 493 c.p.).
Dunque, nel caso in cui un documento venga deliberatamente falsificato vengono applicate le pene di cui agli articoli che regolamentano le falsità in atti pubblici.
Nei reati di falsità in atti è fondamentale la distinzione tra:

- **falsità materiale**: quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato successivamente alla sua formazione;
- **falsità ideologica**: quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

In questo caso il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione. Nel caso della falsità ideologica l'oggetto di falsificazione non è l'atto nella sua materialità, ma la circostanza che il pubblico ufficiale o il privato attesti falsamente che il fatto è stato da lui compiuto o in sua presenza. Nel caso di documenti informatici, il **falso ideologico** potrebbe compiersi mediante l'immissione di dati o informazioni non veritiere in elenchi o registri gestiti informaticamente. In tal caso la perseguibilità amministrativa dell'Amministrazione potrebbe sorgere nel caso in cui non fosse possibile identificare l'autore del reato.
Per poter però essere valido, un documento deve poter essere autenticato e se ne deve poter attribuire la paternità. A tale scopo interviene la **firma digitale** che il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, art. 1, comma 1, lett. s) viene definita come «un particolare tipo di *firma qualificata* basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di docu-

menti informatici». Con la firma digitale dunque si attesta anche l'**integrità** ed il **non ripudio** del documento.

3.2.5 Integrità di dati e sistemi informatici

Il Codice penale regolamenta l'integrità dei dati e dei sistemi informatici attraverso vari articoli, tra cui l'art. 635-*bis* (**Danneggiamento di sistemi informatici e telematici**), il quale afferma che: "*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".
Si ripropone qui il reato di danneggiamento (previsto dall'art. 635 c.p.) esteso anche alle apparecchiature informatiche o telematiche, inclusi dati, informazioni programmi in esse contenute.
L'art. 635-*ter* c.p. (dal canto suo) punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti all'art. 635-*bis* c.p., a prescindere dal prodursi, in concreto, del risultato del danneggiamento, che, se si verifica, costituisce circostanza aggravante della pena. Deve, però, trattarsi di condotte dirette a colpire **informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico** o ad essi pertinenti, o, comunque, di pubblica utilità.
Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza o minaccia alle persone (perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste), o con abuso della qualità di "operatore di sistema" (sempre perseguibile d'ufficio).
Un'aggravante del reato «danneggiamento di sistemi informatici e telematici» è prevista dall'art. 420 c.p. (**attentato a impianti di pubblica utilità**), un'estensione dei reati di danneggiamento a sistemi informatici, che trova qui ora un *inasprimento nel caso in cui il reato di danneggiamento sia compiuto contro impianti di pubblica utilità* e quindi di pericolo per l'ordine pubblico e per gli interessi socioeconomici collettivi.
L'art. 635-*quater* c.p. punisce chiunque mediante le condotte di cui all'art. 635-*bis*, **distrugge, danneggia e rende inservibili sistemi informatici o telematici altrui**, oppure ne ostacola gravemente il funzionamento. L'art. 635-*quinquies* c.p. punisce le medesime condotte descritte all'art. 635-*quater* anche se gli eventi lesivi non si realizzino in concreto. Deve, però, trattarsi di condotte che mettono in pericolo **sistemi informatici o telematici di pubblica utilità**. Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza o minaccia alle persone, o con abuso della qualità di "operatore di sistema". È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi.
Il Codice penale interviene anche estendendo l'art. 392 (*Esercizio arbitrario delle proprie ragioni con violenza sulle cose*) ai sistemi informatici, quando al comma 3 riporta il reato in ambito informatico, con riferimento all'**alterazione, modifica o cancellazione in tutto od in parte di un programma** al fine di turbarne il corretto funzionamento.
L'art. 615-*quinquies* (**Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**) punisce l'acquisizione e diffusione di apparecchiature, dispositivi o programmi in grado di danneggiare, interrompere o alterare il funzionamento di un sistema e/o dei dati/programmi ad esso pertinenti. La norma tende a reprimere, in particolare modo, il comportamento di coloro che diffondono tutti i programmi rientranti sotto la categoria di

malicious software (o ***malware***). Trattandosi di un reato di mera condotta, la consumazione coincide con la messa in circolazione del programma "infetto", a prescindere, quindi, da qualsiasi danno da esso cagionato. Per la sussistenza del reato, *la norma richiede il dolo generico*, ovvero è sufficiente che l'agente sia consapevole di mettere in circolazione un virus. Non è punita la creazione o la semplice detenzione di tali software. Tale reato è punito solo qualora vi sia dolo e non lo è nel momento in cui si accerti una condotta meramente colposa. Ciò serve a scagionare tutti coloro che si vedono vittime ignare ed inconsapevoli della diffusione dei *malware*.

3.2.6 Riservatezza di dati e comunicazioni

Altra categoria di reati informatici è quella inerente la riservatezza dei dati e delle comunicazioni informatiche. L'art. 615-*ter* (**accesso abusivo ad un sistema informatico o telematico**) è principalmente finalizzato a contrastare il fenomeno degli hacker. L'articolo definisce il reato commesso da chi si trova in una delle seguenti situazioni:

- si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza;
- si trattiene entro un sistema informatico o telematico oltre la durata stabilita dal titolare del sistema.

Non è richiesto che il reato sia commesso ai fini di lucro o di danneggiamento del sistema (questione già affrontata con l'art. 635-*bis*), pertanto il reato può realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità o la vulnerabilità dei sistemi altrui. L' accesso deve verificarsi in presenza di misure di sicurezza, cioè misure tecniche, informatiche, organizzative e procedurali volte ad escludere o impedire la cognizione delle informazioni a soggetti non autorizzati.
La pena (reclusione fino a tre anni) aumenta da uno a cinque anni

- se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora la violazione riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
Con questo articolo *il sistema informatico è inteso come vera e propria estensione del domicilio dell'individuo*, al fine di proteggerlo da accessi non autorizzati e da permanenza non gradita (tutela garantita dall'art. 14 Cost.).

Professioni & Concorsi

Manuali ed Eserciziari per la preparazione ai concorsi pubblici
e per l'aggiornamento professionale

Volume indirizzato a quanti intendono prepararsi alla prova scritta e orale dei **profili informatici** (**100 Periti informatici ADM/PINF** e **32 Informatici ADM/INF**) del concorso per complessivi 980 posti nell'Agenzia delle Dogane e dei Monopoli.

L'opera riporta innanzi tutto una **trattazione manualistica** degli argomenti della prova scritta specifici per i profili informatici, sia diplomati (principi di reti di calcolatori, cenni sull'architettura hardware e la configurazione di PC/server/stampanti/dispositivi mobili, sistemi operativi, cenni sulla condivisione di risorse in rete, cenni sulla tecnologia VoIP e sistemi di videoconferenza) che laureati (sicurezza delle reti di calcolatori, project management, architetture sistemi ICT, design pattern, basi di dati, sistemi operativi e data management). Sono poi riportate, fra le estensioni online, le materie comuni ai due profili (ADM/PINF e ADM/INF) che non sono già state oggetto della prova preselettiva: Fini istituzionali, ordinamento e attribuzioni dell'ADM, Norme in materia di dogane, accise e giochi, Elementi di diritto penale con specifico riferimento ai reati contro la P.A., Lingua inglese.

Per ciascuna di tali materie il volume offre una **sintesi** di tutto il programma e **quesiti di verifica** a risposta multipla (disponibili fra le estensioni online) che consentono di esercitarsi in vista della prova di selezione.

ESTENSIONI **ONLINE**
TEST DI **VERIFICA**
SOFTWARE DI **SIMULAZIONE**

Le risorse di studio gratuite sono accessibili per 18 mesi dalla propria area riservata, previa registrazione al sito **edises.it**.
Il **software** consente di **esercitarsi** su un vastissimo database e **simulare** le prove.

EdiSES edizioni

blog.edises.it
infoConcorsi
infoconcorsi.edises.it

€ 36,00

ISBN 978-88-3622-766-2
9 788836 227662