Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

La gestione dei rischi di un'Organizzazione Sanitaria

Raffaella Ferradini

23 novembre 2023

La rilevanza di una gestione Enterprise-wide dei rischi nelle Organizzazioni Sanitarie – Oltre il rischio clinico

Le **Organizzazioni Sanitarie** sono esposte ad un **ampio spettro** di **rischi**, alcuni dei quali sono **specifici** (es. **rischio clinico**), altri speculativamente **assunti** (es. **Cyber Security**, **Frode**, **Safety**, **Business Interruption**, **Third-Party**, **Finanziari**, ecc.), legati all'evoluzione di **fattori interni** o **esterni**, sui quali solo in alcuni casi si è in grado di esercitare qualche tipo di influenza.

Hot Topics in ambito Healthcare

- Nel comparto ospedaliero il **costo del gas** rispetto al 2020 è cresciuto fino a **5,5 volte** e ha trascinato il costo di tutti gli altri fattori, a partire dall'energia, con punte di 2-3 volte il 2020. (1)
- In 5 anni, dal 2016 al 2020, sono stati **12mila gli infortuni sul lavoro** per il personale sanitario legati a **violenze, aggressioni e minacce**, con una media di circa 2.500 l'anno. (2)
- Il rapporto CLUSIT 2022 sulla **sicurezza ICT** in Italia ha evidenziato come il **settore sanitario** sia tra i **principali obiettivi** degli **attacchi informatici**: nell'anno 2021 il **13%** degli **attacchi** ha avuto come **target** una **struttura sanitaria**. (3)
- Il **PNRR** finanzierà il **potenziamento** della **telemedicina** nelle strutture ospedaliere, comportando **nuovi ambiti di rischio** e pericolo e l'ampliamento dell'**arco terapeutico** durante il quale è il **sistema sanitario** a essere **responsabile** di ogni **accadimento** nella **salute** del paziente. (4)
- Secondo una rilevazione **SIMEU (Società Italiana della medicina di emergenza-urgenza)**, nel **2022** sono stati circa **600** i **medici di emergenza-urgenza** che hanno scelto di **dimettersi** dai **PS**, e si stima che solo nei PS manchino all'appello circa 4mila camici bianchi. (5)

Principali famiglie di rischio nelle Organizzazioni ospedaliere

- **BUSINESS CONTINUITY**
- **RELAZIONI CON TERZE PARTI**
- **RISCHIO CYBER & DATA BREACH**
- **ECONOMICO-FINANZIARI**
- **NORMATIVI E REGOLAMENTARI**
- **SANITARI / CLINICI**

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Lesson Learnt

Alcuni casi di rischi emersi nel settore ospedaliero
e il loro impatto per l'organizzazione

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Lesson Learnt

Scenario 1: Cybersecurity

Nel settembre del 2017 l'**Ospedale Universitario di Düsseldorf** è risultato vittima di un **attacco ransomware** che ha comportato il **blocco informatico di 30 server interni** a causa di una vulnerabilità del gateway Citrix.

L'attacco ha compromesso l'infrastruttura digitale su cui l'ospedale faceva affidamento per coordinare le attività di assistenza, costringendo alla cancellazione di molte prestazioni e accessi.

Il Pronto Soccorso è stato quindi costretto a **dirottare l'accesso di una paziente** affetta da un aneurisma aortico all'ospedale di Wuppertal, a 30 km di distanza, ritardando il trattamento di un'ora. La paziente è deceduta poco dopo l'intervento.

Potenziali impatti

- Danno finanziario derivante da **sanzioni** da parte delle Autorità di controllo
- Danno reputazionale causato dall'**impatto mediatico**
- **Interruzione dell'operatività** di sistemi e processi aziendali
- Compromissione della **salute dei pazienti**
- Costi connessi al ripristino dei sistemi e al rafforzamento delle misure di sicurezza

Esempi di soluzioni

- ✓ Esecuzione di un **Cybersecurity Risk Assessment** e di una **BIA** sui processi a rischio, conduzione di **VA/PT** (Vulnerability Assessment/Penetration Test)
- ✓ Formalizzazione di **piani di Continuità operativa** e/o **Disaster Recovery** e delle procedure di gestione degli incidenti, coinvolgendo i fornitori critici
- ✓ Implementazione di **misure di sicurezza** (pianificazione dei backup, utilizzo di tecniche di autenticazione sicure, limitazione e monitoraggio degli accessi a sistemi e reti, aggiornamento di antivirus e antimalware, ecc.)
- ✓ Adozione di un **Sistema di Gestione Integrato della Continuità Operativa** (ISO 22301)
- ✓ **Formazione del personale** per limitare l'errore umano

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Lesson Learnt

Scenario 2: Gestione dei fornitori per l'approvvigionamento dei farmaci

Nel 2021 un ospedale del Lazio ha subito un **allungamento dei tempi di consegna** della **merce ordinata** a causa di un ritardo nel **pagamento verso i fornitori** di prodotti farmaceutici.

Infatti, a causa di **inefficienze nei processi interni** (es. rilavorazione, fatture mancanti), il **dilatarsi dei tempi** di attesa per la consegna dei farmaci ordinati ha costretto **la struttura a trovare temporaneamente fornitori alternativi** e / o il **supporto temporaneo da parte di altri ospedali** della Regione Lazio per ottenere una **fornitura di medicinali** sufficiente a sopperire alle richieste in essere.

La gestione delle relazioni con i fornitori in una struttura ospedaliera è **fondamentale** per **garantire** la **continuità** nell'erogazione delle **prestazioni** ai **pazienti**.

Potenziali impatti

- Ulteriori costi per la **ricerca di fornitori alternativi**
- **Acquisto** di **farmaci** da altri **ospedali**
- **Aumento** della **complessità organizzativa**
- **Danno reputazionale** nei **confronti** dei **fornitori**

Esempi di soluzioni

- ✓ **Analisi** e **mappatura** dei **processi** interni e **identificazione** delle **criticità operative**
- ✓ **Analisi** e **mappatura** dei **fornitori** e delle **forniture critiche**
- ✓ Definizione di un piano di **Business Continuity Management**

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Lesson Learnt

Scenario 3: Responsabilità sanitaria

In una struttura sanitaria dell'Emilia Romagna, accreditata con il SSN e specializzata in ortopedia, un medico chirurgo ha svolto un intervento la cui diagnosi era stata effettuata presso uno studio localizzato in un'altra Regione caratterizzata da una forte mobilità passiva.

In quella sede aveva acquisito tutte le informazioni e le evidenze cliniche a supporto della necessità dell'intervento chirurgico, inserendole all'interno della cartella clinica. Presso l'ospedale emiliano invece, lo stesso medico chirurgo, essendo già a conoscenza della diagnosi, aveva aperto la cartella clinica semplicemente indicando la necessità dell'intervento, senza allegare la documentazione di supporto.

A causa di un evento avverso (infezione) correlato all'intervento di chirurgia e derivante dall'incompleta redazione della cartella clinica del paziente, l'Organizzazione ospedaliera è stata condannata al **risarcimento danni in favore del paziente .**

Sebbene l'azienda sia stata in grado di dimostrare il rispetto di tutti i protocolli sanitari volti alla tutela del paziente, l'analisi del CTU ha messo in evidenza una **carenza documentale nella cartella clinica**, che ha determinato la soccombenza nel giudizio.

Potenziali impatti

- Danno finanziario ed economico derivante dalla **soccombenza in sede di giudizio civile**
- **Aumento del premio** della polizza assicurativa sulla responsabilità sanitaria
- **Ripetibilità** del rischio su ampia scala
- **Penalità** derivanti dai controlli posti in essere dalle autorità regionali

Esempi di soluzioni

- ✓ **Indagini interne** (es. root cause analysis) svolte dal Risk Management sulle richieste di risarcimento danno, non limitando la valutazione ai soli aspetti clinici
- ✓ Comunicazione delle azioni necessarie al Management e definizione di un **Piano di Azione** con monitoraggio delle iniziative intraprese
- ✓ Aggiornamento dei **protocolli interni**
- ✓ **Formazione del personale** per limitare l'errore umano

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

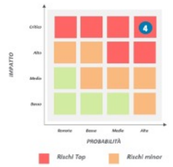
Lesson Learnt

Scenario 4: Allocazione del personale sanitario

Una casa di cura privata accreditata che eroga, tra le altre, prestazioni di riabilitazione estensiva, garantiva ai pazienti la riabilitazione solo durante i giorni feriali. La casa di cura, con l'obiettivo di risparmiare sul costo del personale, aveva infatti scelto di non avvalersi di ulteriori fisioterapisti a supporto delle attività di riabilitazione per coprire i turni dei giorni festivi. Tuttavia, la normativa regionale prevedeva che la riabilitazione dovesse essere garantita tutti i giorni della settimana (festivi inclusi).

La casa di cura ha pertanto subito per anni **penalizzazioni sul fatturato da parte della Regione Lazio** a causa di una **gestione inappropriata delle risorse umane**, una **insufficiente conoscenza della normativa** e una **mancata analisi costi-benefici**, oltre allo scarso coordinamento tra le funzioni interne.

Il risparmio ottenuto di costo del personale, stimato in circa 80.000 € all'anno è risultato, a seguito di successive analisi, di molto inferiore alle penalità inflitte alla struttura dalla Regione, superiori a 1.000.000 € all'anno.



Potenziali impatti

- **Utilizzo inefficace delle risorse**
- **Penalità** derivanti dai controlli posti in essere dalle autorità regionali
- **Ripetibilità** del rischio su ampia scala
- Erogazione di **prestazioni non adeguate** nei confronti dei pazienti rispetto a quanto previsto dai protocolli e dalla normativa

Esempi di soluzioni

- ✓ Approfondimento della **normativa regionale** e dei relativi requisiti, identificando aspetti di potenziale non-compliance
- ✓ Sviluppo di un maggiore **coordinamento tra le funzioni interne** per tematiche trasversali all'organizzazione e disegno di comunicazioni strutturate
- ✓ Strutturare attività di **analisi costi-benefici** sull'allocazione delle risorse umane

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Lesson Learnt

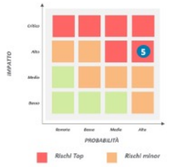
Scenario 5: Gestione dei contratti per l'approvvigionamento energetico

Una casa di cura privata accreditata, nell'ambito dell'attività di efficientamento energetico, ha stipulato nel 2018 un contratto di «relamping e di fornitura di energia elettrica» che ha incluso **l'installazione di un impianto di cogenerazione.**

Il contratto, sottoscritto in assenza di specifiche competenze tecniche e legali sull'argomento, ha previsto dei vincoli quantitativi di generazione di energia da gas, ha previsto inoltre che il contratto di fornitura di gas fosse volturato al soggetto fornitore dell'impianto di cogenerazione.

L'aumento dei prezzi del gas rinveniente in particolare dalla guerra tra l'Ucraina e la Russia, ha determinato un'amplificazione dell'aumento del costo dell'energia sulla struttura.

Impossibilitata nel recesso, impegnata ad un volume minimo di acquisto, priva di titolarità nella potenziale rinegoziazione delle condizioni di acquisto del gas, non essendo più titolare del contratto, la **struttura ha patito un incremento dei costi per l'energia (gas ed energia elettrica) ben superiori rispetto a quelli patiti dai competitors**.



Potenziali impatti

- **Aumento dei costi delle forniture per energia**
- **Costi derivanti dall'avvio di potenziali contenziosi**
- **Ripetibilità** del rischio su altre forme di contratto

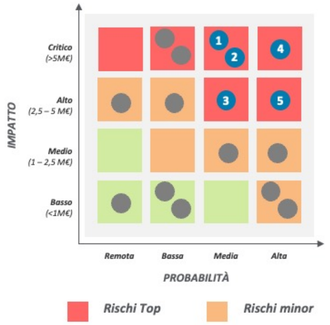
Esempi di soluzioni

- ✓ **Diagnosi energetica**
- ✓ Acquisizione di **servizi di consulenza**: ad esempio «energy manager», legali specializzati nei temi trattati
- ✓ Identificazione e acquisto di **strumenti di copertura finanziaria** del rischio e/o introduzione di *stop-loss*
- ✓ Sviluppo di un maggiore **coordinamento tra le funzioni interne** per tematiche trasversali all'organizzazione e disegno di comunicazioni strutturate
- ✓ Strutturare attività di **analisi costi-benefici**

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Heat Map & Risk Register - *Illustrative*

L'implementazione di un modello **strutturato** e **olistico** di **Enterprise Risk Management** permette di avere una **vista aggiornata** sul **portafoglio** di tutti **rischi** dell'Organizzazione. Il risultato dell'attività di identificazione e valutazione dei rischi si configura nell'**Heat Map**, strumento di **comunicazione** e di **condivisione**, che permette di **confrontare rischi** di **diversa natura**, evidenziare le **priorità** di **intervento** e avere un **quadro sinottico** dei rischi inclusi nel perimetro.



	Top risks	Dimensioni impatto: Economico	Operativo	Reputazionale	Legale	Impatto	Probabilità
1	Attacco Cyber ai sistemi informativi	Alto	Critico	Alto	Medio	Critico	Alto
2	Mancata / ritardo nella consegna dei farmaci	Alto	Critico	Alto	Medio	Critico	Alto
3	Inefficace processo di gestione della documentazione sanitaria	Alto	Medio	Alto	Alto	Alto	Alto
4	Inefficace allocazione delle risorse umane (personale sanitario)	Critico	Alto	Medio	Critico	Critico	Critico
5	Inefficace gestione dei contratti per l'approvvigionamento energetico	Critico	Medio	Lieve	Alto	Alto	Critico

IMPATTO: Critico · Alto · Medio · Lieve

PROBABILITÀ: Alta · Media · Bassa · Remota

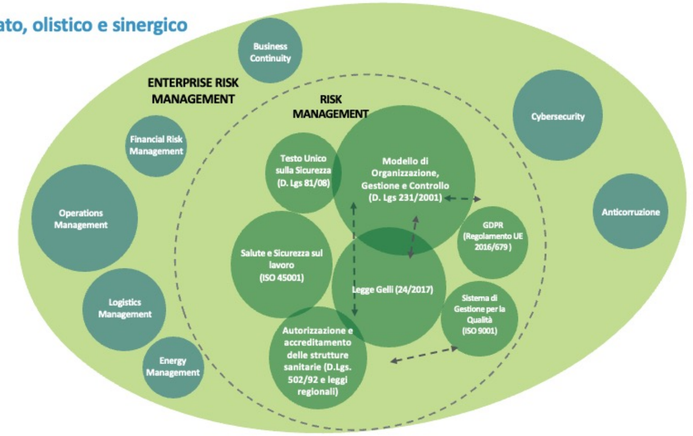
#ForumRisk18

www.forumriskmanagement.it

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Da Silos a Modello integrato, olistico e sinergico

L'Enterprise Risk Management rafforza in modo **sinergico** gli **ambiti di Risk Management già integrati e connessi** all'interno dell'Organizzazione (es. Regolamento GDPR, Modello di Organizzazione, Gestione e Controllo D. Lgs 231, gestione della SSL, ecc.) e permette di consolidare e governare anche **aree di rischio tipicamente meno interconnesse**.



#ForumRisk18
www.forumriskmanagement.it

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Overview di progetto

Un **progetto** di definizione del **modello ERM** si articola in una **serie di interventi incrementali** sulla governance, sulla metodologia e sugli strumenti e pratiche di Risk Assessment, finalizzati a rendere l'ERM quanto più possibile sinergicamente **integrato** ai **processi** di business, dalla **pianificazione strategica** alle **operations**, incorporando i rischi sugli **obiettivi** di **sostenibilità** ed **ESG**.

6. Risk Culture & Awareness Enhancement

Diffusione e rinforzo della conoscenza e consapevolezza in tema di **gestione del rischio** durante tutto il progetto, combinando strumenti didattici tradizionali, workshop, business case e metodi di partecipazione **collaborativa** finalizzati a **massimizzare *l'on-boarding*** e la futura collaborazione alle attività di RM.

AMBITI DI INTERVENTO

1. Strategy – ERM Integration

Sincronizzare i processi di **budget** e **pianificazione** degli **investimenti** con il processo di **analisi** e **valutazione** dei **rischi**, considerando nativamente e sinergicamente temi **ESG** e relativi al **cambiamento climatico**

2. ERM Framework Design e Implementation

Revisionare e aggiornare la **metodologia e della governance di Risk Management**, con particolare attenzione alla rivalutazione della piena e chiara attribuzione delle **responsabilità** su **processi** e **rischi**, **all'efficacia** in termini di **sostegno** al **business**, al **contenimento dei *measurement bias*** (introduzione/miglioramento dei modelli di stima quantitativa, ovunque sia opportuno)

3. Enterprise Risk Assessment Set-up

Definire il **processo** e gli **strumenti di Risk Assessment** al fine di **identificare, analizzare, valutare e gestire i rischi, prevenendoli o disegnando strategie di trattamento e supportare le scelte aziendali in** maniera concreta, efficace ed operativa

4. Enterprise Risk Assessment Execution

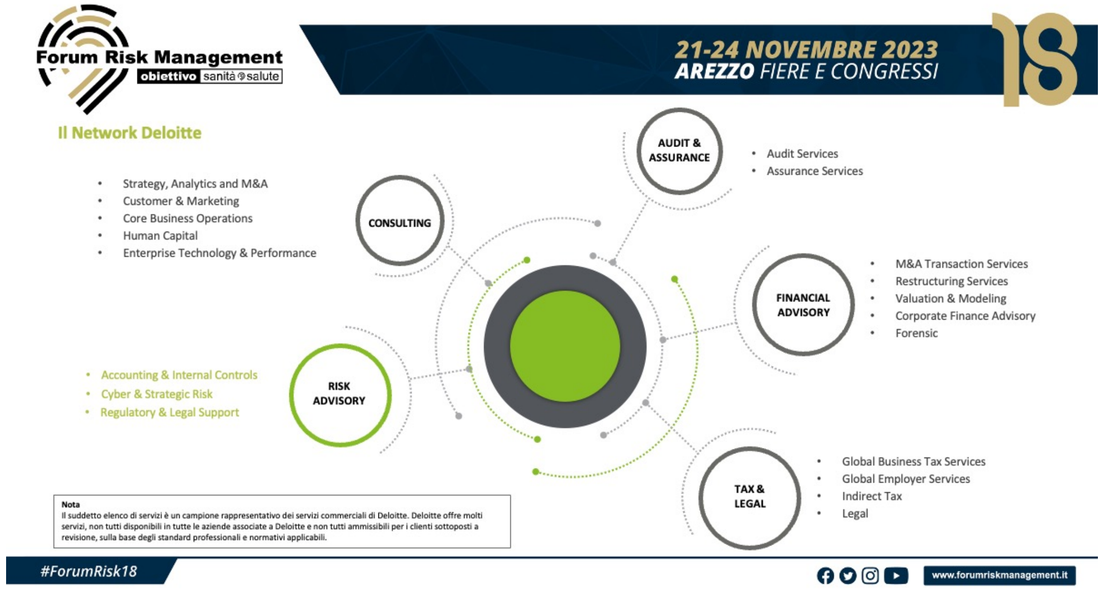
Condurre operativamente il Risk Assessment al fine di **aggiornare** il catalogo dei rischi e la mappa dei **Top Risk**, corredati da **proposte di azioni di mitigazione**. Le tecniche di *assessment* e le modalità di interlocuzione con il management saranno selezionate per massimizzare l'**efficacia** e il livello di ***on-boarding*** **dei Risk Owner**

5. Risk Monitoring & Reporting

Disporre di un **processo di reporting dei rischi strutturato e periodico,** differenziato sulle esigenze di ogni stakeholder, basato su **metriche quali/quantitative oggettive** (KRI) e le relative misure di trattamento

Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Il Network Deloitte



Forum Risk Management
obiettivo sanità salute
21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

Deloitte Risk Advisory è la società del network Deloitte, leader mondiale nei servizi di Corporate Governance, Sistemi di Controllo Interno, Risk management, Regulatory compliance, Sicurezza e Privacy

In Italia, Deloitte Risk Advisory dispone di circa **1800** professionisti dedicati alle tematiche relative a **Internal Audit**, **Regulatory Compliance**, **Prevenzione della Corruzione**, **Corporate Governance** e **Gestione del Rischio**, con competenze specialistiche e multidisciplinari, molte delle quali attestate da certificazioni riconosciute a livello internazionale.

In particolare, la nostra *practice* di **Life Science & Healthcare** offre i propri servizi attraverso una **struttura integrata** con professionisti di comprovata esperienza in ambito: Compliance normativa, Corporate Criminal Law, Risk Management, Internal Audit, Information Technology, Health & Safety.

La nostra **metodologia**, il nostro approccio e i nostri strumenti hanno una **elevata flessibilità** e sono facilmente **integrabili** con gli strumenti e le metodologie del Cliente, garantendo rigore di impostazione, accuratezza dei *deliverable* e dei risultati.

Deloitte garantisce la conoscenza approfondita della **visione operativa e strategica** delle aziende operanti nel settore Life Sciences, in merito ad obiettivi, sfide e possibili **rischi** di conformità normativa, nonché in ordine agli **aspetti di miglioramento del Sistema di Controllo Interno**.

Il **team Life Science & Healthcare di Deloitte**, in virtù delle esperienze maturate in molteplici realtà del settore Life Sciences, possiede una comprensione distintiva del **contesto funzionale e organizzativo** delle Società operati nel settore, nonché dei **principali processi aziendali esposti a rischio**.

In tale contesto, i servizi che proponiamo sono in grado non solo di individuare e gestire i rischi, ma di trasformarli in opportunità.

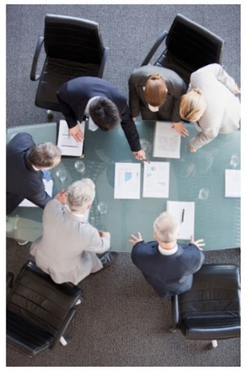
La nostra mission è aiutare le organizzazioni a identificare, comprendere e gestire ogni elemento di incertezza ad ogni livello e lungo tutto il suo ciclo di vita, per mitigare al massimo le minacce e sfruttare al meglio le opportunità che ne possono derivare

Forum Risk Management
obiettivo sanità salute

21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI

18

Contatti



Deloitte Risk Advisory | Life Sciences e Healthcare

Raffaella Ferradini

Deloitte Risk Advisory | Director
Regulatory & Legal Support
Healthcare & Life Sciences Specialist
+39 3403962273
rferradini@deloitte.it

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio