



PARTE SPECIALE 05

# REATI INFORMATICI

---

Directory:

---

Oggetto della modifica:

---

Redazione: Responsabile Qualità

---

Emissione: Direzione

---

Data emissione: XXXXX

Revisione: XXXX

Pagina 1 di 13

## Sommario

<b>1</b>	<b>Destinatari della Parte Speciale n. 05</b>	<b>3</b>
<b>2</b>	<b>I reati informatici (art. 24 bis del D. Lgs. n. 231/2001)</b>	<b>3</b>
2.1	Documenti informatici (art. 491-bis cod. penale) .....	3
2.2	Accesso abusivo a un sistema informatico o telematico (art. 615-ter cod. penale).....	5
2.3	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615- quater cod. penale).....	6
2.4	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. penale) .....	6
2.5	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. penale) .....	6
2.6	Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. penale).....	7
2.7	Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. penale).....	7
2.8	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter cod. penale).....	7
2.9	Danneggiamento di sistemi informatici e telematici (art. 635-quater cod. penale).....	7
2.10	Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies cod. penale).....	7
2.11	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640- quinquies cod. penale).....	8
<b>3</b>	<b>Principi di riferimento generali</b>	<b>8</b>
3.1	Il sistema organizzativo in generale.....	8
3.2	Principi generali di comportamento .....	8
<b>4</b>	<b>Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001</b>	<b>10</b>
<b>5</b>	<b>Principi generali di controllo</b>	<b>10</b>
<b>6</b>	<b>Principi di riferimento specifici relativi alla regolamentazione delle singole</b>	<b>11</b>
6.1	Gestione e monitoraggio degli accessi ai sistemi informatici e telematici .....	11
<b>7</b>	<b>I controlli dell'Organismo di Vigilanza</b>	<b>13</b>

## 1 Destinatari della Parte Speciale n. 05

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti della Clinica, nonché dai suoi consulenti, liberi professionisti e partners coinvolti nei processi sensibili.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.

In questa parte speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione alle fattispecie di Attività Sensibili individuate al fine di prevenire la commissione dei reati informatici.

## 2 I reati informatici (art. 24 bis del D. Lgs. n. 231/2001)

La presente Parte Speciale riguarda i reati informativi, contemplati all'art. 24 bis del D. Lgs. n. 231/2001. La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di organizzazione, gestione e controllo previsto dal decreto. A tal fine, si riporta di seguito una descrizione dei reati richiamati dall'art. 24-bis del D.Lgs. 231/2001, in base al quale:

*"1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*

*2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*

*3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*

*4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".*

### 2.1 Documenti informatici (art. 491-bis cod. penale)

*"Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".*

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.): *"Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni";*

- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.): *“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempite le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni”;*
  
  - Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.): *“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni”;*
  
  - Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.): *“Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476”;*
  
  - Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.): *“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni”;*
  
  - Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.): *“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro”;*
  
  - Falsità materiale commessa da privato (art. 482 c.p.): *“Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo”;*
  
  - Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.): *“Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi”;*
  
  - Falsità in registri e notificazioni (art. 484 c.p.): *“Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00”;*
  
  - Falsità in scrittura privata (art. 485 c.p.): *“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata”;*
- 
-

- Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.): *“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito”*;

- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.): *“Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480”*;

- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.): *“Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private”*;

- Uso di atto falso (art. 489 c.p.): *“Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno”*;

- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.): *“Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente”*;

- Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.): *“Agli effetti delle disposizioni precedenti, nella denominazione di “atti pubblici” e di “scritture private” sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti”*;

- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.): *“Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni”*.

## **2.2 Accesso abusivo a un sistema informatico o telematico (art. 615-ter cod. penale)**

*“ Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:*

*1) 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;*

*2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*

*3) 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 i fatti di cui ai commi primo e secondo riguardino 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".*

### **2.3 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. penale)**

*"Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617quater".*

### **2.4 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. penale)**

*"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro".*

### **2.5 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. penale)**

*" Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni .*

*Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.*

*Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:*

*1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;*

*2) 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, ovvero con abuso della qualità di operatore del sistema;*

*3) da chi esercita anche abusivamente la professione di investigatore privato".*

---

---

## **2.6 Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. penale)**

*“ Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

*La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.”*

## **2.7 Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. penale)**

*“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 ricorre una o più delle circostanze di cui al numero 1 del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.”*

## **2.8 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter cod. penale)**

*“Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

*Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione, o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.*

*Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata.”*

## **2.9 Danneggiamento di sistemi informatici e telematici (art. 635-quater cod. penale)**

*“Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*

*Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata”.*

## **2.10 Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies cod. penale)**

*“Se il fatto di cui all'art.635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*

*Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.*

---

---

*Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata”.*

### **2.11 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cod. penale)**

*“Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00”.*

## **3 Principi di riferimento generali**

### **3.1 Il sistema organizzativo in generale**

La Casa Di Cura considera essenziale allo svolgimento della sua attività la promozione e il mantenimento di un adeguato sistema di controllo interno da intendersi come insieme di tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività di impresa con l'obiettivo di assicurare il rispetto delle leggi e delle procedure aziendali, di proteggere i beni aziendali, di gestire in modo ottimale ed efficiente le attività.

La responsabilità di realizzare un sistema di controllo efficace è comune a ogni livello della struttura organizzativa della Casa Di Cura; di conseguenza, tutti coloro che svolgono la propria attività per la Casa Di Cura, nell'ambito delle funzioni e responsabilità ricoperte, sono impegnati nel definire e nel partecipare attivamente al corretto funzionamento del sistema di controllo interno.

Ciò posto, con specifico riguardo alle problematiche connesse al rischio informatico, la Casa Di Cura, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e (ii) la garanzia della massima continuità del servizio.

### **3.2 Principi generali di comportamento**

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che la Casa Di Cura si pone sono i seguenti:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti della Casa di Cura (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-*bis* del D.Lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente parte speciale. Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:
  - a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
  - b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
  - c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
  - d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
  - e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
  - f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
  - g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
  - h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
  - i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
  - j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
  - k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;

5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

## 4 Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001

La attività sensibile individuata, in riferimento ai Reati Informatici richiamati dall'art. 24- *bis* del D.Lgs. 231/2001, è la gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione
- gestione e protezione della postazione di lavoro
- gestione degli accessi verso l'esterno
- gestione e protezione delle reti
- gestione degli output di sistema e dei dispositivi di memorizzazione
- Sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)

## 5 Principi generali di controllo

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- **Segregazione delle attività:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di (i) gestione di un processo e di controllo dello stesso, (ii) progettazione ed esercizio, (iii) acquisto di beni e risorse e relativa contabilizzazione.
-

- **Esistenza di procedure/norme/circolari:** devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società.
- **Tracciabilità:** ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

## 6 Principi di riferimento specifici relativi alla regolamentazione delle singole

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al paragrafo 5, nel disciplinare la fattispecie di attività sensibile di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

### 6.1 Gestione e monitoraggio degli accessi ai sistemi informatici e telematici

1) Esistenza di una normativa aziendale relativa alla gestione del rischio informatico che individui le seguenti fasi:

- identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
- individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
- individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
- identificazione delle possibili contromisure;
- effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
- definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
- documentazione e accettazione del rischio residuo.

2) Esistenza di una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:

- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;

- puntuale pianificazione delle attività di sicurezza informatica;
  - progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
  - definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale;
  - applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.
- 3) Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
- 4) Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.
- 5) Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.
- 6) Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si espliciti attraverso la verifica e la gestione dei diritti d'accesso.
- 7) Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
- 8) Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
- 9) Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).
- 10) Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.
- 11) Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.
- 12) Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni).
- 13) Predisposizione e attuazione di una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.
- 
-

## 7 I controlli dell'Organismo di Vigilanza

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste nella Parte Generale del presente Modello.