PARTE SPECIALE
Reati Informatici
(Articolo 24-bis, D. Lgs. n. 231/01)

Fondo Mario Negri

1. FINALITA' DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce alle fattispecie di reato espressamente richiamate dall'art. 24-*bis*, introdotto dall'art. 7 della Legge 18 marzo 2008 n. 48, recante la ratifica e l'esecuzione della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica (d'ora innanzi, per brevità, i "**Reati Informatici**") ed, in particolare, i comportamenti che devono essere tenuti dai soggetti che utilizzano gli strumenti informatici del Fondo.

Obiettivo della presente Parte Speciale, al fine di limitare il rischio circa il verificarsi dei Reati Informatici, consiste nel fare in modo che i Soggetti Apicali, ed i Soggetti Sottoposti adottino regole di condotta conformi a quanto prescritto dalla norma, nonché a quanto previsto nel Modello contenente l'insieme dei diritti, doveri e responsabilità che devono essere rispettati da parte dei destinatari della presente Parte Speciale al fine di agire in modo professionale e corretto e nel pieno rispetto della legge.

Di seguito l'elencazione dei Reati Informatici:

- accesso abusivo ad un sistema informatico e telematico (art. 615-*ter,* c.p.);
- detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici (art. 615-*quater,* c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies,* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater,* c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies,* c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis,* c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter,* c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-*quater,* c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies,* c.p.);
- documenti informatici (art. 491-*bis,* c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies,* c.p.).

2. LE FATTISPECIE DI REATI INFORMATICI (ART. 24-*BIS*, D. LGS. N. 231/01)

Di seguito, il testo delle disposizioni del Codice Penale richiamate dall'art. 24-*bis* del Decreto e ritenute rilevanti da parte del Fondo, in considerazione delle attività svolte, unitamente ad un breve commento delle singole fattispecie.

(i) Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*, c.p.)

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero 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".

Il reato in questione è un reato comune, realizzabile ad opera di chiunque; la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore provato, operatore del sistema) integra la circostanza aggravante di cui al 2° comma, n. 1.
Quanto alla condotta penalmente rilevante, da un lato è punito colui che si introduce abusivamente, e cioè senza il consenso del titolare dello *ius excludendi*, in un sistema informatico o telematico munito di sistemi di sicurezza; dall'altro, è punito chi permanga in collegamento con il sistema stesso, nonostante il titolare abbia esercitato, sia pur tacitamente, lo *ius excludendi*.
L'accesso ad un sistema informatico o telematico può avvenire per acquisire informazioni o dati ovvero per manipolare i dati presenti nell'archivio elettronico, al fine di conseguire un vantaggio o per fini meramente distruttivi. In ogni caso, il reato si consuma con il semplice accesso al sistema informatico o telematico, purché esso sia protetto da misure di sicurezza.

La disposizione contenuta nell'ultimo comma appresta una tutela più intensa, attraverso l'inasprimento della pena, a taluni sistemi informatici, che, per la funzione svolta e per il rilevante interesse pubblico, si appalesano come beni di primaria importanza.

(ii) Detenzione e diffusione abusiva di codici di accesso a sistema informatici o telematici (art. 615-*quater,* c.p.)

"*Chiunque, al fine di procurare a sé 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 a un anno e con la multa sino a € 5.164.*
La pena è della reclusione da uno a due anni e della multa da € 5.164 a € 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater[1]".

La norma in esame completa la tutela prevista dalla disposizione precedente e punisce l'abusiva acquisizione in qualunque modo dei mezzi o codici di accesso, che consente a soggetti non legittimati di inserirsi nel sistema informatico o telematico altrui, vanificando l'ostacolo costituito dalle misure di protezione. Si tratta di un reato di pericolo, essendo la condotta prodromica rispetto ad alte condotte delittuose che possono consumarsi una volta superato l'ostacolo rappresentato dalle misure di protezione.
La prima parte della disposizione descrive varie condotte atte ad integrare la fattispecie:

- "**procurarsi**" i mezzi di accesso ad un sistema, ovvero appropriarsi fisicamente della chiave meccanica o della scheda magnetica, oppure individuare i codici di accesso attraverso procedimenti logici tipici del computer, soprattutto quando la combinazione alfa-numerica è di semplice decodificazione;
- "**riprodurre**", nel senso di realizzare una copia abusiva di un codice di accesso, idonea all'uso;
- "**divulgare**" a terzi del codice o della parola-chiave, mediante la diffusione, la comunicazione, la consegna, condotte che possono concorrere con il mero procacciamento.

Il reato in questione è un reato comune, realizzabile ad opera di chiunque; la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato, operatore del sistema) integra la circostanza aggravante di cui al 2° comma.

[1] Le circostanze aggravanti previste dai numeri 1) e 2) del 4° comma dell'art. 617- *quater* c.p. ricorrono qualora il fatto sia 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*".

(iii) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies*, c.p.)

"*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 fino a due anni e con la multa fino a € 10.329*".

La condotta criminosa si realizza attraverso comportamenti, quali il procacciamento, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione, la consegna o la messa a disposizione di terzi di programmi informatici virali, al fine di danneggiare illecitamente, o interrompere totalmente o parzialmente, o alterare, un programma informatico o telematico o i dati e le informazioni in esso contenute o ad esso pertinenti.

(iv) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*, c.p.)

"*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*".

La norma prevede due distinte ipotesi criminose. La prima, prevista al 1° comma, consiste nell'intercettare, impedire o interrompere comunicazioni con e tra mezzi informatici o telematici. Per intercettazione si intende la presa di cognizione totale o parziale della comunicazione consistente

nell'intromissione nel corso della comunicazione. L'interruzione si verifica quando la comunicazione sia iniziata e, successivamente, sia fatta cessare. L'impedimento, invece, esclude anche il mero inizio della comunicazione, rendendola impossibile.
La seconda ipotesi criminosa, prevista al 2° comma, consiste nella rivelazione di notizie illegittimamente apprese e deve essere rivolta al pubblico, per cui non costituiscono reato le comunicazioni personali e riservate.
Il reato in questione è un reato comune, realizzabile ad opera di chiunque. Il 4° comma, tuttavia, prevede una serie di circostanze aggravanti, in presenza delle quali il delitto, perseguibile a querela delle persone offese nelle ipotesi contemplate dai primi due commi, diviene perseguibile d'ufficio con contestuale aumento della pena. Tali aggravanti riguardano la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato, operatore del sistema) o la qualità oggettiva del sistema informatico o telematico in danno del quale si agisce (" … *utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità*").

(v) Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies,* c.p.)

"*Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire od 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'articolo 617-quater".

La condotta consiste nell'installazione di strumenti idonei ad intercettare, impedire o interrompere le comunicazioni; non è necessario che questi strumenti vengano effettivamente utilizzati, essendo sufficiente la loro posa in opera e la loro attitudine agli scopi per i quali essere sono stati installati.
Il reato si consuma con il solo fatto di aver collocato gli apparati idonei agli scopi sopra indicati.

(vi) Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis,* c.p.)

"*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 la circostanza di cui al numero 1) del secondo comma dell'articolo 635[2]*, 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*".

La disposizione in commento punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime informazioni, dati o programmi informatici altrui.
Il reato prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema. Al ricorrere di una delle aggravanti previste, il reato è perseguibile d'ufficio, altrimenti a querela.

(vii) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter*, c.p.)

"*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'articolo 635, ovvero il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti all'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante ai fini 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. Rientrano, pertanto, in tale fattispecie, anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.
Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

[2] L'art. 635, 2° comma, n. 1, c.p. prevede l'aumento della pena nel caso in cui il danneggiamento è commesso "*con violenza alla persona o con minaccia*".

(viii) Danneggiamento di sistemi informatici o telematici (art. 635-*quater*, c.p.)

"*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) del secondo comma dell'articolo 635 ovvero il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma in esame punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-*bis* c.p., 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. Per dirsi consumato il reato in oggetto, il sistema su cui è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.
Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

(ix) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies*, c.p.)

"*Se il fatto di cui all'articolo 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) del secondo comma dell'articolo 635, ovvero il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma in esame punisce le medesime condotte descritte nell'articolo che precede, perpetrate, però, su sistemi informatici o telematici di pubblica utilità. A tal proposito, si rileva che, a differenza del testo letterale dell'art. 635-*ter* c.p., questa norma non fa più alcun riferimento all'utilizzo dei sistemi informatici o telematici da parte di enti pubblici. Per la configurazione del reato in oggetto parrebbe, quindi, che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità". Non sarebbe, cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, dall'altro

lato, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.
Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

(x) Falsità di un documento informatico pubblico o privato avente efficacia probatoria (art. 491-*bis,* c.p.)

"*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*".

L'articolo in esame dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 c.p. Si citano, tra gli altri, i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

3. LE SANZIONI PREVISTE IN RELAZIONE AI REATI INFORMATICI

Si riporta di seguito una tabella riepilogativa delle relative sanzioni previste dall'articolo 24-*bis*, D. Lgs. n. 231/01, con particolare riferimento ai soli reati rilevanti per il Fondo, indicati al precedente paragrafo 2.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.) Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.) Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.) Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.)	Da 100 a 500 quote	Art. 9, comma 2, lett. a), b), e): – interdizione dall'esercizio dell'attività; – sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; – divieto di pubblicizzare beni o servizi.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quate*r c.p.) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615-*quinquies* c.p.)	Fino a 300 quote	Art. 9, comma 2, lett. b), e): – sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; – divieto di pubblicizzare beni o servizi.
Documenti informatici (art. 491-*bis* c.p.)	Fino a 400 quote	Art. 9, comma 2, lett. c), d), e): – divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; – esclusione da agevolazioni, finanziamenti, contributi o sussidi o eventuale revoca di quelli già concessi; – divieto di pubblicizzare beni o servizi.

4. I PROCESSI SENSIBILI NELL'AMBITO DEI REATI INFORMATICI E LE POSSIBILI MODALITA' DI COMMISSIONE

Con riferimento ai Reati Informatici indicati al precedente paragrafo 2, ritenuti applicabili e rilevanti per il Fondo, vengono di seguito indicati i principali Processi Sensibili, unitamente alle principali possibili modalità di realizzazione dei reati medesimi.

Per tutti i reati individuati, la funzione aziendale coinvolta è il Servizio Sistemi Informativi.

Nei successivi paragrafi 5 e 6 sono, quindi, individuate le norme di comportamento, rispettivamente, generale e particolare volte a prevenire ed impedire il verificarsi degli stessi.

1) Accesso abusivo a un sistema informatico o telematico (art. 615-*ter,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica;
- modalità di autenticazione ed autorizzazione per l'accesso ai sistemi informatici.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 615-*ter*, c.p.:

- ✓ utilizzare i sistemi informatici dal Fondo e/o personali, per accedere a sistemi informatici dal Fondo o di altri soggetti, contro la volontà o all'insaputa del legittimo titolare, anche mediante l'utilizzo di *username* e *passwords* ottenute in maniera fraudolenta e/o per mezzo di tecniche di *hacking*, o in altro modo improprio, da parte di utenti/specialisti IT;
- ✓ prestare o cedere a terzi qualsiasi apparecchiatura informatica appartenente al Fondo, o le relative credenziali di accesso, per consentire o agevolare l'accesso abusivo ad un sistema informatico o telematico;

- ✓ fornire supporto e competenze tecniche ai fini dell'accesso abusivo a un sistema informatico o telematico.

2) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica;
- modalità di autenticazione ed autorizzazione per l'accesso ai sistemi informatici.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 615-*quater,* c.p.:

- ✓ utilizzo di tecniche di "*social engineering*" (ad esempio, *phishing*);
- ✓ accesso indebito agli archivi contenenti le credenziali di accesso ai sistemi;
- ✓ fornire supporto e competenze tecniche ai fini della realizzazione del reato *de quo*.

3) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;

- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica;
- modalità di autenticazione ed autorizzazione per l'accesso ai sistemi informatici.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 615-*quinquies*, c.p.:

- ✓ danneggiamento delle infrastrutture tecnologiche di terzi al fine di impedirne l'attività o danneggiarne l'immagine;
- ✓ danneggiamento di informazioni, dati e programmi aziendali e/o di terzi causato mediante la diffusione di virus o altri programmi malevoli, commessa da soggetti che utilizzano lecitamente o illecitamente la rete o i sistemi di posta del Fondo;
- ✓ violazione dei sistemi di sicurezza di terzi tramite tecniche di *hacking*;
- ✓ installazione di apparecchiature per l'intercettazione di comunicazioni pubbliche o private di *competitors*;
- ✓ fornire supporto e competenze tecniche ai fini della realizzazione del reato *de quo*.

4) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 617-*quater,* c.p.:

- ✓ impedimento/interruzione di una comunicazione al fine di evitare che un concorrente trasmetta i dati e/o l'offerta per la partecipazione a una gara;

- ✓ installazione e/o utilizzo non autorizzati di dispositivi *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici, e/o di interferire nelle comunicazioni del concorrente;
- ✓ intercettazione fraudolenta di comunicazioni di enti concorrenti nella partecipazione di gare d'appalto o di fornitura svolte su base elettronica (c.d. *e-marketplace*), per evitare che i concorrenti possano presentare al compratore un'offerta migliore, ovvero anche solo per conoscere l'entità dell'offerta concorrente, qualora essa non sia in chiaro;
- ✓ intercettazione fraudolenta di una comunicazione che avviene tra più parti al fine di veicolare informazioni false o comunque alterare, con lo scopo, ad esempio, di danneggiare l'immagine di un *competitor*;
- ✓ intromissione in una comunicazione in corso, per acquisire la *password* inviata dall'utente abilitato al sistema, al fine di utilizzarla successivamente per sostituirsi alla persona legittimata ed introdursi nel sistema;
- ✓ intercettazione o impedimento di comunicazioni informatiche o telematiche per mezzo dell'installazione di apparecchiature atte a intercettare e/o impedire comunicazioni informatiche commesse dal personale incaricato della gestione degli apparati e dei sistemi componenti l'infrastruttura di rete aziendale;
- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

5) Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies*, c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 617-*quinquies*, c.p.:

- ✓ installazione e/o utilizzo non autorizzati di dispositivi *software* e/o *hardware* atti ad interferire nelle comunicazioni del concorrente;

- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

6) Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis*, c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- modalità di classificazione dei dati ed identificazione delle relative misure di protezione;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 635-*bis*, c.p.:

- ✓ accesso indebito a sistemi di terzi con violazione dei dispositivi di sicurezza e danneggiamento o distruzione di informazioni, dati o programmi informatici o telematici;
- ✓ alterazione di dati presenti su sistemi di terzi;
- ✓ violazione fisica delle protezioni ai sistemi e danneggiamento delle infrastrutture tecnologiche dei concorrenti;
- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

7) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter*, c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;

- gestione dei servizi-utente potenzialmente incompatibili;
- modalità di classificazione dei dati ed identificazione delle relative misure di protezione;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hard-ware*, *soft-ware* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *soft-ware* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 635-*ter*, c.p.:

- ✓ accesso indebito a sistemi dello Stato, di altro ente pubblico o di pubblica utilità, mediante violazione dei dispositivi di sicurezza al fine di danneggiare o distruggere le informazioni e/o i dati ivi custoditi o i programmi informatici o telematici da tali sistemi utilizzati;
- ✓ alterazione di dati presenti su sistemi informatici o telematici dello Stato, di altri enti pubblici o comunque di pubblica utilità;
- ✓ violazione fisica delle protezioni ai sistemi e danneggiamento delle infrastrutture tecnologiche dello Stato, di altro ente pubblico o di pubblica utilità;
- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

8) Danneggiamento di sistemi informatici o telematici (art. 635-*quater*, c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- modalità di classificazione dei dati ed identificazione delle relative misure di protezione;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 635-*quater*, c.p.:

- ✓ accesso indebito mediante l'utilizzo di tecniche di *hacking*, e conseguente danneggiamento, dei siti web e/o dei sistemi informatici dei concorrenti, siano essi pubblici che privati;
- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

9) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;
- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- modalità di classificazione dei dati ed identificazione delle relative misure di protezione;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica.

In particolare, sono state ipotizzate le seguenti principali modalità di commissione del reato di cui all'art. 635-*quinquies*, c.p.:

- ✓ accesso indebito mediante l'utilizzo di tecniche di *hacking*, e conseguente danneggiamento, dei siti web e/o dei sistemi informatici dei concorrenti, siano essi pubblici che privati;
- ✓ fornire supporto e competenze tecniche nella commissione del reato *de quo*.

10) Falsità di un documento informatico pubblico o privato avente efficacia probatoria (art. 491-*bis,* c.p.)

In relazione a tale fattispecie di reato, sono stati individuati i seguenti processi sensibili:

- gestione delle tematiche di sicurezza aziendale;
- gestione delle *policies* e delle procedure formalizzate in tema di sicurezza informatica;

- modalità di connessione, monitoraggio e revoca di profili di accesso alle apparecchiature informatiche;
- gestione dei servizi-utente potenzialmente incompatibili;
- modalità di classificazione dei dati ed identificazione delle relative misure di protezione;
- gestione della sicurezza perimetrale fisica e logica delle apparecchiature informatiche;
- monitoraggio delle attività svolte;
- utilizzo del processo formale di *Change Management*;
- gestione della sicurezza nei rapporti con parti terze;
- modalità di acquisizione di strumenti *hardware*, *software* e di gestione della manutenzione evolutiva e correttiva;
- gestione dei *software* di protezione informatica;
- modalità di autenticazione ed autorizzazione per l'accesso ai sistemi informatici.

In particolare, il reato di falsità di un documento informatico pubblico o privato avente efficacia probatoria (art. 491-*bis*, c.p.) potrebbe potenzialmente configurarsi qualora i Soggetti Apicali e/o i Soggetti Sottoposti, nonché più in generale i Destinatari, falsifichino materialmente o ideologicamente i documenti informatici pubblici o privati aventi efficacia probatoria.

5. NORME DI COMPORTAMENTO GENERALI

Al fine di prevenire ed impedire il verificarsi dei Reati Informatici individuati al precedente paragrafo 2, i Soggetti Apicali ed i Soggetti Sottoposti coinvolti nello svolgimento delle attività poc'anzi descritte, nonché i *partners* e i collaboratori esterni operanti sulla base di un rapporto contrattuale con il Fondo, sono tenuti al rispetto dei seguenti principi generali di condotta, oltre a quanto previsto dal Codice Etico e dagli specifici Protocolli Organizzativi descritti al successivo paragrafo 6:

1. astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato riportate nella presente Parte Speciale;
2. astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati indicati nella presente Parte Speciale, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

- ✓ introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;
- ✓ accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati del Fondo, o a parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
- ✓ intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- ✓ utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio, *virus*, *worm*, *troian*, *spyware*, *dialer*, *keylogger*, *rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- ✓ distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
- ✓ introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- ✓ detenere, procurarsi, riprodurre, o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- ✓ procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;

- ✓ alterare, mediante l’utilizzo di firma elettronica o comunque in qualsiasi modo, documenti informatici;
- ✓ produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o alterati.

6. NORME DI COMPORTAMENTO PARTICOLARI

Ferma restando la necessità di porre in essere le condotte di carattere generale indicate al precedente paragrafo 5, con specifico riferimento ai Reati Informatici e ai Processi Sensibili individuati al precedente paragrafo 4, il Fondo ha adottato e attuato specifici Protocolli Organizzativi, tra cui quelli di seguito indicati.

Di tutte le modifiche e/o integrazioni, così come di tutti i nuovi controlli e/o procedure, approvati successivamente all'adozione della presente Parte Speciale, sarà prontamente data notizia a tutti i destinatari della presente Parte Speciale, i quali hanno l'obbligo di prenderne conoscenza e di rispettarne i termini e le modalità ivi contenuti.

1. Codice Etico

Il Codice Etico adottato dal Fondo contiene specifiche previsioni riguardanti i Reati Informatici ed il trattamento illecito di dati.

In particolare, esso indica che il Fondo persegue l'obiettivo del corretto utilizzo dei servizi informatici o telematici, in modo da garantire l'integrità e la genuinità dei dati trattati ed in modo da non ledere gli altrui diritti, a tutela del Fondo stesso e dei terzi, con particolare riferimento alle Autorità ed alle Pubbliche Istituzioni.

In particolare, l'utilizzo degli strumenti e dei servizi informatici deve avvenire nel pieno rispetto delle vigenti normative in materia, delle procedure interne esistenti e di quelle che eventualmente saranno successivamente approvate ed emanante, al fine di evitare di esporre il Fondo a qualsivoglia forma di responsabilità e/o sanzione.

2. Diffusione del Codice Etico nel contesto dell'intera organizzazione aziendale

Il Codice Etico attualmente in vigore è disponibile *on-line* sul sito *internet* del Fondo.

Inoltre, il Fondo si è impegnato a garantire una puntuale diffusione interna del Codice Etico mediante:
- distribuzione a tutti i componenti degli organi sociali ed a tutto il personale dipendente;
- affissione in luogo accessibile a tutti.

A tal fine, il Fondo richiede a ciascun dipendente, collaboratore esterno o fornitore di firmare una dichiarazione di conferma dell'avvenuta presa conoscenza del Codice e di impegnarsi a rispettare le previsioni in esso riportate.
Infine, nei contratti con terze parti, è prevista l'introduzione di clausole e/o la sottoscrizione di dichiarazioni volte sia a formalizzare l'impegno al rispetto del

Codice Etico, sia a disciplinare le sanzioni di natura contrattuale in caso di violazione di tale impegno.

3. Definizione di regole in tema di sicurezza informatica

La gestione delle tematiche di sicurezza è stata affidata alla Funzione Sistemi Informativi, appartenente all'Area Previdenza & Finanza.

In particolare, le tematiche in materia di sicurezza riconducibili al trattamento dei dati di natura personale *ex* D.Lgs. 196/03 sono gestite dalla funzione Controllo Interno appartenente all'Area Affari Generali.

Infine, allo scopo di formare e sensibilizzare i propri dipendenti nell'ambito degli aspetti connessi alla gestione dei sistemi informativi, il Fondo si avvale della consulenza di professionisti esterni.

4. Adozione di una procedura volta a regolamentare la gestione dei sistemi informativi del Fondo Mario Negri da parte dei singoli utenti

Il Fondo ha formalizzato ed adottato la Procedura *"Gestione Utenti dei Sistemi Informativi*" volta, tra l'altro, a prevedere, nell'ambito dello svolgimento delle normali attività operative, la responsabilità di tutti i dipendenti del Fondo nell'assicurare la massima cura e riservatezza all'atto dell'utilizzo dei sistemi informatici assegnati.

5. Predisposizione di una *policy* aziendale relativa al corretto utilizzo degli strumenti informatici

All'interno della procedura di "*Gestione Utenti dei Sistemi Informativi*" è presente l'allegato "*Policy sulla sicurezza aziendale*", in cui vengono sintetizzate le principali regole di utilizzo degli strumenti informatici aziendali quali:

- *Password*;
- PC aziendali;
- *Software*;
- Posta elettronica (identificato come "*bene dell'azienda il cui utilizzo deve essere correlato alle attività produttive, coerente con gli obiettivi aziendali e rispettoso delle regole del buonsenso*");
- Connessione alla rete *internet*, resa disponibile dal Fondo e volta a consentire il reperimento di dati ed informazioni utili allo svolgimento delle attività legate al *business*.

La "*Policy sulla sicurezza aziendale*" viene sottoscritta dai dipendenti del Fondo. In tal modo, relativamente agli aspetti riguardanti l'utilizzo di *hardware*, *software*, strumenti di comunicazione da e verso l'esterno del Fondo, l'utente che, per le mansioni che è chiamato a svolgere, debba accedere ai sistemi, è tenuto ad osservare le *policy* di sicurezza aziendale, comunicate con ordine di servizio e firmate per accettazione.

6. Attività di monitoraggio sulle modalità di connessione ed accesso alle apparecchiature informatiche, alla rete ed ai sistemi informativi

Il Fondo definisce le modalità con cui ogni utenza è associata in maniera univoca ad un dipendente attraverso la procedura di "*Gestione Utenti dei Sistemi Informativi*".

In particolare, essa detta le principali linee guida per l'abilitazione, accesso, modifica e disattivazione dell'utenza a sistema.

Inoltre, in caso di incompatibilità tra le mansioni attribuite al singolo utente e le operazioni che il sistema di rete permette di effettuare, il Responsabile di Servizio competente è tenuto ad effettuare le necessarie modifiche al profilo dell'utente interessato al fine di evitare e/o risolvere il conflitto verificatosi.

7. Classificazione dei dati ed identificazione delle conseguenti misure di protezione

Il Fondo definisce, nell'ambito del Documento Programmatico per la Sicurezza (DPS), i criteri di classificazione dei dati basati su differenti livelli di riservatezza.

Ogni trattamento dei dati svolto tramite l'ausilio di strumenti informatici è supportato dalla relativa documentazione cartacea, appositamente ed adeguatamente depositata presso un archivio gestito da una società esterna fornitrice del servizio.

8. Protezione perimetrale fisica e logica delle linee e delle apparecchiature informatiche

Il Fondo, al fine di garantire la sicurezza perimetrale della rete, si avvale di un apparato *firewall* localizzato presso il gestore esterno della rete stessa.

Inoltre il Fondo, con lo scopo di regolamentare i controlli di sicurezza fisica, al fine di proteggere il Fondo da accessi non autorizzati ai locali, ha adottato una *policy* sulla sicurezza fisica, applicata a tutti i locali di proprietà del Fondo contenenti beni e risorse critiche aziendali.

Inoltre, nell'ambito della stessa *policy* sulla sicurezza aziendale vengono disciplinate le principali regole sull'utilizzo di *software* autorizzati. Gli utilizzatori, infatti, sono tra l'altro tenuti a:

- Utilizzare il *software* solo per ragioni di lavoro;
- Fare esclusivamente uso del *software* installato dal Servizio Sistemi Informativi;
- Non copiare *software* di titolarità o concessi in licenza al Fondo e non installare alcun *software* sul proprio PC senza previa autorizzazione del Servizio Sistemi Informativi.

Infine, nell'ambito della Procedura di *"Back-up*", contenuta nel DPS adottato dal Fondo, vengono stabilite le principali regole per il salvataggio dei dati. In particolare, il Fondo esegue una doppia procedura di salvataggio, sia sulle cartelle dati, sia su programmi, consistente in:

- Procedura di B*ack-up* per AS/400, Archidoc, REMS, e cartelle in rete;
- Procedura di conservazione archivi *Back-up*.

9. Protezione in caso di Change Management

Il Fondo è dotato di una Procedura formale di *"Change Management*", suddivisa nelle seguenti fasi:

- Richiesta di modifica;
- Sviluppo della modifica;
- *Testing* delle modifiche;
- Rilascio in produzione.

10. Protezione dei sistemi mediante soluzioni antivirus e antispam aggiornate

Il Fondo adotta su tutti i Personal Computer e i server aziendali *software antivirus* e *antispyware*. Sono stati, altresì, installati sistemi *antivirus* e *antispam* sui *server* di posta elettronica.

7. COMPITI DELL'ODV

Fermi restando i compiti e le funzioni dell'OdV statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati Informatici, lo stesso è tenuto ad effettuare specifici controlli e, periodicamente, controlli a campione sulle attività connesse ai Processi Sensibili descritti ai precedenti paragrafi di questa Parte Speciale, diretti a verificare la corretta implementazione delle stesse in relazione alle regole di cui al presente Modello.
A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.