# Modello di Organizzazione Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, N. 231

## Rimorchiatori Napoletani Srl

# PARTE SPECIALE G

## Delitti informatici e Delitti relativi al trattamento illecito dei dati

# INDICE

## *Parte Speciale G*

1..... .

PREMESSA

La presente Parte Speciale ha la finalità di definire i principi generali di comportamento e i protocolli di controllo cui tutti i Destinatari di Rimorchiatori Napoletani Srl dovranno conformarsi al fine di prevenire la commissione dei reati di seguito richiamati e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale G del Modello ha lo scopo di:

- indicare le regole che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo;
- Codice Etico;
- Procedure Operative;
- Procure.

Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

E' inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di Legge.

2..... .

LA TIPOLOGIA DEI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI (ART. 24 BIS DEL DECRETO)

La legge 18 marzo 2008 n. 48 ha ratificato ed eseguito la Convenzione di Budapest del 23 novembre 2001, promossa dal Consiglio d'Europa in tema di criminalità informatica e riguardante, in particolare, i reati commessi avvalendosi in qualsiasi modo di un sistema informatico od in suo danno, ovvero che pongano in qualsiasi modo l'esigenza di raccogliere prove in forma informatica.

Ai sensi dell'art. 1 della Convenzione, rientra nella nozione di "sistema informatico" "qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati". Tra i "dati informatici" rientra, inoltre, "qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione".

L'art. 24 bis contempla la responsabilità degli enti con riguardo a tre distinte categorie:

a) reati che comportano un "danneggiamento informatico" (art. 24 bis, co. 1);

b) reati derivanti dalla detenzione o diffusione di codici o programmi atti al danneggiamento informatico (art. 24 bis, co. 2);

c) reati relativi al falso in documento informatico e frode del soggetto che presta servizi di certificazione attraverso la firma digitale (art. 24 bis, co. 3).

- L'art. 24 bis prevede la responsabilità degli enti in relazione a sette distinti reati che hanno come fattore comune il "danneggiamento informatico", ossia che determinano l'interruzione del funzionamento di un sistema informatico o il danneggiamento del software, sotto forma di programma o dato. Più in particolare, ricorre il danneggiamento informatico quando, considerando sia la componente hardware che quella software, anche separatamente, si verifica una modifica tale da impedirne, anche temporaneamente, il funzionamento. Rilevano in particolare i reati di:

  1) *Accesso abusivo ad un sistema informatico o telematico* (art. 615 ter), che ricorre a seguito dell'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza. La fattispecie presuppone dunque l'esistenza di protezioni poste dal proprietario del sistema informatico o telematico volte a limitare o regolamentare l'accesso al medesimo;
  2) *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617 quater), che ricorre a seguito dell'intercettazione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti fra più sistemi, ovvero dell'impedimento o dell'interruzione delle stesse. Il reato è aggravato, tra l'altro, nel caso in cui la condotta rechi danno ad un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica utilità;
  3) *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche* (art. 617 quinquies), che sussiste nel caso di chi – 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;
  4) *Danneggiamento di informazioni, dati e programmi informatici* (art. 635 bis) e *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* (art. 635 ter); *Danneggiamento di sistemi informatici o telematici* (art. 635 quater) e *Danneggiamento di sistemi informatici o telematici di pubblica utilità* (art. 635 quinquies). I reati in esame sono caratterizzati dall'elemento comune della condotta di distruzione, deterioramento, cancellazione, alterazione o soppressione e si differenziano in relazione all'oggetto materiale (informazioni, dati, programmi informatici ovvero sistemi informatici o telematici), aventi o meno rilievo pubblicistico in quanto utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

- I reati contemplati dall'art. 24 bis, co. 2, possono considerarsi accessori rispetto a quelli in precedenza presi in esame: la detenzione o diffusione di codici di accesso o la detenzione o diffusione di programmi (virus o spyware) o dispositivi diretti a danneggiare o interrompere un sistema telematico, possono infatti essere utilizzati per un accesso

abusivo ad un sistema o nella gestione di un'intercettazione di informazioni. In particolare, si prevedono i seguenti reati:

1) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater), che sanziona chi, 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;
2) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies), che sanziona il fatto di chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, 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.

– L'art. 24, co. 3, sanziona infine l'utilizzo del mezzo elettronico finalizzato a minare l'affidabilità di mezzi utilizzati per garantire la certezza nei rapporti tra i consociati: il documento informatico e la firma digitale, la cui disciplina è oggi compiutamente delineata dal Codice dell'amministrazione digitale (D. Lgs. n. 82 del 2005). In particolare:
  1) l'art. 491 bis cp estende la disciplina posta dal codice penale in materia di falsità documentali anche al documento informatico pubblico o privato avente efficacia probatoria. In virtù di tale estensione, dunque, la falsificazione di un documento informatico potrà dar luogo, tra l'altro, ai reati di falso materiale ed ideologico in atto pubblico, certificati, autorizzazioni amministrative, copie autentiche di atti pubblici o privati, attestati del contenuto di atti (artt. 476-479 c.p.), falsità materiale del privato (art. 482 c.p.), falsità ideologica del privato in atto pubblico (art. 483 c.p.), falsità in registri e notificazioni (art. 484 c.p.), falsità in scrittura privata (art. 485 c.p.), uso di atto falso (art. 489 c.p.);
  2) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies), che sanziona il soggetto che, prestando servizi di certificazione di firma elettronica, viola gli obblighi posti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di recare ad altri danno.

3..... .

LA TIPOLOGIA DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25 NONIES DEL DECRETO)

Con L. 23.07.2009, n. 99 è stata prevista la responsabilità amministrativa degli Enti in relazione anche ai reati in materia di protezione del diritto d'autore e di altri diritti connessi al suo esercizio. Si tratta, più in particolare, di alcune delle fattispecie di reati posti a tutela del diritto dell'autore e allo sfruttamento esclusivo delle opere dell'ingegno che sanzionano nello specifico:

- la messa a disposizione del pubblico, tramite l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o di parti di esse, ivi comprese quelle non destinate alla pubblicazione, ovvero l'usurpazione della paternità dell'opera, la deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti un'offesa all'onore od alla reputazione dell'autore (art. 171, co. 1, lett- a-bis) e 3);
- la duplicazione abusiva, per trarne profitto, di programmi per elaboratore ovvero l'importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o la concessione in locazione, sempre al fine di trarne profitto, di programmi contenuti in supporti non contrassegnati dalla SIAE, ovvero di mezzi di qualsiasi tipo intesi unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori (art. 171 bis, co. 1);
- la riproduzione, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o dimostrazione in pubblico, al fine di trarne profitto, su supporti non contrassegnati SIAE, di una banca di dati in violazione delle disposizioni di legge a tutela dei diritti dell'autore ovvero l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di legge a tutela dei diritti del costitutore della banca di dati (artt. 102 bis e 102 ter), ovvero la distribuzione, vendita o concessione in locazione di una banca dati (art. 171 bis);
- se commesse a scopo di lucro e non a fini personali, la duplicazione abusiva, la riproduzione, la trasmissione, la diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, ovvero, anche al di fuori delle ipotesi di concorso, l'introduzione nel territorio dello Stato, la detenzione per la vendita, la distribuzione, il commercio, la concessione in noleggio o la cessione, proiezione in pubblico, trasmissione a mezzo della televisione, radio, la diffusione in pubblico di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fotogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento, di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, nonché qualsiasi supporto contenente opere dell'ingegno per le quali è richiesta l'apposizione del contrassegno SIAE, ovvero di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto (art. 171 ter, lett. a, b, c, d e f);
- la ritrasmissione o diffusione, in assenza di accordo con il legittimo distributore, con qualsiasi mezzo, di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato (art. 171 ter, lett. e);
- la fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per vendita o noleggio, la detenzione per scopi commerciali di qualsiasi mezzo o servizio idoneo a facilitare l'elusione delle misure tecnologiche poste a protezione delle opere o dei materiali protetti ovvero la rimozione delle informazioni elettroniche sul regime dei diritti (art. 171 ter, lett. f bis e h);

- la mancata comunicazione entro 30 giorni dalla data di immissione in commercio sul territorio nazionale dei dati necessari alla univoca identificazione dei supporti non soggetti al contrassegno, ovvero la falsa dichiarazione relativa all'avvenuto assolvimento degli obblighi in materia di contrassegno SIAE (art. 181 bis, co. 2) (art. 171 septies);
- la produzione, messa in vendita, importazione, promozione, installazione, modificazione, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, satellite, cavo, in forma sia analogica sia digitale (art. 171 octies).

4.....

DESTINATARI DELLA PARTE SPECIALE - PRINCIPI GENERALI DI COMPORTAMENTO E DI CONTROLLO E PROTOCOLLI SPECIFICI DI CONTROLLO NELLE AREE A RISCHIO

Con specifico riferimento alle analisi e valutazioni condotte in materia di criminalità informatica, per sua natura tema pervasivo di diversi ambiti ed attività aziendale, l'attenzione è stata posta su quello che può essere definito quale il processo di "gestione della sicurezza informatica".

A titolo esemplificativo delle modalità attraverso le quali potrebbero essere realizzati i reati in esame si menzionano:

- accesso abusivo ad un sistema informatico o telematico: tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società si introduca abusivamente 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. Ad esempio, un dipendente di Rimorchiatori Napoletani accede, anche indirettamente tramite un apposito programma ("spyware", "trojan horse" o "bot"), al computer di un'azienda concorrente, enti detentori di informazioni di interesse ovvero potenziali clienti, al fine di visualizzare i termini dell'offerta che quest'ultima intende presentare;
- accesso abusivo ad un sistema informatico o telematico di una banca o di una pubblica amministrazione, allo scopo di modificare i dati relativi alla Società;
- accesso abusivo ad un sistema informatico o telematico facente capo alla Società medesima, allo scopo, ad esempio, di manipolare i dati destinati a confluire nel bilancio;
- accesso abusivo ad un sistema informatico o telematico facente capo ad un cliente per modificare i dati relativi ad una commessa effettuata o in corso di effettuazione da parte della Società (ad esempio, sistemi di fatturazione od ordinativi);
- intercettazione fraudolenta di comunicazioni tra i dipendenti al fine di conoscere preventivamente eventuali strategie in sede sindacale o di verificarne la produttività. Ad esempio, un dipendente di Rimorchiatori Napoletani installa in alcuni terminali aziendali un software ("trojan horse" o "spyware"") che contiene una scheda che consente di intercettare informazioni riservate da rivendere ai concorrenti;

- intercettazione fraudolenta di comunicazioni di enti concorrenti nel contesto di una partecipazione ad una gara di appalto o di fornitura svolta su base elettronica al fine di falsarne o conoscerne preventivamente l'esito;
- impedimento/interruzione di una comunicazione al fine di ostacolare un concorrente nell'invio della documentazione relativa ad una gara ovvero di materiale destinato alla clientela in modo da determinarne l'inadempimento;
- danneggiamento dei sistemi informatici/telematici facenti capo ad un concorrente al fine di impedirne l'attività o comprometterne l'immagine. Ad esempio, Rimorchiatori Napoletani assolda un hacker che modifica il sito web dell'azienda concorrente (cosiddetto "web defacing"), facendo apparire informazioni false o tali da compromettere la reputazione dell'azienda stessa;
- danneggiamento dei sistemi informatici/telematici facenti capo ad una controparte commerciale al fine di poter procedere alla fornitura di nuovi prodotti o di dimostrare l'inaffidabilità di quelli in precedenza forniti da un concorrente;
- danneggiamento, la distruzione o la manomissione di documenti informatici aventi efficacia probatoria presenti negli archivi di pubbliche amministrazioni nell'interesse della Società. Ad esempio, un dirigente di Rimorchiatori Napoletani ruba la smart card necessaria per utilizzare la firma digitale "forte" di un amministratore delegato di un'azienda concorrente, al fine di modificare un documento informatico avente valore legale, laddove per firma digitale "forte" si intende la firma elettronica la cui provenienza e integrità è stata preventivamente certificata da un Ente certificatore legalmente autorizzato.

Le aree a rischio reato individuate con riferimento ai reati richiamati dagli artt. 24 bis e 25-nonies del Decreto sono le seguenti:

1. Gestione dei profili utente e del processo di autenticazione
2. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio
3. Gestione e protezione della postazione di lavoro
4. Gestione degli accessi da e verso l'esterno
5. Gestione e protezione delle reti
6. Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)
7. Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.)
8. Gestione dei dispositivi o programmi informatici e dei servizi di installazione e manutenzione di hardware, software, reti.

Destinatari della presente Parte Speciale sono gli Amministratori, i Sindaci, il Presidente, i Direttori, i Dirigenti, i Dipendenti in linea gerarchica operanti nelle aree a rischio, nonché i Consulenti, i collaboratori, i Fornitori e i Partner (di seguito definiti i "Destinatari").

La presente Parte Speciale prevede l'espresso divieto – a carico dei suddetti Destinatari – di porre in essere comportamenti:

- tali da integrare le fattispecie di reato sopra considerate (art. 24-bis e 25-nonies del Decreto);
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato, rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

Eventuali violazioni di suddette norme aziendali, devono essere segnalate ai Responsabili e/o all'OdV (attraverso l'invio di una Segnalazione da effettuarsi nelle circostanze e secondo le modalità definite nell'ambito della Parte Generale).

Con riguardo all'utilizzo e gestione dei sistemi, strumenti, documenti o dati informatici ovvero di opere di qualsiasi natura coperte dal diritto d'autore, tutti coloro che operano per conto della Società debbono conformarsi ai seguenti principi:

- rispetto delle procedure per la gestione della sicurezza informatica, delle procedure e policy nell'utilizzo degli strumenti informatici e telematici, delle reti aziendali, nella gestione delle password, della posta elettronica ecc.
- applicazione delle procedure atte a prevenire e/o impedire la realizzazione di illeciti informatici da parte degli esponenti aziendali.

### 4.1 DIVIETI

Nell'ambito dei suddetti comportamenti **è fatto divieto** di:

- utilizzare gli strumenti, i dati ed i sistemi informatici e telematici in modo da recare danno a terzi, in particolare interrompendo il funzionamento di un sistema informatico o l'alterazione di dati o programmi informatici, anche a seguito dell'accesso abusivo, ovvero dell'intercettazione di comunicazioni;
- detenere o diffondere indebitamente codici o programmi atti al danneggiamento informatico;
- alterare o falsificare documenti informatici di qualsiasi natura o utilizzare indebitamente la firma elettronica;
- utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore;
- porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy; regolamenti Consob ecc.), nonché della normativa in materia di tutela del diritto d'autore (L. 22.04.1941).

### 4.2 PRINCIPI GENERALI DI CONTROLLO

Tutte le aree a rischio devono essere gestite nel rispetto dei seguenti principi generali di controllo:

- Principi etico-comportamentali: disciplinati nella presente Parte Speciale e/o nel Codice Etico.
- Procedure Operative e protocolli specifici di controllo: si tratta di regole formali o prassi consolidate idonee a definire ruoli, responsabilità, sistema autorizzativo, modalità operative e attività di controllo cui attenersi per lo svolgimento delle attività aziendali, ivi incluse quelle sensibili.
- Tracciabilità e verificabilità ex post: principio secondo il quale: i) ogni operazione relativa all'area a rischio deve essere, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'area a rischio deve essere verificabile ex post, anche tramite appositi supporti documentali.
- Segregazione dei compiti: preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti. In particolare, deve essere garantita la separazione delle responsabilità tra chi autorizza, chi esegue e chi controlla il processo.
- Procure: i poteri autorizzativi e di firma devono essere: i) coerenti con le responsabilità organizzative e chiaramente definiti e conosciuti all'interno della Società.

## 4.3 PROTOCOLLI SPECIFICI DI CONTROLLO

Con riferimento alle aree a rischio identificate sono da considerarsi vigenti i seguenti principi di controllo:

- sono individuate – in base al principio della separazione dei ruoli – le strutture aziendali preposte alla gestione della sicurezza ed integrità dei dati e delle informazioni, nonché alla gestione delle infrastrutture di rete e dei sistemi e sono attribuiti alle medesime specifici compiti in materia di prevenzione dei delitti informatici e di trattamento illeciti di dati. In particolare, la responsabilità della sicurezza delle informazioni è affidata alla Direzione Assicurazione Qualità;
- l'accesso ai sistemi e applicativi informatici avviene sulla base di un'opportuna profilazione e autorizzazione degli utenti;
- i criteri con cui si assegnano i privilegi ed i diritti di accesso alle risorse informatiche e ai dati devono essere determinati sulla base dell'analisi delle effettive necessità, connesse al tipo di incarico svolto. Deve inoltre essere prevista una revisione periodica dei privilegi concessi.
- la revisione delle condizioni che hanno portato a concedere i vari privilegi di accesso deve costituire un processo continuo e formalizzato e deve avvenire nel rispetto dei seguenti principi:
  - revisione dei diritti di accesso degli utenti ad intervalli regolari;
  - revisione delle autorizzazioni per gli account privilegiati (amministratori di sistema, ecc.) ad intervalli più frequenti;
  - controllo della distribuzione dei privilegi a intervalli regolari finalizzati a garantire che utenti non autorizzati abbiano ottenuto privilegi non di loro spettanza;

- rispetto del principio generale del "need-to-know" (ognuno deve avere accesso solo ai dati e applicazioni di propria competenza e necessari per lo svolgimento delle proprie mansioni).

- sono predisposti strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici o in violazione del diritto d'autore da parte degli esponenti aziendali attraverso, in particolare, l'uso indebito o non autorizzato della password, la detenzione o installazione di software non previsto dalle procedure aziendali, ivi compresi virus e spyware di ogni genere e natura e dispositivi atti all'interruzione di servizi o alle intercettazioni, l'accesso a siti protetti ovvero non visitabili, il collegamento non consentito di hardware alla rete aziendale. Tali misure devono in particolare prevedere regole in merito:
  - all'attribuzione e revoca delle password, tenendo conto delle mansioni aziendali per la quale viene richiesta/concessa;
  - alla rimozione dei diritti di accesso al termine del rapporto di lavoro;
  - il controllo e la tracciabilità degli accessi;
  - alle modalità di svolgimento delle attività di gestione e manutenzione dei sistemi;
  - alla previsione di controlli sulla idoneità della rete aziendale e sul suo corretto instradamento;

- sono adottate specifiche misure di protezione e mappatura dei documenti elettronici utilizzati per comunicazioni verso l'esterno;

- sono adottate specifiche misure a garanzia del corretto utilizzo dei materiali coperti da diritti di proprietà intellettuale, anche attraverso procedure di controllo della installazione di software sui sistemi operativi;

- sono adottati specifici strumenti per la individuazione, prevenzione e ripristino dei sistemi rispetto a virus e altre vulnerabilità;

- sono previsti e attuati programmi di informazione, formazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

- deve essere previsto nei contratti con terze parti l'introduzione di specifiche clausole a previsione delle politiche e procedure di sicurezza informatica volte a prevenire i rischi dovuti alle connessioni esistenti con i loro sistemi;

5..... .

ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

Nell'ambito dei suoi compiti di vigilanza dell'OdV potrà:

- verificare periodicamente – con il supporto delle altre funzioni competenti – l'osservanza delle norme aziendali in materia di gestione della sicurezza informatica;

- verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole standard finalizzate:

- alla possibilità di Rimorchiatori Napoleatani di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
- all'attuazione di meccanismi sanzionatori (quali la risoluzione del contratto nei riguardi di Fornitori, Appaltatori, Consulenti e Outsourcer in materia di sistemi informatici) qualora si accertino violazioni delle prescrizioni;

- verificare l'adeguatezza e l'aggiornamento della documentazione e delle procedure predisposte con riguardo alla prevenzione dei delitti informatici e al trattamento illecito dei dati, nonché alla tutela del diritto d'autore;
- verificare l'osservanza, attuazione ed adeguatezza del Modello ai fini della prevenzione dei delitti informatici e del trattamento illecito dei dati e a tutela del diritto d'autore;
- verificare il rispetto dei protocolli procedurali, con particolare riferimento alla gestione della sicurezza informatica e alla tutela del diritto d'autore.

Inoltre in ambito aziendale, dovrà essere portata a conoscenza dell'OdV attraverso un flusso informativo periodico, ogni modifica e/o aggiornamento della documentazione relativa al agli aspetti di sicurezza informatica ed eventuali incidenti di sicurezza informatica.