NEOS
(gruppo Alpitour)

Modello di organizzazione, gestione e controllo
(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

PARTE SPECIALE - 8 -

Reati informatici

INDICE

PARTE SPECIALE - 8 -

1. LE MODIFICHE LEGISLATIVE INTRODOTTE CON LA LEGGE 23.03.2008, N. 48 : I REATI INFORMATICI IN GENERALE ……3

2. DESTINATARI E OBIETTIVI DELLE DISPOSIZIONI CONTENUTE NELLA PARTE SPECIALE ……10

3. AREE SENSIBILI E PRINCIPI GENERALI COMPORTAMENTO……11

4. REGOLE SPECIFICHE DI CONDOTTA……12

1. Le modifiche legislative introdotte con la legge 28.03.2008, n. 48 : I reati informatici in generale

La legge 18.03.2008, n. 48 applica la Convenzione di Budapest sul crimine informatico e modifica il decreto legislativo 231/2001 nell'ambito della responsabilità penale delle imprese.

Nel corpo del provvedimento legislativo in oggetto è prevista l'ennesima novella al decreto legislativo 231/2001, oltre a comportare delle rilevanti integrazioni al codice penale e di procedura penale in materia di reati informatici.

A distanza di quattordici anni, il Parlamento ha modificato la legge sui reati informatici recependo la Convenzione sul crimine informatico e introducendo una novità particolarmente importante sulle tecniche di indagine utilizzate dalle forze di polizia rispetto a tali reati.

In particolare gli artt. 244 - *casi e forme delle ispezioni* - e 247 - *casi e forme delle perquisizioni* - del codice di procedura penale sono stati modificati nel senso di imporre alle forze di polizia giudiziaria di adottare misure tecniche volte ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Viene inoltre estesa anche alle perquisizioni informatiche la possibilità per la polizia giudiziaria di procedere anche in presenza di misure di sicurezza, tuttavia, la norma specifica, *"adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*, il che potrebbe voler significare che è illegittimo "bucare" un sistema nel caso in cui non si possiedano le *password,* anche se per fini di acquisizione di prove in ambito giudiziario.

Dal punto di vista dei reati, viene introdotto quello di falsa dichiarazione al certificatore di firme elettroniche: in pratica è sanzionato con la reclusione fino ad un anno il furto di identità o l'uso di false generalità nei confronti di chi deve certificare l'identità del titolare della firma elettronica.
Simmetricamente, la legge punisce il certificatore di firma elettronica che non rispetta le regole normative.

Inoltre, la legge tenta di razionalizzare i reati che puniscono il *cracking* di sistema e il danneggiamento di informazioni. Sono previsti, in successione, i reati di: danneggiamento di dati, informazioni e programmi, fatto esteso da uno specifico articolo anche quando siano utilizzati dallo Stato e da altri enti pubblici; nonché il reato di danneggiamento di sistemi informatici anche di pubblica utilità.

Nella Convenzione è peraltro stabilito che le sanzioni da adottare da parte degli Stati devono essere effettive, proporzionate, dissuasive e con previsione anche di pene detentive.

Il legislatore ha collocato i nuovi reati informatici accanto alle figure di reato già esistenti:

Vecchio testo	Nuovo testo
Documenti informatici (art. 491 bis) *Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni.*	***Documenti informatici (art. 491 bis)*** Norma parzialmente modificata dalla legge 48 / 2008: Al primo periodo, dopo la parola *"privato"* sono inserite le seguenti *"avente efficacia probatoria".* Il secondo periodo è soppresso.
Fattispecie di reato non prevista in epoca precedente alla legge 48 / 2008.	***Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri (art. 495 bis)***
Accesso abusivo ad un sistema informatico o telematico (art. 615 ter)	Fattispecie di reato rimasta invariata.
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater)	Fattispecie di reato rimasta invariata.
Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies)	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies*) 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 altre apparecchiature, dispositivi o programmi telematici

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater)	Fattispecie di reato già esistente nell'ordinamento.
Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)	Fattispecie di reato già esistente nell'ordinamento.
Danneggiamento di sistemi informatici e telematici (art. 635 bis) Fattispecie di reato parzialmente modificata dalla legge 48 / 2008.	***Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis***) *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 ....*
Fattispecie di reato non prevista in epoca precedente alla legge 48 /2008.	***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter)***
Fattispecie di reato non prevista in epoca precedente alla legge 48 / 2008.	***Danneggiamento di sistemi informatici o telematici (art. 635 quater)***
Fattispecie di reato non prevista in epoca precedente alla legge 48 / 2008.	***Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies)***
Frode informatica (art. 640 ter)	Fattispecie di reato rimasta invariata.
Fattispecie di reato non prevista in epoca precedente alla legge 48 / 2008.	***Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies)***

La legge 48/ 2008 introduce nel corpo del decreto legislativo 231 /2001 la norma di cui all'art. 24 *bis* che di fatto estende la lista dei reati che le imprese devono prevenire, includendo, dunque, molti reati informatici e in particolare quelli relativi alle falsificazioni dei *files*, agli accessi abusivi e alle frodi digitali, in particolare:

- ***(art. 615 ter) Accesso abusivo ad un sistema informatico o telematico:*** L'articolo in questione punisce *"chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza"*. Ancora una volta il legislatore italiano ha voluto ricalcare una figura di reato già esistente quale la violazione di domicilio di cui all'art. 614 c.p.

  A livello europeo tutte le norme che regolano l'accesso abusivo ad un sistema informatico presentano delle costanti:

  * si richiede che siano state violate delle misure di protezione;
  * si punisce l'accesso abusivo qualora chi commette il reato non sia autorizzato ad accedere a dei settori di memoria protetti;
  * deve essere minacciata la riservatezza dei dati o dei programmi che il sistema informatico attaccato custodisce.

  L'introduzione abusiva può anche essere opera di soggetti legittimati all'uso del sistema ma autorizzati ad accedere solo ad una parte dei dati contenuti in memoria. In tali casi il sistema protetto diviene solo quella parte di memoria cui l'accesso non è autorizzato.

  Considerando l'intenzione del legislatore di tutelare solo i sistemi protetti da misure di sicurezza pare plausibile l'intenzione di salvaguardare la riservatezza dei dati, si assume infatti che il titolare debba manifestare il suo interesse a tutelare la riservatezza dei dati, adottando misure di sicurezza indipendentemente dalla loro complessità tecnica di implementazione.

  In questa ottica resta estraneo dall'applicazione dell'art. 615 *ter* c.p. l'accesso abusivo in sistemi informatici predisposti esclusivamente al controllo e alla gestione di altri apparecchi in quanto, non contenendo dati rilevanti, non viene messa a rischio la loro riservatezza. In questo caso non vi è un danneggiamento logico del sistema, l'intrusione potrebbe essere finalizzata all'usufruire di servizi senza pagarne il corrispettivo dovuto.

  Non rientrano, altresì, in quanto previste dall'art. 615 *quater* c.p., l'indebita acquisizione di carte di credito telefoniche poiché l'indebito utilizzo permetterebbe solo di usufruire delle prestazioni telefoniche dell'apparecchio.

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

  Contempla la condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema informatico intercorrente fra più sistemi, ovvero le impedisce o le interrompe.

  Salvo che il fatto costituisca più grave reato, la pena più grave si applica a chi diffonde con qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di cui al primo comma.

- ***(art. 617 quinquies) Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche:***

  Contempla la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, interrompere, impedire comunicazioni relative ad un sistema informatico o telematico.

- ***(art. 635 bis) Danneggiamento di informazioni, dati e programmi telematici:***

  Salvo che il fatto non costituisca più grave reato, si contempla la condotta di

chi distrugge, deteriora, sopprime informazioni, dati o programmi informatici altrui.

- ***(art. 635 ter) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità:***
  Salvo che il fatto non costituisca più grave reato, si contempla la condotta di chi pone in essere un comportamento da cui può derivare il deterioramento, la cancellazione, la distruzione di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico, ovvero di pubblica utilità.

- ***(art. 635 quater) Danneggiamento di sistemi informatici o telematici:***
  Salvo che il fatto costituisca un più grave reato, la condotta viene integrata qualora attraverso l'introduzione o la trasmissione di dati o informazioni, si danneggia o si rende inservibile, in tutto o in parte, un sistema informatico o telematico.

- ***(art. 635 quinquies) Danneggiamento di sistemi informatici o telematici di pubblica utilità:***
  La fattispecie in questione viene ad integrarsi se il fatto di cui al precedente art. 635 *quater* è diretto a distruggere, danneggiare o comunque ad ostacolarne il funzionamento.

Nei casi qui di sopra citati è previsto che venga applicata all'ente una sanzione pecuniaria *da cento a cinquecento quote*.

e ancora:

- ***(art. 615 quater) Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici:***
  Le condotte previste e punite, in quanto abusive, dall'articolo in questione sono molteplici e riguardano:
  * l'utilizzo non autorizzato di codici di accesso,
  * la diffusione che si manifesta nel rendere tali codici disponibili ad un numero indeterminato di soggetti,
  * la comunicazione che consiste nel rendere disponibile tali codici ad un numero indeterminato di soggetti,
  * la comunicazione o diffusione di istruzioni che permettono di eludere le protezioni di un sistema.
  Si richiede che la condotta in questione venga posta in essere allo scopo di procurare a sé o ad altri un profitto o di arrecare ad altri un ingiusto danno.

- ***(art. 615 quinquies) Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico:***
  Tale fattispecie contempla la condotta di chi, allo scopo di danneggiare illecitamente un sistema informatico diffonde le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, consentendo in tal modo la interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Nelle ultime due citate ipotesi di reato è previsto che all'ente si applichi una sanzione

pecuniaria *fino a trecento quote*.

- ***(art. 491 bis) Documenti informatici:***
  La fattispecie è integrata attraverso la condotta di chi pone in essere una delle falsità previste dal medesimo capo del codice penale e integranti già reato, riguardante un documento pubblico o privato avente efficacia probatoria.

- ***(art. 640 quinquies) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica:***
  La fattispecie contempla la condotta di chi è addetto ai servizi di certificazione, il quale allo scopo di procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno viola gli obblighi propri di rilascio di un certificato qualificato.

La punibilità del concorso nel reato di natura informatica e la responsabilità (penale, civile o amministrativa) delle persone giuridiche sono dunque previste quando tale reato sia commesso da una persona fisica esercitante poteri direttivi.

Oggi, dunque, l'introduzione dei sopra menzionati reati all'interno del decreto legislativo 231 del 2001 risponde alla nuova esigenza di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi, con la conseguente esigenza per le persone giuridiche di dover predisporre preventive ed idonee misure di sicurezza, controllo e dissuasione per prevenire che al loro interno si commettano le suddette tipologie di reati informatici.

Le aziende risponderanno dei sopra elencati reati nel caso in cui gli illeciti vengano commessi a loro vantaggio da chiunque, agendo a titolo individuale o in quanto membro di un organo societario, rivesta nell'ambito di una società una posizione preminente che sia basata sul potere di rappresentanza dell'azienda o sul potere di prendere decisioni per conto della medesima, oppure sull'esercizio dei poteri di controllo nella stessa.

Le aziende, inoltre, saranno ritenute responsabili dei suddetti reati qualora uno dei soggetti innanzi citati, omettendo la sorveglianza o il controllo dovuti, abbia reso possibile la commissione, a beneficio dell'azienda, dei reati sopra menzionati da parte di persona soggetta alla sua autorità.

Le sanzioni applicabili alle società comprendono sanzioni pecuniarie, interdittive, la confisca, la pubblicazione della sentenza.

Per espressa disposizione di legge, la suddetta responsabilità sorge solo in seguito alla commissione (o al tentativo di commissione) di reati tassativamente previsti dal decreto legislativo 231/ 2001.

L'ente, tuttavia, può essere esonerato dalla predetta responsabilità qualora sia in grado di provare l'adozione e l'efficace attuazione di misure di organizzazione, gestione e controllo idonee a prevenire la commissione di illeciti della specie di quello verificatosi.

Ovviamente, la responsabilità delle persone giuridiche non escluderà il radicarsi dei procedimenti penali contro le persone fisiche resesi colpevoli quali autori, istigatori o complici di una di quelle condotte riconducibili alle fattispecie di reato in questione.

Tutto quanto sopra premesso significa che per evitare di pagare sanzioni che possono arrivare fino ad un milione e mezzo di euro, le imprese dovranno e devono rivedere i propri processi di gestione dei sistemi informatici per far si che i livelli di sicurezza dichiarati dalle *policy* aziendali corrispondano effettivamente a quelli in concreto utilizzati.

Bisognerà perciò che le aziende e le persone giuridiche tutte sappiano farvi fronte attivando *in primis* efficaci piani di sicurezza e sistematici monitoraggi delle reti e dei comportamenti in seno all'azienda.

Se è vero che gran parte dei procedimenti penali sono occasionati dalla detenzione in *server* aziendali di materiale di natura pedo-pornografica, è pur vero che sempre più frequenti sono però destinati a divenire processi per carenza di sorveglianza sui computer aziendali da cui siano scaturite condotte che abbiano leso, o anche solo minacciato di pregiudicare, l'integrità dei sistemi informatici di altre imprese o dei dati in essi riportati o transitati.

2. Destinatari e obiettivi delle disposizioni contenute nella Parte Speciale

Destinatari della presente Parte Speciale sono gli amministratori, il direttore generale - "soggetti apicali" - di Neos S.p.A., nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio.

In senso allargato, destinatari della presente Parte Speciale sono gli *stakeholder* intendendosi con tale termine, secondo quanto già riportato nel Codice Etico, tutti i soggetti rientranti nei singoli gruppi i cui interessi sono influenzati dagli effetti diretti e indiretti dell'attività di Neos S.p.A. - collaboratori (quindi amministratori, dirigenti e dipendenti della Società), azionisti, clienti, fornitori e *partners* d'affari - qui di seguito tutti denominati "destinatari".

Ciascuno dei sopra indicati soggetti, nella misura in cui agisce per conto della Società in occasione dello svolgimento della propria attività professionale, nell'ambito delle proprie funzioni e responsabilità, è impegnato ad osservare e a far osservare i contenuti del Codice Etico, del Documento Programmatico di Sicurezza e dunque anche della presente Parte Speciale.

Per quanto riguarda gli amministratori, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto".

Ai sensi dell'art. 2639 c.c., infatti, risponde dei reati societari previsti dal codice civile sia chi è tenuto a svolgere la medesima funzione diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o funzione.

Obiettivo della presente Parte Speciale è che tutti i destinatari come sopra individuati, nella misura in cui possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei delitti informatici, siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi

adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti all'art. 24 *bis* del decreto legislativo 231/ 2001.

Nello specifico, la presente Parte Speciale ha lo scopo di:

1_ indicare i comportamenti che i destinatari sono chiamati a osservare e quelli che sono tenuti a non seguire ai fini della corretta applicazione del Modello di Organizzazione e Gestione;

2_ fornire all'Organismo di Vigilanza, nonché ai responsabili delle funzioni aziendali che con lo stesso O.d.V. cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Al fine di evitare la commissione di uno di tali reati, è fatto espresso richiamo al rispetto della normativa aziendale e di Gruppo predisposta e adottata al fine di disciplinare l'utilizzo delle risorse e degli strumenti informatici:

- La normativa, le *policy* e le procedure aziendali per l'utilizzo dei sistemi informatici.

3. Aree sensibili e principi generali di comportamento

Come già ampiamente accennato e ricordato, i reati in questione previsti dall'art. 24 *bis*, così come le altre fattispecie contemplate nel Modello di Organizzazione e Gestione, presuppongono l'esistenza dell'interesse o vantaggio per la Società.

La responsabilità della Società, dunque, potrebbe essere rilevata in caso di attacco ad un sistema informatico posto in essere per arrecare vantaggio alla stessa (si pensi ad esempio alle ipotesi di spionaggio o sabotaggio industriale).

In specie, rispetto a tali reati e con riferimento alla Neos S.p.A., può essere considerata area a rischio quella riguardante i rapporti con autorità ed istituzioni pubbliche ovvero altri soggetti rappresentativi di interessi collettivi o con le persone fisiche che li rappresentano.

A tale proposito, sono previste due particolari fattispecie di reati, quali il *danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità* e il *danneggiamento di sistemi informatici o telematici di pubblica utilità.*

Ulteriore area a rischio riguarda i reciproci rapporti tra la Neos S.p.A. e la sua controllante – Alpitour S.p.A. -, nonché i reciproci rapporti tra Neos S.p.A. e le altre società facenti parte del gruppo Alpitour.

Con riferimento ai reati elencati all'art. 24 bis sono ipotizzabili delle oggettive difficoltà nella individuazione del reo, col conseguente rischio di potersi configurare una responsabilità della società proprietaria del computer, senza che l'autore sia individuato o individuabile.

Al fine di ovviare a tale inconveniente, risulta dunque opportuno, se non necessario, predisporre o rafforzare i sistemi e le procedure volte alla identificazione e all'accesso

dei soggetti operatori dei sistemi informatici, come più avanti riportato, nonché fornire ai destinatari una adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ad al rischio della commissione di reati informatici.

La presente Parte Speciale, conformemente a quanto previsto e richiesto nel Codice Etico, prevede, come principi di condotta generale, l'espresso divieto a carico dei destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato previste dall'art. 24 *bis* del decreto, così come precedentemente individuate ed enunciate;

- altresì, porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente divenirlo.

In particolare:

- limitare l'accesso attraverso risorse aziendali a reti e sistemi informatici esterni alla società compatibilmente con le esigenze lavorative;

- effettuare controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali quali ad esempio attività eccezionali dei server al di fuori degli orari di operatività;

- predisporre e mantenere adeguate difese a protezione dei server della Società e più in generale a protezione di ogni sistema informatico societario anche attraverso la predisposizione di un sistema di controllo degli accessi alle sale server prevedendo, ove possibile, controlli per prevenire l'ingresso e l'uscita di materiale non autorizzato

4. Regole specifiche di condotta

Conformemente a quanto previsto dal Codice Etico e dalle altre procedure aziendali, ai soggetti come sopra individuati è fatto obbligo di:

- porre in essere un comportamento corretto, trasparente nell'utilizzo di qualsiasi mezzo o sistema informatico;

- evitare di diffondere la propria *password* e il proprio codice di accesso;

- utilizzare sempre e solo la propria *password* e il proprio codice di accesso;

- altresì, segnalare, in qualunque momento, ogni violazione riguardante l'accesso ovvero l'utilizzo dei sistemi magnetici o informatici.

Tutto il personale e più in generale i destinatari sono tenuti, nell'utilizzo degli strumenti elettronici aziendali, all'uso dello specifico codice identificativo e della parola chiave assegnati.

Ciascuno deve rigorosamente utilizzare il proprio codice identificativo e la propria *password*; anche al fine di garantire una più agevole identificazione dell'operatore che utilizzando i sistemi informatici della Società abbia posto in essere una condotta integrante gli estremi di uno dei reati informatici contemplati nell'art. 24 *bis*.

Sia il codice identificativo che la parola chiave o *password* sono strumenti strettamente personali, il cui uso più o meno accorto è responsabilità del personale.

L'accesso ai sistemi e ai dati è definito dal Responsabile IT congiuntamente al Titolare del trattamento al fine di individuare le categorie omogenee di incaricati aventi le necessarie autorizzazioni a trattare particolari dati.

Rispetto ai soggetti destinatari in posizione apicale con compiti di vigilanza e controllo, vi è l'obbligo di valutare periodicamente l'efficacia ed efficienza dei sistemi informatici, dunque:

- attuare adeguate attività di monitoraggio;
- eventualmente, avviare le opportune operazioni e azioni correttive e preventive in funzione degli esiti;
- apporre - nel caso rafforzare - gli opportuni mezzi di sicurezza dei sistemi informatici.

Al fine di dare attuazione alle norme comportamentali sopra elencate, è necessario attuare i seguenti principi procedurali specifici:

- informare adeguatamente gli utilizzatori di sistemi informatici dell'impotenza di mantenere i propri codici di accesso – *username* e *password* – confidenziali e di non divulgare gli stessi a soggetti terzi;
- diffondere agli utilizzatori di sistemi informatici uno specifico documento con il quale gli stessi si impegnano al corretto utilizzo delle risorse informatiche e aziendali;
- informare gli utilizzatori dei sistemi informatici della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro;
- impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- l'accesso da e verso l'esterno - connessione alla rete Internet - deve essere autorizzato e deve essere effettuato solo con le modalità consentite ad ai fini di utilizzo per scopi lavorativi;
- dotare la stanza *server* di porta con un controllo di accesso fisico consentito solo a personale autorizzato;
- proteggere ogni sistema informatico societario, al fine di prevenire l'illecita

installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero capace di impedirle o interromperle;

- fornire ogni sistema informatico di adeguato *software firewall* e antivirus e fare in modo che, ove possibile questi non possano essere disattivati;

- vietare l'installazione e l'utilizzo di *software* – programmi – non approvati dalla Società e non correlati all'attività professionale espletata da parte dei destinatari o degli utilizzatori;

- limitare l'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti – virus – capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti, quali ad esempio siti di posta elettronica o *files*;

- vietare, in particolare, l'installazione e l'utilizzo sui sistemi informatici della Società di *software* mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di *files* senza alcun tipo di controllo da parte della Società;

- qualora per la connessione alla rete si utilizzino collegamenti *wireless* - ossia senza fili, mediante *routers* - sarà importante proteggere gli stessi impostando una chiave d'accesso per impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai dipendenti della Società;

- prevedere, ove possibile, un procedimento di autenticazione mediante *username* e *password* al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di destinatari.

I delitti di criminalità informatica estendono la responsabilità delle persone giuridiche ai reati di falso; in particolare, tutti i dipendenti ed Organi Sociali, nonché Consulenti e *Partners*, rispettando principi tali da evitare le possibilità che siano commessi i reati di falso in generale attraverso modalità informatiche.

E' pertanto assolutamente vietata la trasmissione di qualsiasi atto non veritiero, contraffatto o non autentico attraverso un invio telematico.

Si richiede, in particolare, un rafforzamento nonché controllo periodico dei mezzi di sicurezza informatici, quali i *firewall*, *password*, dei sistemi di accesso al sistema operativo locale e alla rete;

Si richiedono, inoltre, protezioni per l'accesso e l'utilizzo rispetto alla *console* dei *server*, che necessariamente devono essere permessi ai soli incaricati alla gestione e manutenzione degli strumenti elettronici.

Con specifico riferimento ai controlli dell'Organismo di Vigilanza, si contempla la opportunità/necessità di effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificarne la corretta esplicazione.

L'Organismo di Vigilanza può anche intervenire a seguito di eventuali segnalazioni ricevute.