**Allegato 4**

**PARTE SPECIALE**

**REATI INFORMATICI**

**Rev. 1.0 del XX/XX/XXXX**

## 1. Tipologia di reati

La legge 18 marzo 2008, n. 48 - di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica - ha introdotto nel D. Lgs. 231/2001 il nuovo art. 24-bis recante disposizioni in tema di responsabilità dell'ente in relazione a "Delitti informatici e trattamento illecito di dati" (in vigore dal 5.04.2008).

Anche i crimini informatici, dunque, vengono inseriti tra i reati rilevanti ai fini 231 ampliando ulteriormente la responsabilità amministrativa dell'ente.

Le nuove fattispecie criminose introdotte nel D. Lgs. 231/2001 ed elencate all'art. 24-bis, mediante specifico rimando al codice penale, sono:

I) **FALSITA' IN UN DOCUMENTO INFORMATICO PUBBLICO O PRIVATO AVENTE EFFICACIA PROBATORIA** (art. 491-bis c.p.).
La norma punisce la falsificazione dei documenti informatici attraverso le disposizioni penali sino ad oggi riguardanti esclusivamente la falsificazione dei documenti cartacei.
Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

II) **ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO** (art. 615-ter c.p.)

Chiunque si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantenga contro la volontà di chi ha il diritto di escluderlo. La norma tutela il "domicilio informatico" dell'utente (persona fisica, giuridica, privata o pubblica, o altro ente) qualunque sia il contenuto dei dati racchiusi in esso. La duplicazione di dati acquisiti con accesso abusivo ad un sistema informatico integra la condotta tipica di cui alla norma in oggetto.

III) **DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI 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 o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni idonee a tale scopo.

IV) **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 in esso contenute ovvero di favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, diffonde comunica o comunque mette a disposizione di altri apparecchiature o programmi informatici.

V) **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.

VI) **INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE** (art. 617-quinquies c.p.)

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

VII) **DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI** (art. 635-bis c.p.)

Chiunque distrugge, deteriora, cancella altera o sopprime informazioni, dati o programmi informatici altrui.

VIII) **DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITA'** (art. 635-ter c.p.)

Chiunque commette un fatto diretto a distruggere, deteriorare, cancellare alterare o soprrimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità.

IX) **DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI** (art. 635-quater c.p.)

Chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

X) **DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITA'** (art. 635-quinquies c.p.)
Se il fatto di cui all'art. 635-quater è diretto a distruggere, danneggiare o rendere inservibili sistemi informatici o telematici di pubblica utilità.

XI) **FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA** (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.
Per ognuna di tali fattispecie la norma prevede, a carico dell'ente, una sanzione pecuniaria ed una interdittiva.

## 2. Processi sensibili

I nuovi reati informatici investono il processo di gestione dei sistemi informativi nella sua interezza: ai fini del Modello, dunque, sono da considerarsi potenzialmente a rischio tutte le attività supportate da sistemi informatici e telematici per l'elaborazione e la trasmissione di dati contabili, fiscali e gestionali.

Le principali attività del processo fanno riferimento a:

- la definizione della funzione responsabile dei sistemi informativi;
- la protezione fisica dei dati;
- l'uso dei sistemi informativi;
- i controlli specifici.

## 3. Organizzazione aziendale

In ragione dei rilievi effettuati, mediante specifici questionari sottoposti ai soggetti coinvolti nella funzione aziendale a rischio quanto ai nuovi reati informatici introdotti nel D. Lgs. 231/2001, il grado di adeguatezza del sistema informatico aziendale appare soddisfaciente.

Infatti lo sviluppo raggiunto dalla S.p.A. NAVICELLI di Pisa riscontrato nell'analisi della Disposizione Organizzativa concernente la GESTIONE DEI SISTEMI INFORMATIVI, appare sufficientemente organizzato ed adeguato e tale da garantire una separazione delle funzioni e dunque delle responsabilità in materia.

- In particolare, riferiscono al responsabile …….. della GESTIONE DEI SISTEMI INFORMATIVI:

Garantisce la manutenzione correttiva e migliorativa degli applicativi in esercizio; definisce il piano di lavoro di dettaglio relativamente alle nuove iniziative (tempi, costi e risorse);

realizza i progetti di manutenzione evolutiva e di nuovi sviluppi, nonché monitora eventuali scostamenti e/o variazioni rispetto alle esigenze definite e pianificate.

- GESTIONE, ANALISI ED ELABORAZIONE DATA BASE:

Assicura la corretta analisi e gestione dei dati al fine di normalizzare gli archivi dei data base gestiti; fornisce le estrazioni dei dati dagli archivi aziendali richieste dai Clienti interni; definisce e condivide con i clienti livelli di servizio, ne monitora il rispetto e provvede alla consuntivazione e comunicazione degli indicatori di performance ai fruitori dei servizi.

- GESTIONE DELLA SICUREZZA INFORMATICA:

Garantisce la sicurezza del sistema informativo della Società; definisce e controlla l'applicazione delle misure preventive per evitare danni o guasti ai sistemi informativi causati da "intrusioni"; definisce e controlla lo svolgimento delle attività necessarie al ripristino dei Sistemi qualora interventi esterni ne abbiano alterato il corretto funzionamento.

Sinteticamente si riportano i passaggi principali delle interviste effettuate ai responsabili delle unità operative (che verranno conservate presso gli archivi dell'OdV):

- Quanto all'uso dei sistemi informativi, invece, la Società non dispone di specifici protocolli per l'accesso e l'uso degli stessi;
- Ogni cliente utilizzatore del sistema informatico ha una propria password di accesso e ciascun *pc* è protetto da antivirus. La protezione e l'aggiornamento del sistema sono affidati a consulenti esterni alla Società;
- L'aggiornamento del sistema informativo non ha frequenza prestabilita (anche automatico);
- Quanto alla protezione dei dati, la Società dispone di sistema di protezione del locale adibito a server aziendale.

## 4. Prescrizioni generali di comportamento

Fotografato lo stato della società, scopo del presente documento (di adeguamento) è la creazione, all'interno del processo di gestione del sistema informativo aziendale, di un apparato di controlli - per l'adeguamento della struttura organizzativa ai fini del D. Lgs. 231/2001 - atto a scongiurare gli specifici rischi connessi ai reati di criminalità informatica.

Tale sistema di controlli persegue l'obiettivo di ridurre il rischio che le procedure per la salvaguardia, l'accesso, l'elaborazione e l'utilizzo di programmi software, siano manomesse, consentendo altresì la corretta gestione dei dati elaborati.

Ulteriore obiettivo è quello di ridurre il rischio che le attrezzature hardware e software dell'organizzazione aziendale siano utilizzate in modo illegittimo al fine di commettere reati di criminalità informatica.

Coerentemente con la logica ispiratrice del Modello, ciascuna delle attività dei singoli processi aziendali deve prevedere un sistema di autorizzazioni, deleghe e separazione dei compiti.

Nel caso specifico, dunque la Società dovrà porre particolare attenzione affinchè, nelle procedure riguardanti il processo di gestione dei sistemi informativi e tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e affinchè tali responsabilità risultino altresì coerenti con il quadro dei controlli specifici ai fini 231.

## 5. Prescrizioni procedurali specifiche

### a) PROTEZIONE FISICA DEI DATI

E’ necessario garantire la salvaguardia delle attrezzature hardware e dei programmi software mediante:

- installazione e gestione di sistemi di allarme, antifurto, antincendio o simili;
- installazione e gestione di apparecchiature di continuità dell’energia elettrica;
- installazione e gestione di package antivirus, costantemente aggiornati;
- controllo degli accessi ai locali del Centro Elaborazione dati;
- inventario periodico delle attrezzature hardware, dei programmi software e delle licenze d’uso.

**b) USO DEI SISTEMI INFORMATIVI**

E’ necessario che la Società risulti sempre conforme alle seguenti prescrizioni specifiche:

- possesso di password di accesso, per profilo aziendale e per dipendente, personalizzate in funzione dei ruoli e dei compiti attribuiti al personale utilizzatore del sistema informatico;
- conservazione delle password di accesso in luoghi protetti e gestione delle stesse affidata alla sola funzione responsabile del sistema per l’attribuzione e la modifica periodica;
- periodici salvataggi di back-up dei dati;
- conservazione dei programmi applicativi e dei supporti di back-up in luoghi idonei alla loro salvaguardia;
- controllo degli accessi ad internet e alla trasmissione dei dati a soggetti esterni all’Azienda.

**c) CONTROLLI SPECIFICI**

E’ opportuno che la funzione responsabile dei sistemi informativi effettui verifiche sull’efficienza del sistema, preferibilmente mediante soggetti esterni alla Socità, attraverso interventi periodici di manutenzione e simulazioni di alterazioni di funzionamento (in tale senso la Società si serve di soggetti esterni – per assistenza sistemistica hardware reti e back-up - ed Engeneering – per sviluppo e personalizzazione utenti e programmi di fatturazione, magazzino, ordini e contabilità).

In particolare, è necessario che la Società risulti sempre conforme alle seguenti prescrizioni specifiche di controllo:

- possibilità di accesso ai programmi e alle reti esterne senza l’uso delle password;
- possibilità di alterazione di documenti già stampati, in particolare modifiche a fatture, dati di apertura di bilancio, registrazioni effettuate in esercizi precedenti;
- possibilità di cracking delle password;

In ultimo appare fondamentale l’evidenziazione di eventuali usi illegittimi dell’hardware e/o del software da parte del soggetto che ne cura la manutenzione.

**d) OBBLIGHI DI INFORMAZIONE**

La funzione preposta deve informare l’Organismo di Vigilanza periodicamente, e comunque con frequenza almeno semestrale, attraverso uno specifico report, sugli aspetti significativi afferenti le attività di propria competenza, in particolare per quanto attiene a:

- le attività di salvaguardia delle attrezzature hardware e dei programmi software;

- i controlli e le verifiche periodiche sull'efficienza del sistema;
- le evidenze su eventuali usi illegittimi da parte del personale delle attrezzature software e hardware ricevute in dotazione.

Nel caso in cui di dette attività si occupino soggetti esterni alla Società, quest'ultima deve provvedere a che detti soggetti informino la funzione preposta delle evenienze su riportate.

La funzione preposta (o chi per essa, se soggetto esterno), dunque, ha l'obbligo di comunicare (immediatamente) all'Organismo di Vigilanza ogni deroga alle procedure inerenti il processo, decisa in caso di emergenza o di impossibilità temporanea di attuazione - indicandone la motivazione – nonché ogni anomalia significativa riscontrata.