GRUPPO FINMATICA

Modello di Organizzazione e di Gestione ex decreto legislativo 8 giugno 2001 n. 231

PARTE SPECIFICA “B”

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

FINMATICA

FINMATICA S.p.A. - Via della Liberazione 15 - 40128 Bologna
Tel +39 (0)51 6307411 Fax +39 (0)51 6307498 web www.finmatica.it e-mail marketing@ads.it
Capitale sociale € 1.032.000 - N. iscrizione registro imprese, C.F. e P.I. 03549220378 - C.C.I.A.A. 299006

Modello di Organizzazione e di Gestione
ex decreto legislativo 8 giugno 2001 n.231
PARTE SPECIFICA "B"
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Natura del documento: Edizione definitiva

Approvazione: Consiglio d'Amministrazione

Data Approvazione: 28/02/2017

Tabella Edizioni e revisioni

Edizione	Revisione	Data Revisione	Motivazione	Data approvazione Consiglio d'Amministrazione
1	0	31/01/2017	Prima emissione	28/02/2017

Indice

B.1 LE TIPOLOGIE DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS DEL DECRETO)

L'articolo 24-bis del D. Lgs. n. 231 del 2001 individua un gruppo di delitti informatici e trattamento illecito di dati che possono essere commessi nell'ambito delle attività aziendali (di seguito "Delitti informatici").

B.1.1 Articolo 24-bis D.Lgs. 231/2001

L'articolo 24-bis del D. Lgs. n. 231 del 2001, rubricato "Delitti informatici e trattamento illecito di dati", così recita:

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

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

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

4. Nei caso di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

Si tratta dei seguenti reati previsti dal codice penale:

- Art. 491-bis - Documenti informatici
- Art. 615-ter - Accesso abusivo ad un sistema informatico o telematico
- Art. 615-quater - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Art. 615-quinquies - Diffusione di apparecchiature ,dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Art. 617-quater - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Art. 617-quinquies - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- Art. 635-bis – Danneggiamento di informazioni, dati e programmi informatici
- Art. 635-ter - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica
- Art. 635-quater - Danneggiamento di sistemi informatici o telematici
- Art. 635-quinquies - Danneggiamento di sistemi informatici o telematici di pubblica utilità
- Art. 640-quinquies– Frode informatica del certificatore di firma elettronica

B.1.2 Delitti informatici e trattamento illecito di dati richiamati dall'art. 24-bis del D.Lgs. 231/2001

Si descrivono di seguito le ipotesi di reato previste dall'art. 24-bis del D.Lgs. n. 231/01 (di seguito "Delitti informatici"), che vengono qui raccolte, ai fini della presente analisi.

Art. 491-bis c.p. – Documenti informatici

Questo fattispecie di reato estende la penale perseguibilità dei reati previsti all'interno del Libro II, Titolo VII, Capo III del Codice Penale, ovvero le ipotesi di falsità, materiale o ideologica, commesse su atti pubblici, certificati, autorizzazioni, scritture private o atti privati, da parte di un rappresentante della Pubblica Amministrazione ovvero da un privato, qualora le stesse abbiano ad oggetto un "documento informatico avente efficacia probatoria", ossia un documento informatico munito quanto meno di firma elettronica semplice.

Per "documento informatico" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art.1, c.1, lett.p, L.82/2005).

Art. 615-ter c.p. – Accesso abusivo ad un sistema informatico o telematico

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

Art. 615-quater c.p. 2623 – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Il delitto in esame sanziona la condotta di chi 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 in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

Art. 615-quinquies c.p. – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Tale fattispecie di reato sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione 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.

Art. 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Tale norma punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

Art. 617-quinquies c.p. – Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche

La fattispecie in esame sanziona la condotta 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 fra più sistemi.

Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici

Tale fattispecie punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

Art. 635-ter c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità

Tale norma sanziona la condotta di chi 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, salvo che il fatto costituisca più grave reato.

Art. 635-quater c.p. – Danneggiamento di sistemi informatici o telematici

La fattispecie in esame punisce la condotta di chi, 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, salvo che il fatto costituisca più grave reato.

Art. 635-quinquies c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità

La norma in oggetto incrimina la condotta descritta al precedente articolo 635-quater, qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Art. 640-quinquies c.p. – Frode informatica del certificatore di firma

Tale norma punisce il soggetto che presta servizi di certificazione di firma elettronica qualora questi, 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.

B.2 AREE A RISCHIO

In relazione ai reati ed alle condotte criminose sopra esplicitate e in base all'attività di analisi dei rischi svolta, le aree ritenute maggiormente a rischio risultano essere per FINMATICA, ai fini della presente Parte Specifica del Modello, le seguenti:

1) Gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT
2) Gestione della sicurezza fisica dei sistemi informativi e telematici della società
3) Gestione della sicurezza logica (accessi a sistemi informativi o telematici e reti di dati)
4) Gestione e trattamento di dati personali
5) Tutte le attività aziendali svolte dai destinatari tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso ad internet
6) Gestione dei flussi informativi elettronici con la pubblica amministrazione
7) Gestione di reti di telecomunicazione
8) Gestione della sicurezza fisica delle sedi aziendali.

Per un'individuazione analitica di aree, processi e attività risultanti più a rischio per la Società si rinvia alla Mappatura delle Aree a Rischio Delitti informatici e trattamento illecito di dati, allegata alla presente Parte Specifica.

Eventuali integrazioni delle suddette aree a rischio potranno – su proposta dell'Organismo di Vigilanza - essere disposte dal Presidente del Consiglio di Amministrazione, al quale viene dato mandato di individuare le

relative ipotesi e di definire gli opportuni provvedimenti operativi.

B.3 DESTINATARI E OBIETTIVO DELLA PARTE SPECIFICA

La presente Parte Specifica si riferisce a comportamenti posti in essere da Amministratori, Sindaci, Liquidatori, Dirigenti e Dipendenti ("Esponenti Aziendali") della Società, nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito tutti definiti i "Destinatari").

Obiettivo della presente Parte Specifica è che tutti i Destinatari, come sopra individuati, si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento di attività nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di FINMATICA – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti informatici e trattamento illecito di dati.

In particolare, la presente Parte Specifica ha la funzione di fornire:

a) un elenco dei principi generali e dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

b) all'Organismo di Vigilanza (d'ora in poi anche "ODV"), e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

B.4 PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO

In relazione alle rispettive funzioni, oltre alle regole di cui al presente Modello, gli Esponenti Aziendali devono in generale conoscere e rispettare tutte le regole, procedure e principi contenuti nei seguenti documenti:

- il Codice Etico;
- lo Statuto Sociale;
- il Regolamento interno per l'utilizzo del sistema informatico e telecomunicazioni;
- il Sistema di autoregolamentazione inerente la corporate governance, la struttura organizzativa, la gestione amministrativa, contabile e finanziaria, il sistema di controllo interno della Società (Regolamenti, manuali, procedure aziendali, istruzioni operative e ogni altra disposizione);
- ogni altra documentazione relativa al sistema di controllo interno in essere nella Società;
- le norme inerenti il sistema informativo e il trattamento dei dati diffuse dalla Società;
- la normativa applicabile.

L'insieme organico di tali documenti - che determina, per le diverse aree di intervento, le regole a cui gli Esponenti Aziendali nonché i soggetti esterni, in funzione del rapporto che li lega a FINMATICA devono conformarsi – deve regolamentare rispettivamente:

- il governo della sicurezza delle informazioni (relativo ad esempio, alla determinazione dei Piani di Sicurezza dei sistemi informativi, alla segnalazione e risposta agli incidenti di sicurezza delle informazioni, alla formazione e sensibilizzazione per la sicurezza delle informazioni, etc.);
- i controlli di sicurezza specifici per tipologia di asset informativo (relativi ad esempio alla selezione di contromisure per piattaforme e sistemi, applicazione, database, etc.);

- i controlli di sicurezza indipendenti dalla tipologia di asset, volti ad indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali (ad esempio in relazione all'uso accettabile delle risorse informative, alla gestione dei diritti di accesso alle risorse, alla tracciabilità degli eventi, etc.).

La presente Parte prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, e a carico dei Collaboratori esterni, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la Società - di:

- porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino - direttamente o indirettamente - le fattispecie di reato sopra considerate dall'art. 24-bis del Decreto (anche solo nella forma del tentativo);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- violare le prescrizioni della presente Parte Specifica;
- porre in essere comportamenti non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

In particolare, nell'espletamento delle rispettive attività, oltre alle previsioni di legge esistenti in materia, i principi generali e i criteri di condotta disposti dal Codice Etico e alle prescrizioni contenute nella Parte Generale del presente Modello, i Destinatari sono tenuti ad attenersi ai seguenti principi generali di condotta:

a) tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività che comportano l'utilizzo di apparecchiature informatiche e telematiche;

b) osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità delle informazioni contenute nei sistemi informatici e non danneggiare e/o distruggere i dati in essi contenuti;

c) rispettare le regole in materia di trattamento dei dati personali in attuazione del D.Lgs. 196/03 (c.d. Legge Privacy)

d) selezionare con particolare attenzione e in base ad apposita procedura, le controparti destinate a fornire servizi di IT (Information Technology), valutandone l'affidabilità ex ante.

Ai Destinatari che intrattengono rapporti negoziali per conto di FINMATICA con soggetti terzi deve essere formalmente conferita una delega in tal senso (con apposita procura scritta, qualora debbano essere compiuti atti idonei ad impegnare la Società).

Accanto al rispetto dei principi generali di condotta, dei principi procedurali specifici di cui al successivo paragrafo B.5, tutti i Destinatari sono tenuti al rispetto dei principi di comportamento contenuti nei documenti organizzativi al fine di prevenire la commissione dei Reati di cui all'art. 24 bis del Decreto.

Infine, per ciò che concerne i rapporti con Partner, Fornitori e con eventuali altre Controparti coinvolte in attività a rischio, anch'essi Destinatari della presente Parte Specifica, ai medesimi deve essere resa nota l'adozione del Modello e del Codice etico da parte di FINMATICA, la cui conoscenza e il cui rispetto costituirà obbligo contrattuale a loro carico.

B.5 AREE DI ATTIVITA' A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE

B.5.1 Responsabile interno

Per tutte le operazioni a rischio che concernono le attività sensibili individuate nel paragrafo B.2 di questa Parte Specifica, i protocolli di prevenzione individuano un Responsabile Interno per l'attuazione

dell'operazione, che corrisponde, salvo diversa indicazione da parte del Presidente della Società o di un dirigente da questi incaricato, al responsabile della funzione competente per la gestione dell'operazione a rischio considerata.

Il Responsabile Interno:

- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che si occupano o si sono occupati dell'operazione a rischio;
- informa tempestivamente l'ODV di qualunque criticità sorta durante lo svolgimento dell'operazione a rischio;
- può interpellare l'Organismo di Vigilanza in tutti i casi di inefficacia, inadeguatezza o difficoltà di attuazione dei protocolli di prevenzione o delle procedure operative di attuazione degli stessi o al fine di ottenere chiarimenti in merito agli obiettivi e alle modalità di prevenzione previste dal Modello.

B.5.2 Principi procedurali specifici

Si indicano qui di seguito i principi procedurali specifici che - in relazione ad ogni singola Area a Rischio (come individuate nel paragrafo B.2) - i Destinatari sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte dell'Organismo di Vigilanza.

Ai fini dell'attuazione dei principi generali indicati al paragrafo precedente, oltre che delle prescrizioni della Parte Generale del presente Modello, nell'adottare procedure relative alle attività sensibili dovranno essere osservati anche i principi di riferimento di seguito indicati.

Costituiscono parte integrante del Modello le procedure aziendali che danno attuazione ai principi e alle misure di prevenzione indicate nel Codice Etico e nel Modello per prevenire i Delitti informatici e trattamento illecito di dati.

Le procedure devono essere monitorate e mantenute aggiornate.

Per la prevenzione delle fattispecie di reato, anche tentato, rientranti tra quelle richiamate dall'art. 24-bis del Decreto i Destinatari (cioè, Esponenti Aziendali nonché altri Soggetti esterni eventualmente autorizzati) sono tenuti a rispettare le seguenti prescrizioni.

In particolare, è vietato:

- connettere ai sistemi informatici di FINMATICA, personal computer, periferiche, altre apparecchiature o installare e/o utilizzare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
- modificare in qualunque modo la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate da FINMATICA;
- divulgare, cedere o condividere con personale interno o esterno a FINMATICA le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

- accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- comunicare a persone non autorizzate, interne o esterne a FINMATICA, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- lo spamming come pure ogni azione di risposta al medesimo;
- inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi.

FINMATICA si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1) informare adeguatamente i Dipendenti e tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, dell'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
2) prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
3) far sottoscrivere ai Dipendenti, nonché a tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;
4) informare i Dipendenti, nonché tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
5) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzate per un determinato periodo di tempo, si blocchino automaticamente;
6) limitare gli accessi alle stanze server unicamente al personale autorizzato;
7) proteggere, per quanto possibile, 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;
8) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
9) impedire l'installazione e l'utilizzo di software non approvati da FINMATICA e non correlati con l'attività professionale espletata per la stessa;

10) limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;
11) impedire l'installazione e l'utilizzo, sui sistemi informatici di FINMATICA, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, etc.) senza alcuna possibilità di controllo da parte di FINMATICA;
12) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a FINMATICA, possano illecitamente collegarsi alla rete Internet tramite i router della stessa e compiere illeciti ascrivibili ai Dipendenti;
13) prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti e di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
14) limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti e di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
15) provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale.

Per ciò che specificamente attiene i controlli aziendali, FINMATICA attribuisce alla Funzione Sistemi Informativi i seguenti compiti:

- monitorare centralmente in tempo reale, in collaborazione con le Direzioni/Funzioni interessate, lo stato della sicurezza operativa delle varie piattaforme ICT (sistemi e reti) di processo e gestionali, attraverso strumenti diagnostici e coordinare le relative azioni di gestione;
- monitorare centralmente in tempo reale i sistemi anti-intrusione e di controllo degli accessi ai siti aziendali e gestire le autorizzazioni;
- gestire il processo di identificazione ed autorizzazione all'accesso alle risorse ICT aziendali;
- gestire i processi/procedure di escalation interne ed esterne in occasione di situazioni di emergenza e/o crisi, con il supporto delle Direzioni/Funzioni responsabili interessate;
- svolgere analisi degli incidenti avvenuti;
- svolgere analisi di vulnerabilità;
- produrre report a supporto del vertice aziendale.

B.5.3 Contratti

Nei contratti e nelle lettere di incarico con Partner, Fornitori e eventuali altre Controparti coinvolte nelle attività a rischio deve essere contenuta apposita clausola che regoli le conseguenze della violazione, da parte delle controparti stesse, delle norme di cui al Decreto nonché di quanto disposto dal Modello e dal Codice Etico adottati dalla Società.

B.6 ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i Delitti informatici, di cui all'art. 24-bis del Decreto, sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Specifica e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 24-bis del Decreto. Con riferimento a tale punto l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Specifica e proporrà ai soggetti competenti della Società eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme in materia e/o delle disposizioni della presente Parte Specifica, ovvero in occasione di mutamenti nell'organizzazione e nell'attività, anche in relazione al progresso scientifico e tecnologico;
- proporre e collaborare alla predisposizione e all'aggiornamento delle istruzioni standardizzate (scritte e conservate su supporto cartaceo o informatico) relative a:
    - comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente Parte Specifica;
    - flussi informativi a favore dell'ODV;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- verificare periodicamente il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli Esponenti Aziendali.

Allo scopo di svolgere le proprie funzioni, l'Organismo di Vigilanza può:

a) partecipare agli incontri organizzati dalla Società tra le funzioni aziendali competenti, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

b) accedere a tutta la documentazione e a tutte le sedi aziendali rilevanti per lo svolgimento dei propri compiti.

La Società istituisce a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per esercitare le sue attività di monitoraggio e di verifica dell'efficace esecuzione delle procedure, dei regolamenti e dei controlli previsti dal Modello e, in particolare, dalla presente Parte Specifica.

In particolare, l'informativa all'ODV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nel paragrafo B.5 della presente Parte Specifica ovvero alle procedure, policy e normative aziendali attinenti alle aree sensibili sopra individuate.

In ogni caso, indipendentemente dalla presenza o meno di criticità, dovrà essere data un'informativa periodica all'ODV da parte dei responsabili di funzione.

Le modalità di informativa all'ODV sono oggetto di specifica procedura aziendale.

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nella presente Parte Specifica deve essere conservata da ciascun Destinatario coinvolto nel processo per le attività di propria competenza e messa a disposizione dell'Organismo di Vigilanza.

I Destinatari sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

B.7 ALLEGATI

Mappatura delle Aree a Rischio Delitti informatici e trattamento illecito di dati

Elenco Procedure