

ALLEGATO 3

MODELLO DI ORGANIZZAZIONE E GESTIONE *ai sensi del D.Lgs. n. 231/2001*

PARTE SPECIALE 3 *Reati informatici*

PARTE SPECIALE 3 – I **REATI INFORMATICI**

A. TIPOLOGIA DI REATI

La presente parte speciale si riferisce ai reati informatici elencati all'art. 24-bis del D. Lgs. n.231/2001, limitatamente ai casi che potrebbero configurarsi in capo a TRC S.p.A..

Obiettivo della presente parte speciale è garantire che i soggetti coinvolti nelle aree sensibili mantengano condotte conformi ai principi di riferimento di seguito enunciati, ciò al fine di prevenire la commissione dei reati oggetto della sezione.

Il D.Lgs. 231/01 ha recepito con la Legge n. 48, art. 7, del 18 marzo 2008, pubblicata in G.U. n. 80 del 4 aprile 2008, la **Convenzione del Consiglio d'Europa sulla criminalità informatica**, redatta a Budapest il 23 novembre 2001.

A seguito della ratifica ed esecuzione della Convenzione suddetta è stata inserita nel D.Lgs. n.231/01 e rubricata all'art. 24bis la disposizione in tema di *“Delitti informatici e trattamento illecito di dati”*.

Il recepimento della convenzione ha esteso la responsabilità amministrativa degli enti ai seguenti reati informatici:

- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);

con previsione di sanzione pecuniaria da cento a cinquecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere a), b) ed e).

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);

con previsione di sanzione pecuniaria sino a trecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere b) ed e).

- falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491bis c.p.);
- frode informatica del certificatore di firma elettronica (art. 640quinquies c.p.);

con previsione di sanzione pecuniaria sino a quattrocento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere c), d) ed e).

In considerazione della tipologia di attività svolta da TRC è astrattamente ipotizzabile la commissione dei seguenti reati:

Art. 24 bis, comma 1, D.Lgs. n. 231/2001

- *Art. 615 ter del Codice Penale - Accesso abusivo ad un sistema informatico o telematico*

Fattispecie

Chiunque abusivamente si introduce 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, è punito con la reclusione fino a tre anni. La pena è rappresentata dalla reclusione da uno a cinque anni:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

La norma non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*ius excludendi alios*", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli

aspetti economico-patrimoniali dei dati sia che titolare dello "*ius excludendi*" sia persona fisica, sia giuridica, privata o pubblica, o altro ente.

Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi un'effettiva lesione alla stessa.

L'art. 1 della Convenzione di Budapest chiarisce che per "sistema informatico" si considera "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico", che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".

- *Art.617 quater del Codice Penale – Intercettazione, impedimento o interruzione illecita di comunicazione informatiche o telematiche*

Fattispecie

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è rappresentata dalla reclusione da uno a cinque anni se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- 3) da chi esercita anche abusivamente la professione di investigatore privato.

- *Art. 617 quinquies del Codice Penale – installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*

Fattispecie

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è rappresentata dalla reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617 quater c.p..

- *Art.635 bis del Codice Penale – danneggiamento di informazioni, dati e programmi informatici*

Fattispecie

Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Antecedentemente all'entrata in vigore della *legge 23 dicembre 1993 n. 547* (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi *dell'art. 635 c.p.* in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore.

(Nell'affermare detto principio, giurisprudenza ha precisato che tra il delitto di cui *all'art. 635 c.p.* e l'analoga speciale fattispecie criminosa prevista dall'*art. 9 della legge n. 547 del 1993* - che ha introdotto *l'art. 635-bis c.p.* sul danneggiamento di sistemi informatici e telematici - esiste un rapporto di successione di leggi nel tempo, disciplinato *dall'art. 2 c.p.*).

- *Art.635 ter del Codice Penale – danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*

Fattispecie

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati

dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, la pena è rappresentata dalla reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 c.p., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

➤ *Art.635 quater del Codice Penale – danneggiamento di sistemi informatici o telematici*

Fattispecie

Salvo che il fatto non costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni programmi, rende, il tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre una o più delle circostanze di cui al secondo comma dell'art. 635 c.p., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è la reclusione da due a sette anni.

➤ *Art. 635 quinquies del Codice Penale – danneggiamento di sistemi informatici o telematici di pubblica utilità*

Fattispecie

Se il fatto di cui all'art. 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolare gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 c.p. ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Gli articoli del Codice Penale summenzionati, previsti nel comma 1 dell'art. 24 bis D.Lgs. 231/2001, hanno quale fattore comune il "danneggiamento informatico": si parla di danneggiamento informatico quando, considerando la componente hardware e software, interviene una modifica tale da impedirne il funzionamento, anche solo parziale.

Art. 24 bis, comma 2, D.Lgs. 231/2001

- *Art. 615 quater del Codice Penale – detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*

Fattispecie

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

- *Art.615 quinquies del Codice Penale – diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*

Fattispecie

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329.

Gli articoli del Codice Penale summenzionati, previsti nel comma 2 dell'art. 24 bis D.Lgs. 231/2001, hanno quale fattore comune la detenzione o diffusione di codici o programmi atti al danneggiamento informatico.

Da un punto di vista tecnico, gli artt. 615 quater e 615 quinquies c.p. possono essere considerati accessori ai precedenti artt. 615 ter, 635 bis, 635 ter e 635 quater, c.p.: la detenzione o dissezione di codici di accesso o la detenzione o diffusione di programmi o dispositivi diretti a danneggiare o interrompere un sistema telematico, di per sé non compiono alcun danneggiamento, se non utilizzati per un accesso abusivo ad un sistema o nella gestione di un'intercettazione di informazioni.

Art. 24 bis, comma 3, D.Lgs. 231/2001

- *Art. 491 bis del Codice Penale – falsità in un documento informatico pubblico o avente efficacia probatoria*

Fattispecie

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 si ribadisce che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli. Il reato si configura nella falsità concernente direttamente i dati o le informazioni dotati, già di per sé, di efficacia probatoria relativa a programmi specificatamente destinati ad elaborarli indipendentemente da un riscontro cartaceo.

Si chiarisce inoltre nella norma che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Documenti informatici (art. 491-bis cod. penale).

“Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private”.

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.):

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni”;

- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.):

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni”;

- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.):

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.

Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni”;

- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.):

“Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476”; - Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.): *“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni”;*

- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.):

“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro”;

- Falsità materiale commessa da privato (art. 482 c.p.):

“Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo”;

- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):

“Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi”;

- Falsità in registri e notificazioni (art. 484 c.p.):

“Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali,

commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00”;

- Falsità in scrittura privata (art. 485 c.p.):

“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata”;

- Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.):

“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito”;

- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):

“Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480”;

- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.):

“Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private”;

- Uso di atto falso (art. 489 c.p.):

“Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno”;

- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.):

“Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente”;

- Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.):

“Agli effetti delle disposizioni precedenti, nella denominazione di “atti pubblici” e di “scritture private” sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti”;

- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art.493 c.p.):

“Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni”.

- *Art. 640 quinquies del Codice Penale – frode informatica del certificatore di firma elettronica*

Fattispecie

Il certificatore che, violando gli obblighi previsti dall'art. 32 del codice dell'amministrazione digitale, di cui al D. Lgs. 82/2005 e successive modifiche , per il rilascio di un certificato, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione fino a tre anni o con la multa fino a 25.000 Euro.

Gli articoli del Codice Penale summenzionati, previsti nel comma 3 dell'art. 24 bis D.Lgs.231/2001, disciplinano illeciti che, a differenza di quelli sopradescritti (veri e propri reati informatici), sono compiuti attraverso l'uso di un sistema informatico.

B. DESTINATARI

La presente parte speciale si riferisce a comportamenti posti in essere dagli Organi sociali, dai dipendenti, nonché dai consulenti, come meglio definiti nella parte generale, coinvolti nelle attività sensibili.

C. PRINCIPI DI COMPORTAMENTO

TRC considera essenziale per lo svolgimento della sua attività la promozione ed il mantenimento di un adeguato sistema di controllo interno, il quale risulta essere costituito dall'insieme di tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività di impresa con l'obiettivo di

assicurare il rispetto delle leggi e delle procedure aziendali, di proteggere i beni aziendali, di gestire in modo ottimale ed efficiente le attività.

La responsabilità di realizzare un sistema di controllo efficace è comune a ogni livello della struttura organizzativa di TRC; di conseguenza, tutti coloro che svolgono la propria attività per la società, nell'ambito delle funzioni e delle responsabilità ricoperte, sono impegnati nel definire e nel partecipare attivamente al corretto funzionamento del sistema di controllo interno.

Ciò posto, con specifico riguardo alle problematiche connesse al rischio informatico, TRC, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso:

- I. la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi);
- II. la garanzia della massima continuità del servizio.

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che TRC si pone sono i seguenti:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'esplicito divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di TRC (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-*bis* del D.Lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente parte speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;

5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

D. PRINCIPALI AREE DI RISCHIO

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24- *bis* del D.Lgs. 231/2001 ipotizzabili in capo a TRC, sono le seguenti:

Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito dei quali sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione
- gestione e protezione della postazione di lavoro
- gestione degli accessi verso l'esterno (internet)
- gestione e protezione delle reti
- gestione degli output di sistema e dei dispositivi di memorizzazione
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)
- installazione di programmi e dispositivi
- gestione del processo di conservazione sostitutiva documentale.

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

Segregazione delle attività

Si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di

- (i) gestione di un processo e di controllo dello stesso,
- (ii) progettazione ed esercizio,
- (iii) acquisto di beni e risorse e relativa contabilizzazione.

Esistenza di procedure/norme/circolari

Esistono disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.

Poteri autorizzativi e di firma

I poteri autorizzativi e di firma devono:

- (i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese;
- (ii) essere chiaramente definiti e conosciuti all'interno della Società.

Tracciabilità

Ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

Ai fini dell'attuazione delle regole innanzi elencate, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui alla presente sezione, nel disciplinare la fattispecie di attività sensibile di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

E. PROCEDURE

Per ciò che concerne la gestione ed il monitoraggio degli accessi ai sistemi informatici e telematici è presente in TRC:

1) una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:

- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;

- costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
 - puntuale pianificazione delle attività di sicurezza informatica;
 - progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
 - definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
 - applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.
- 2) Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
 - 3) Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.
 - 4) Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.
 - 5) Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si espliciti attraverso la verifica e la gestione dei diritti d'accesso.
 - 6) Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
 - 7) Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
 - 8) Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).
 - 9) Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.
 - 10) Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.

- 11) Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni).

- 12) Predisposizione e attuazione di una policy aziendale (Regolamento IT) che stabilisce
 - (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi
 - (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito oppure negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.