Allegato 2

MODELLO ORGANIZZATIVO - PARTE SPECIALE

SETTORE FORMAZIONE PROFESSIONALE, ISTRUZIONE E LAVORO PROVINCIA DI LECCO

Standard di controllo per i reati ex d.lgs. 231 / 2001

INDICE

Il presente documento rappresenta le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex d.lgs. 231/2001. Le linee guida si riferiscono a comportamenti relativi all'area del "fare" e del "non fare", specificando in chiave operativa quanto espresso dai principi del Codice Etico.

"AREA DEL FARE"

- I responsabili, in quanto parte della Pubblica Amministrazione devono:
  - fornire ai propri collaboratori direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici diversi, secondo le peculiarità del proprio ambito di attività, trasferendo conoscenza della norma e consapevolezza delle situazioni a rischio reato.
- E' fatta raccomandazione a dipendenti e collaboratori esterni di segnalare all'Organismo di Vigilanza ogni violazione o sospetto di violazione del Modello Organizzativo. L'Ente e l'Organismo di Vigilanza tutelano dipendenti e collaboratori esterni da ogni effetto pregiudizievole che possa derivare dalla segnalazione. L'Organismo di Vigilanza assicura la riservatezza dell'identità dei segnalanti.
- I responsabili di settore devono segnalare all'Organismo di Vigilanza i comportamenti a rischio di reato ex d.lgs. 231/2001, inerenti ai processi operativi di competenza, di cui siano venuti a conoscenza in via diretta o per il tramite di informativa ricevuta dai propri collaboratori. In particolare, in caso di tentata concussione da parte di un pubblico funzionario nei confronti di un dipendente (o altri collaboratori) sono da adottare i seguenti comportamenti:
  - non dare seguito alla richiesta,
  - fornire informativa tempestiva al proprio Responsabile,
  - attivare formale informativa, da parte del Responsabile, verso l'Organismo di Vigilanza.
- I responsabili di settore che vengano ufficialmente a conoscenza di notizie, anche provenienti da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto sull'Ente, devono segnalarle all'Organismo di Vigilanza.

"AREA DEL NON FARE"

Con riferimento alle tipologie di reato rilevanti ai sensi del D. Lgs. 231/01, si segnalano, se pur a titolo non esaustivo, i comportamenti a rischio da evitare. Nei rapporti con altri rappresentanti della PA è fatto divieto di:

- promettere o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali e di servizio,
- promettere o concedere "soluzioni privilegiate" (ad esempio: interessamento per l'erogazione di servizi al di fuori delle modalità standard, interessamento per facilitare l'assunzione di parenti/affini/amici, ecc.),
- accettare omaggi/regalie dirette o indirette non di modico valore,
- fornire o promettere di fornire informazioni e/o documenti riservati,

1. Standard di controllo in relazione ai reati contro la Pubblica Amministrazione

Gli standard di controllo presi a riferimento per la gap analysis sono elaborati, principalmente, sulla base dei principi e delle indicazioni contenute nelle Linee Guida di Regione Lombardia, nonché delle "best practices" internazionali in tema di rischio di frode e di corruzione. Gli standard di controllo di primo livello sono i seguenti:

a) Segregazione delle attività: deve esistere segregazione delle attività tra chi esegue, chi controlla e chi autorizza;
b) Norme: devono esistere disposizioni interne all'Ente, idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile;
c) Poteri di firma e poteri autorizzativi: devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni;
d) Tracciabilità: deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi.

Più in dettaglio, gli standard di controllo di secondo livello sono i seguenti:

1) Report: devono esistere report periodici sull'utilizzo di risorse finanziarie con motivazioni e beneficiari, inviati al livello gerarchico superiore e archiviati. Devono sussistere i seguenti requisiti:

- Documentazione: devono esistere documenti giustificativi delle risorse finanziarie utilizzate con motivazione, attestazione di inerenza e congruità, validati dal superiore

gerarchico e archiviati;

- Modalità di pagamento: il pagamento non deve essere effettuato in contanti o con strumenti di pagamento analoghi e deve essere effettuato sul conto corrente indicato nel contratto e nel rispetto della procedura interna sulle attività di approvvigionamento. Il conto corrente non deve essere cifrato.

2) Segregazione dei ruoli nella gestione di finanziamenti pubblici:

- Autorizzazione formale: deve esistere una autorizzazione formalizzata per chiedere erogazioni pubbliche, con limiti, vincoli e responsabilità;
- Attribuzione formale delle responsabilità: deve esistere un ordine di servizio o comunicazione organizzativa con attribuzione di responsabilità per la gestione del finanziamento e della rendicontazione;
- Report: devono esistere report periodici sullo stato di avanzamento del progetto e sull'utilizzo delle erogazioni pubbliche validati dal livello gerarchico superiore e archiviati.
- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - Presentazione della richiesta di finanziamento e di successiva erogazione dello stesso.
  - Realizzazione dell'attività oggetto di finanziamento,
  - Certificazione dell'esecuzione di lavori/prestazioni,
  - Predisposizione dei rendiconti dei costi,
  - Controllo super partes;
- Definizione, per ogni progetto, di un piano di informazione, verso tutte le strutture coinvolte, circa le regole di attuazione degli interventi finanziati e della loro successiva gestione;
- Effettuazione della certificazione dell'esecuzione di lavori/prestazioni;
- Esistenza di riconciliazione fra dati tecnici ed amministrativi e di connessa verifica di finanziabilità delle spese esposte;
- Effettuazione di verifica di congruenza degli stati di avanzamento del progetto con il piano finanziario definito dal provvedimento di concessione/finanziamento;
- Esistenza di un organismo di controllo super partes, costituito da adeguato mix professionale tecnico-amministrativo, responsabile, sulla base di valutazioni di

rischiosità, di:

- monitorare lo stato di avanzamento del progetto, in conformità con le regole di attuazione definite, con interventi di verifica in corso d'opera;
- salvaguardare - mediante attività di riscontro di merito su base campionaria - la correttezza e l'autenticità delle condizioni/documenti prescritti dal decreto/concessione.

ISTRUZIONI E VERIFICHE DELL'OdV

È compito dell'OdV:

a) curare l'emanazione e l'aggiornamento di istruzioni relative ai comportamenti da seguire nell'ambito delle Aree di Rischio, come individuate;

b) verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli Esponenti Interni e/o al Responsabile di riferimento o ai Sub Responsabili di riferimento;

c) verificare periodicamente, con il supporto delle altre funzioni competenti, la validità delle clausole finalizzate:

- all'osservanza da parte dei Destinatari delle disposizioni del Decreto;
- alla possibilità per l'Ente di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificarne il rispetto;
- all'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni;

d) esaminare eventuali segnalazioni specifiche provenienti da qualsiasi fonte ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;

e) indicare alla dirigenza le opportune integrazioni ai sistemi gestionali delle risorse finanziarie (sia in entrata che in uscita), con l'introduzione di alcuni accorgimenti suscettibili di rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

2. Standard di controllo in relazione ai processi strumentali

I processi strumentali consistono in tutte quelle attività aziendali che consentono di produrre le risorse atte al potenziale compimento dei reati sopra descritti. Gli standard di controllo presi a riferimento per la gap analysis sono elaborati, principalmente, sulla base dei principi e delle indicazioni contenute nelle Linee Guida di Regione Lombardia, nonché delle "best practices" internazionali in tema di rischio di frode e di corruzione.

2.1 Consulenze e prestazioni professionali

Il processo di assegnazione di incarichi di consulenza/prestazione professionale costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di corruzione. Quest'ultimo potrebbe essere commesso attraverso l'assegnazione non trasparente degli incarichi.

L'indebito beneficio, realizzato attraverso il processo d'acquisto, è l'elemento costitutivo del reato in oggetto, da associare alla qualità di pubblico ufficiale o incaricato di pubblico servizio del soggetto e all'atto d'ufficio da compiere, omettere o ritardare. Il sistema di controllo si basa sui due elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti, a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - Richiesta della consulenza/prestazione,
  - Autorizzazione,
  - Definizione contrattuale,
  - Certificazione dell'esecuzione dei servizi (rilascio benestare),
  - Effettuazione del pagamento;
- Esistenza di requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti (Albo Fornitori) e di meccanismi di valutazione complessiva del servizio reso (Vendor Rating);
- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili);

- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati;
- Esistenza di livelli di approvazione per la formulazione delle richieste di consulenza / prestazione e per la certificazione / validazione del servizio reso;
- Esistenza di livelli di approvazione per le richieste;
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni;
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

Devono, inoltre, essere definite modalità operative e connessi meccanismi di escalation autorizzativa per eventuali deroghe ai principi sopra riportati, laddove ritenuto necessario, ad esempio per esigenze di riservatezza e tempestività.

Per quanto riguarda i flussi informativi verso l'organismo di vigilanza l'Amministratore ed il Responsabile della Funzione Amministrazione (per quanto di competenza) devono comunicare, con periodicità definita, il Piano Consulenze di periodo e relativi aggiornamenti, l'elenco incarichi gestiti in deroga ai principi standard; il consuntivo attività di consulenza/prestazioni professionali suddivise per fornitore.

2.2 Acquisti di beni e servizi

Il processo di acquisizione di beni e servizi costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di corruzione. Il reato di corruzione potrebbe essere commesso attraverso la gestione non trasparente del processo di acquisizione. L'indebito beneficio, realizzato attraverso il processo d'acquisizione, è l'elemento costitutivo del reato in oggetto, da associare alla qualità di pubblico ufficiale o incaricato di pubblico servizio del soggetto e all'atto d'ufficio da compiere, omettere o ritardare. Il sistema di controllo si basa sugli elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti e della valutazione complessiva delle forniture. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Richiesta della fornitura,
    - Effettuazione dell'acquisto,

    - Certificazione dell'esecuzione dei servizi/consegna dei beni (rilascio benestare),
    - Effettuazione del pagamento;
- Esistenza di criteri tecnico-economici per:
    - la selezione di potenziali fornitori (Qualificazione e inserimento in un Albo Fornitori),
    - la validazione della fornitura e dei beni/servizi forniti (Qualità Entrante),
    - la valutazione complessiva dei fornitori (Vendor Rating);
- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili);
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati;
- Esistenza di livelli di approvazione per la formulazione delle richieste di acquisto e per la certificazione della fornitura/erogazione;
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni;
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

Devono, inoltre, essere definite modalità di escalation autorizzativa per le attività d'acquisizione gestite in deroga ai requisiti sopra esposti (ad esempio: per scelta di fornitori non presenti in Albo, mancata comparazione fra offerte alternative, ecc.). Per quanto riguarda i flussi informativi verso l'Organismo di Vigilanza il Responsabile della Funzione Amministrazione (per quanto di competenza) deve comunicare con periodicità definita l'elenco degli acquisti effettuati in deroga ai requisiti sopra esposti.

ISTRUZIONI E VERIFICHE DELL'OdV

È compito dell'OdV:

a) curare l'emanazione e l'aggiornamento di istruzioni relative ai comportamenti da seguire nell'ambito delle Aree di Rischio, come individuate;

b) verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la

qualifica non corrisponda ai poteri di rappresentanza conferiti agli Esponenti Interni e/o al Responsabile di riferimento o ai Sub Responsabili di riferimento;

c) verificare periodicamente, con il supporto delle altre funzioni competenti, la validità delle clausole finalizzate:

- all'osservanza da parte dei Destinatari delle disposizioni del Decreto;
- alla possibilità per l'Ente di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificarne il rispetto;
- all'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni;

d) esaminare eventuali segnalazioni specifiche provenienti da qualsiasi fonte ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;

e) indicare alla dirigenza le opportune integrazioni ai sistemi gestionali delle risorse finanziarie (sia in entrata che in uscita), con l'introduzione di alcuni accorgimenti suscettibili di rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

3. Standard di controllo in relazione ai reati in materia di sicurezza sul lavoro

La legge 3 agosto 2007 n. 123, recante "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia", ha introdotto nel corpus del Decreto l'art. 25 septies, che ha inserito nel catalogo dei reati-presupposto le lesioni colpose gravi e gravissime e l'omicidio colposo derivanti dalla violazione di norme antinfortunistiche e di tutela di igiene e salute sul luogo di lavoro.

Il predetto art. 25 septies è stato poi sostituito, ad opera dell'art. 300 del d.lgs. 9 aprile 2008, n. 81, recante il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro. Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati dal novellato art. 25 septies del Decreto (di seguito anche "Reati in materia di Sicurezza sul Lavoro"). I reati considerati sono:

• *omicidio colposo (art. 589 c.p.)*

L'ipotesi di reato si configura qualora dalla violazione di norme antinfortunistiche derivi la morte di un lavoratore.

L'omicidio colposo implica la sussistenza dei seguenti elementi, legati da un nesso di causalità:

- la condotta del datore di lavoro (insieme eventualmente ad altri soggetti), che consiste nel mancato rispetto delle norme antinfortunistiche;
- l'evento lesivo, che consiste nella morte di una persona. Sotto il profilo soggettivo l'omicidio è colposo quando si verifica per colpa dell'agente, vale a dire per negligenza, imperizia o inosservanza delle leggi.

• *lesioni personali colpose (art. 590, comma 3, c.p.)*

L'ipotesi di reato si configura qualora dalla violazione di norme antinfortunistiche derivino lesioni gravi o gravissime in danno di un lavoratore. Le lesioni personali sono gravi se dal fatto deriva:

- una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- l'indebolimento permanente di un senso o di un organo.

Le lesioni personali sono gravissime se dal fatto deriva:

- una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
- la deformazione, ovvero lo sfregio permanente del viso.

Il reato di lesioni personali colpose implica la sussistenza dei medesimi elementi descritti al punto precedente. Per i Reati in esame si applica all'ente una sanzione pecuniaria in misura non inferiore a duecentocinquanta quote (250.000 euro). In caso di condanna per uno dei suddetti delitti si applicano le sanzioni interdittive di cui all'art. 9 del Decreto, per una durata non superiore ad un anno in caso di condanna.

DESTINATARI

Destinatari della presente Parte Speciale (i "Destinatari") sono i Dirigenti (i "Soggetti apicali") ed i Dipendenti e Collaboratori Interni soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio e inoltre i Collaboratori Esterni, come già definiti nella Parte Generale, che operino nelle aree di attività a rischio di cui al capitolo successivo.

AREE A RISCHIO

In relazione ai reati e alle condotte criminose in precedenza esplicitate, tenuto conto dell'attività svolta dall'ente, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale del Modello, quelle connesse agli adempimenti ed incombenze connesse agli obblighi stabiliti dalla normativa vigente in materia di tutela della sicurezza e della salute dei lavoratori durante il lavoro con particolare riferimento a quanto previsto dal d.lgs. n. 81/2008.

PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello. Obiettivo della presente Parte Speciale è che tutti i Destinatari coinvolti nello svolgimento di attività nelle Aree a Rischio adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati in materia di salute e sicurezza sul lavoro, pur tenendo conto della diversa posizione di ciascuno dei possibili Destinatari e della conseguente diversità dei loro obblighi come specificati nel Modello.

La presente Parte Speciale ha inoltre la funzione di:

1. indicare i principi procedurali generali e specifici cui i Destinatari sono tenuti ad attenersi in funzione di una corretta applicazione del Modello;
2. fornire all'OdV e ai responsabili delle funzioni interne chiamati a cooperare con lo stesso gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

La presente Parte Speciale è altresì volta alla puntuale individuazione ed alla regolamentazione dei seguenti obblighi:

a) di rispetto degli standard tecnico-strutturali di legge relativi alle attrezzature, agli impianti, ai luoghi di lavoro;

b) di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) inerenti le attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) concernenti le attività di sorveglianza sanitaria;

e) attinenti le attività di informazione e formazione dei lavoratori;

f) riguardanti le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) di acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) di verifica periodica dell'applicazione e dell'efficacia delle procedure adottate.

Ciò in ossequio all'art. 30 del d.lgs. 9 aprile 2008, n. 81, al fine di garantire al Modello l'efficacia esimente della responsabilità amministrativa prevista dal Decreto. La presente Parte Speciale prevede l'espresso obbligo, a carico degli Esponenti interni, in via diretta, ed a carico dei Collaboratori Esterni, tramite apposite clausole contrattuali di:

- astenersi dal porre in essere comportamenti tali da integrare le fattispecie di Reato sopra considerate (art. 25 octies del Decreto);
- astenersi dal 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.

Nell'ambito dei suddetti comportamenti è fatto inoltre obbligo di:

- adempiere alle disposizioni di leggi e regolamenti vigenti;
- operare nel rispetto dei poteri di rappresentanza e di firma sociale, delle deleghe e procure loro conferite;
- rispettare le prescrizioni previste dalle procedure di riferimento;
- ottemperare alle istruzioni impartite dai superiori gerarchici.

PRINCIPI PROCEDURALI SPECIFICI

Si indicano qui di seguito i principi procedurali e le modalità di attuazione che, in relazione ad ogni singola Area a Rischio gli Esponenti Interni sono tenuti a rispettare, e che devono trovare attuazione in specifiche procedure interne e nei protocolli di prevenzione.

Nel processo di gestione del sistema di prevenzione e protezione è necessario, in conformità alla previsione della normativa vigente:

1. istituire il servizio di prevenzione e protezione, designare il responsabile ed eventuali addetti;
2. nominare il medico competente;
3. designare il Rappresentante dei lavoratori per la sicurezza;
4. elaborare il DVR e procedere al relativo aggiornamento in occasione di significative modifiche dei processi lavorativi;
5. adottare le misure di prevenzione incendi, lotta antincendio, evacuazione dei lavoratori, pronto soccorso e di gestione dell'emergenza.

Nel processo riferito alle risorse umane particolare attenzione deve essere posta alle attività riguardanti l'assunzione e gestione operativa delle risorse, nel rispetto di quanto disposto dal DVR e dal medico competente.

Al fine di garantire l'osservanza delle prescrizioni normative nella gestione delle attività sopra citate i Destinatari devono procedere:

1. all'adozione per tutti i Dipendenti e Collaboratori Interni delle misure di prevenzione e protezione previste dal DVR;
2. all'impiego dei Dipendenti e dei Collaboratori Interni nel rispetto della normativa vigente in materia di prestazione lavorativa (orario di lavoro, riposi, straordinari, etc.);
3. a fare osservare a tutti i Dipendenti e Collaboratori Interni le norme di legge e le disposizioni aziendali in materia di salute, sicurezza ed igiene sul lavoro, in riferimento alla specifica attività svolta;
4. a consultare i rappresentanti dei lavoratori per la sicurezza (RLS) secondo la normativa vigente;
5. ad utilizzare il personale secondo l'idoneità fisica attestata dal medico competente.

Relativamente al processo di manutenzione attrezzature, impianti e infrastrutture, i Destinatari devono:

1. programmare gli interventi manutentivi e di pulizia coerentemente con il piano di manutenzione;
2. eseguire tutti gli interventi programmati e certificare il loro assolvimento;
3. adeguare gli impianti in relazione alle modifiche di legge intervenute;
4. assicurare la manutenzione periodica dei dispositivi di sicurezza.

Oltre alle regole e ai principi sopra descritti, i Destinatari devono osservare le specifiche prescrizioni previste dal sistema di prevenzione e protezione sui luoghi di lavoro che è parte integrante del Modello.

ISTRUZIONI E VERIFICHE DELL'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati in materia di Sicurezza sul Lavoro sono i seguenti:

a) monitorare costantemente, eventualmente per il tramite del Responsabile del Servizio di Prevenzione e Protezione, l'efficacia delle misure di prevenzione dei Reati in materia di Sicurezza sul Lavoro;

b) esaminare eventuali segnalazioni specifiche provenienti da qualsiasi fonte ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;

c) verificare l'attuazione dei meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.

L'OdV può indire in ogni momento una riunione con il Datore di Lavoro, o i suoi delegati, nonché il Responsabile del Servizio di Prevenzione e Protezione e il Rappresentante dei lavoratori per la sicurezza.

4. Standard di controllo in relazione ai reati informatici

Per quanto concerne la presente Parte Speciale, si riporta di seguito una breve descrizione dei reati contemplati dall'art. 24 bis del Decreto (di seguito anche "Reati informatici"), introdotto con la Legge n. 48 del 18 marzo 2008 ("Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"), al fine di contrastare la criminalità informatica.

I reati considerati sono:

• *Accesso abusivo ad un sistema informatico o telematico (Art. 615 ter c.p.)*

Il reato, punibile a querela della persona offesa, consiste nel fatto di chi si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Circostanze aggravanti sono previste nel caso in cui:

• il fatto sia 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;

• il fatto sia commesso da soggetti che per commettere il fatto usino violenza sulle cose o alle persone, ovvero se siano palesemente armati;

• dal fatto derivi 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;

• i fatti 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.

In tali casi il reato è perseguibile d'ufficio. L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema; la norma, infatti, considera punibile la semplice intrusione, indipendentemente dal verificarsi di un danneggiamento o furto dei dati. L'intrusione abusiva può concretizzarsi anche nel caso in cui i soggetti, legittimati all'uso del sistema ed autorizzati ad accedere solo ad una parte dei dati contenuti, accedano ad una parte di memoria a cui non sono autorizzati. Con il termine "si mantenga [nel sistema informatico]" si intende una permanenza non autorizzata, ad esempio, quando ad un accesso al sistema inizialmente autorizzato faccia seguito una permanenza contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

• *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)*

Il reato consiste nell'intercettazione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero nel loro impedimento o interruzione.

Sono puniti anche coloro che rivelino mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni.

I delitti sono punibili a querela della persona offesa, ma si procede d'ufficio, con aggravio delle pene previste, qualora il fatto sia 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,
3. ovvero con abuso della qualità di operatore del sistema;
4. da chi esercita anche abusivamente la professione di investigatore privato.

• *Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)*

L'ipotesi di reato si configura quando chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. È considerata circostanza aggravante la commissione dei fatti:

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.

• *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)*

Tale ipotesi di reato consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui.

Se il fatto è commesso con violenza alla persona, minaccia o abuso della qualità di operatore del sistema, la pena è aumentata; in tali casi il reato è perseguibile d'ufficio.

• *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.)*

Tale ipotesi di reato consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Sono considerate fattispecie aggravanti:

1. la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici;
2. la commissione del fatto con violenza alla persona, minaccia o abuso della qualità di operatore del sistema;
3. danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.).

L'ipotesi di reato si configura quando chiunque, mediante le condotte di cui all'art.635 bis [Danneggiamento di informazioni, dati e programmi informatici], o 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.

Se il fatto è commesso con violenza alla persona, minaccia o abuso della qualità di operatore del sistema, la pena è aumentata.

• *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)*

L'ipotesi di reato si configura quando chiunque, mediante le condotte di cui all'art.635 bis [Danneggiamento di informazioni, dati e programmi informatici], o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento. La distruzione, il danneggiamento o l'inservibilità del sistema comporta un aumento delle pene previste. La medesima conseguenza si verifica quando il fatto è commesso con violenza alla persona, minaccia o abuso della qualità di operatore del sistema.

• *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)*

L'ipotesi di reato si configura quando 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 a tale scopo.

Le pene sono aumentate qualora il reato sia commesso:

• 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;

• 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.

L'oggetto del reato consiste in qualsiasi azione che permetta di superare la protezione di un sistema informatico, indipendentemente dalla natura del mezzo. Le condotte punite, in sintesi, sono le seguenti:

• l'utilizzo non autorizzato di codici d'accesso;

• la diffusione, che si manifesta nel rendere disponibili tali codici ad un numero indeterminato di soggetti;

• la comunicazione, che consiste nel rendere disponibili tali codici ad un numero limitato di soggetti;

• la consegna, che riguarda cose materiali (es. smart cards);

• la comunicazione o diffusione di istruzioni che permettono di eludere le protezioni di un sistema.

Resta irrilevante il fatto che i codici siano procurati abusivamente o mediante l'autonoma elaborazione.

• *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)*

L'ipotesi di reato si configura quando 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 informatici.

• *Documenti informatici (art. 491 bis c.p.)*

L'ipotesi di reato si configura quando una delle falsità previste dal Titolo VII, Capo III (falsità in atti) riguardi un documento informatico pubblico o privato avente efficacia probatoria. In tal caso si rendono applicabili le disposizioni concernenti rispettivamente gli atti pubblici e le scritture private. I documenti informatici sono pertanto passibili delle medesime condotte di falsificazione previste per i documenti tradizionali. La locuzione "aventi efficacia probatoria" è riferita direttamente ai dati ed alle informazioni (oltre che, indirettamente, ai programmi destinati ad elaborarli) e non ai singoli supporti materiali che li contengono; infatti oggetto di tutela sono i dati informatici che circolano e si comunicano in quanto tali ed il loro contenuto rappresentativo, probatorio di sottostanti atti, fatti o rapporti giuridicamente rilevanti. Risulta quindi ipotizzabile, ad esempio, la falsità materiale in atti pubblici commessa da privato (artt. 476 - 482 c.p.), a condizione che sia stato formato in tutto o in parte un atto falso per via informatica, o alterato nella sua rappresentazione un atto vero o un atto destinato a far fede fino a querela di falso, come nel caso in cui il contenuto di un atto venga composto o variato al fine di modificarne sensibilmente il contenuto. È inoltre ipotizzabile il caso della falsità ideologica informatica (artt. 479 - 481 c.p.). qualora venga posta in essere una condotta attiva od omissiva che non rappresenti effettivamente la realtà, alterandone un'oggettiva rappresentazione destinata ad avere particolari effetti giuridici formali o sostanziali. Non sono ricompresi nella fattispecie in esame i casi di falso documentale che si collocano al di fuori del capo III del titolo VII, libro II, del codice penale.

• *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

L'ipotesi di reato si configura quando il soggetto che presta servizi di certificazione di firma elettronica, 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.

DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale (i "Destinatari") sono i Dirigenti (i "Soggetti apicali") ed i Dipendenti e Collaboratori Interni e inoltre i Collaboratori Esterni, come già definiti nella Parte Generale, che operino nelle aree di attività a rischio di cui al paragrafo successivo.

AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale "E", le seguenti:

1. utilizzo dei sistemi informatici;
2. gestione delle password per l'accesso a sistemi informatici o telematici;
3. predisposizione, rappresentazione o comunicazione di documenti informatici a Terzi;
4. adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito di atti, documenti e pratiche per via informatica.

PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello.

Obiettivo della presente Parte Speciale è che tutti i Destinatari coinvolti nello svolgimento di attività nelle Aree a Rischio adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati Informatici previsti nel Decreto, pur tenendo conto della diversa posizione di ciascuno dei possibili Destinatari e della conseguente diversità dei loro obblighi come specificati nel Modello. La presente Parte Speciale ha inoltre la funzione di:

a) indicare i principi procedurali generali e specifici cui i Destinatari sono tenuti ad attenersi in funzione di una corretta applicazione del Modello;

b) fornire all'OdV e ai responsabili delle funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli Esponenti Interni, con riferimento alle rispettive aree di attività, sono tenuti alla stretta osservanza delle leggi e dei regolamenti che disciplinano l'attività interna, nonché a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

• il Codice Etico;

• ogni normativa e procedura interna volta alla sicurezza (organizzativa, logica e fisica) dei sistemi elettronici e dei dati gestiti tramite i sistemi stessi;
• le disposizioni di legge e i regolamenti vigenti.

La presente Parte Speciale prevede l'espresso obbligo, a carico degli Esponenti Interni, in via diretta, e a carico dei Collaboratori Esterni, tramite apposite clausole contrattuali di:

• astenersi dal porre in essere comportamenti tali da integrare le fattispecie di Reato sopra considerate (art. 24 bis del Decreto);
• astenersi dal 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.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

• consentire l'accesso ai server (fisico o per via remota) a persone non autorizzate;
• alterare in qualsiasi modo, manomettere o modificare autonomamente i sistemi applicativi, le infrastrutture hardware e i dati in uso, di proprietà o di Terzi, o manipolarne i dati;
• cedere a Terzi le proprie credenziali di autenticazione;
• danneggiare i sistemi informatici di proprietà o di Terzi;
• predisporre, rappresentare o comunicare documenti informatici falsi o comunque suscettibili di fornire dati e informazioni non rispondenti alla realtà.

Ai fini dell'attuazione dei comportamenti di cui sopra, è fatto obbligo di:

• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle specifiche procedure aziendali;
• effettuare un costante monitoraggio dell'integrità dei sistemi informatici, dei livelli ed autorizzazioni di accesso, del corretto trattamento delle password e credenziali per l'accesso a sistemi informatici di proprietà o di Terzi;
• assicurare la massima tracciabilità delle attività compiute per via informatica.

PRINCIPI PROCEDURALI SPECIFICI

Si indicano qui di seguito i principi procedurali e le modalità di attuazione che, in relazione ad ogni singola Area a Rischio gli Esponenti Interni sono tenuti a rispettare, e che devono trovare attuazione in specifiche procedure aziendali e nei protocolli di prevenzione.

In relazione alle Aree a Rischio individuate è fatto obbligo di:

• accedere alle sole risorse informatiche a cui si è autorizzati;
• custodire le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;
• definire nei contratti con i Fornitori per l'esecuzione di incarichi relativi ad uno o più processi del sistema informatico (ad esempio per lo sviluppo software, per l'utilizzo delle applicazioni, per le manutenzioni, etc.), i controlli e le misure necessarie per garantire la sicurezza del servizio, verificandone altresì l'attendibilità commerciale e professionale;
• procedere ad attività di testing su ogni nuovo software o suo aggiornamento ovvero, ancora, su ogni nuovo applicativo o soluzione informatica suscettibile di incidere nelle Aree a Rischio;
• mantenere evidenza, in apposite registrazioni su archivi informatici, dei livelli di autorizzazione all'accesso (alla rete interna e/o a sistemi di proprietà di Terzi) degli utenti, ai fini della tracciabilità degli accessi e delle attività informatiche poste in essere nelle Aree a Rischio.

ISTRUZIONI E VERIFICHE DELL'OdV

È compito dell'OdV, in relazione all'osservanza del Modello per quanto concerne i Reati Informatici:
a) proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
b) esaminare eventuali segnalazioni specifiche provenienti da qualsiasi fonte ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
c) monitorare costantemente l'efficacia delle procedure interne in essere e vigilare sull'idoneità di quelle di futura introduzione;
d) verificare l'attuazione dei meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.