

MODELLO ORGANIZZATIVO DI SIAER SOC. CONS. A R.L.

(ai sensi del D.Lgs. n. 231/2001)

**REVISIONATO ED AGGIORNATO
MAGGIO 2024**

COMPOSIZIONE DEL MODELLO

- 1) MODELLO DI ORGANIZZAZIONE E GESTIONE**
- 2) CODICE ETICO**
- 3) ANALISI DEL RISCHIO**
- 4) RAPPORTI CON LA P.A.**
- 5) GESTIONE DELLA DOCUMENTAZIONE**
- 6) APPROVVIGIONAMENTI**

Avv.ti Montagnani R. e Loberti P. S.t.p.
Via J.F. Kennedy n. 37
44122 FERRARA
Tel. 0532/767918 Fax 0532/767555
e-mail: r.montagnani@studiomontagnaniloberti.it

MODELLO DI ORGANIZZAZIONE E GESTIONE

Sommario

1 Il Decreto Legislativo 8 giugno 2001, n. 231

- 1.1 Contenuti principali
- 1.2 L'applicabilità della "responsabilità amministrativa" ed i soggetti interessati
- 1.3 Il Modello di organizzazione e gestione e relative attività connesse
- 1.4 Le sanzioni previste dal Decreto

2 Riferimenti

3 Definizioni

4 SIAER Soc. Cons. a r.l.

- 4.1 La storia
- 4.2 Cenni sullo Statuto e sugli Organi
- 4.3 Cenni sull'assetto organizzativo della Società
- 4.4 Struttura generale del Sistema di controllo interno

5 Il Modello di organizzazione e gestione di SIAER

- 5.1 Obiettivi cui tende il Modello
- 5.2 I principi regolatori del Modello
- 5.3 Composizione del Modello
- 5.4 Costruzione del Modello
- 5.5 Rilevazione dei processi sensibili
- 5.6 Attività sensibili per l'Ente

6 L'esposizione al Rischio

- 6.1 Premessa metodologica
- 6.2 *Reati contro la PA*
La definizione di pubblica amministrazione
L'esposizione al rischio
Misure per la prevenzione
- 6.3 *Induzione a rendere false dichiarazioni all'Autorità Giudiziaria*
L'esposizione al rischio
Misure per la prevenzione
- 6.4 *Reati informatici*
L'esposizione al rischio
Misure per la prevenzione
- 6.5 *Delitti in materia di violazioni della Legge sul diritto d'autore*
L'esposizione al rischio
Misure per la prevenzione
- 6.6 *Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di beni di provenienza illecita*
L'esposizione al rischio
Misure per la prevenzione
- 6.7 *Reati societari*
L'esposizione al rischio
Misure per la prevenzione
- 6.8 *Reati di criminalità organizzata*
L'esposizione al rischio
Misure per la prevenzione

6.9 *Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro*

L'esposizione al rischio

Misure per la prevenzione

6.10 *Reati ambientali*

L'esposizione al rischio

Misure per la prevenzione

6.11 *Reati di xenofobia e razzismo*

L'esposizione al rischio

Misure per la prevenzione

6.12 *Reati tributari*

L'esposizione al rischio

Misure per la prevenzione

7 L'Organismo di Vigilanza e Controllo

7.1 Generalità

7.2 Nomina e composizione

7.3 I requisiti dell'Organismo di Vigilanza e controllo

7.4 Le risorse dell'Organismo di Vigilanza

7.5 Compiti e poteri dell'Organismo di Vigilanza

7.6 Flusso di informazione verso l'Organismo di Vigilanza

7.7 Reporting e gestione dei documenti

8 Sistema sanzionatorio

8.1 Criteri generali di irrogazione della sanzione

8.2 Le sanzioni

9 Informazione e formazione del personale

9.1 Informazione e formazione dei dipendenti

1 Il Decreto Legislativo 8 giugno 2001, n. 231

1.1 Contenuti principali

Con il Decreto legislativo 8 Giugno 2001 n. 231, emanato in esecuzione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, è stata introdotta nell'ordinamento giuridico italiano la «responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica» a seguito della commissione di illecito.

I reati per i quali il decreto risulta applicabile sono:

art. 24: *“indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico”*, che correla la responsabilità amministrativa dell'ente alla commissione di reati quali l'indebita percezione di erogazioni a danno dello Stato (o di altro ente pubblico, o della Comunità europea) la truffa (a danno dello Stato o di un altro ente pubblico) la frode informatica (se commessa in danno dello Stato o di altro ente pubblico);

art. 24-bis: *“delitti informatici e trattamento illecito di dati”* correla la responsabilità amministrativa dell'ente alla commissione di reati quali il reato di accesso abusivo ad un sistema informatico o telematico, il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, il reato di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, il reato di falsificazioni informatiche ed il reato di danneggiamento di informazioni, dati e programmi informatici, ancorché, utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;

art. 24-ter: *“delitti di criminalità organizzata”*;

art. 25: “*concussione e corruzione*”, che correla la responsabilità amministrativa dell’ente alla commissione di reati quali la concussione, la corruzione per un atto d’ufficio o per un atto contrario ai doveri d’ufficio;

art. 25-bis: “*falsità in monete, in carte di pubblico credito, in valori in bollo ed in strumenti o segni di riconoscimento*” che correla la responsabilità amministrativa dell’ente alla commissione dei reati di falso nummario, di uso di valori contraffatti, di contraffazione e uso di segni distintivi e brevetti nonché l’introduzione ed il commercio di prodotti con segni falsi;

art. 25-bis 1: “*delitti contro l’industria ed il commercio*”;

art. 25-ter: “*reati societari*”, che correlano la responsabilità amministrativa dell’ente alla commissione di illeciti quali le false comunicazioni sociali, la falsità delle relazioni o nelle comunicazioni delle società di revisione, l’aggiotaggio, la illegale ripartizione degli utili e delle riserve, le illecite operazioni sulle azioni o quote sociali o della società controllante, le operazioni in pregiudizio dei creditori, l’illecita influenza sull’assemblea, l’omessa comunicazione del conflitto d’interessi, l’ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza, la corruzione tra privati e l’istigazione alla corruzione tra privati;

art. 25-quater: “*delitti con finalità di terrorismo o di eversione dell’ordine democratico*”, che correlano la responsabilità amministrativa dell’ente alla commissione dei delitti aventi finalità di terrorismo o di eversione dell’ordine democratico previsti sia nel codice penale che nelle leggi speciali;

art. 25-quater-1: “*pratiche di mutilazione degli organi genitali femminili*”;

art. 25-quinquies: “*delitti contro la personalità individuale*”, che correlano la responsabilità amministrativa dell’ente alla commissione di illeciti quali la detenzione di materiale pornografico (prodotto mediante lo sfruttamento sessuale di minori) e le iniziative turistiche volte allo sfruttamento della prostituzione minorile;

art. 25-sexies: “*reati di abuso del mercato*”, che correlano la responsabilità amministrativa dell’ente alla commissione degli illeciti di abuso di informazioni privilegiate e manipolazione del mercato;

art. 25-septies: “*reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro*”;

art. 25-octies: “*ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita*”;

art. 25-novies: “*delitti in materia di violazione del diritto d’autore*”;

art. 25-decies: “*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria*”;

art. 25-undecies: “*reati ambientali*”;

art. 25-duodecies “*impiego di lavoratori stranieri privi di permesso di soggiorno o con permesso scaduto*”;

art. 25-terdecies “*delitti di razzismo e xenofobia*”;

art. 25-quaterdecies “*frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d’azzardo esercitati a mezzo di apparecchi vietati*”;

art. 25-quinquiesdecies “*reati tributari*”, che concernono la condotta di colui che utilizza fatture o altri documenti probatori per dichiarare passività inesistenti all’interno della dichiarazione IVA o nella dichiarazione dei redditi, al fine di ridurre fraudolentemente l’imponibile oggetto del prelievo fiscale; oppure occultare e distrugge documenti contabili, oppure ancora si sottrae fraudolentemente al pagamento delle imposte;

art. 25-sexiesdecies “*delitti di contrabbando*”, previsti dal Decreto del Presidente della Repubblica 23 gennaio 1973, n. 43;

“*reati transnazionali*”: introdotti con la legge 16 Marzo 2006, n° 146, correlano la responsabilità amministrativa dell’ente a reati quali il riciclaggio e l’associazione per delinquere su scala internazionale.

1.2 L’applicabilità della “responsabilità amministrativa” ed i soggetti interessati

Ai sensi dell’art. 5, D.Lgs. 231/2001, perché possa risultare integrata la responsabilità amministrativa dell’organizzazione allorché sia stato commesso un reato da una persona fisica funzionalmente collegata all’ente stesso, occorre che il reato sia stato commesso «nel suo interesse o a suo vantaggio», dacché l’ente non risponde se il suo autore ha «agito nell’interesse esclusivo proprio o di terzi».

Inoltre, affinché, parallelamente alla responsabilità penale dell'autore del reato (persona fisica) possa profilarsi la responsabilità amministrativa dell'ente, è necessario che il reato sia stato commesso da soggetti che rivestano una posizione apicale all'interno dell'ente o da soggetti in posizione subordinata. Più precisamente, sempre ai sensi dell'art. 5, «l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (cosiddetti soggetti *apicali*);
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (cosiddetti *sottoposti*)».

La responsabilità amministrativa dell'ente sorge anche nelle ipotesi in cui sia commesso, nella forma del tentativo, uno dei reati previsti dal Decreto.

1.3 Il Modello di organizzazione e gestione e relative attività connesse

Laddove il reato sia stato commesso da soggetti in posizione apicale, il decreto legislativo stabilisce che l'ente non risponda amministrativamente se fornisce la prova che (art. 6):

- a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Ai sensi del comma II dell'art. 6, il Modello di organizzazione e gestione deve rispondere all'esigenza di:

- 1) individuare le attività nel cui ambito possono essere commessi reati;
- 2) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- 3) individuare le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- 4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- 5) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Nell'ipotesi in cui, invece, il reato sia stato perpetrato da «soggetti sottoposti all'altrui direzione», l'art. 7 del decreto legislativo prevede che l'ente sia responsabile «se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza», inosservanza che è esclusa «se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi».

La medesima norma dispone poi che il Modello debba prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio; lo stesso articolo inoltre stabilisce che l'efficace attuazione del Modello richiede sia la «verifica periodica» e la «eventuale modifica» del Modello nei casi in cui siano «scoperte significative violazioni delle prescrizioni» od in cui «intervengano mutamenti nell'organizzazione o nell'attività», sia un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

Con il D.Lgs. n. 24 del 10 marzo 2023 è stata introdotta la nuova disciplina del whistleblowing in Italia; il decreto è entrato in vigore il 30 marzo 2023.

Le nuove disposizioni hanno avuto effetto a partire dal 15 luglio 2023, con una deroga per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati non superiore a 249.

Per questi l'obbligo di istituzione del canale di segnalazione interna ha avuto effetto a decorrere dal 17 dicembre 2023.

Il provvedimento, attuativo della Direttiva europea 2019/1937, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato.

Per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove, l'obbligo di istituzione del canale di segnalazione interna ai sensi del D.Lgs. n. 24 del 10 marzo 2023 ha avuto effetto a decorrere dal 17 dicembre 2023 e, fino ad allora, hanno continuato ad applicarsi l'articolo 6, comma 2-bis, lettere a) e b), del D. Lgs n. 231 del 2001.

Dopodichè risulta abrogato l'articolo 6, commi 2-ter e 2-quater, del D. Lgs. 8 giugno 2001, n. 231.

Nel caso di specie, SIAER ha adottato un Protocollo per le segnalazioni di illeciti, violazioni e irregolarità, che prevede le seguenti modalità di segnalazione interna.

Le segnalazioni devono essere trasmesse al Responsabile delle segnalazioni incaricato da SIAER, ovvero l'OdV di questo, tramite i seguenti canali tassativi:

- verbalmente mediante incontro in presenza, previo appuntamento telefonico al recapito dell'OdV.
- tramite posta cartacea tradizionale, con la dicitura "riservato", inviata presso lo Studio professionale dell'OdV.
- tramite posta elettronica all'indirizzo e-mail gestito direttamente dal Responsabile delle segnalazioni incaricato da SIAER.

Tali attività appaiono adeguate per il raggiungimento degli scopi previsti dalla normativa e, conseguentemente, appare efficace la struttura posta in essere da SIAER, che consiste in:

- a) un canale che consente a coloro che a qualsiasi titolo rappresentino o dirigano la Società di presentare, a tutela dell'integrità della stessa, segnalazioni circostanziate di condotte illecite;
- b) un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c) misure idonee a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione, nei limiti in cui l'anonimato e la riservatezza siano opponibili per legge.

1.4 Le sanzioni previste dal Decreto

L'art. 9, comma 1, del D. Lgs. 231/01, elenca le sanzioni distinguendole in: sanzione pecuniaria, sanzioni interdittive, confisca e pubblicazione della sentenza. In riferimento alla sanzione pecuniaria, che deve essere sempre applicata, è stato stabilito un sistema di calcolo per quote, da determinarsi per quantità e valore, questo per meglio adattare l'entità della sanzione alla realtà del caso. Ogni quota va da un valore minimo di 258,00 euro, ad un massimo di 1.549,00 euro; non potranno essere applicate complessivamente un numero di quote inferiore a cento (100) né superiore a mille (1000).

Riprendendo l'art. 9 del Decreto, al comma 2, si elencano le sanzioni interdittive; esse sono: l'interdizione dall'esercizio dell'attività; la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

A differenza della sanzione pecuniaria, che si applica sempre, le sanzioni interdittive trovano applicazione in quanto espressamente previste dalla legge ed a condizione che ricorra almeno una delle condizioni richiamate dall'art. 13, cioè che:

- i) l'ente abbia tratto dal reato un profitto di rilevante entità;
- ii) il reato sia stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

iii) in caso di reiterazione degli illeciti.

2 Riferimenti

- Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche ed integrazioni.
- Decreto Legislativo 9 aprile 2008, n. 81 e successive modifiche ed integrazioni.
- Legge 23 dicembre 2000, n. 388.
- Legge 27 dicembre 2002, n. 289.
- Legge 29 Settembre 2000, n. 300.

3 Definizioni

SIAER Soc. Cons. a r.l. con sede legale in Bologna (BO), via Rimini n. 7 (brevemente anche SIAER o Società).

D.Lgs. 231/2001: il Decreto Legislativo 8 giugno 2001, n. 231.

Modello: il Modello di organizzazione e gestione ai sensi del decreto legislativo 8 Giugno 2001, n. 231.

Attività Sensibili: le attività nel cui ambito sussiste il rischio di commissione dei reati.

Reati presupposto: le fattispecie di reato nominate dal Decreto e sue integrazioni e presupposto della responsabilità amministrativa ex D. Lgs. 231/2001.

OdV: l'Organismo di Vigilanza, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché al relativo aggiornamento.

Soggetti apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società, nonché persone che esercitano, anche di fatto, la gestione o il controllo della stessa.

Soggetti subordinati: le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al punto precedente.

Consulenti: i soggetti che agiscono in nome e/o per conto di SIAER in forza di un rapporto contrattuale di collaborazione o di specifico mandato.

Dipendenti: i soggetti aventi un rapporto di lavoro subordinato con la Società, ivi inclusi i dirigenti.

P.A.: la Pubblica Amministrazione.

Fornitori: le controparti contrattuali di SIAER, sia persone fisiche, sia persone giuridiche.

4 SIAER Soc. Cons. a r.l.

4.1 La storia

SIAER è una società consortile a responsabilità limitata, costituita dalle Società di servizi provinciali delle CNA dell'Emilia-Romagna.

SIAER, nella sua attuale composizione, nasce nell'anno 2009 a seguito della fusione per incorporazione con Sofista s.r.l.

Ha natura di società consortile a responsabilità limitata, ai sensi dell'art. 2615-ter del codice civile.

Esiste un legame, di origine e di operatività, che unisce SIAER alle Società di servizi delle CNA provinciali dell'Emilia-Romagna e, in senso più ampio, al Sistema CNA. Tale legame non costituisce un vincolo, bensì un riferimento strategico per l'attività propria di SIAER.

L'assetto attuale di SIAER deriva da una storia ormai più che trentennale. Infatti, fu agli inizi degli anni '80 che nacque l'esigenza di costituire un centro unico regionale dei servizi informatici nell'ambito della rete CNA. Inizialmente, l'operare di SIAER, come struttura regionale, fu indirizzato al consolidamento delle procedure informative ed informatiche, tese alla costruzione di una banca dati regionale e di un sistema di servizi integrato.

Per lungo tempo SIAER ha rappresentato il fulcro dei servizi software per tutto il Sistema CNA dell'Emilia-Romagna, finché, giunto a ricoprire un ruolo nazionale, ha conferito a fine 2008 il ramo d'azienda più importante, quello dei servizi software, a CNA Informatica S.p.a.

SIAER promuove, realizza e diffonde, con l'impiego di attrezzature elettroniche ed automatizzate, l'applicazione delle più avanzate tecniche organizzative e di gestione amministrativa aziendale, nonché l'introduzione di sistemi informativi integrati.

4.2 Cenni sullo Statuto e sugli organi societari

SIAER nasce come società consortile a responsabilità limitata; opera principalmente per il comparto delle imprese artigiane e P.M.I., in un quadro di relazioni coerenti con gli obiettivi di sviluppo e di qualificazione produttiva e gestionale dei soci.

Sono organi di SIAER:

- **l'Assemblea:** composta da tutti i soci

L'Assemblea elegge il Consiglio di Amministrazione ed eventualmente il Presidente e nomina il l'Organo di Revisione ed il Presidente di questo.

- **Il Consiglio di Amministrazione:** composto da minimo tre a massimo diciotto membri.

Il Consiglio nomina al proprio interno il Presidente, se non eletto dall'Assemblea, cui è data la rappresentanza di SIAER in giudizio e di fronte a terzi.

Al Consiglio di Amministrazione spettano i poteri di ordinaria e straordinaria amministrazione ed in particolare:

- vigila su tutti i servizi prestati ed iniziative promosse da SIAER;
- provvede alla redazione dei bilanci;
- predispone il modello organizzativo, gli organici e i regolamenti interni di SIAER, previa approvazione dell'Assemblea.

In alternativa al Consiglio di Amministrazione è previsto l'Amministratore Unico, con gli stessi poteri del CdA.

- **L'Organo di Controllo** che può essere monocratico o collegiale.

I componenti dell'Organo di Controllo hanno i doveri di cui agli artt. 2403, 2404 e 2407 del Codice civile.

In alternativa all'Organo di Controllo è previsto il Revisore Unico.

4.3 Cenni sull'assetto organizzativo di SIAER

La responsabilità operativa di SIAER è affidata ad un Amministratore Unico, se nominato, altrimenti spetta al Consiglio di Amministrazione.

4.4 Struttura generale del Sistema di controllo interno

SIAER, nella definizione dei propri sistemi di controllo e delle specifiche misure di prevenzione da reato, ha adottato un sistema normativo basato sulla modularità coerente e funzionale. Questa scelta permette di rintracciare distinti livelli di misure di prevenzione e controllo di seguito rappresentati:

Codice Etico, documento che evidenzia i valori e i principi fondamentali ai quali si ispira la Società ed ai quali tutti i dipendenti e collaboratori devono uniformarsi nello svolgimento dei compiti e delle funzioni loro affidate.

Modello di organizzazione, gestione e controllo, documento che fissa le misure di prevenzione e controllo in ragione della tipologia e del grado di esposizione al rischio reato nei processi individuati come sensibili.

Regolamenti e procedure, che individuano specifiche misure di prevenzione e controllo per il corretto svolgimento delle attività nelle singole funzioni e nelle relazioni interfunzionali, definite con l'obiettivo di adeguarsi costantemente e tempestivamente alla normativa cui è soggetto SIAER.

5 Il Modello di organizzazione e gestione di SIAER

5.1 Obiettivi cui tende il Modello

La Società, per la particolare natura che riveste ed attività che svolge, coerentemente con gli obiettivi che persegue, è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione delle

attività istituzionali, a tutela della propria posizione ed immagine, del lavoro dei propri dipendenti e del settore in cui opera.

Muovendo da queste premesse, SIAER ha ritenuto conforme alla propria politica procedere all'attuazione del Modello di organizzazione e di gestione previsto dal D.Lgs. 231/2001.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello possa:

- costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto della Società, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto (e successive modifiche e/o integrazioni);
- affermare che SIAER opera nel quadro di regole certe che tutti i dipendenti devono rispettare.

Il Modello è destinato ai componenti degli Organi sociali ed ai dipendenti, intendendosi come tali tutti coloro che sono legati alla Società da un rapporto di lavoro subordinato ivi compresi i dirigenti, nonché in genere a quanti si trovino a svolgere, in nome o per conto di SIAER, una o più delle attività identificate come a rischio.

Il rispetto del Modello viene garantito anche mediante la previsione di clausole contrattuali che richiamino i collaboratori esterni, consulenti e partner commerciali, al rispetto dei principi contenuti nel presente Modello e nel Codice Etico.

Scopo del Modello è dunque la costruzione di un sistema strutturato e organico di procedure, protocolli, codici comportamentali, nonché di attività di controllo, in linea ed a complemento del Sistema dei controlli già previsti ed esistenti, da svolgersi anche in via preventiva (c.d. controllo *ex ante*) volto a prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto.

In particolare, mediante l'individuazione delle "aree di attività a rischio" e la conseguente definizione di specifiche procedure, il Modello si propone come finalità quelle di:

- determinare in tutti coloro che operano in nome e per conto di SIAER nelle aree di attività a rischio la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni sul piano penale e amministrativo non solo nei propri confronti, ma anche nei confronti della Società;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da SIAER, in quanto sono assolutamente contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società ispira la propria missione istituzionale;
- consentire all'organizzazione, grazie a un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

5.2 I principi regolatori del Modello

Nella definizione, costruzione ed applicazione del proprio Modello, SIAER osserva i seguenti principi regolatori:

- una chiara e formalizzata assegnazione di poteri e responsabilità, coerente con le mansioni attribuite;
- la separazione delle funzioni, incoraggiando però ed incentivando l'assunzione diretta di responsabilità del proprio operato. Tale principio dovrà comunque consentire la gestione efficiente dell'attività istituzionale;
- la definizione di regole comportamentali idonee a garantire l'esercizio delle attività istituzionali nel rispetto delle leggi, dei regolamenti e dell'integrità del patrimonio della Società;
- la distinzione fra le singole attività istituzionali, ognuna delle quali può vedere l'attivazione di procure, deleghe e procedure.

In particolare il sistema delle deleghe prevede che:

- le deleghe siano coerenti con la posizione organizzativa ed aggiornate in conseguenza a variazioni organizzative;
- in ogni delega siano specificati i poteri del delegato ed il soggetto cui il delegato riporta;
- i poteri specificati nella delega siano allineati e coerenti con gli obiettivi della Società;

- il delegato possieda autonomia decisionale e di spesa adeguati alla funzione ed ai compiti conferiti.

Il sistema delle procure prevede che:

- le procure siano assegnate a soggetti provvisti di delega interna;
- le procure descrivano i poteri conferiti e ove necessario siano accompagnate da una comunicazione che illustri i limiti di estensione, fermi restando i vincoli di budget;
- le procure siano assegnate a persone fisiche.

Il sistema delle procedure prevede che:

- sia garantita, ove possibile, l'oggettività dei processi decisionali (ad esempio con la definizione di criteri oggettivi di selezione e valutazione del personale);
- sia assicurata la tracciabilità delle operazioni (sia legate alle attività operative che a quelle di controllo) volta a garantire che ogni operazione, transazione e/o azione sia verificabile, documentata, coerente e congrua.

Punti cardine del Modello sono, oltre ai principi già indicati:

- l'attività di diffusione a tutti i livelli della Società delle regole comportamentali e delle procedure istituite;
- la mappatura delle aree di attività a rischio, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati previsti da D. Lgs. 231/01;
- l'individuazione delle aree di attività ove la proceduralizzazione necessaria a prevenire i reati sia assente o insufficiente e la conseguente individuazione di piani di azione necessari affinché anche tali aree giungano ad un livello di rischio-reato "accettabile";
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di controllo sull'efficace e corretto funzionamento del Modello;
- la verifica dei comportamenti, nonché del funzionamento del Modello con conseguente aggiornamento periodico (controllo ex post).

5.3 Composizione del Modello

Il Modello Organizzativo di SIAER è così strutturato:

- 1. Modello di organizzazione e gestione**, documento che descrive i principi regolatori, gli aspetti generali ed alcuni aspetti puntuali riferiti ad elementi operativi correlati al decreto (es. Organismo di Vigilanza e Controllo, sistema sanzionatorio, ecc.);
- 2. Codice Etico**, documento che illustra i valori-guida della attività, raccomandando, promuovendo o vietando determinati comportamenti, il codice etico prevede divieti e prescrizioni in relazione ai reati considerati;
- 3. Analisi del rischio**, documento che descrive le attività all'interno di ogni processo, l'esposizione a rischio (declinata per tipologia specifica di reato) ed i controlli suggeriti a seguito della valutazione;
- 4. Rapporti con la P.A.**, documento che ha lo scopo di fornire ai destinatari informazioni utili a scongiurare la commissione di reati derivanti da rapporti con la Pubblica Amministrazione, ovvero le fattispecie previste dagli articoli 24, 25 e 25-*novies* del D.Lgs. 231/2001;
- 5. Gestione della documentazione**, documento che descrive modalità e responsabilità di gestione dei documenti e dei dati previsti dal Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/2001;
- 6. Approvvigionamenti**, documento che ha lo scopo di descrivere attività e responsabilità legate al processo di gestione degli approvvigionamenti di beni e affidamento di incarichi professionali, nonché alle attività di selezione, qualifica e monitoraggio dei fornitori.

5.4 Costruzione del Modello

Secondo le prescrizioni del D.Lgs. 231/2001 l'attività di creazione del Modello di organizzazione e gestione e la sua implementazione è stata articolata nelle seguenti fasi:

– identificazione dei processi e delle relative interazioni

L'attività di identificazione dei processi (sia direttamente connessi alle attività istituzionali svolte, che di supporto) ha permesso di stabilire la sequenza e le interazioni:

- Processi di Realizzazione delle Attività istituzionali

- Consiglio di Amministrazione

- Presidente

- Processi di Supporto

- Amministrazione

- Gestione dell'infrastruttura IT;

- Gestione della Salute e Sicurezza sul Lavoro

- **identificazione delle attività a rischio**

durante tale fase sono state condotte alcune interviste, raccolte di documenti ed analisi dei dati relativi a tutti i processi dell'organizzazione, evidenziando le eventuali attività esposte al rischio di illecito.

Sono state inoltre analizzate le aree riferite alla struttura organizzativa e alle prassi amministrative e gestionali;

- **identificazione ed analisi degli attuali presidi al rischio**

sulla base dei risultati ottenuti, è stato operato il confronto tra le procedure/prassi esistenti e le attività a rischio evidenziate. Al termine dell'attività è stato possibile definire la "gap analysis", ovvero le aree e/o le attività da maggiormente presidiare al fine di garantire l'efficacia del Modello di Organizzazione e Gestione;

- **definizione dei protocolli**

l'attività comporta l'integrazione della documentazione della Società, già esistente, con le attività ed i controlli definiti dal CdA e/o la produzione di documentazione normativa ex novo.

5.5 Rilevazione dei processi sensibili

La mappatura delle attività a rischio reato consente l'identificazione delle attività e dei relativi processi "sensibili" alla possibilità di una condotta delittuosa.

Con riferimento a tali processi risulta assolutamente prioritario che tutti i processi "aziendali" sensibili siano uniformati, ove possibile, ai seguenti principi generali:

a) separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;

b) chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa; tale previsione è significativamente riferibile alla categoria dei dirigenti e funzionari della Società;

c) esistenza di regole comportamentali idonee a garantire l'esercizio delle attività di Società nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio della stessa;

d) tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali che attestino le caratteristiche e le motivazioni dell'operazione ed individuino i soggetti a vario titolo coinvolti nell'operazione (autorizzazione, effettuazione, registrazione, verifica dell'operazione);

e) garantire, ove necessario, l'oggettivazione dei processi decisionali e limitare decisioni "aziendali" basate su scelte soggettive non legate a predefiniti criteri oggettivi (es.: esistenza di criteri oggettivi di valutazione);

f) esistenza e documentazione di attività di controllo e supervisione, compiute sulle transazioni "aziendali";

g) esistenza di meccanismi di sicurezza anche informatici che garantiscano un'adeguata protezione/accesso ai dati e ai beni della Società, il tutto tuttavia, tenendo conto delle dimensioni organizzative e della particolare attività svolta da questa.

Quest'ultima, infatti, sin dalla sua costituzione, ha tra i suoi obiettivi di operare con una sempre maggiore efficacia ed efficienza, utilizzando procedure di gestione delle attività per processi, ed è sensibile all'esigenza di mantenere la necessaria flessibilità gestionale e di garantire, al contempo, il più rigoroso adeguamento ai dettami del Decreto.

In questa direzione, la Società ha ritenuto opportuna l'attivazione di un processo "virtuoso" finalizzato all'adeguamento ed integrazione, ove necessario, di alcuni protocolli specifici per la regolamentazione delle attività relative ai processi strumentali individuati.

Essi rispondono, tra l'altro, all'esigenza di documentare e rendere verificabili le varie fasi del processo decisionale, onde consentirne la tracciabilità.

I risultati dell'attività di mappatura, hanno consentito di:

1. identificare le unità organizzative che, in considerazione dei compiti e delle responsabilità attribuite, potrebbero potenzialmente essere coinvolte nelle attività "a rischio reato";
2. individuare le principali fattispecie di rischio/reato;
3. delineare le possibili modalità di realizzazione dei comportamenti illeciti.

5.6 Attività sensibili per SIAER

Alla luce dell'Analisi di rischio dell'organizzazione, svolta ai fini della predisposizione del presente Modello, si considerano potenzialmente rilevanti per SIAER i reati presupposto di cui agli artt. 24, 24-bis, 24-ter, 25, 25-ter, 25-septies, 25-octies, 25-decies e 25-quinquiesdecies del Decreto, ovvero:

- reati commessi nei rapporti con la P.A. (artt. 24 e 25);
- reati informatici (24-bis);
- delitti di criminalità organizzata (24-ter);
- corruzione e concussione (25);
- reati societari (art. 25-ter),
- reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (25-septies);
- ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies);
- reato di falsità nelle dichiarazioni rese all'autorità giudiziaria (art. 25-decies);
- reati tributari (art. 25-quinquiesdecies).

Per contro la Società non risulta significativamente esposta, al fine di trarne beneficio, alla commissione degli altri reati presupposto, previsti dal Decreto, ovvero: delitti di criminalità organizzata (24-ter); reati di falsità in monete, carte di pubblico credito, valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis), delitti contro l'industria ed il commercio (art. 25-bis 1), delitti in materia di terrorismo e di eversione dell'ordine democratico (art. 25-quater), mutilazione degli organi genitali femminili e delitti contro la personalità individuale (artt. 25-quater 1 e quinquies), reati di abuso di mercato (art. 25 sexies), delitti in materia di violazione del diritto d'autore (25-novies), reati ambientali (art. 25-undecies), impiego di lavoratori stranieri privi di permesso di soggiorno o con permesso scaduto (art. 25-duodecies), delitti di razzismo e xenofobia (art. 25-terdecies), frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies), reati di contrabbando (art. 25-sexiesdecies) e infine i reati transnazionali.

Le aree e/o processi nell'ambito dei quali i predetti reati possono essere commessi, per questo considerati sensibili, sono:

- Consiglio di Amministrazione
- Presidente
- Amministrazione
- Gestione dell'infrastruttura IT
- Gestione della Salute e Sicurezza sul Lavoro.

6 L'esposizione al Rischio

6.1 Premessa metodologica

I processi definiti ed individuati possono essere esposti al rischio di commissione dei reati previsti dal D.Lgs. n. 231/2001 secondo tre modalità distinte:

- esposizione diretta, se l'esecuzione delle attività all'interno del processo sono di per se stesse esposte al rischio di commissione di illecito. Ad esempio: l'utilizzo di fondi pubblici, o di provenienza pubblica, o il rapporto con le Autorità di Vigilanza (anche sotto forma di monitoraggio), comportando un contatto diretto con la Pubblica Amministrazione, espone il personale incaricato direttamente ai reati di truffa, corruzione o indebita percezione di fondi;
- esposizione strumentale, se il processo di per se pur non essendo esposto a rischio di illecito, lo è il suo risultato. Ad esempio: l'assunzione di dipendenti legati a figure della Pubblica Amministrazione può costituire la "dazione" attraverso la quale si perfeziona il reato di corruzione per un atto dovuto o contrario ai doveri d'ufficio; ovvero la stipula di contratti di consulenza, se effettuata senza particolari attenzioni o cautele, può costituire la modalità attraverso la quale costituire fondi da utilizzare per scopi di natura illecita;
- nessuna esposizione, se l'attività o il processo non presentano una significativa esposizione al rischio di commettere determinate categorie di reati.

In base al tipo ed al grado di esposizione a rischio, ogni processo/attività è regolamentato da specifica documentazione interna: per tutte le aree operative valgono, inoltre, i principi di comportamento contenuti nel Codice Etico.

Nella presente sezione vengono presentati in maniera sintetica, ripartendoli in base ai reati previsti dal decreto, i risultati dell'analisi di rischio condotta, ed i relativi controlli implementati per ridurre il profilo di rischio eventualmente evidenziato.

6.2 I reati contro la P.A.

La definizione di Pubblica Amministrazione

Per Pubblica Amministrazione si intendono tutti gli enti pubblici, territoriali e non, i membri e gli organi interni degli enti, compresi i pubblici funzionari.

Agli effetti della legge penale viene considerato comunemente come "Ente della Pubblica Amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o giuridica in forza di norme di diritto pubblico e di atti autorizzativi. L'art.1, comma 2 del D.Lgs. n. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato. Non tutte le persone fisiche che agiscono nella sfera e in relazione dei suddetti enti sono soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie delittuose previste dal D.Lgs. n. 231/2001.

In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei "pubblici ufficiali" e degli "incaricati di pubblico servizio", distinguendosi, questi ultimi in pubblici impiegati e non.

L'esposizione al rischio

I risultati dell'analisi di rischio conducono ad identificare, nell'ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui la Società risulta maggiormente esposta (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione
- Presidente
- Amministrazione

È il caso di segnalare che i settori degli approvvigionamenti (ordini/contratti con fornitori e soprattutto con professionisti e consulenti) benché non implicino diretto contatto con la Pubblica Amministrazione, possono comportare il rischio di commissione di fatti corruttivi. Ad esempio la stipulazione di un contratto per una prestazione inesistente può costituire il mezzo per far ottenere, direttamente o indirettamente, il prezzo della stessa ad un Pubblico Ufficiale o ad un Incaricato di Pubblico Servizio, ovvero può risultare funzionale per la costituzione di fondi «extracontabili», operazioni queste, dirette alla creazione di dispo-

bilità occulte attraverso l'emissione di fatture per operazioni inesistenti, spostamenti di denaro non giustificati, pagamenti di consulenze mai effettivamente prestate ovvero di valore nettamente inferiore a quello dichiarato.

In ogni caso, e più in generale, è necessario prestare attenzione alla circostanza che, in ogni settore o attività in cui vi siano contatti diretti o indiretti dell'Ente o meglio di soggetti funzionalmente legati ad esso, siano essi apicali o subordinati) con la Pubblica Amministrazione, la stessa appare potenzialmente esposta al rischio di commissione dei reati di cui all'art. 24 e di parte dei reati previsti dall'art. 25 del D.Lgs. 231/2001, rischio che comporta, parallelamente alla responsabilità dell'autore del reato, la responsabilità amministrativa a carico dell'ente sussistendone i presupposti, ai sensi del Decreto in esame.

Una particolare attenzione si pone nelle attività di gestione dei rapporti con le Istituzioni e le Autorità Pubbliche di Vigilanza e di gestione di contenziosi giudiziali e stragiudiziali, oltre che più in generale in tutte le attività sopra elencate.

Assumono inoltre rilievo ai sensi e per gli effetti di cui al D. Lgs. n. 231/2001 le fattispecie di corruzione «impropria», vale a dire di corruzione per un «atto d'ufficio» (art. 318 c.p.) e quello di «istigazione alla corruzione», di cui all'art. 322 c.p.

Con riferimento alla fattispecie prevista dall'art. 317 c.p. (concussione) la stessa appare solo astrattamente ed in linea teorica configurabile: il reato è infatti oggettivamente legato alla qualifica di Pubblico Ufficiale o Incaricato di un pubblico servizio, qualifica estranea a SIAER.

All'art. 25, rubricato “Concussione e corruzione”, dopo la parole “Concussione” sono state inserite, dalla legge 6 novembre 2012, n. 190, le parole “induzione indebita a dare o promettere utilità”. Ciò in quanto è stato introdotto nell'ordinamento l'art. 319 quater del codice penale, che, per l'appunto, punisce con la reclusione da 3 ad 8 anni, salvo che il fatto costituisca più grave reato, *“il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità, è punito con la reclusione fino a 3 anni”*.

In sostanza, con l'entrata in vigore della Legge Anticorruzione, la Società è chiamata a valutare se le nuove fattispecie criminose costituiscono un rischio al quale è esposta la sua attività.

Infatti, nel caso previsto dal “nuovo” art. 319 quater c.p., si deve avere riguardo al fatto che non viene punito solo il pubblico ufficiale o l'incaricato di pubblico servizio che induce qualcuno a dare o promettere indebitamente denaro o altra utilità, ma anche il soggetto che dà o promette denaro o altra utilità, ossia il soggetto che, in un qualche modo, rimane “vittima” della induzione.

Misure di prevenzione

Per prevenire la responsabilità amministrativa, e quindi la conseguente irrogazione della sanzione, è necessario che la Società tenga sotto controllo l'attività connessa al trasferimento di denaro, evitando forme di incasso e pagamento con strumenti non tracciabili (segnatamente limitando al massimo l'uso del denaro contante), onde prevenire la costituzione di fondi neri.

Inoltre, i soggetti abilitati ad effettuare incassi e pagamenti devono essere precisamente individuati, le procedure devono essere definite.

In sostanza, si conferma assolutamente prioritario che tutti i processi aziendali sensibili siano uniformati, ove possibile, ai seguenti principi generali:

- separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- chiara assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
- esistenza di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;

- “proceduralizzazione” delle attività aziendali “a rischio reato”, al fine di:

- a) definire e regolamentare le modalità e tempistiche di svolgimento delle attività medesime;
 - b) garantire la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali che attestino le caratteristiche e le motivazioni dell’operazione ed individuino i soggetti a vario titolo coinvolti nell’operazione (autorizzazione, effettuazione, registrazione, verifica dell’operazione);
- garantire, ove necessario, l’oggettivazione dei processi decisionali e limitare decisioni aziendali basate su scelte soggettive non legate a predefiniti criteri oggettivi;
- esistenza e documentazione di attività di controllo e supervisione compiute sulle transazioni aziendali;
- esistenza di meccanismi di sicurezza anche informatici che garantiscano un’adeguata protezione/accesso ai dati e ai beni aziendali, il tutto tuttavia, tenendo conto delle dimensioni organizzative e della particolare attività svolta da SIAER.

Per quel che riguarda le attività ed controlli implementati al fine di prevenire i reati contro o ai danni della Pubblica Amministrazione, la Società adotta i seguenti controlli/attività:

- a) Il Codice Etico prevede i principi generali di comportamento volti ad evitare la commissione, anche nelle forme del tentativo o sotto qualsiasi forma di atti con natura corruttiva.
- b) Una prassi definita per i rapporti con la Pubblica Amministrazione che regola in particolare la gestione dei rapporti con le Istituzioni e le Autorità Pubbliche di Vigilanza e la gestione delle ispezioni.
- c) Una procedura approvigionamenti beni e servizi, che definisce:
 - i poteri di controllo ed autorizzazione necessari al rilascio dell’ordine al fornitore;
 - i criteri per la scelta dei fornitori;
 - le modalità di controllo della congruità della fornitura.

Nel caso specifico di ricorso a professionisti esterni coinvolti nell’attività commerciale, il rapporto di collaborazione è stato implementato con specifiche clausole di controllo tra cui:

- la dichiarazione sottoscritta di non esser mai stati sottoposto o comunque implicato in procedimenti penali per reati contemplati dal D.Lgs. n. 231/2001;
- la dichiarazione di impegno al rispetto del Codice Etico.

6.3 Induzione a rendere false dichiarazioni all’Autorità Giudiziaria

Questo reato è stato aggiunto tra i reati presupposto con la Legge n. 116/2009.

Il reato in oggetto è rubricato, nel codice penale, tra i reati “contro l’amministrazione della giustizia”, quei reati cioè il cui carattere specifico non li rende come genericamente contemplati tra i reati contro la pubblica amministrazione.

Ed è proprio questo carattere di specialità rispetto ai reati analizzati nel paragrafo precedente che rende la sua analisi separata e successiva rispetto ai reati contro la Pubblica Amministrazione.

L’esposizione al rischio

I risultati dell’analisi di rischio conducono ad identificare e qualificare come diretta l’esposizione al rischio verso il reato in oggetto ogni qual volta la Società sia chiamata come “parte” in un procedimento penale od abbia un qualche interesse nello stesso.

Le seguenti funzioni appaiono singolarmente maggiormente esposte (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione
- Presidente

Misure per la prevenzione

SIAER diffonde e coltiva al proprio interno i principi adottati dal Codice Etico.

6.4 I reati informatici

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” ha apportato significative modifiche al Codice Penale e al D.Lgs. n. 231/2001.

Tra le principali novità si possono segnalare: la eliminazione della diversità nella definizione di "documento informatico" tra il diritto civile e il diritto penale; l'introduzione del delitto di false dichiarazioni al Certificatore (art. 495-bis c.p.); la profonda modifica dell'art. 615-quinquies (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico); la rivisitazione del danneggiamento di dati, programmi, e dei sistemi informatici, anche di pubblica utilità, con l'introduzione della punibilità a querela del danneggiamento di dati "privati"; l'introduzione di una nuova fattispecie di frode informatica, commessa dal soggetto che presta servizi di certificazione di firma elettronica; l'estensione ai reati "informatici" della responsabilità amministrativa degli enti, di cui al D.Lgs. n. 231/2001.

L'esposizione al rischio

I risultati dell'analisi di rischio conducono ad identificare, nell'ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui SIAER risulta maggiormente esposto (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione
- Gestione dell'infrastruttura IT

I reati di cui potenzialmente sussiste il rischio di commissione nell'ambito dell'attività della Società e quindi assumono rilievo ai sensi e per gli effetti di cui al D.Lgs. n. 231/2001, sono le fattispecie di "accesso abusivo ad un sistema informatico o telematico" (art 615 ter c.p.) e di "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.).

Misure per la prevenzione

Le attività sensibili che vengono svolte all'interno di SIAER sono le seguenti:

- Gestione dell'attività di manutenzione dei sistemi esistenti
- Gestione dell'attività di elaborazione dei dati
- Gestione della sicurezza informatica sia a livello fisico che a livello logico.

SIAER implementa tutte le attività correlate alla gestione della propria infrastruttura IT, che prevede in particolare:

- a) limitazioni per gli utenti e conseguente definizione come esclusive prerogative ("privilegi") dell'amministratore;
- b) individuazione dei controlli sulla configurazione hardware e software delle macchine;
- c) configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne;
- d) gestione e protezione dei backup dei dati;
- e) elaborazione di un "disaster recovery plan" a tutela del patrimonio informativo.

6.5 Delitti in materia di violazioni della Legge sul diritto d'autore

La Legge n. 99 del 23 luglio 2009 ha introdotto nei reati presupposto della responsabilità amministrativa degli enti alcune norme penali contenute nella legge sul diritto d'autore (L. 633/41).

In via generale è possibile affermare che questi articoli colpiscono la riproduzione e duplicazione di opere dell'ingegno.

Tali, ai sensi dell'art 2 punto 8 della L. 633/41, sono anche: "i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso".

L'esposizione al rischio

I risultati dell'analisi di rischio conducono ad identificare, nell'ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui la Società può teoricamente risultare esposto (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione

- Gestione infrastruttura IT

La descrizione delle opere dell'ingegno comprese nella protezione è data dall'art. 2 della L. 633/41 che in particolare tutela:

- 1) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso;
- 2) le banche dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto;

Misure per la prevenzione

SIAER non ritiene di essere particolarmente esposto a questo tipo di rischio.

Ad ogni buon conto implementa tutte le attività correlate alla gestione della propria infrastruttura IT, che prevede in particolare:

- a) limitazioni per gli utenti e conseguente definizione come esclusive prerogative ("privilegi") dell'amministratore;
- b) individuazione dei controlli sulla configurazione hardware e software delle macchine;
- c) implementazione di un filtro Proxy controllato dall'Amministratore (in conformità alla normativa Privacy).

Le attività sensibili sono correlate alla detenzione, utilizzo o messa in commercio di supporti o altri strumenti informatici per i quali sia prescritto il contrassegno SIAE.

I protocolli preventivi consistono nel rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ed in particolare l'informazione agli utenti che è vietato installare software sconosciuti, illeciti e non autorizzati dai responsabili dell'Area di appartenenza.

6.6 I reati di ricettazione, riciclaggio, autoriciclaggio e impiego di beni di provenienza illecita

L'art. 3 comma 5 della legge 15 dicembre 2014, n. 186 ha introdotto nel nostro ordinamento il nuovo reato di autoriciclaggio, attraverso l'inserimento nel codice penale dell'art. 648 *ter* 1.

Tale nuovo delitto è stato inserito nel novero dei "reati presupposto" di cui al D.Lgs. n. 231/2001, il cui art. 25-octies è stato così riformulato:

"Art. 25-octies. (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio) 1. In relazione ai reati di cui agli articoli 648, 648-bis, 648-ter e 648-ter.1 del codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote. 2. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore a due anni. 3. In relazione agli illeciti di cui ai commi 1 e 2, il Ministero della giustizia, sentito il parere dell'UIF, formula le osservazioni di cui all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231".

L'art. 648 *ter* 1 c.p. prevede la pena della reclusione da due a otto anni e la multa da euro 5.000 a euro 25.000 per chi, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione del delitto, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Le nuove disposizioni sono in vigore dal 1° gennaio 2015.

L'esposizione al rischio

La particolare struttura del reato di autoriciclaggio rende del tutto peculiare il rapporto tra il medesimo rea-

to ed il D.Lgs. n. 231/2001.

Se, infatti, l'art. 648 *ter.* 1 c.p., dal punto vista penale, trova applicazione nei confronti di chiunque investa il provento derivante dalla precedente commissione di un qualsiasi delitto non colposo, dalla prospettiva degli enti, l'inserimento del delitto in parola nell'elenco dei reati presupposto di cui al D.Lgs. n. 231/2001, apre la strada ad una serie di reati, formalmente esclusi dallo stesso decreto.

Partendo, infatti, dal presupposto che l'autoriciclaggio si configura se sussistono contemporaneamente le tre seguenti condizioni:

- 1) sia creata o si sia concorso a creare – attraverso un primo delitto non colposo – una provvista consistente in denaro, beni o altre utilità;
- 2) si impieghi la predetta provvista, attraverso un comportamento ulteriore e autonomo, in attività imprenditoriali, economiche e finanziarie;
- 3) si crei un concreto ostacolo alla identificazione della provenienza delittuosa della anzidetta provvista.

Ne consegue che tutti i delitti non colposi, capaci di generare profitto, rappresentano un potenziale pericolo per la Società, dal momento che la loro consumazione costituisce il primo passo per la consumazione del delitto di autoriciclaggio.

E' del tutto evidente, quindi, che anche in ambito aziendale la prevenzione del reato di autoriciclaggio deve essere incentrata sulla prevenzione di quei delitti non colposi, in grado di generare un profitto investibile.

Il nuovo reato di autoriciclaggio si presenta come fattispecie plurioffensiva, volta a consolidare la lesione del patrimonio della vittima del reato presupposto e di ledere anche l'amministrazione della giustizia e l'economia pubblica nel suo insieme.

Chi effettua autoriciclaggio, con investimenti e acquisti di vario genere, impedisce o rende più difficoltose le operazioni di ristoro della vittima, inquina il credito e l'andamento dei prezzi e, in definitiva, tutto il sistema delle relazioni economiche.

La disponibilità "in proprio" di mezzi economici di provenienza illecita (come tali non soggetti a imposizione fiscale, svincolati da qualsiasi controllo e generati attraverso modalità a loro volta alterative della concorrenza), ne permette l'impiego verso ulteriori attività illecite, oppure direttamente in impieghi che pongono l'utilizzatore in una condizione di privilegio rispetto ai relativi competitori, rispettosi delle regole.

In quest'ottica l'autoriciclaggio rappresenta un'ulteriore diversa condotta, caratterizzata da un proprio specifico disvalore e, proprio in quanto tale, autonomamente punibile.

La condotta tipica del reato si atteggia secondo tre diversi modelli fattuali:

- sostituzione ;
- trasferimento;
- impiego, in attività economiche o finanziarie, del denaro, dei beni o delle altre utilità, provenienti dalla commissione del delitto non colposo.

Per SIAER l'attinenza alle sopra evidenziate fattispecie potrebbe ad esempio ravvisarsi nell'ipotesi di utilizzazione di capitali illeciti per la gestione di un affare, o nell'utilizzo di capitali frutto di evasione fiscale per compiere operazioni apparentemente lecite, quali l'acquisto di partecipazioni societarie o il finanziamento di iniziative economiche. Viceversa, non è ravvisabile l'interesse o il vantaggio per la Società nell'ipotesi in cui il soggetto apicale o il dipendente acquistino beni che non abbiano alcun legame con l'esercizio dell'impresa in cui operano. Lo stesso può dirsi per l'impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale. Per fare alcuni esempi:

- la Società impiega in investimenti finanziari, con modalità tali da occultarne la provenienza, la liquidità de-

rivante dalla non veritiere esposizione delle passività nel bilancio;

- la Società impiega i proventi derivanti da una truffa perpetrata ai danni dello Stato in operazioni con controparti estere in modo tale da occultarne la provenienza delittuosa;
- la Società trasferisce i proventi derivanti dall'omesso versamento delle ritenute previdenziali su conti correnti aperti in Paesi Black List in modo tale da occultarne la provenienza delittuosa;
- la Società riceve indebitamente pagamenti preferenziali da una controparte in stato di decozione e li impiega in attività finanziarie in modo da occultarne la provenienza delittuosa.

Va evidenziato che l'impiego in attività economico/imprenditoriali di somme provenienti da risparmi fiscali illeciti e/o fraudolenti è astrattamente in grado di integrare il delitto di autoriciclaggio.

Nel caso di reati tributari, che per la loro natura producono normalmente un vantaggio economico, la possibilità di commettere il nuovo delitto di autoriciclaggio è particolarmente elevata, stante la possibile ricorrenza delle condotte previste dalla nuova norma e cioè la sostituzione, trasferimento o impiego in attività economiche e finanziarie del denaro o delle utilità, in modo da ostacolarne concretamente l'identificazione della provenienza delittuosa.

I delitti tributari, la cui consumazione costituisce un potenziale pericolo per la successiva contestazione dell'autoriciclaggio, sono, quindi, i seguenti:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- dichiarazione fraudolenta mediante altri artifici;
- dichiarazione infedele;
- omessa dichiarazione;
- emissione di fatture o altri documenti per operazioni inesistenti;
- occultamento o distrazione di documenti contabili;
- omesso versamento di ritenute certificate;
- omesso versamento di IVA;
- indebita compensazione;
- sottrazione fraudolenta al pagamento di imposte.

I risultati dell'analisi di rischio conducono ad identificare, nell'ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui la Cassa Edile risulta maggiormente esposta (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione
- Presidente
- Amministrazione

Misure per la prevenzione

La Società ritiene di non essere particolarmente esposta a questa tipologia di reati. Al fine di rendere SIAER esente da responsabilità anche per la commissione dei reati in esame, mantiene un rigoroso controllo sulla rispondenza dei documenti fiscali utilizzati (sia quelli emessi che quelli ricevuti) con la effettiva attività svolta, incrociando i dati contabili con quelli finanziari (flussi di cassa).

Inoltre, al fine di prevenire la commissione dei reati di ricettazione, riciclaggio e impiego di beni di provenienza illecita, la Società adotta i seguenti controlli/attività:

- a) una procedura approvvigionamenti beni e servizi che definisce:
 - i poteri di controllo ed autorizzazione necessari al rilascio dell'ordine al fornitore;
 - i criteri per la scelta dei fornitori;
 - le modalità di controllo della congruità della fornitura.

- b) dichiarazione da parte dei fornitori non occasionali di impegno al rispetto di quanto prescritto nel Codice Etico;
- c) obbligo di pagamento esclusivamente a seguito della ricezione di documenti fiscalmente validi e se vi è identità tra il soggetto che ha fornito il bene e il servizio è il soggetto che riceverà il pagamento.

6.7 I reati societari

La materia dei reati societari è stata in questi ultimi anni oggetto di particolare interesse. Diversi sono stati gli interventi normativi susseguitisi a poca distanza che la riguardano, dapprima con la sostanziale riforma dei reati societari ad opera del D. Lgs. 61/2002, successivamente con la Legge 18 aprile 2005, n. 62 (c.d. Market Abuse) di recepimento della Direttiva comunitaria 2003/6/CE che ha modificato il Testo Unico della Finanza e da ultimo con la Legge 262/2005 (c.d. Tutela del Risparmio) che ha inciso per lo più sulle sanzioni.

Ulteriori modifiche sono state apportate dal D. Lgs. 27 gennaio 2010, n. 39, che con l'art. 37, ha abrogato l'art. 2624 del c.c. (falsità nelle relazioni o nelle comunicazioni delle società di revisione) ad oggi comunque previsto nell'art. 27 dello stesso D. Lgs. 39/2010 e modificato l'art. 2625 del c.c. (impedito controllo).

La tipologia dei reati in oggetto, che vale la pena di anticipare essere reati propri - hanno cioè come autori soggetti qualificati - a destato e desta particolare interesse sia per la frequenza nella loro commissione sia per la molteplicità degli interessi che si vuole proteggere: la tutela dell'integrità del patrimonio aziendale, la tutela dei soci e dei creditori, la concorrenza leale, la trasparenza dei mercati finanziari, la tutela degli investitori non istituzionali e dell'intero mercato, ecc.

Infine, all'art. 25-ter, che si occupa dei "Reati societari", dopo la lettera s) l'art. 1, comma 77 della legge 6 novembre 2012, n. 190 ha aggiunto la lettera s-bis), che prevede che per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'art. 2635 del codice civile, si applichi la sanzione pecuniaria da 200 a 400 quote.

Per capire la disposizione, va riferito che l'art. 2635 c.c. è stato integralmente sostituito, ed è stato rubricato come "Corruzione tra privati"; il terzo comma, nella nuova formulazione, recita: *"Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste"*. Le persone indicate sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori; le pene sono da uno a tre anni di reclusione, che si riducono ad un massimo di un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza dei soggetti prima indicati. La condotta criminosa consiste nel compiere od omettere atti in violazione degli obblighi del proprio ufficio o degli obblighi di fedeltà, cagionando nocimento alla società, a fronte della dazione o della promessa di denaro o altra utilità.

L'esposizione al rischio

Dall'analisi effettuata è emerso che le aree alle quali bisogna prestare maggiore attenzione, sia singolarmente che complessivamente considerate, e nel cui ambito potrebbero astrattamente verificarsi ipotesi di reati societari (come più dettagliatamente di seguito) risultano quelle interessate, preposte o comunque collegate alle seguenti attività:

- la gestione di informazioni inerenti la situazione economica, patrimoniale e finanziaria di SIAER;
- la gestione dei rapporti con le Autorità di vigilanza;
- la gestione delle attività economiche, patrimoniali e finanziarie e le relative rendicontazioni contabili;
- la gestione dei rapporti con gli organi societari.

Misure per la prevenzione

Dalle sopra esposte considerazioni e pur considerando che dall'analisi dei processi non sono emerse criticità particolari che vanno a toccare nello specifico le attività di natura gestionale-contabile-amministrativa, sono comunque adottati alcuni ulteriori accorgimenti da adottare in via preventiva per abbassare ulteriormente la soglia di rischio agendo in particolare sulla sfera relativa alla gestione dei rapporti con le autorità di

vigilanza ed alle inter-relazioni tra gli organi sociali e di controllo già previsti dalla legislazione vigente e più in generale dalla documentazione aziendale, in particolare sono adottati:

- a) una specifica procedura per la gestione dei rapporti con le Istituzioni e le Autorità Pubbliche di Vigilanza e la relativa gestione delle ispezioni;
- b) l'obbligo di incontri periodici, singoli o collegiali, tra l'OdV, l'Organo amministrativo e l'Organo di Revisione e l'obbligo di trasmissione con congruo anticipo all'OdV ed all'Organo di Revisione di tutta la documentazione afferente argomenti all'ordine del giorno dell'Assemblea o, comunque, da sottoporre agli stessi;
- c) la definizione di specifiche modalità di interazione con l'Organo di Revisione in termini sia di trasmissione e comunicazione dei dati al revisore incaricato di svolgere l'attività di controllo, sia di presa visione della documentazione redatta dall'Organo di Revisione nello svolgimento della propria attività.

6.8 Reati di criminalità organizzata

La Legge 15 luglio 2009, n. 94 "Disposizioni in materia di sicurezza pubblica" (con l'art. 2, c. 29) ha introdotto l'art. 24-ter prevedendo l'estensione della responsabilità degli enti anche agli illeciti dipendenti dai delitti di criminalità organizzata commessi nel territorio dello Stato e privi del requisito della transnazionalità. L'inclusione dei delitti in oggetto tra i reati presupposto della responsabilità amministrativa degli enti è stata voluta quale ulteriore (per quanto residuale) strumento di lotta alla criminalità organizzata, prima ristretta alle sole fattispecie di reati transnazionali inserite nel corpus del D.Lgs. n. 231/01 dall'art. 10 della Legge 146/06 "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001" sulla lotta alla criminalità organizzata transnazionale.

L'art. 24-ter sanziona i c.d. reati associativi che vanno dal delitto di associazione per delinquere (art. 416 c.p., ad eccezione del sesto comma) all'associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309) e che per loro natura trovano difficile collocazione nell'attività di SIAER né tantomeno ricollegabili all'interesse o vantaggio di esso.

Ciò nonostante si è ritenuto opportuno condurre una analisi sui processi della Società in considerazione, ed è questo l'aspetto che interessa, che sono delitti di criminalità organizzata tutti i delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p., cioè quei reati commessi "avvalendosi della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri", ovvero commessi al fine di agevolare l'attività delle associazioni illecite. Quest'ultima previsione assume particolare rilievo, atteso che fa riferimento a fenomeni di agevolazione che possono perfezionarsi a mezzo di innumerevoli, in quanto non tipizzate, condotte.

L'art. 24 ter prevede quindi la possibile insorgenza della responsabilità dell'Ente, in presenza della commissione di un qualsiasi delitto commesso per agevolare in qualunque modo e sotto qualsiasi forma l'attività delle associazioni criminali

Misure per la prevenzione

Per quanto SIAER ritenga minimo il rischio di commissione dei reati in oggetto, anche in ottica di massima trasparenza, ha deciso di adottare la seguente misura di prevenzione: sottoscrizione da parte delle aziende con le quali mantiene rapporti di partnership, di una autodichiarazione di non aver subito condanne per i reati previsti dall'art. 24 ter del Decreto.

Inoltre, vengono attivati dei protocolli specifici atti a rendere oltremodo difficoltosa la commissione dei reati presupposto

Le procedure individuate, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. le principali attività del processo finanziario riguardano: a) la gestione dei flussi di cassa; b) tutte le attività dei singoli processi devono prevedere un sistema di autorizzazioni, deleghe e separazioni dei compiti (Consiglio di Amministrazione, Amministrazione);
2. finanziamenti; c) gli investimenti finanziari;
3. compiti precisi di autorizzazione e responsabilizzazione per le operazioni di contabilizzazione (Amministrazione);
4. strumenti di revisione e di convalida, periodica, dei saldi dei conti del piano dei conti afferenti gli elementi monetari, finanziari e patrimoniali (Amministrazione);
5. sistemi rigorosi di autorizzazione e di documentazione per l'accesso ai valori monetari, ai titoli patrimoniali mobiliari e immobiliari e, in generale, alle informazioni finanziarie (Amministrazione);
6. con riferimento alla gestione dei flussi di cassa occorre distinguere tra: 1) gestione per pagamenti; 2) gestione per incassi; 3) gestione banche;
7. per la gestione dei flussi di cassa per pagamenti occorre: registrazione e periodico aggiornamento di uno scadenziario analitico delle posizioni debitorie; autorizzazione al pagamento tramite un sistema di deleghe e poteri di firma, tale per cui non ci sia commistione tra chi impegna l'impresa all'acquisto e chi decide il pagamento delle forniture e delle prestazioni; verifica dell'anagrafica fornitori; ricorso limitato al pagamento in contanti o tramite assegni; obbligo di emissione di assegni "non trasferibili"; custodia dei libretti di assegni in luoghi ad accesso controllato; custodia della password per effettuare pagamenti "home banking"; controllo dell'impossibilità da parte degli operatori di variare le coordinate bancarie lavorando "home banking"; controlli fisici periodici della consistenza delle casse; valutazione dell'efficienza e della regolarità delle operazioni di verifica effettuate sulle casse, con riferimento agli adempimenti formali, di legge e contabili; verifiche di regolarità, adeguatezza, completezza ed aggiornamento della documentazione contabile ed extracontabile (tutte queste operazioni sono a carico dell'Amministrazione);
8. per la gestione dei flussi di cassa per incassi occorre: registrazione e periodico aggiornamento di uno scadenziario analitico delle posizioni creditorie; esistenza di documentazione giustificativa per ogni incasso; predisposizione di un protocollo di registrazione dei valori pervenuti; adozione di misure di controllo in caso di ricorrenti incassi parziali; obbligo di versamento degli incassi in contanti entro le ventiquattro ore successive; un controllo periodico dei documenti attestanti l'incasso per contante al fine di consentire che tutte le operazioni siano state rilevate; riconciliazione tra registro dei valori pervenuti e risultanze delle registrazioni di cassa; verifiche di regolarità, adeguatezza, completezza e aggiornamento della documentazione contabile ed extracontabile; accertamento della corretta contabilizzazione e dell'effettivo versamento nei fondi dell'impresa di tutti i valori ricevuti (tutte queste operazioni sono a carico dell'Amministrazione);
9. per la gestione banche occorre: che le operazioni di apertura, utilizzo e controllo dei conti correnti siano sempre regolati da una specifica procedura in coerenza con la politica creditizia dell'impresa, sulla base di adeguate separazioni dei compiti e della regolarità contabile; l'autorizzazione all'apertura e chiusura di conti correnti da parte della funzione delegata e definizione dei poteri di firma; la verifica periodica delle condizioni negoziate con le banche e gli altri istituti di credito; il periodico esame dei movimenti effettuati sui conti correnti; le periodiche riconciliazioni bancarie effettuate da funzione diversa di chi ha operato sui conti correnti e da chi ha contabilizzato (Amministrazione);
10. per la gestione dei finanziamenti occorre: stabilire ruoli, competenze e responsabilità relativamente alla definizione dei fabbisogni finanziari a medio e lungo termine e delle forme e fonti di copertura; una politica finanziaria organica; una valutazione economica comparativa per la selezione delle più idonee fonti di finanziamento; la corretta rappresentazione a bilancio delle operazioni finanziarie a medio e lungo termine; accertare la regolare ed economica stipula di contratti per l'acquisizione dei finanziamenti a medio e lungo termine; l'autorizzazione da parte del Consiglio di Amministrazione

per l'assunzione di passività a medio e lungo termine; il controllo delle condizioni applicate e dei vincoli di garanzia; la verifica del corretto impiego delle fonti; le riconciliazioni periodiche tra le risultanze contabili e i piani di ammortamento; il controllo delle garanzie rilasciate e delle loro eventuali cancellazioni (Amministrazione);

11. per la gestione degli investimenti finanziari occorre: che gli investimenti finanziari a medio e lungo termine siano preventivamente autorizzati dal Consiglio di Amministrazione, in aderenza agli indirizzi politici e strategici ed attuati avvalendosi, anche all'estero, quando possibile, di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di stabilità conforme a quella adottata negli stati membri della UE; l'analisi e la valutazione degli investimenti; la verifica del rispetto delle norme di legge e statutarie; la deliberazione del Consiglio di Amministrazione che autorizzi l'investimento; l'adozione di idonee scritture analitiche, contabili ed extracontabili, per verificare nel tempo la valutazione iniziale; la custodia dei titoli in luoghi protetti e controllati con accesso limitato alle funzioni autorizzate; la corretta ed economica gestione dei titoli rappresentativi degli investimenti finanziari di breve, medio e lungo termine nel rispetto delle norme di legge e delle regole del mercato mobiliare (Amministrazione);
12. obbligo di tracciabilità dei flussi finanziari nei confronti della P.A. ai sensi della legge 13 agosto 2010 n. 136.

6.9 I reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

In data 1 aprile 2008 è stato approvato dal Consiglio dei Ministri il Decreto attuativo della Legge 123 del 3 agosto 2007 riferita alla sicurezza nei luoghi di lavoro; tale Decreto cita all'articolo 30 i Modelli di Organizzazione e Gestione, affermando che:

1. Il Modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto Legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria;
- e) alle attività di informazione e formazione dei lavoratori;
- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2. Il Modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

3. Il Modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

4. Il Modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del Modello organizzativo devono essere adottati, quando siano scoperte viola-

zioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

L'esposizione al rischio

La definizione delle attività sensibili ai sensi del Decreto è stata effettuata considerando le attività entro le quali si possono verificare gli infortuni e quelle nell'ambito delle quali può essere commesso il reato di violazione colposa della normativa e delle misure di prevenzione a seguito della quale si sia verificato un evento dannoso penalmente rilevante. In considerazione di tale dicotomia si possono distinguere:

- a) le attività a rischio infortunio e malattia professionale evidenziate nel Documento di Valutazione dei Rischi, ed intese come le attività dove potenzialmente si possono verificare gli eventi dannosi;
- b) le attività a rischio reato, intese come le attività che possono potenzialmente originare i reati richiamati dall'art. 25-septies del Decreto, in quanto una loro omissione od inefficace attuazione potrebbe integrare la responsabilità di SIAER, nell'ambito della gestione delle risorse e nell'ambito della realizzazione del servizio.

I risultati dell'analisi di rischio conducono ad identificare, nell'ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui la Società risulta maggiormente esposta (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione
- Ufficio Risorse Umane

Misure per la prevenzione

Il presente Modello non intende sostituirsi alle prerogative e responsabilità di legge disciplinate in capo ai soggetti individuati dal D.Lgs. n. 81/2008. Esso costituisce, invece, un presidio ulteriore di controllo e di verifica dell'esistenza, efficacia ed adeguatezza, della struttura del sistema di gestione per la tutela della salute e sicurezza sui luoghi di lavoro.

Il primo presupposto del Modello, al fine della prevenzione degli infortuni sui luoghi di lavoro, è dato dal rispetto di alcuni principi e dalla tenuta di alcuni comportamenti che dovranno essere osservati da parte di tutti i dipendenti, nonché da tutti i soggetti esterni che si trovino legittimamente presso i locali della Società, in particolare:

- rispettare la normativa e le procedure aziendali interne per la protezione individuale e collettiva, esercitando ogni opportuno controllo ed attività idonee a salvaguardare le salute e la sicurezza propria, dei colleghi e del personale esterno, eventualmente presente sui luoghi di lavoro;
- non adottare comportamenti imprudenti quanto alla salvaguardia della propria salute e sicurezza;
- utilizzare correttamente i macchinari, le apparecchiature, ed ogni altro mezzo o attrezzature di lavoro;
- utilizzare in modo appropriato e corretto i dispositivi di sicurezza e di protezione messi a disposizione;
- segnalare, senza indugio, in ragione delle responsabilità attribuite le anomalie, nonché le eventuali altre situazioni di pericolo di cui si viene a conoscenza;
- sottoporsi ai controlli sanitari previsti;
- sottoporsi agli interventi formativi previsti.

La Società, in forza di tali principi, per quanto non registri una significativa frequenza di infortuni, ha provveduto a:

- adottare come parte integrante di questo Modello, il "sistema" degli adempimenti aziendali nascenti dal D.Lgs. 81/2008;
- individuare una serie di raccordi tra i soggetti richiamati dalla normativa speciale in materia di salute e sicurezza sui luoghi di lavoro ed il sistema di controllo ai sensi del D. Lgs. n. 231/2001;
- affidare specificatamente all'Organismo di Vigilanza il potere/compito di monitorare l'attività aziendale nonché la funzionalità dell'intero Sistema di Gestione preventivo in materia di salute e sicurezza;
- qualificare come obbligo di informazione tutte le segnalazioni su possibili carenze od inadeguatezze dei luoghi o delle attrezzature da lavoro, non prontamente riscontrate dalle funzioni competenti.

6.10 I reati ambientali

Il D.Lgs. 7 luglio 2011, n. 121, recante “Attuazione della Dir. n. 2008/99/CE sulla tutela penale dell'ambiente, composto da cinque articoli, ed entrato in vigore il 16 agosto 2011, conclude, almeno per il momento, la questione del recepimento della direttiva comunitaria in materia di tutela penale dell'ambiente, varata dal legislatore comunitario per rafforzare la disciplina di contrasto contro i fenomeni di aggressione all'ambiente considerato nel suo complesso.

Trattasi delle fattispecie relative all'uccisione, distruzione, prelievo o possesso di esemplari di specie animali e vegetali selvatiche protette (art. 727-bis c.p.) nonché alla distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.).

Indubbiamente la più rilevante novità introdotta dal D.Lgs. n. 121/2011 è quella dell'inserimento di alcuni reati ambientali nei cataloghi dei reati presupposto della responsabilità degli enti previsti dal D.Lgs. n. 231/2001.

Il legislatore delegato, per configurare le ipotesi di responsabilità degli enti per illeciti ambientali, ha selezionato alcune figure di reato già previste dall'ordinamento penale, nonché quelle introdotte all'uopo dalla novella (e cioè quelle di cui agli artt. 727-bis e 733-bis, c.p.) e ritenute corrispondere al catalogo richiamato dalla normativa sovranazionale alla quale la legge delega aveva pedissequamente rinviato in proposito.

E' stato così inserito all'art. 25-undecies, D.Lgs. n. 231/2001, un nuovo catalogo di reati presupposto della responsabilità degli enti.

Misure per la prevenzione

SIAER considera giustamente minimo il rischio di commissione dei reati in oggetto; tuttavia, in ottica di massima trasparenza, ha deciso di adottare le seguenti misure di prevenzione: dichiarazione, da parte delle aziende con le quali mantiene rapporti di partnership, di non aver subito condanne per i reati previsti dall'art. 24 undecies del Decreto.

In particolare, i rischi ambientali sono limitati alla gestione dei rifiuti e, segnatamente:

1) smaltimento toner; 2) smaltimento RAE (rifiuti apparecchiature elettriche).

Al riguardo la Società, se per un verso ha stipulato un idoneo “accordo di smaltimento” con un soggetto autorizzato a smaltire i rifiuti prodotti dalla stessa, per l'altro verso si è dotato di una serie di regole di condotta così come riportate di seguito.

I destinatari sono:

- Rappresentante Legale (Datore di lavoro)
- Dipendenti
- Soggetti terzi.

Tutti i destinatari, come sopra individuati, nella misura in cui gli stessi possano essere coinvolti nello svolgimento delle rispettive attività aziendali, si devono attenere a regole di condotta conformi a quanto ivi previsto, al fine di prevenire e impedire il verificarsi di fatti illeciti.

Tutti i destinatari, in ciò coinvolti, sono tenuti a conoscere ed a rispettare le regole ed i principi contenuti:

- in questo documento;
- D.lgs. n. 205/2011;
- D.lgs. n. 152/06.

I destinatari dovranno inoltre:

- 1) astenersi dal tenere comportamenti, che possono provocare le situazioni previste dai suddetti reati;
- 2) astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- 3) osservare scrupolosamente tutte le norme poste dalla legge in tema di prevenzione alla commissione di reati ambientali.

Atteso che la Società non ha l'obbligo di tenere il registro di carico/scarico dei rifiuti, i principali processi aziendali sono:

- 1) attività di selezione delle aziende a cui:
 - attribuire lo smaltimento dei rifiuti;
 - attribuire la verifica della regolare immissione in atmosfera.

2) gestione emergenze ambientali.

Ai sensi del D.lgs. n. 152/06 (T.U. in materia ambientale) i rifiuti vengono classificati secondo:

- l'origine: in urbani e speciali;
- caratteristiche di pericolosità: in pericolosi e non pericolosi.

6.11 I reati di xenofobia e razzismo

È stata pubblicata la Legge 20 novembre 2017, n. 167 “*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2017*”.

In attuazione della Decisione Quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia, la Legge Europea 2017 ha disposto l'aggiunta al corpo normativo del Decreto Legislativo 8 giugno 2001, n. 231 dell'art. 25 - terdecies, in materia di lotta al razzismo e alla xenofobia.

I nuovi reati-presupposto sono quelli previsti dall'articolo 3, comma 3, della legge 13 ottobre 1975, n. 654, così come modificato dalla stessa Legge Europea, ai sensi del quale: “*si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia, della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello Statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232*”.

Misure per la prevenzione

SIAER ritiene totalmente estranei alla propria cultura i principi su cui si basano i delitti di razzismo e xenofobia; in ogni caso, appare efficace la struttura dei controlli in essere.

Al fine di rendere la Società esente da responsabilità, anche indirettamente, per la commissione dei reati di razzismo e xenofobia, si vieta l'utilizzo dei propri locali da parte di organizzazioni xenofobe e si vietano tutte le forme di finanziamento di eventi e manifestazioni finalizzate a perseguire tali scopi.

6.12 I reati tributari

La legge 17 dicembre 2019, n. 157 ha convertito il decreto legge n. 124/2019 (c.d. decreto fiscale), contenente, fra le varie disposizioni, anche alcune modifiche della disciplina dei reati tributari e l'inserimento di alcuni di questi fra i reati presupposto di cui al D.Lgs. n. 231/2001.

L'art. 39 del decreto legge in esame, rubricato “*Modifiche della disciplina penale e della responsabilità amministrativa degli enti*”, prevede infatti al comma 2 che, dopo l'art. 25-quaterdecies del D. Lgs. n. 231/2001, sia aggiunto il seguente art. 25-quinquiesdecies, rubricato Reati tributari:

“1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
- d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
- g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a

quattrocento quote.

2. *Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria e' aumentata di un terzo.*

3. *Nei casi previsti dai commi 1 e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e)''.*

In sostanza, con l'estensione della responsabilità amministrativa dell'ente ai reati di cui al D. Lgs. n. 74/2000, il legislatore ha posto fine alla diatriba concernente l'inclusione o meno dei reati tributari nel catalogo dei reati presupposto.

La norma che interessa è circoscritta agli artt. 2, 3, 8, 10 e 11 del D.lgs. n. 74/2000, con la conseguenza che solamente i delitti ivi contemplati vengono in rilievo.

Rimangono escluse dal novero dei reati presupposto tutte le altre fattispecie dichiarative od omissive, quali la dichiarazione infedele di cui all'art. 4, la dichiarazione omessa di cui all'art. 5 e l'omesso versamento dell'IVA di cui all'art. 10-ter.

Le condotte penalmente rilevanti consistono in:

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

È una delle fattispecie più gravi tra i reati tributari, la cui disciplina è fissata dal D. Lgs. n. 74/2000. La norma penale, contenuta nell'art. 2 del decreto, sanziona la condotta di colui che utilizza fatture o altri documenti probatori per dichiarare passività inesistenti all'interno della dichiarazione IVA o nella dichiarazione dei redditi, al fine di ridurre fraudolentemente l'imponibile oggetto del prelievo fiscale. Soggetto attivo del reato può essere unicamente il *contribuente*, cioè il soggetto obbligato alla tenuta di scritture contabili ai fini del pagamento dell'IVA (oppure amministratore, liquidatore o rappresentante del contribuente soggetto ad imposizione, art. 1, comma 1, lett. c), D.Lgs. n. 74/2000), ma anche il soggetto tenuto soltanto all'obbligatoria presentazione della dichiarazione annuale dei redditi.

In base all'art. 1, lett a), per "*fatture e i documenti per operazioni inesistenti*" rilevano tutti quei documenti aventi valore probatorio per l'Amministrazione tributaria emessi a fronte di operazioni non realmente effettuate in tutto o in parte, o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero che riferiscono l'operazione a soggetti diversi da quelli effettivi.

Il reato è consumato nel momento della presentazione della dichiarazione fraudolenta, pertanto, in presenza di plurime dichiarazioni fraudolente, si avranno più violazioni della norma penale.

Dichiarazione fraudolenta mediante altri artifici

La norma punisce chiunque, al fine di evadere le imposte sui redditi o l'IVA, compiendo operazioni simulate oggettivamente o soggettivamente, ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'Amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo se, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a ciascuna delle singole imposte, a trentamila euro;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore ad un milione e cinquecentomila euro, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al 5% dell'ammontare dell'imposta medesima, o comunque a trentamila euro.

Emissione di fatture o altri documenti per operazioni inesistenti

La pena per questo reato è severa (reclusione da 4 a 8 anni) atteso il grande disvalore della condotta di chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o dell'IVA, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Occultamento e distruzione di documenti contabili

Il reato di distruzione e occultamento della contabilità, previsto nel nostro ordinamento dall'art. 10 del D.Lgs. n. 74/2000, punisce con la reclusione da un anno e sei mesi a 6 anni chiunque al fine di evadere le

imposte sui redditi o l’IVA, o di consentire l’evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti fiscali di cui è obbligatoria la conservazione, per non consentire di conseguenza la ricostruzione dei redditi o del volume d’affari.

Sottrazione fraudolenta al pagamento delle imposte

L’art. 11 del D.lgs. n.74/2000 punisce chiunque al fine di sottrarsi al pagamento delle imposte sui redditi o dell’IVA ovvero di interessi o sanzioni amministrative di ammontare complessivo superiore ad € 50.000, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

La sanzione prevista è la reclusione da sei mesi a quattro anni, elevati ad un anno fino a sei anni nel caso in cui l’ammontare dell’imposta, sanzioni ed interessi sia superiore ad € 200.000.

Il reato di sottrazione fraudolenta al pagamento di imposte presidia l’interesse alla regolare percezione dei tributi da parte dello Stato contro eventuali azioni fraudolente dirette ad intaccare la garanzia patrimoniale dei contribuenti verso il Fisco.

Il concetto di operazioni inesistenti

La più recente giurisprudenza ha provveduto a precisare la nozione di operazione inesistente che viene in rilievo ai sensi dell’art. 2 del D.Lgs. n. 74/2000 quale elemento centrale della fattispecie.

Innanzitutto, relativamente al soggetto che emette la fattura/documento per l’operazione inesistente, la Cassazione ha superato l’orientamento che limitava l’operatività della fattispecie *de qua* ai casi in cui le fatture siano state emesse da terzi, in tal modo evidenziando la differenza con i delitti puniti agli artt. 3 e 8 del medesimo decreto. Nel ragionamento della Corte, la condotta sanzionata dall’art. 2 è “*la falsificazione della dichiarazione dei redditi che si consuma attraverso la rappresentazione di operazioni inesistenti, essendo indifferente che la documentazione falsa provenga dallo stesso autore della dichiarazione piuttosto che da terzi. (...) Si ritiene, in conclusione, che la fattispecie prevista dal D.Lgs. n. 74 del 2000, art. 2 sanziona i comportamenti che si risolvono nella presentazione di una dichiarazione dei redditi che rappresenti operazioni inesistenti, nulla rilevando che le fatture o i documenti che attestano tali operazioni siano creati dalla stessa persona che presenta la dichiarazione o da terzi?*” (Cass., Sez. fer., n. 47603/2017).

L’inesistenza dell’operazione, a cui si riferisce la norma dell’art. 2, può essere sia di natura oggettiva che soggettiva.

L’inesistenza è oggettiva nel caso in cui sia stata documentata in fattura un’operazione mai avvenuta o avvenuta solo in parte.

L’inesistenza è soggettiva, invece, nel caso in cui l’operazione sia avvenuta tra soggetti differenti da quelli indicati in fattura. In tal senso la Cassazione ha precisato che “*la falsità può essere riferita anche all’indicazione dei soggetti con cui è intercorsa l’operazione, intendendosi per “soggetti diversi da quelli effettivi”, ai sensi del citato d.lgs., art. 1, lett. a), coloro che, pur avendo apparentemente emesso il documento, non hanno effettuato la prestazione, sono irreali, come nel caso di nomi di fantasia, o non hanno avuto alcun rapporto con il contribuente finale*” (Cass., Sez. III, n. 47823/2017).

Le sanzioni

Le sanzioni pecuniarie a carico dell’ente variano: fino ad un massimo di 400 quote (artt. 8, comma 2-bis, 10 e 11 del D. Lgs. n. 74/2000) e fino ad un massimo di 500 quote (artt. 2, 3 e 8, comma 1 del D. Lgs. n. 74/2000).

Si applicano le sanzioni interdittive di cui all’articolo 9, comma 2, lettere c), d) ed e), vale a dire:

- a) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- b) l’esclusione da agevolazioni, finanziamenti, contributi o sussidi e l’eventuale revoca di quelli già concessi;
- c) il divieto di pubblicizzare beni o servizi.

I risultati dell’analisi di rischio conducono ad identificare, nell’ambito dei processi individuati, le seguenti attività come quelle, ora singolarmente, ora complessivamente considerate, in cui l’Ente risulta maggiormente esposto (sia in via diretta che strumentale) al rischio di commissione dei citati reati:

- Consiglio di Amministrazione

- Amministrazione

Misure per la prevenzione

SIAER ritiene di non essere particolarmente esposto a questa tipologia di reati. Al fine di rendere la Società esente da responsabilità anche per la commissione dei reati in esame, mantiene un rigoroso controllo sulla rispondenza dei documenti fiscali utilizzati (sia quelli emessi che quelli ricevuti) con la effettiva attività svolta, incrociando i dati contabili con quelli finanziari (flussi di cassa).

7 L'Organismo di Vigilanza e Controllo

7.1 Generalità

Il decreto legislativo prevede, all'art. 6, comma 1, lett. b) tra gli altri, che l'organizzazione non risponde per gli eventuali reati commessi al suo interno se il compito di vigilare sul funzionamento e l'osservanza del Modello di organizzazione e gestione predisposto, nonché di curarne l'aggiornamento, sia stato affidato ad un Organismo (OdV) dotato di autonomi poteri di iniziativa e controllo.

In conformità a tale prescrizione, SIAER si è dotato di un Organismo di Vigilanza di natura monocratica e nominato direttamente dal Consiglio di Amministrazione.

La compiuta esecuzione dei propri compiti da parte dell'OdV costituisce elemento essenziale per l'esimente prevista dal Decreto.

7.2 Nomina e composizione

L'OdV è organo di natura monocratica.

Esso è scelto tra soggetti qualificati e dotati di spiccata professionalità ed in possesso dei requisiti di onorabilità da intendersi così come richiamati dall'art.4, Decreto 30 Dicembre 1998, n.516.

I criteri cui si ispira per la costituzione dell'OdV sono:

- a) Composizione monocratica
- b) Risorsa professionale esterna
- c) Assenza di un potenziale conflitto di interessi

L'OdV viene nominato con delibera dal Consiglio di Amministrazione; con la medesima delibera viene fissato il compenso ad esso spettante.

La delibera di nomina, nonché i compiti ed i poteri, vengono comunicati tempestivamente mediante adeguati mezzi di comunicazione.

7.3 I requisiti dell'Organismo di Vigilanza e controllo

Autonomia ed indipendenza

La Società garantisce all'OdV piena autonomia di iniziativa e si impegna a preservarlo da qualsiasi forma di interferenza o di condizionamento. A tale fine è previsto che:

- l'OdV sia privo di compiti direttamente operativi, tenuto conto del grado di esposizione al rischio reato nella funzione in cui opera e non abbia possibilità di ingerenza nell'operatività della Società;
- l'Organismo nello svolgimento della propria funzione non sia soggetto a potere gerarchico;
- rapporti direttamente al Consiglio di Amministrazione;
- l'adozione delle sue decisioni nonché la determinazione della sua attività siano insindacabili.

Professionalità

Per assicurare il corretto svolgimento dei propri compiti, è essenziale che l'Organismo garantisca una adeguata professionalità. Sotto tale aspetto assume rilevanza:

- a) la conoscenza di materie giuridiche (in particolare della struttura e delle modalità di commissione dei reati presupposto, nonché del Decreto nel suo complesso);
- b) una buona conoscenza della struttura organizzativa;
- c) una adeguata competenza in materia di auditing e controllo (tecniche di analisi e valutazione dei rischi).

Onorabilità ed assenza di conflitto di interessi

Tale requisito va inteso nei seguenti termini:

- l'OdV è scelto tra soggetti qualificati e dotati di spiccata professionalità;
- l'OdV non deve avere vincoli di parentela con il vertice della Società, né tantomeno può essere legato ad essa da interessi economici rilevanti; esso deve, inoltre, essere libero da qualsiasi situazione che possa generare in concreto conflitto di interessi.

Continuità d'azione

La continuità dell'azione dell'OdV viene garantita attraverso la durata in carica per tre anni, fermo il successivo rinnovo e la possibilità di revoca solo per giusta causa nei termini sopra descritti.

L'attività dell'OdV è su base continua e si esplica in:

- a) conduzione di verifiche sull'applicazione del Modello di controllo tramite:
 - verifiche sulla corretta strutturazione dell'organizzazione aziendale;
 - verifiche sostanziali sulla completezza di applicazione dei controlli finalizzati alla prevenzione dei reati;
- b) disponibilità/facoltà continua di raccogliere segnalazioni di rischi di compimento di reati ed in generale di tutte le informazioni che siano necessarie a svolgere le attività di verifica;
- c) comunicazione continua tra i membri per segnalare nuovi eventuali rischi e condividere l'esito delle attività di verifica.

7.4 Le risorse dell'Organismo di Vigilanza

Il Consiglio di Amministrazione assegna all'OdV le risorse umane e finanziarie ritenute opportune al fine dello svolgimento dell'incarico, comunque adeguate al grado di esposizione al rischio.

Per quanto attiene alle risorse umane l'OdV potrà avvalersi del personale assegnatogli, di consulenti esterni e dell'ausilio di tutte le strutture dell'organizzazione.

Con precipuo riferimento alle questioni connesse alla tutela della salute e sicurezza sul lavoro (D.Lgs. 81/08) l'OdV dovrà avvalersi di tutte le risorse disponibili per la gestione dei relativi aspetti.

7.5 Compiti e poteri dell'Organismo di Vigilanza

In conformità a quanto previsto dall'art. 6, comma 1 del Decreto, che gli affida il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento, all'OdV fanno capo i seguenti compiti:

- a) verificare l'adeguatezza del Modello, ovvero la sua idoneità a prevenire il verificarsi di comportamenti illeciti, ed a evidenziarne l'eventuale commissione o il tentativo;
- b) vigilare sull'efficacia del sistema di gestione della Società:
 - 1) programmando l'attività di verifica ispettiva, e riesaminando i risultati delle verifiche ispettive precedenti,
 - 2) effettuando verifiche sulle attività od operazioni individuate nelle aree a rischio (es. aggiornamento delle procedure, sistema di deleghe in termine di coerenza tra poteri conferiti ed attività espletate, conoscenza del Modello),
 - 3) effettuando incontri periodici al fine di confrontarsi, verificare e relazionare sull'andamento del Modello di organizzazione e gestione;
- c) verificare l'effettività del Modello, ovvero la corrispondenza tra i comportamenti concreti e quelli formalmente previsti dal Modello stesso;
- d) predisporre un'efficace ed efficiente sistema di comunicazione interna al fine di ottenere il rapporto di informazioni rilevanti ai sensi del decreto (segnalazione di possibili violazioni e/o inosservanze del Modello) con particolare attenzione al rispetto del sistema di gestione della salute e sicurezza sul lavoro;
- e) eseguire un'attività completa, tempestiva, accurata, accessibile e continua di formazione ed informazione rivolta ai dipendenti e collaboratori della Società, in particolare promuovendo e definendo le iniziative per la diffusione della conoscenza circa il decreto e le conseguenze derivanti dalla sua applicazione (Modello di organizzazione e gestione, analisi di rischio etc.);

- f) curare l'aggiornamento del Modello;
- g) garantire un flusso di informazioni verso il Consiglio di Amministrazione.

Per l'espletamento dei compiti ad esso assegnati, all'Organismo sono riconosciuti dalla Direzione tutti i poteri necessari ad assicurare una puntuale ed efficiente vigilanza, in particolare:

- di effettuare, anche senza avviso, tutte le verifiche ispettive ritenute opportune;
- di accedere liberamente presso le aree di tutte le funzioni, gli archivi ed i documenti;
- di avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture dell'organizzazione o di consulenti esterni;
- di disporre direttamente delle risorse finanziarie all'uopo stanziato.

7.6 Flusso di informazione verso l'Organismo di Vigilanza

Ai sensi dell'art. 6, comma 2, lett. d) del decreto, viene istituito l'obbligo di informazione verso l'OdV in merito a situazioni di potenziale rischio di illecito, o ad atti che si configurino come violazioni del Sistema.

È istituito inoltre un obbligo di rapporto funzionale a carico del Coordinatore; in particolare, questi deve riportare all'OdV periodicamente, ovvero in tutte le situazioni in cui se ne ravvisa la necessità, sull'attività svolta (controlli effettuati, modifiche suggerite a procedure operative, nuove attività avviate esposte ai rischi di reato previste dal D.Lgs. 231/2001) mediante apposita modulistica o relazione scritta.

a) Segnalazione

Il personale dipendente (ovvero collaboratore esterno) che intenda segnalare una violazione (o presunta violazione) del Sistema è tenuto a contattare l'OdV attraverso un'apposita casella e-mail oppure tramite comunicazione scritta. Nel caso di segnalazioni anonime e non in forma scritta, l'OdV le valuterà a sua discrezione a seconda della gravità della violazione denunciata.

L'OdV garantisce l'anonimato e la riservatezza di ogni informazione inerente il soggetto segnalante al fine di garantirlo da potenziali atti ritorsivi di qualsiasi natura, fatti salvi gli obblighi di legge.

b) Attivazione dell'OdV

L'OdV esamina tutte le segnalazioni pervenute alla propria attenzione, le valuta e, in caso lo ritenga necessario, si attiva avviando tutte le necessarie indagini, quali:

- la convocazione del responsabile della violazione (o presunta tale);
- il coinvolgimento delle funzioni interessate dalla segnalazione;
- l'accesso a qualunque fonte di informazione, documento o dato ritenuto rilevante ai fini dell'inchiesta.

c) Altre informazioni

È fatto obbligo a tutta l'Organizzazione (Organi, Dirigenti, responsabili e dipendenti) di comunicare tempestivamente all'OdV le informazioni riguardanti:

- i provvedimenti e/o notizie provenienti da ogni autorità giudiziaria, dai quali emerga lo svolgimento di indagini per illeciti ai sensi del D.Lgs. 231/2001 in cui possa essere coinvolta l'Associazione;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ai sensi del D.Lgs. 231/2001;
- le notizie relative ai procedimenti disciplinari ed alle eventuali sanzioni comminate nei confronti dei dipendenti, oppure dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- la tipologia, il numero, i destinatari e le motivazioni a supporto di tutti gli atti di liberalità posti in essere;
- tutte le eventuali segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti possibili carenze o inadeguatezze dei luoghi o delle attrezzature di lavoro, ovvero dei dispositivi di protezione messi a disposizione, sia ogni altra situazione di pericolo connesso alla salute e sicurezza sul lavoro.

Viene inoltre istituito un flusso di comunicazioni periodico nei confronti dell'OdV, da parte del Consiglio di Amministrazione, per quelle informazioni, in riferimento all'attività, che possono assumere rilevanza quanto all'espletamento delle funzioni dell'Organismo, in particolare:

- i verbali dell'Organo di Controllo
- tutti i dati relativi ad eventuali infortuni sul lavoro occorsi
- il bilancio annuale corredato della nota integrativa.

Tale elenco potrà essere integrato di volta in volta con richieste specifiche emesse dall'OdV nei confronti dei vari responsabili di struttura.

L'OdV, dopo aver valutato le segnalazioni, pianifica le attività, anche di natura ispettiva, utilizzando le risorse necessarie.

7.7 Reporting e gestione dei documenti

Al fine di garantire la sua piena autonomia e indipendenza, l'OdV riporta direttamente al Consiglio di Amministrazione.

In sede di approvazione del bilancio l'OdV riferisce mediante relazione scritta, con particolare riferimento agli esiti dell'attività di vigilanza espletata durante l'anno ed agli interventi opportuni per l'implementazione del Sistema dei controlli.

L'OdV potrà essere convocato in ogni momento dal Consiglio di Amministrazione per riferire su particolari eventi o situazioni relative all'efficacia ed all'efficienza del Modello; potrà altresì in ogni momento chiedere di essere sentito qualora ritenga opportuno un esame o un intervento del suddetto organo circa l'adeguatezza del Modello.

8 Sistema sanzionatorio

SIAER condanna qualsiasi comportamento difforme alle previsioni del presente Modello e del Codice Etico, anche qualora detto comportamento venga posto in essere nell'interesse od a vantaggio della Società stessa.

Il sistema sanzionatorio del presente Modello è finalizzato esclusivamente a rafforzarne l'efficacia ed il rispetto da parte del personale tutto.

Le misure sanzionatorie stabilite non sostituiscono eventuali ulteriori sanzioni di altra natura che possano derivare come conseguenza del medesimo fatto di reato (sanzione penale, amministrativa, civile).

L'adeguatezza del sistema disciplinare alle prescrizioni del Decreto deve essere costantemente monitorata dall'OdV.

8.1 Criteri generali di irrogazione della sanzione

La tipologia e l'entità della sanzione da applicare, una volta accertata la violazione, è definita in base ai seguenti criteri:

- valutazione della condotta in base al dolo, colpa, negligenza o imperizia, rilevanza degli obblighi violati;
- livello di responsabilità del soggetto coinvolto in base a criteri gerarchici;
- presenza di circostanze aggravanti o attenuanti.

Costituiscono infrazioni disciplinari per le quali potranno essere applicate le sanzioni previste nei successivi paragrafi i seguenti comportamenti:

- l'inadempimento dell'obbligo di vigilanza e controllo da parte dei soggetti che hanno tale responsabilità sui propri sottoposti;
- la violazione, commissiva od omissiva, delle procedure previste e/o stabilite per l'attuazione del Modello;
- la mancata collaborazione o reticenza del personale nel fornire le informazioni all'OdV;
- la violazione (con dolo o colpa grave) all'obbligo di comunicazione verso l'OdV, secondo quanto stabilito dal presente Modello sui flussi comunicativi;
- la redazione, nonché l'agevolazione alla redazione, di documentazione incompleta e non veritiera; l'omessa redazione della documentazione prevista dal presente Modello o dalle procedure previste per l'attuazione dello stesso;
- la violazione o l'elusione del sistema di controllo previsto da Modello.

8.2 Le sanzioni

Sanzioni per i lavoratori dipendenti

Con riguardo ai lavoratori dipendenti, il Decreto prevede che il sistema disciplinare deve rispettare i limiti connessi al potere sanzionatorio imposti dall'art. 7 della Legge n. 300/1970 (c.d. "Statuto dei lavoratori") e dalla contrattazione collettiva di settore e aziendale, sia per quanto riguarda le sanzioni irrogabili sia per quanto riguarda la forma di esercizio di tale potere.

Con riferimento alle sanzioni irrogabili, si precisa che esse saranno adottate ed applicate nel rispetto delle procedure previste dalle normative collettive nazionali ed aziendali applicabili al rapporto di lavoro.

Fermo restando il principio di collegamento tra i provvedimenti disciplinari irrogabili e le fattispecie in relazione alle quali le stesse possono essere assunti, nell'irrogazione della sanzione disciplinare deve necessariamente essere rispettato il principio della proporzionalità tra infrazione e sanzione.

La violazione delle disposizioni del Modello potrà costituire inadempimento delle obbligazioni contrattuali, con ogni conseguenza di legge e nel rispetto in particolare degli artt. 2104, 2106, 2118 e 2119 del Codice Civile, dell'art. 7 della Legge n. 300/1970.

Le sanzioni individuate sono:

- il rimprovero verbale per le violazioni di lieve entità;
- il rimprovero scritto, per le reiterate violazioni di lieve entità;
- la sospensione dal servizio e del trattamento economico, per violazioni di grave entità che aumenti il grado di esposizione al rischio di commissione reato; la sospensione dal servizio e dal trattamento economico è temporanea, comunque, non superiore a 10 giorni;
- il licenziamento per inadempimento degli obblighi contrattuali:

Misure nei confronti degli amministratori

In caso di violazione della normativa vigente, del Modello o del Codice Etico da parte degli Organi sociali, l'OdV informerà, in mancanza di altro Organo cui riferire per ragioni di opportunità, l'Assemblea dei soci.

Le sanzioni individuate sono:

- richiamo formale scritto, in caso di violazione non grave;
- revoca, totale o parziale, delle eventuali procure.

Qualora la violazione dell'amministratore sia grave e tale da ledere la fiducia nei suoi confronti, l'Assemblea dei soci propone la revoca dalla carica.

Misure nei confronti dei componenti l'OdV

In caso di violazione delle norme del presente Modello o della normativa vigente, tali da configurarsi come un grave inadempimento dei propri doveri così come definiti nel presente Modello o una grave negligenza nell'espletamento dei compiti connessi all'incarico, oltre alla revoca dall'incarico potrà essere applicata la sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile e, nei casi più gravi, la risoluzione del rapporto di lavoro.

Misure nei confronti dei sindaci

In caso di violazione da parte di un componente dell'Organo di Controllo, l'OdV deve darne immediata comunicazione al Consiglio di Amministrazione mediante relazione scritta. Il Consiglio di Amministrazione, qualora si tratti di violazioni gravi tali da integrare giusta causa, dispone la revoca del componente del Organo di Controllo o dell'intero Collegio.

Misure nei confronti dei consulenti, partner e fornitori

Consulenti, partner e fornitori restano esclusi dai procedimenti e provvedimenti disciplinari sopra descritti sulla base delle normative vigenti relative ai lavoratori subordinati.

In ogni caso, ogni violazione della normativa vigente, del Modello o del Codice Etico da parte di consulenti, professionisti, partner e fornitori è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti, sulla base delle disposizioni di legge applicabili, di atti di recesso per giusta causa, con ogni eventuale conseguenza anche sotto il profilo risarcitorio.

9 Informazione e formazione del personale

9.1 Informazione e formazione dei dipendenti

L'adozione del presente Modello è comunicata ai dipendenti al momento dell'adozione stessa.

Ai fini dell'efficacia del presente Modello, è obiettivo della Società garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti del personale. Tale obiettivo riguarda tutte le risorse aziendali sia quelle già presenti in azienda che quelle da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione sia al diverso livello di coinvolgimento delle risorse medesime nelle c.d. attività sensibili, sia in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza di SIAER.

In particolare, sono previsti livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione per la totalità dei dipendenti che rivestono la qualifica di dirigenti e dei dipendenti che non rivestono la qualifica di dirigenti mediante una formazione mirata e modulata in funzione del livello di rischio e della tipologia di funzioni svolte. .

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività dell'OdV.

Al fine di verificare l'effettività e l'efficacia della formazione si provvede a registrare:

- il programma di formazione;
- il materiale didattico fornito;
- l'elenco dei partecipanti alla formazione;
- ove possibile i test di apprendimento/gradimento sulla formazione ricevuta compilati dal personale.

CODICE ETICO

Sommario

- 1 Premessa
- 2 SIAER e la sua missione
- 3 Obiettivi e ambito di applicazione del codice etico
- 4 Principi generali
 - 4.1 Legalità
 - 4.2 Trasparenza, correttezza ed equità
 - 4.3 Valore delle risorse umane
 - 4.4 Cultura del rischio
 - 4.5 Tutela della salute e sicurezza sui luoghi di lavoro
 - 4.6 Tutela della privacy e sicurezza informatica
 - 4.7 Conflitto d'interessi
 - 4.8 Operazioni, transazioni e gestione documentale
 - 4.9 Gestione delle attività amministrative
- 5 Relazioni con le parti interessate
 - 5.1 Rapporti interni
 - 5.2 Pubblica Amministrazione
 - 5.3 Fornitori
 - 5.4 Attività di promozione e rapporti con organi di informazione e mass media
 - 5.5 Risorse umane
- 6 Il ruolo di garanzia
 - 6.1 L'Organismo di Vigilanza
 - 6.2 Diffusione e formazione sul codice etico
 - 6.3 Sistema sanzionatorio

1 Premessa

Il D. Lgs. 8 giugno 2001, n 231 (di seguito anche Decreto), recante la “Disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni, anche prive di personalità giuridica” ha introdotto il principio della responsabilità degli Enti, a seguito dei reati commessi nel loro interesse o a loro vantaggio, dai dipendenti, dalle figure c.d. apicali, dai soggetti sottoposti alla loro direzione o vigilanza e da tutti coloro che, anche di fatto, siano in grado di impegnare l'Ente.

Il decreto prevede, tra le altre condizioni, che il Codice Etico collocato all'interno di un effettivo modello organizzativo di gestione e controllo, possa assumere una forza scriminante e di protezione a beneficio dell'Organizzazione, che rimarrebbe al riparo dall'applicazione delle sanzioni previste.

SIAER ha ritenuto opportuno definire e formalizzare il presente Codice Etico che è parte integrante del Modello organizzativo adottato, come riconferma delle regole, dei valori e dei principi guida già adottati ed a cui si riconosce valore positivo.

La creazione e diffusione dei valori, infatti, non può essere disgiunta da un effettivo rispetto dei principi fondamentali quali la correttezza professionale, l'indipendenza, la trasparenza, l'integrità personale e l'effettiva tutela della salute nell'ambiente di lavoro.

2 SIAER e la sua missione

SIAER è un ente di natura privatistica, promosso da CNA Emilia-Romagna, costituito dalle Società di servizi provinciali delle CNA dell'Emilia Romagna; ha natura di società consortile a responsabilità limitata, ai sensi dell'art. 2615-ter del codice civile.

SIAER nasce con gli obiettivi di:

- promuovere e stimolare l'applicazione delle più avanzate tecniche organizzative e di gestione amministrativa aziendale;
- fornire consulenze e servizi in campo telematico;
- effettuare servizi di razionalizzazione nella gestione finanziaria, anche attraverso l'organizzazione di operazioni di "cash pooling";
- favorire la competitività delle imprese;
- valorizzare le risorse umane.

SIAER promuove e organizza la partecipazione a Fiere ed altri eventi in genere, per favorire l'ingresso ed il consolidamento della presenza dei soci e loro associati nel mercato.

3 Obiettivi e ambito di applicazione del codice etico

In linea con il quadro d'azione delineato dall'Unione Europea, SIAER è interessato a sviluppare ed applicare tutte le iniziative che concorrono a promuovere una consapevole responsabilità sociale dell'impresa.

In tal senso SIAER ha scelto di impegnarsi ad adottare comportamenti responsabili sul piano dei rapporti interni con i dipendenti, nella tutela del patrimonio aziendale e della tutela e della sicurezza dei luoghi di lavoro, della tutela ambientale oltre che norme etiche nei rapporti con i terzi, con particolare riguardo ed attenzione ai rapporti con quanti si rivolgono alla nostra struttura.

Il CdA, consapevole che l'etica nei comportamenti costituisce valore e condizione di successo per ogni organizzazione e che principi quali l'onestà, l'integrità morale, la trasparenza, l'affidabilità e il senso di responsabilità rappresentano la base fondamentale di tutte le attività che caratterizzano la sua *mission*, definisce le linee guida a cui dovranno essere improntati i comportamenti nelle relazioni interne e nei rapporti con l'esterno.

Per questi motivi SIAER, nella consapevolezza dell'importanza degli interessi coinvolti nell'attività che svolge, adotta il presente codice come carta dei diritti e dei doveri morali, in un'ottica di "responsabilità sociale", cui devono ispirarsi, senza alcuna eccezione, tutto il personale dipendente e i collaboratori (Organi sociali e propri membri, dirigenti, dipendenti, consulenti, fornitori) nei rapporti sia interni sia esterni e per la realizzazione dello scopo sociale.

In tale prospettiva, il presente codice è pertanto una riconferma delle regole e dei principi - guida da sempre adottati, che intende con ciò rafforzare il clima di fiducia e di positiva collaborazione con tutti coloro che, a vario titolo, sono interessati al comune sviluppo e diffusione dei valori di SIAER.

SIAER considera il presente Codice Etico strumento di regolamentazione e di disciplina della propria attività.

Ciascun dipendente e collaboratore, indipendentemente dalla posizione o dallo status, nonché i componenti degli Organi sociali, è responsabile delle proprie azioni nel rispetto del presente codice, delle politiche di SIAER e della legge.

Tutti i rapporti, di qualsiasi natura, con SIAER implicano il riconoscimento dei valori espressi nel presente codice. Ciò comporta per tutti i soggetti interessati, tra l'altro, l'astensione da qualsiasi comportamento che possa nuocere all'immagine ed all'interesse comune.

Nei rapporti e nelle relazioni esterne SIAER richiede che i soggetti terzi agiscano nei suoi confronti con un'analogia condotta etica. Il personale è tenuto a non avviare o mantenere alcun rapporto con soggetti terzi i quali evidenzino l'intenzione di non osservare tale condotta.

La violazione delle norme del presente codice lede il rapporto di fiducia instaurato e potrà portare all'attivazione di azioni legali oltre che all'adozione di provvedimenti nei confronti dei destinatari in coerenza con le disposizioni di legge e con i previsti regimi contrattuali, con ogni conseguente responsabilità personale.

L'approvazione del Codice Etico avviene nell'ambito dell'adozione da parte di SIAER del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001, di cui il presente codice è parte integrante.

A tal fine SIAER si impegna a far conoscere i principi contenuti nel presente codice.

4 Principi generali

Le azioni, i rapporti, le transazioni, la gestione delle risorse umane ed i comportamenti svolti nell'esercizio delle competenze e delle funzioni assegnate devono essere improntati al rispetto dei seguenti principi etici.

4.1 Legalità

Siaer si impegna a condurre e far condurre la propria attività nel rispetto ed applicazione della legge respingendo la corruzione, le forme di riciclaggio e ogni pratica illegale, con particolare attenzione ed impegno alle disposizioni in materia di responsabilità amministrativa dell'Organizzazione ex D. Lgs. 231/01.

I componenti degli organi di governo di SIAER ed in generale i dipendenti ed i collaboratori, nell'ambito della loro attività professionale, sono tenuti a rispettare con diligenza la normativa vigente, il presente Codice Etico ed i protocolli e regolamenti interni.

Il perseguimento, ancorché non esclusivo, di un interesse di SIAER non potrà essere considerato, in nessun caso, un'esimente al mancato rispetto della legge, né potrà giustificare una condotta non onesta.

4.2 Trasparenza, correttezza ed equità

In tutti i rapporti, SIAER segue e richiede il rispetto dei principi di massima trasparenza e correttezza, onestà, obbiettività ed equità.

L'imparzialità di trattamento è un valore fondamentale nello svolgimento di ogni relazione interna ed esterna, pertanto si respinge, contrasta e sanziona ogni discriminazione con riguardo all'età, al sesso, alle attitudini sessuali, allo stato di salute, alla razza, alla nazionalità, alle opinioni politiche ed alle credenze religiose di tutti i suoi interlocutori, nonché ogni indebita interferenza con tale principio.

Tutta l'Organizzazione nello svolgimento dei rispettivi doveri professionali, deve attenersi al principio di imparzialità, evitando di preferire o agevolare persone o soluzioni che non siano basate su valutazioni tecnico-professionali.

4.3 Valore delle risorse umane

SIAER considera l'individuo, i suoi valori ed i suoi diritti, valori intangibili e da tutelare.

Le risorse umane sono riconosciute come elemento irrinunciabile e fondamentale per il raggiungimento degli obiettivi perseguiti.

In particolare SIAER censura ogni comportamento offensivo, ivi compresa ogni forma di vessazione psicologica e fisica. Ne fanno parte anche i comportamenti riconducibili alla categoria delle c.d. "molestie sessuali", intendendo come tali: la subordinazione di prospettive retributive o di carriera all'accettazione di favori sessuali nonché l'offerta di relazioni interpersonali private, condotte nonostante un rifiuto esplicito o ragionevolmente evidente, che, in relazione alla specifica circostanza, abbia la capacità di turbare la serenità dell'individuo che ne è destinatario. SIAER censura inoltre ogni comportamento che possa essere considerato lesivo della sensibilità degli altri quali, a titolo esemplificativo ma non esaustivo, il prestare servizio sotto gli effetti dell'abuso di sostanze alcoliche, stupefacenti o di analogo effetto, nonché consumare o cedere a qualsiasi titolo sostanze stupefacenti nel corso dell'attività lavorativa.

4.4 Cultura del rischio

SIAER intende far crescere nei propri dipendenti una sensibilità ai rischi sottostanti alla loro quotidiana operatività, diffondendo la percezione di come il sistema di controllo interno presidi in concreto tali rischi senza dannose sovrapposizioni o colpevoli lacune.

4.5 Tutela della salute e sicurezza sui luoghi di lavoro

È garantito il massimo impegno a rispettare la normativa vigente in tema di sicurezza sul luogo di lavoro e ad operare per preservare, soprattutto con azioni preventive, la salute e la sicurezza dei lavoratori.

A tal fine, la struttura interna, attenta all'evoluzione degli scenari di riferimento ed al conseguente mutamento dei rischi, realizza interventi di natura tecnica ed organizzativa, attraverso:

- l'introduzione di un sistema di gestione dei rischi e della sicurezza;

- una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere;
- l'adozione delle migliori soluzioni delle migliori modalità e tempistiche di lavoro.

4.6 Tutela della privacy e sicurezza informatica

SIAER assicura e garantisce il pieno rispetto delle norme poste a tutela della privacy, adottando ed attuando idonee procedure ed efficaci strumenti di gestione.

Per quanto concerne le misure a tutela della sicurezza dei sistemi informativi aziendali (comprendendo questa definizione sia dispositivi hardware software nonché i dati con essi trattati) SIAER adotta specifici protocolli di prevenzione e controllo del tutto in linea con quanto previsto dalla normativa cogente (L.48/08 e Disciplina tecnica misure minime di sicurezza all. B al D. Lgs. 196/03) nonché dalle più diffuse best-practice di riferimento.

Questi standard prevedono inoltre il divieto, fatte salve le ipotesi previste dalla legge, di comunicare/diffondere i dati personali senza previo consenso dell'interessato e stabiliscono le regole per il controllo, da parte di ciascun titolare, delle norme a protezione della privacy ai sensi del D. Lgs. 196/03.

4.7 Conflitto d'interessi

Per "conflitto di interessi" si intende la situazione in cui chiunque legato a SIAER (sia questi un dipendente a qualsiasi livello gerarchico, o componente di organi sociali) a causa di interessi o attività personali, possa agire non in conformità con le prescrizioni etiche e/o venga condizionato nella propria capacità di operare nell'esclusivo interesse dell'Organizzazione stessa.

Tutti coloro, ad ogni livello, che hanno rapporti diretti o indiretti con SIAER devono evitare azioni ed attività che possano condurre a conflitto d'interesse, in ogni caso è fatto obbligo ai dipendenti ed ai collaboratori, di informare l'Organismo di Vigilanza e Controllo circa la presenza o il sopraggiungere di una qualsiasi forma di conflitto di interesse, reale o potenziale.

4.8 Operazioni, transazioni e gestione documentale

Ogni operazione e transazione deve essere legittima, autorizzata, registrata, verificabile e coerente con le prescrizioni di SIAER. In qualunque momento dovrà essere possibile risalire all'iter di decisione, autorizzazione e successivo svolgimento della operazione/transazione.

Ogni operazione/transazione deve essere correlata da un adeguato supporto documentale che ne consenta di individuare le caratteristiche di decisione, autorizzazione e svolgimento. Per "adeguato supporto documentale" si intende una documentazione che sia leggibile, facilmente identificabile e rintracciabile.

Nella redazione dei documenti, il personale è tenuto a seguire i principi di accuratezza, onestà, obiettività, trasparenza. In particolare, le registrazioni contabili non devono riportare voci false e fondi, proprietà o transazioni occultati o non registrati. Tutti i libri contabili ed i documenti finanziari devono essere conformi alle disposizioni di legge ed ai principi di contabilità comunemente accettati.

4.9 Gestione delle attività amministrative

SIAER si impegna ad osservare le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili.

Nell'attività di contabilizzazione si provvede a conservare la documentazione di supporto dell'attività svolta in modo da consentire l'agevole registrazione e la tracciabilità delle valutazioni, l'individuazione dei diversi livelli di responsabilità e la ricostruzione accurata dell'operazione riducendo la probabilità di violazioni o errori interpretativi.

In altri termini, ogni operazione deve essere, oltre che correttamente registrata: autorizzata, verificabile, legittima, coerente e congrua.

5 Relazioni con le parti interessate

5.1 Rapporti interni

SIAER si impegna a mantenere la massima correttezza, trasparenza, imparzialità ed equità nei rapporti interni.

SIAER si adopera al fine di

- impedire che qualsiasi componente l'organizzazione possa agire in maniera tale da influenzare il comportamento di organi o uffici al fine di trarne un vantaggio personale, ancorché esclusivo;
- garantire che tutte le informazioni fornite a qualsiasi titolo alla P.A. siano veritiere, trasparenti e complete;
- assicurare che tutto il personale impegnato nella formazione del bilancio svolga i propri compiti e controlli accuratamente i dati elaborati, segnali eventuali situazioni di conflitto di interesse, e fornisca informazioni veritiere, chiare e corrette;
- scoraggiare atteggiamenti o favorire pratiche, sotto qualsiasi forma, che possano indurre a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- garantire il costante controllo sulle attività di predisposizione e gestione dei progetti formativi ex ante e sulle attività durante il loro svolgimento.

5.2 Pubblica Amministrazione

Nei rapporti con la Pubblica Amministrazione o con Enti che svolgono attività di pubblica utilità o di pubblico interesse, si richiede il rispetto rigoroso della normativa comunitaria, nazionale e organizzativa applicabile. Non è ammessa alcuna forma di comportamento illegale, quali, a titolo esemplificativo ma non esaustivo, tentativi di corruzione, indebita percezione di erogazioni, truffa in danno dello Stato.

La gestione dei rapporti, di qualsiasi genere, con la Pubblica Amministrazione, pubblici ufficiali o soggetti incaricati di pubblico servizio, possono essere esercitati esclusivamente da soggetti autorizzati ed improntati al rispetto dei principi del presente Codice.

Nei rapporti con la P.A. i destinatari del presente Codice non possono, direttamente o indirettamente (tramite terzi soggetti) offrire regali, doni, denaro, pagamenti, omaggi a vario titolo sia di natura materiale che immateriale.

Nel caso in cui SIAER sia parte in procedimenti contenziosi in sede civile, penale od amministrativa, anche di natura stragiudiziale, gli organi sociali, i dipendenti e i professionisti incaricati non dovranno in alcun modo adottare comportamenti che possano indurre a provvedimenti che vadano illegittimamente a vantaggio della stessa. È assolutamente contrario ai principi riconosciuti tenere atteggiamenti o favorire pratiche, sotto qualsiasi forma, che possano indurre a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria.

SIAER esige, inoltre, che gli organi sociali ed i loro componenti, dipendenti, consulenti, collaboratori e quanti agiscano in nome e per conto della stessa, operino con la massima disponibilità e trasparenza nei confronti di chiunque venga a svolgere ispezioni e controlli legittimamente autorizzati dalle competenti Autorità.

È fatto obbligo a coloro che eventualmente dovessero essere soggetti, per fatti connessi al rapporto di lavoro ed anche a titolo personale ad indagini o ispezioni o che dovessero ricevere mandati di comparizione, e/o coloro ai quali venissero notificati altri provvedimenti giudiziari, di informare l'OdV.

5.3 Fornitori

SIAER impronta i propri processi di acquisto alla ricerca della più elevata efficienza salvaguardando lealtà ed imparzialità nei confronti dei propri fornitori selezionati, ricercandone la massima collaborazione e fiducia a garanzia della qualità e del livello del servizio richiesto.

I collaboratori a qualunque titolo ed i consulenti sono tenuti, nell'esecuzione del rapporto contrattuale instaurato o dell'incarico dallo stesso ricevuto, a comportarsi con correttezza, buona fede e lealtà, rispettando, per quanto loro applicabili, le previsioni del presente codice etico, le normative interne e le istruzioni e prescrizioni impartite al personale.

I soggetti tenuti ad agire in nome o per conto di SIAER, nello svolgimento degli incarichi professionali nell'interesse o a vantaggio dello stesso, sono tenuti al rispetto delle disposizioni di cui al presente codice.

I compensi e/o le somme comunque corrisposte ai collaboratori o fornitori nell'espletamento delle prestazioni devono essere ragionevoli e proporzionate all'attività svolta, sia tenuto conto delle condizioni di mercato sia delle caratteristiche specifiche della prestazione eseguita.

In nessun caso saranno ammesse pressioni indebite da parte dei fornitori e/o soggetti terzi.

5.4 Attività di promozione e rapporti con organi di informazione e mass media

Qualunque comunicazione da parte di Siaer verso l'ambiente esterno deve essere veritiera, chiara, trasparente, non strumentale, conforme alle politiche ed ai programmi dell'organizzazione.

In ogni caso, la comunicazione è soggetta ai vincoli di rispetto della tutela dei dati personali e può essere divulgata solo dalle figure espressamente autorizzate.

Nelle sue attività di comunicazione in campagne promozionali e altro SIAER si impegna a rispettare e tutelare la normativa in materia di diritto d'autore.

5.5 Risorse umane

SIAER considera le risorse umane un patrimonio strategico ed indispensabile per la diffusione dell'etica e della qualità, intesa principalmente come perseguimento della soddisfazione del cliente.

Per ogni destinatario, quindi, il rispetto delle norme del codice costituisce obbligo contrattuale.

Per tutelare ed accrescere il patrimonio umano SIAER è impegnato:

- alla definizione di ruoli, deleghe, responsabilità e disponibilità di informazioni tali da consentire a tutto il personale di assumere le decisioni che gli competono nell'interesse dell'organizzazione;
- a far sì che tutti i locali di lavoro siano in condizioni idonee e decorose per lo svolgimento delle attività lavorative, così come idonee e decorose devono essere le attrezzature affidate ai dipendenti;
- ad offrire pari opportunità di sviluppo e crescita delle funzioni professionali in base a criteri di merito e competenza;
- a collegare i riconoscimenti economici, oltre che ai risultati quantitativi, anche all'osservanza delle leggi, dei regolamenti e delle norme del presente codice;
- a programmare e sviluppare la crescita professionale ed una coscienza etica e della responsabilità sociale dell'impresa attraverso adeguata formazione.

6 Il ruolo di garanzia

6.1 L'Organismo di Vigilanza

La vigilanza sull'osservanza e il rispetto delle norme etiche è demandata in via ordinaria all'Organismo di Vigilanza e Controllo.

All'OdV sono attribuiti i seguenti compiti:

- promuovere iniziative, attraverso piani di comunicazione e formazione, atte a diffondere la conoscenza del codice etico e dei suoi principi fondamentali;
- coordinare la revisione, la modifica e la integrazione del codice e delle sue eventuali procedure attuative perché si mantengano sempre conformi alle leggi vigenti;
- fornire pareri vincolanti nella interpretazione, valutazione, attuazione delle prescrizioni del presente codice, al fine di renderlo lo strumento di riferimento del corretto comportamento da tenere all'interno dell'organizzazione;
- attivare le funzioni competenti, a seguito di violazioni del codice e di comportamenti anomali in ogni modo rilevati, mediante segnalazioni e rapporti affinché assumano i necessari provvedimenti correttivi;
- garantire la tutela dei soggetti segnalanti;
- assicurare, salvi gli obblighi di legge, la riservatezza dell'identità del segnalante;
- relazionare annualmente al Consiglio di Amministrazione in merito allo stato di attuazione del codice etico, sulle iniziative assunte e sull'efficacia dei provvedimenti correttivi assunti.

6.2 Diffusione e formazione sul codice etico

SIAER si impegna a garantire una puntuale diffusione interna ed esterna del codice etico mediante:

- distribuzione a tutti il personale e a tutti i membri degli Organi sociali;
- divulgazione dei principi, valori e norme comportamentali ai soggetti terzi che hanno rapporti con l'organizzazione;
- messa a disposizione di qualunque altro interlocutore.

Nei contratti con i terzi, è inoltre prevista l'introduzione di clausole e/o la sottoscrizione di dichiarazioni volte sia a formalizzare l'impegno al rispetto del codice etico, sia a disciplinare le sanzioni di natura contrattuale nell'ipotesi di violazione.

6.3 Sistema sanzionatorio

Il rispetto delle prescrizioni contenute nel presente Codice, obbliga, senza alcuna eccezione, tutti i dipendenti (indipendentemente dalla posizione o dallo status), i collaboratori, nonché quanti intrattengono rapporti con SIAER (Organi sociali e propri membri, dirigenti, dipendenti, consulenti, fornitori) nei rapporti sia interni sia esterni e per la realizzazione dello scopo sociale.

Il rispetto dei principi e delle norme di comportamento, rientra tra gli obblighi assunti dal personale all'atto della costituzione del rapporto di lavoro.

Il rispetto delle prescrizioni contenute nel presente Codice costituisce obbligo contrattuale anche per tutti i soggetti che intrattengono rapporti commerciali con SIAER (consulenti, partner e fornitori).

Le misure sanzionatorie previste per l'inosservanza dei principi etici e i criteri generali per la loro irrogazione sono regolati da specifico capitolo del Modello di organizzazione, gestione e controllo di cui si ricorda che il presente codice etico è parte integrante.

ANALISI DEL RISCHIO

Indice

1. Contenuto del documento
2. L'analisi di rischio: executive summary
- 2.1 Tabella riepilogativa reati-processi
3. Il dettaglio dell'analisi di rischio
- 3.1 Tabella riepilogativa criticità-controlli

1. Contenuto del documento

Il presente documento:

A. identifica i processi esposti a rischio di commissione dei reati previsti dal D.Lgs. 231/2001, evidenziandone l'eventuale grado di esposizione. I reati per i quali è stata condotta l'analisi sono quelli elencati di seguito (tra parentesi è riportato il richiamo al rispettivo articolo del D.Lgs. 231/2001):

- delitti contro la pubblica amministrazione (artt. 24 e 25);
- delitti informatici e trattamento illecito dei dati (art. 24-bis);
- delitti di criminalità organizzata (art. 24-ter);
- falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
- delitti contro l'industria e il commercio (art. 25-bis 1);
- reati societari (art. 25-ter);
- delitti in materia di terrorismo e di eversione dell'ordine democratico (art. 25-quater);
- reati di mutilazione degli organi genitali femminili (art. 25-quater 1);
- delitti contro la personalità individuale (art. 25-quinquies);
- reati di abuso del mercato (25-sexies);
- reati di omicidio colposo e lesioni colpose gravi o gravissime, commesse con violazione delle norme antinforturistiche e sulla tutela dell'igiene e della sicurezza sul lavoro (art. 25-septies);
- reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (25-octies);
- delitti in materia di violazioni del diritto d'autore (art. 25-novies);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies);
- reati ambientali (25-undecies);
- reati di impiego di lavoratori stranieri privi di permesso di soggiorno o con permesso scaduto (art. 25-duodecies);
- delitti di razzismo e xenofobia (25-terdecies);
- frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies);
- reati tributari (25-quinquiesdecies);
- delitti di contrabbando, previsti dal Decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 (art. 25-sexiesdecies);
- reati transnazionali introdotti nell'ordinamento italiano dalla Legge 16.3.2006 n. 146;

B. suggerisce i controlli da implementare al fine di contrastare o ridurre efficacemente la probabilità di commissione reato e/o mitigare quei rischi la cui esposizione sia da considerare di livello non accettabile ai fini di un efficace modello di organizzazione, gestione e controllo.

2. L'analisi di rischio: executive summary

Al fine di svolgere una sistematica rilevazione del livello di rischio a cui è esposto SIAER sono state realizzate delle interviste con il personale.

Il Team di analisi è stato composto da personale dello Studio legale Avv.ti R. Montagnani – P. Loberti S.T.P.:

Avv. Roberto Montagnani

Dott.ssa Fulvia Montagnani

Le interviste sono state condotte al fine di acquisire le seguenti informazioni:

1. una descrizione delle principali attività svolte dal personale nell'ambito dell'operatività dell'Associazione;
2. la rilevazione della documentazione normativa esistente (es. regolamenti, policy, procedure, organigrammi e mansionari);
3. l'identificazione del sistema dei controlli (es. esistenza e/o adozione di codici di comportamento o di specifiche direttive, esistenza di meccanismi e/o di organi di controllo interni).

Il personale da intervistare e le aree oggetto di intervista sono state individuate in modo congiunto tra il Team ed il referente interno di SIAER nella persona del Responsabile dell'Amministrazione.

Il punto di partenza per l'esecuzione di una verifica di conformità al D.Lgs. 231/2001 è l'identificazione dei processi aziendali. Nell'attività di analisi si è cercato di seguire, ove possibile, una logica di processo anziché di mera responsabilità funzionale, anche e soprattutto, tenendo conto della natura e dell'attività di SIAER, che è una Società consortile che ha la finalità di gestire ed amministrare le risorse che le sono attribuite in favore dei soci consorziati.

Di seguito sono indicati le Aree/Processi analizzati:

- Direzione
- Amministrazione
- Area Informatica

Le interviste condotte e l'analisi documentale evidenziano una realtà complessa, dovuta anche alla natura delle attività di SIAER, in cui il ruolo della Direzione è ben presente in tutti i processi aziendali ed è condiviso con tutto il personale.

L'analisi di rischio ha rilevato come l'attività sia adeguatamente regolamentata attraverso procedure documentate e/o coerenti con l'attuale operatività, con positive ricadute sull'applicazione dei principi di segregazione dei compiti e tracciabilità delle attività principali del processo.

2.1 Tabella riepilogativa reati-processi

Il dettaglio delle criticità connesse ad ogni area/processo analizzati ed i relativi controlli suggeriti, sono evidenziati nella descrizione dei processi riportata nel documento allegato: "Schede processo".

Di seguito si riepilogano i processi di SIAER teoricamente esposti ai reati previsti dal D.Lgs. 231/2001:

Reati contro la Pubblica Amministrazione (artt. 24 e 25)

Direzione

Amministrazione

Delitti informatici e trattamento illecito dei dati (art. 24-bis)

Direzione

Area Informatica

Delitti di criminalità organizzata

(art. 24-ter)

La Società non risulta significativamente esposta a questa classe di reati

**Falsità in monete, in carte di pubblico credito, in valori di bollo
e in strumenti o segni di riconoscimento**

(art. 25-bis)

La Società non risulta significativamente esposta a questa classe di reati

Delitti contro l'industria ed il commercio

(art. 25-bis 1)

La Società non risulta significativamente esposta a questa classe di reati

Reati societari

(art. 25-ter)

La Società non risulta significativamente esposta a questa classe di reati

**Delitti in materia di terrorismo e di eversione
dell'ordine democratico**

(art. 25-quater)

La Società non risulta significativamente esposta a questa classe di reati

Mutilazione dei genitali femminili

(art. 25-quater 1)

La Società non risulta significativamente esposta a questa classe di reati

Delitti contro la personalità individuale

(art. 25-quinquies)

La Società non risulta significativamente esposta a questa classe di reati

Reati di abuso del mercato

(art. 25-sexies)

La Società non risulta significativamente esposta a questa classe di reati

**Reati di omicidio colposo e lesioni colpose, gravi o gravissime,
commesse con violazione delle norme infortunistiche e sulla
tutela dell'igiene e della sicurezza sul lavoro**

(art. 25-septies)

Direzione

Amministrazione

**Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro,
beni o utilità di provenienza illecita**

(art. 25-octies)

Direzione

Amministrazione

Delitti in materia di violazione del diritto d'autore

(art. 25-novies)

La Società non risulta significativamente esposta a questa classe di reati

**Induzione a non rendere dichiarazioni
o a rendere dichiarazioni mendaci all'autorità giudiziaria
(art. 25-decies)**

Direzione

**Reati ambientali
(art. 25-undecies)**

La Società non risulta significativamente esposta a questa classe di reati

**Reati di impiego di lavoratori stranieri privi di permesso
di soggiorno o con permesso scaduto
(art. 25-duodecies)**

La Società non risulta significativamente esposta a questa classe di reati

**Delitti in materia di razzismo e xenofobia
(art. 25-terdecies)**

La Società non risulta significativamente esposta a questa classe di reati

**Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa
e giochi d'azzardo esercitati a mezzo di apparecchi vietati
(art. 25-quaterdecies)**

La Società non risulta significativamente esposta a questa classe di reati

**Reati tributari
(art. 25-quinquiesdecies)**

Direzione

Amministrazione

**Reati transnazionali introdotti
dalla legge 16.03.2006 n. 146**

La Società non risulta significativamente esposta a questa classe di reati

3. Il dettaglio dell'analisi del rischio

A fronte delle informazioni raccolte, confrontando la rilevanza delle attività svolte con il sistema di controlli esistente, è stato attribuito ai processi aziendali un indice di rischio su due livelli (basso-medio).

3.1 Tabella riepilogativa criticità-controlli

La tabella successiva riepiloga, per ognuna delle aree analizzate, gli elementi emersi dalla rilevazione ed i controlli suggeriti.

Direzione

I reati che vengono in evidenza sono:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- violazione delle norme sulla tutela e sicurezza del lavoro (art. 25-septies);
- ricettazione, riciclaggio, autoriciclaggio (art. 25-octies);

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci All'autorità Giudiziaria (art. 25-decies)

Indice di rischio: medio

Criticità

La mancata formalizzazione di alcune logiche operative dei momenti di controllo sull'attività della Società, espone quest'ultima a possibili fraintendimenti sul rischio di esposizione di fatti illeciti, anche a titolo di concorso, (esempio: reati ai danni della P.A.). Tale rischio è ancor più difficile da prevedere se l'attività è gestita di concerto da più soggetti o unità cooperanti.

Esiste sempre il rischio, nel contatto diretto con le Istituzioni Pubbliche, di commissione di atti corruttivi.

Per quanto concerne i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, è necessario assicurare un sistema di gestione che garantisca il controllo sulla conformità agli adempimenti previsti dalla normativa in materia SSL.

Controlli suggeriti

Come riportato nel Codice Etico, ogni operazione e transazione deve essere legittima, autorizzata, registrata, verificabile e coerente con le prescrizioni di SIAER. In qualunque momento dovrà essere possibile risalire all'iter di decisione, autorizzazione e successivo svolgimento della operazione/transazione.

Ogni operazione/transazione deve essere correlata da un adeguato supporto documentale che ne consenta di individuare le caratteristiche di decisione, autorizzazione e svolgimento.

Per la prevenzione degli infortuni sul lavoro, serve la definizione di specifici flussi informativi e momenti di comunicazione ai soggetti interessati. In particolare va assicurato il rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro e va curata la predisposizione delle misure di prevenzione e di protezione conseguenti. Si raccomandano periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Amministrazione

I reati che vengono in evidenza sono:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- ricettazione, riciclaggio, autoriciclaggio (art. 25-octies);

Indice di rischio: medio

Criticità

Sussiste il rischio di commissione di fatti corruttivi in maniera strisciante, laddove si consideri che la stipulazione di un contratto per una prestazione inesistente può costituire il mezzo per far ottenere, direttamente o indirettamente, il prezzo della stessa ad un Pubblico Ufficiale o a un Incaricato di Pubblico Servizio; oppure attraverso la costituzione di fondi neri, da utilizzare a fini corruttivi.

Controlli suggeriti

La scelta dei fornitori sulla base di criteri oggettivi, e le modalità di controllo della congruità delle forniture, rappresentano un buono schermo alla possibilità della commissione dei reati in esame.

Il pagamento delle forniture deve avvenire esclusivamente a seguito della ricezione di documenti fiscalmente validi.

Inoltre il pagamento deve avvenire solamente se vi è identità tra il soggetto che ha fornito il bene o servizio e il soggetto destinatario del pagamento.

Si raccomandano controlli di congruità delle forniture, atti a dimostrarne la coerenza con l'ordine di acquisto.

I sistemi di incasso/pagamento devono essere tutti fondati su strumenti tracciabili.

Il rispetto dei ruoli e del sistema delle deleghe non può essere solamente formale, ma sostanziale.

Il controllo sui documenti (fatture, ricevute, ecc.) oltre che di natura documentale (importo fattura/ordine) deve essere anche di merito. I documenti di spesa devono essere siglati e si deve poter risalire al decisore.

Vengono effettuati bilanci di verifica infrannuali, oltre al bilancio preventivo, che viene costruito in collaborazione con la Direzione.

I rapporti con gli Organi preposti alla vigilanza (Organo di Controllo e OdV) devono essere improntati alla collaborazione e correttezza.

Le delibere devono essere tenute raccolte e in ordine cronologico.

Il sistema delle deleghe consente un controllo incrociato dotato di coerenza interna e di sistematicità.

Area Informatica

I reati che vengono in evidenza sono:

- delitti informatici (art. 24-bis);

Indice di rischio: basso

Criticità

Non si ha evidenza di specifiche misure di prevenzione e/o controllo adottate, oltre quelle disciplinate dal Disciplinare Tecnico, Misure minime di sicurezza all. B del D. Lgs. n. 196/03.

Tali contromisure non sono sufficientemente efficaci a contrastare il rischio di commissione dei reati previsti dagli artt. 24-bis e soprattutto 25-novies, con riferimento particolare al rischio di utilizzo di programmi non originali.

Controlli suggeriti

Adottare alcune limitazioni per gli utenti, definendo quali sono le esclusive prerogative (“privilegi”) dell’amministratore, riconoscendole quindi come soli “privilegi amministratore”(installazione software e loro utilizzo, ecc.).

Implementazione di un filtro Proxy (in conformità alla normativa Privacy).

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Sommario

- 1 Scopo e applicabilità
- 2 Generalità
- 3 Divieti generali di comportamento
- 4 Visite ispettive da parte della P.A.
- 5 Gestione dei procedimenti giudiziari o arbitrali

1 Scopo e applicabilità

La presente procedura ha lo scopo di fornire ai destinatari informazioni utili a scongiurare la commissione di reati derivanti da rapporti con la Pubblica Amministrazione, ovvero le fattispecie previste dagli articoli 24, 25 e 25-*novies* del D. Lgs. 231/01.

Si applica alle seguenti attività considerate a rischio reato ex D.Lgs. 231/2001:

- la gestione del contenzioso nelle varie sedi di interesse (penale, civile, amministrativo, tributario, giuslavoristico, arbitrale etc.);
- la gestione dei rapporti con le Istituzioni e le Autorità Pubbliche di Vigilanza e la gestione delle ispezioni.

Eventuali integrazioni delle suddette attività a rischio potranno essere disposte dall'Organismo di Vigilanza.

2 Generalità

Al fine di perseguire l'obiettivo della massima integrità e correttezza, ispirandosi alla più rigorosa osservanza delle disposizioni di legge, la gestione dei rapporti, di qualsiasi genere, con la PA è riservata esclusivamente ai soggetti autorizzati e deve esserne garantita la tracciabilità dei contatti.

La gestione dei rapporti con la PA prevede il coinvolgimento di più figure:

1. Coordinatore
2. Amministrazione, per gli aspetti economici

3 Divieti generali di comportamento

La presente procedura vieta, coerentemente a quanto previsto nel Codice Etico, ai destinatari che operino nelle attività a rischio reato, ovvero le fattispecie previste dagli articoli 24, 25 e 25-*novies* del D.Lgs. n. 231/2001, di porre in essere, collaborare o, comunque, dare causa alla realizzazione di comportamenti che, individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato sopra considerate.

Nell'ambito dei suddetti comportamenti i destinatari sono obbligati ad astenersi:

- dall'effettuare elargizioni in denaro, distribuire qualsiasi forma di regalo o accordare vantaggi di qualsiasi natura in favore di funzionari pubblici italiani ed esteri o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi indebito vantaggio alla Cassa Edile;
- dal destinare somme ricevute da organismi pubblici nazionali o comunitari a scopi diversi da quelli per cui sono stati destinati;
- dal presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di trarre un ingiustificato vantaggio, o dall'indurre, in qualunque modo e sotto qualsiasi forma, a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- dall'adottare comportamenti che possano indurre a provvedimenti che vadano illegittimamente a vantaggio della Cassa Edile quando sia "parte" in procedimenti contenziosi in sede civile, penale od amministrativa;

- dall'ostacolare od interferire con l'attività di chiunque venga a svolgere ispezioni e controlli legittimamente autorizzati dalle competenti Autorità.

4 Visite ispettive da parte della Pubblica Amministrazione

Segnalazione

In caso di ispezione (preventivamente comunicata o improvvisa) da parte di rappresentanti della PA, il Responsabile della funzione interessata dall'ispezione inoltra immediata segnalazione al CdA. Questi ne dà pronta comunicazione all'OdV.

Gestione del rapporto e chiusura dell'attività

L'Amministrazione dovrà:

- attivare tutti gli interventi di natura organizzativa-contabile utili a fornire la massima collaborazione all'Ente Pubblico richiedente, secondo le modalità e le tempistiche stabiliti dalla normativa applicabile;
- garantire, nel corso dell'attività ispettiva, che da parte delle funzioni e delle articolazioni organizzative ispezionate, ci sia massima collaborazione all'espletamento degli accertamenti;
- partecipare alle ispezioni;
- redigere una specifica nota sull'andamento dell'ispezione, nel caso in cui la PA non dovesse rilasciare alcun verbale o in accompagnamento a questo.

I verbali redatti dalle pubbliche autorità dovranno essere conservati a cura dell'Amministrazione.

Copia dei verbali dovrà essere inviata all'OdV.

5 Gestione di procedimenti giudiziari o arbitrari

Segnalazione

Qualora SIAER, in persona del legale rappresentante, sia coinvolto in un procedimento giudiziale, del procedimento se ne dà comunicazione all'Organismo di Vigilanza.

In base alla tipologia della citazione, il Presidente provvede alla nomina di un legale secondo quanto previsto dalla procedura di affidamento Incarichi Professionali, attribuendogli formale procura secondo quanto previsto dalle norme del Modello.

Tutte le attività successive sono coordinate dal legale incaricato e dove coinvolgano il personale della Società come supporto tecnico-informativo in sede di giudizio, questi dovranno essere in possesso di procure speciali o deleghe di rappresentanza.

Nel caso di proposta di transazione, il Legale incaricato ne informa il Consiglio di Amministrazione, che procede ad una valutazione il cui esito è registrato in specifico verbale.

GESTIONE DELLA DOCUMENTAZIONE

Sommario

- 1 Scopo e campo di applicazione
- 2 Generalità
- 3 Gestione dei Documenti
 - 3.1 Redazione ed approvazione
 - 3.2 Struttura dei documenti
 - 3.3 Distribuzione dei documenti e comunicazione modifiche
 - 3.4 Documenti di origine esterna

1 Scopo e campo di applicazione

La presente procedura descrive modalità e responsabilità di gestione dei documenti e dei dati previsti dal Modello di Organizzazione Gestione e Controllo ex D.lgs. n. 231/2001.

2 Generalità

Il Modello di SIAER prevede le seguenti tipologie di documenti:

- il Modello stesso;
- il Codice Etico;
- Regolamenti;
- Procedure: esplicitano ruoli, responsabilità, regole e meccanismi operativi di funzionamento e di controllo di un processo aziendale;
- Disposizioni Operative: integrano, ove necessario, le procedure descrivendo in dettaglio o chiarendo le attività svolte nell'attuazione di un processo. Generalmente sono a diffusione interna alle funzioni interessate;
- Modulistica: è una tipologia di documenti costituiti da Tabelle e Moduli da utilizzare nello svolgimento di specifiche attività di processo;
- Documenti di registrazione: si tratta dei documenti che vengono prodotti come esito delle attività svolte, così come previsto dall'operatività aziendale. Tali documenti attestano l'avvenuta esecuzione delle attività stesse;
- Documenti di origine esterna: leggi e decreti applicabili alla realtà della Società.

Tutti i documenti in vigore sono pubblicati e disponibili all'interno della rete locale e il loro stato di aggiornamento e conservazione è a carico dell'Amministrazione.

3 Gestione dei Documenti

3.1 Redazione ed approvazione

L'emissione dei documenti, distinta in base alla tipologia, prevede una fase di redazione ed una di approvazione del contenuto che ne autorizza la circolazione ufficiale, per taluni documenti è prevista una fase di verifica. Dove previsto, a seguito della sua approvazione il documento è pubblicato all'interno della rete locale.

La Direzione approva i documenti e ne autorizza la circolazione.

3.2 Struttura dei documenti

I documenti possono essere redatti in formato libero ma, a seconda della tipologia, devono riportare le seguenti informazioni:

Modello

Frontespizio

Identificazione

Autore

la dicitura SIAER Soc. Cons. a r.l.

sigla dove viene data la connotazione del documento (Relazione, Programma ..)
nominativo dell'autore

Intestazione
Piè di pagina

riferimento all'Area di provenienza
numerazione e eventuale dicitura "Riservato"

3.3 Distribuzione dei documenti e comunicazione modifiche

La distribuzione dei documenti avviene tramite pubblicazione all'interno della rete locale, accompagnata da una comunicazione interna ai vari responsabili, i quali sono preposti a portare a conoscenza di tutti i propri collaboratori i contenuti degli stessi.

Tutta la documentazione in vigore è accessibile in sola lettura ai dipendenti nell'apposita sezione della rete locale.

3.4 Documenti di origine esterna

Sono documenti prodotti da strutture esterne alla Società e il cui contenuto ha impatto sui processi e sulle attività.

Responsabile del loro aggiornamento è l'Amministrazione.

APPROVVIGIONAMENTI E INCARICHI PROFESSIONALI

Sommario

- 1 Scopo e applicabilità
- 2 Generalità
- 3 Qualifica dei fornitori
- 4 Acquisto di beni e servizi
 - 4.1 Esigenza di acquisto e autorizzazione
 - 4.2 Selezione del fornitore
- 5 Affidamento di incarichi professionali
- 6 Verifica della fornitura

1 Scopo e applicabilità

La presente procedura ha lo scopo di descrivere attività e responsabilità legate al processo di gestione degli approvvigionamenti di beni e affidamento di incarichi professionali, nonché alle attività di selezione, qualifica e monitoraggio dei fornitori.

La presente procedura è definita in conformità alle previsioni di cui al Modello di organizzazione e gestione adottato da SIAER, diretto alla prevenzione dei reati, ovvero le fattispecie previste dagli articoli 24, 25 e 25-*octies* del D.Lgs. n. 231/2001.

2 Generalità

SIAER ha deciso di disciplinare il processo di acquisto di forniture e servizi necessari all'attuazione degli scopi istituzionali.

3 Qualifica dei fornitori

La gestione del processo di approvvigionamento e affidamento di incarichi professionali prevede che sia possibile emettere ordini relativi a beni e servizi di norma nei confronti di partner preventivamente qualificati. L'iter di qualifica avviene secondo quanto previsto nella presente procedura.

La qualifica è effettuata prendendo in considerazione i seguenti elementi:

- solidità economico/finanziaria (quando possibile);
- referenze disponibili;
- storicità;
- capacità tecnica e qualitativa della fornitura o del servizio consulenziale,
- rispetto di eventuali vincoli legislativi.

I Professionisti (consulente legale, consulente lavoro, docente, ecc.) sono selezionati secondo i seguenti elementi:

- posizionamento sul mercato;
- referenze disponibili;
- storicità;
- iscrizione ad albi.

Per ogni fornitore qualificato è conservata la documentazione che ha portato il fornitore alla qualifica, ove possibile, per alcune categorie merceologiche considerate non strategiche (es. commodities), all'interno dell'elenco verrà inserito più di un fornitore per categoria.

4 Acquisto di beni e servizi

4.1 Esigenza di acquisto e autorizzazione

L'Amministrazione cura i rapporti con i fornitori, e stila gli ordini di acquisto.

Per gli acquisti di rilevante importo è richiesto il preventivo assenso del Presidente, mentre il Coordinatore vista gli acquisti di importo modesto.

4.2 Selezione del fornitore

Al verificarsi della prima necessità di acquisto, per prodotti o servizi mai approvvigionati, per ogni tipologia di bene o servizio, ad eccezione degli incarichi professionali e delle docenze, l'Area richiedente procede attraverso trattativa privata seguendo le seguenti fasi:

- invio ai fornitori della richiesta di offerta (oggetto della fornitura, requisiti richiesti, termine e modalità di presentazione delle offerte);
- ricezione offerte;
- valutazione delle stesse (secondo il criterio dell'offerta economicamente più vantaggiosa) da parte dell'Amministrazione.

Per gli acquisti presso fornitori qualificati la selezione del fornitore può avvenire per affidamento diretto ad un partner qualificato, applicando ove possibile un criterio di rotazione. Se fosse necessario rivolgersi a nuovi fornitori questi devono essere preventivamente qualificati secondo quanto previsto nella presente procedura.

5 Affidamento incarichi professionali

La determinazione dell'incarico professionale muove da diverse esigenze:

- consulenza e tutela legale (civile, penale, amministrativa)
- consulenza amministrativa, organizzativa e fiscale
- consulenza per attività di formazione e qualificazione professionale

Individuata l'esigenza, l'Amministrazione o il Consiglio di Amministrazione si attiva per la ricerca del Professionista, provvedendo dopo apposita valutazione dell'offerta all'affidamento dell'incarico.

Ci si attiva per la ricerca sul mercato, in base ai seguenti criteri:

- tipologia del servizio di consulenza richiesta;
- referenze reperibili sul mercato;
- precedenti relazioni avute con il fornitore.

6 Verifica della fornitura

L'Amministrazione verifica la qualità della fornitura.

Le eventuali anomalie rilevate devono essere comunicate all'Organismo di Vigilanza.

A fronte dell'esito positivo della verifica si procede al pagamento delle fatture relative.

Per gli affidamenti di incarichi professionali l'evidenza del controllo è riconducibile al benessere al pagamento delle fatture relative.