ESEB
ENTE SISTEMA EDILIZIA BRESCIA

MODELLO DI ORGANIZZAZIONE E GESTIONE

Ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

INDICE

PARTE GENERALE

1. IL DECRETO LEGISLATIVO 231/2001

a. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI
b. I REATI PREVISTI DAL DECRETO
c. LE SANZIONI PREVISTE DAL DECRETO
d. CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA
e. I REATI COMMESSI ALL'ESTERO

2. L'ADOZIONE DEL MODELLO

a. ESEB Ente Sistema Edilizia Brescia
b. APPROCCIO METODOLOGICO AL MODELLO
c. IL MODELLO E IL CODICE ETICO A CONFRONTO
d. I DESTINATARI DEL MODELLO

3. L'ORGANISMO DI VIGILANZA

a. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA INTERNO "OdV"
b. FUNZIONI E POTERI
c. REPORTING DELL'ORGANISMO DI VIGILANZA AGLI ORGANI SOCIETARI
d. REPORTING: PRESCRIZIONI GENERALI E PRESCRIZIONI SPECIFICHE OBBLIGATORIE
e. RACCOLTA, CONSERVAZIONE E ARCHIVIAZIONE DELLE INFORMAZIONI

4. FORMAZIONE E DIFFUSIONE DEL MODELLO

a. DIPENDENTI
b. COLLABORATORI ESTERNI E PARTNER

5. IL SISTEMA DISCIPLINARE

a. PRINCIPI GENERALI
b. MISURE NEI CONFRONTI DEI DIPENDENTI
c. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI
d. MISURE NEI CONFRONTI DI SOGGETTI ESTERNI: COLLABORATORI, CONSULENTI E ALTRI SOGGETTI TERZI

PARTE SPECIALE

INTRODUZIONE

6. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

a. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)
b. AREE DI ATTIVITA' A RISCHIO ("ATTIVITA' SENSIBILI")
c. DESTINATARI DELLA PARTE SPECIALE
d. PRINCIPI GENERALI DI COMPORTAMENTO
e. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI PRESCRITTI
f. PROCEDURE DI PREVENZIONE

7. REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O ALTRE UTILITÀ DI PROVENIENZA ILLECITA E AUTORICICLAGGIO

a. LA FATTISPECIE DI REATO
b. DESTINATARI DELLA PARTE SPECIALE
c. AREE DI ATTIVITA' A RISCHIO
d. PRINCIPI DI CONTROLLO RILEVANTI

8. REATI SOCIETARI

a. LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25 TER DEL DECRETO)
b. AREE DI ATTIVITA' A RISCHIO
c. DESTINATARI DELLA PARTE SPECIALE

d. PRINCIPI GENERALI DI COMPORTAMENTO
e. PRINCIPI DI CONTROLLO

9. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

a. LA FATTISPECIE DI REATO
b. AREE DI ATTIVITA' A RISCHIO
c. DESTINATARI DELLA PARTE SPECIALE
d. PRINCIPI GENERALI DI COMPORTAMENTO
e. PROCEDURE DI PREVENZIONE

10. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME

a. LA FATTISPECIE DI REATO
b. AREE DI ATTIVITA' A RISCHIO
c. DESTINATARI DELLA PARTE SPECIALE
d. PRINCIPI GENERALI DI COMPORTAMENTO
e. PROCEDURE DI PREVENZIONE

11. REATI IN MATERIA DI VIOLAZIONE DEI DIRITTI D'AUTORE

a. LA FATTISPECIE DI REATO
b. AREE DI ATTIVITA' A RISCHIO
c. DESTINATARI DELLA PARTE SPECIALE
d. PRINCIPI GENERALI DI COMPORTAMENTO
e. PROCEDURE DI PREVENZIONE

12. REATI AMBIENTALI

a. REATI AMBIENTALI (art.25- *undecies*, D.lvo n. 231/01)- FATTISPECIE DI REATO RILEVANTI
b. ATTIVITA' SENSIBILI
c. MODALITA' DI ATTUAZIONE DEI REATI ASTRATTAMENTE IPOTIZZABILI
d. PROCEDURE DI PREVENZIONE

13. ATTIVITA' STRUMENTALI ALLA COMMISSIONE DEI REATI

a. ATTIVITA' STRUMENTALI ALLA COMMISSIONE DEI REATI

STATUTO ORGANISMO DI VIGILANZA

REGOLAMENTO ORGANISMO DI VIGILANZA

SISTEMA DISCIPLINARE

CODICE ETICO

Parte Generale

1 Il Decreto Legislativo 231/2001

A) La Responsabilità amministrativa degli enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 (di seguito denominato anche il "Decreto" o "D.Lgs. 231/2001"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione di funzionari delle Comunità Europee o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Il Decreto ha introdotto nell'ordinamento giuridico la responsabilità amministrativa degli enti per gli illeciti dipendenti da reato. Le disposizioni in esso previste si applicano agli "*enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica" (di seguito anche solo "enti")*.

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta tuttavia taluni caratteri propri della responsabilità penale, essendo ad esempio rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare ed essendo estese all'ente le garanzie del processo penale.

Il Decreto stabilisce che:

1. 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;
    b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
2. L'ente non risponde se le persone indicate nel punto 1 hanno agito nell'interesse esclusivo proprio o di terzi.

Oltre all'esistenza degli elementi oggettivi e soggettivi sopra descritti, il D.Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è in definitiva riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione dei reati elencati al successivo paragrafo, da parte dei soggetti individuati nel Decreto.

La responsabilità amministrativa dell'ente è quindi ulteriore e diversa da quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile.

La responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma di tentativo (ai sensi dell'art. 26 del D.Lgs. 231/2001), vale a dire quando il soggetto agente compie atti idonei diretti in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica.

B) I reati previsti dal Decreto

I reati, dal cui compimento può derivare la responsabilità amministrativa dell'ente, sono quelli espressamente richiamati dal D.Lgs. 231/2001 e successive modifiche ed integrazioni.

Si elencano di seguito le "famiglie di reato" attualmente ricomprese nell'ambito di applicazione del D.Lgs. 231/2001:

1. **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**(Art. 24, D.Lgs. n. 231/2001)
2. **Delitti informatici e trattamento illecito di dati** (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008]
3. **Delitti di criminalità organizzata** (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009]
4. **Concussione, induzione indebita a dare o promettere altra utilità e corruzione** (Art. 25, D.Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012]
5. **Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (**Art. 25-bis, D.Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009]
6. **Delitti contro l'industria e il commercio** (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]
7. **Reati societari** (Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012 e dalla L. n. 69/2015]
8. **Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali** (Art. 25-quater, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003]
9. **Pratiche di mutilazione degli organi genitali femminili** (Art. 583-bis c.p.) (Art. 25- quater.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006]
10. **Delitti contro la personalità individuale** (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003]
11. **Reati di abuso di mercato** (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]
12. **Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con**

violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25- septies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007]

13. **Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 231/2007; modificato dalla L. n. 186/2014]
14. **Delitti in materia di violazione del diritto d'autore** (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]
15. **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]
16. **Reati ambientali** (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011 e modificato dalla L. n. 68/2015]
17. **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (Art. 25- duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012]
18. **Reati transnazionali** (L. n. 146/2006)

C) Le sanzioni previste dal Decreto

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale. L'accertamento della responsabilità può comportare l'applicazione di sanzioni gravi e pregiudizievoli per la vita dell'ente stesso, quali:

a) sanzioni pecuniarie;
b) sanzioni interdittive;
c) confisca;
d) pubblicazione della sentenza.

In particolare le sanzioni interdittive, che si applicano in relazione ai reati per i quali sono espressamente previste, possono comportare importanti restrizioni all'esercizio dell'attività di impresa dell'ente, quali:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrattare con la Pubblica Amministrazione, salvo che per le prestazioni del pubblico servizio;
d) esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
e) divieto di pubblicizzare beni o servizi.

Tali misure possono essere applicate all'ente anche in via cautelare, e dunque prima dell'accertamento nel merito in ordine alla sussistenza del reato e dell'illecito amministrativo che da esso dipende, nell'ipotesi in cui si ravvisi l'esistenza di gravi indizi tali da far ritenere la responsabilità dell'ente, nonché il pericolo di reiterazione dell'illecito.

Nell'ipotesi in cui il giudice ravvisi l'esistenza dei presupposti per l'applicazione di una misura interdittiva a carico di un ente che svolga attività di interesse pubblico ovvero abbia un consistente numero di dipendenti, lo stesso potrà disporre che l'ente continui a operare sotto la guida di un commissario giudiziale.

D) Condizione esimente della Responsabilità amministrativa

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da soggetti apicali, non risponda qualora dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (c.d. "Organismo di Vigilanza, nel seguito anche "Organismo" o "O.d.V.");

c) le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;

d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui il reato sia stato commesso da soggetti sottoposti alla direzione o alla vigilanza del personale apicale, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, adotti e dia concreta attuazione ad un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, va esente da responsabilità se risultano integrate le condizioni di cui all'art. 6 del Decreto.

In tal senso il Decreto fornisce specifiche indicazioni in merito alle esigenze cui i Modelli Organizzativi devono rispondere:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
- prevedere specifici "protocolli" diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'O.d.V.;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Tuttavia la mera adozione di un Modello Organizzativo, non è di per sé sufficiente ad escludere detta responsabilità, essendo necessario che il modello sia effettivamente ed efficacemente attuato. In particolare ai fini di un efficace attuazione del Modello, il Decreto richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

D I) reati commessi all'estero

In forza dell'art. 4 del Decreto, l'ente può essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati. In particolare, l'art. 4 del Decreto prevede che gli enti aventi la sede principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, l'ente è perseguibile quando:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica);
- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità *ex* art. 6 del codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

2 L'adozione del Modello

A) ESEB Ente Sistema Edilizia Brescia

La Ente Sistema Edilizia Brescia (E.S.E.B.) è un Ente Paritetico Sociale con compiti di interesse pubblico, la cui attività statutaria è la promozione della formazione e della sicurezza nel settore edile.
E' gestita da un consiglio di Amministrazione costituito da rappresentanti eletti dalle organizzazioni imprenditoriali (Collegio Costruttori) e sindacali (Filca-Cisl, Feneal-Uil, Fillea-Cgil).

Sin dalla sua fondazione a Brescia nel 1946, il pensiero fu rivolto all'importanza dell'istruzione professionale, intesa nel senso di promozione della cultura del mestiere.
Seguendo di pari passo i molteplici mutamenti nel tessuto sociale, la ente ha da sempre risposto con un'offerta formativa all'insegna della qualità.

Nell'anno 2002 la Regione Lombardia riconosce la Ente Sistema Edilizia Brescia come "Ente accreditato", nel 2017 la Scuola Edile si è fusa con il CTP. Questi traguardi hanno consentito di ampliare l'offerta formativa grazie anche ai finanziamenti concessi dal Fondo Sociale Europeo.

Mission

Mission dell'ente è lo svolgimento di attività formative e di supporto alle imprese edili nell'ottica di una attenzione focalizzata al cliente e di una corretta comunicazione verso lo stesso come espresso nella politica qualità. .
Si persegue, inoltre, una diffusione e condivisione della mission e dei valori dell'Ente fra tutti coloro che operano per il raggiungimento della buona riuscita delle attività e dei servizi formativi offerti da ESEB, siano essi componenti della organizzazione che fornitori della stessa.

ESEB sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, nonché consapevole dell'importanza di assicurare condizioni di correttezza nella conduzione degli affari e nelle attività

aziendali a tutela della posizione e dell'immagine propria e delle aspettative dei soci, ***adotta il Modello di Organizzazione, Gestione e Controllo*** *previsto dal decreto, fissandone i principi di riferimento.*

Obiettivi del Modello e suoi punti cardine
Tale iniziativa, sebbene non imposta dal decreto[1], si propone inoltre di sensibilizzare tutti coloro che operano in nome e/o per conto della Ente, affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari al fine di prevenire il rischio di commissione dei reati contemplati nel decreto stesso.

Il Modello è stato predisposto sulla base delle prescrizioni del Decreto e delle Linee Guida elaborate da CONFINDUSTRIA, sulle altre linee guida elaborate da enti e associazioni di categoria e alla luce della più recente giurisprudenza.

Il Modello si pone come obiettivo principale quello di configurare un sistema strutturato e organico di procedure e attività di controllo, volto a prevenire, per quanto possibile, la commissione di condotte idonee a integrare i reati contemplati dal Decreto.

Attraverso l'individuazione delle attività esposte al rischio di reato (**"attività sensibili"**) e la loro conseguente proceduralizzazione, si vuole:

- da un lato determinare una piena consapevolezza di tutti coloro che operano in nome e per conto di ESEB di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla Ente, in quanto contraria ai suoi interessi anche quando, apparentemente, potrebbe trarne un vantaggio economico immediato;
- dall'altro, grazie ad un monitoraggio costante dell'attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione di reati stessi.

Punti cardine del Modello, oltre ai principi sopra riportati, sono:

- la mappatura delle attività a rischio, ossia quelle attività nel cui ambito è più probabile la commissione dei reati previsti dal Decreto, le "attività sensibili" appunto;
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- la verifica e la documentazione di ogni operazione rilevante;
- l'applicazione ed il rispetto del principio di separazione delle funzioni, in base al quale nessuno può gestire in autonomia un intero processo;
- l'attribuzione di poteri coerenti con le responsabilità organizzative;
- la verifica ex post dei comportamenti aziendali, nonché del funzionamento del Modello, con conseguente aggiornamento periodico;
- la diffusione ed il coinvolgimento di tutti i livelli aziendali nell'attuazione di regole comportamentali, procedure e politiche aziendali.

Struttura del Modello: Parte Generale e Parte Speciale
Il Modello è suddiviso nelle seguenti parti:

- **Parte Generale**, che contiene i punti cardine del Modello e tratta del funzionamento dell'Organismo di Vigilanza e del sistema sanzionatorio, facendo peraltro rinvio al Codice Etico;
- **Parte Speciale**, il cui contenuto è costituito dalle diverse tipologie di reato previste dal Decreto, ossia i reati realizzabili nei rapporti con la Pubblica Amministrazione, reati di ricettazione, riciclaggio ed impiego di denaro, beni o altre utilità di provenienza illecita, i reati societari, i reati informatici e trattamento illecito di dati, i reati di omicidio colposo e lesioni colpose gravi e gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro, reati commessi in materia di violazione dei diritti d'autore, reati ambientali. Infine l'ultimo capitolo è dedicato alle "Attività strumentali alla commissione dei reati".

Nell'eventualità in cui si rendesse necessario procedere all'integrazione della Parte Speciale, relativamente a nuove fattispecie di reato che fossero in futuro incluse nell'ambito di applicazione del Decreto, è demandato

[1] Che indicano il Modello come elemento facoltativo e non obbligatorio. L'adozione del Modello è un requisito richiesto dall'accreditamento regionale.

all'organo amministrativo della Ente il potere di integrare il presente Modello in una fase successiva, mediante apposita delibera.

Approvazione del Modello
Il presente Modello, costituito dalla Parte Generale, dalla Parte Speciale è stato approvato dal Consiglio di Amministrazione di ESEB in data 21 dicembre 2017.

Modifiche e aggiornamento del Modello Come sancito dal Decreto, il Modello è "atto di emanazione dell'organo dirigente"[2]. Di conseguenza le successive modifiche nonché eventuali integrazioni sostanziali sono rimesse alle competenze del Consiglio di Amministrazione di ESEB.

Tuttavia è riconosciuta, in via generale, al Presidente dell'Ente – previa informativa all'Organismo di Vigilanza – la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

Approccio metodologico al Modello

Ai fini della redazione ed implementazione del Modello organizzativo e di gestione ex D.Lgs. n. 231/2001, l'approccio metodologico adottato ha previsto le seguenti fasi:

- individuazione delle aree potenzialmente esposte al rischio di commissione di reati;
- "*risk assessment*" dei processi inerenti alle aree di rischio individuate, con descrizione delle relative criticità eventualmente riscontrate;
- individuazione di soluzioni ed azioni volte al superamento o alla mitigazione delle criticità rilevate;
- adeguamento e stesura di procedure organizzative sulle aree individuate e potenzialmente a rischio, contenenti disposizioni vincolanti ai fini della ragionevole prevenzione delle irregolarità di cui al Decreto;
- elaborazione del Codice Etico;
- redazione di un sistema disciplinare per sanzionare il mancato rispetto delle misure indicate nel Modello;
- regolamento dell'Organismo di Vigilanza;
- piano di formazione e comunicazione del Modello.

1. La metodologia di risk assessment

L'efficace esecuzione del progetto e l'esigenza di adottare criteri oggettivi, trasparenti e tracciabili per la costruzione del Modello organizzativo ha richiesto l'utilizzo di adeguate metodologie e di strumenti tra loro integrati.
L'attività condotta è stata improntata al rispetto del Decreto e delle altre norme e regolamenti applicabili alla Ente per gli aspetti non regolamentati, al rispetto:

- delle linee guida emanate da CONFINDUSTRA in tema di "modelli organizzativi e di gestione" nonché di quelle che saranno eventualmente elaborate da altre associazioni nel corso della durata del progetto;
- del principio di "*best practice*" in materia di controlli .

L'attività preliminare di valutazione è stata indirizzata ai processi ed alle funzioni aziendali che, in base ai risultati dell'analisi di "risk assessment preliminare", sono stati individuati come più esposti ai reati previsti dal Decreto. Come, ad esempio:

- le funzioni che abitualmente intrattengono relazioni significative con pubbliche amministrazioni, ai diversi livelli nazionali, regionali, provinciali e comunitari;
- i processi e le funzioni aziendali che assumono rilievo nelle aree amministrative, finanziarie e degli acquisti che, anche per esplicito richiamo normativo, costituiscono aree a più alta esposizione a rischio.

2. Fasi operative

L'approccio metodologico adottato è stato implementato e sviluppato attraverso una serie di fasi operative. L'inizio di tale attività ha richiesto una preventiva acquisizione di dati ed informazioni sul sistema organizzativo della Ente e sui processi operativi, utili ai fini della pianificazione di dettaglio delle singole fasi.
L'implementazione della suddetta metodologia si è articolata nelle seguenti fasi:

[2] Art. 6, comma 1, lettera a) del Decreto.

- Pianificazione
- Diagnosi
- Progettazione
- Predisposizione
- Implementazione.

Fase 1: Pianificazione

In questa fase si è proceduto alla raccolta della documentazione ed al reperimento delle informazioni utili alla conoscenza dell'attività e del sistema organizzativo dell'Ente.

Tali informazioni riguardano, tra l'altro, a mero titolo informativo:

- i settori in cui la Ente opera;
- la tipologia delle relazioni e delle attività intrattenute con le Pubbliche Amministrazioni;
- i casi di eventuali presunte irregolarità avvenute in passato;
- il quadro regolamentare e procedurale interno (ad esempio: deleghe di funzioni, processi decisionali, procedure operative ISO o non ISO, protocolli);
- la documentazione inerente ordini di servizio, comunicazioni interne ed ogni altra evidenza documentale utile alla migliore comprensione delle attività svolte dall'Ente e del sistema organizzativo.

La raccolta delle informazioni è stata svolta mediante analisi documentale e interviste ai responsabili delle diverse funzioni/settori aziendali e, comunque, al personale che è stato ritenuto utile allo scopo sulla base delle specifiche competenze.

Si evidenzia che la nozione di Pubblica Amministrazione considerata ai fini della individuazione delle aree a rischio è stata dedotta dagli artt. 357 e 358 c.p. , in base ai quali: sono pubblici ufficiali e incaricati di pubblico servizio tutti coloro che – legati o meno da un rapporto di dipendenza con la P.A. – svolgono un'attività regolata da norme di diritto pubblico e atti autoritativi.

Fase 2: Diagnosi

Tale fase è stata caratterizzata dal completamento dell'analisi di risk assessment avviata nella fase precedente di pianificazione, allo scopo di:

- effettuare una ricognizione delle funzioni/attività aziendali potenzialmente esposte ai rischi di reato ex D.Lgs 231/2001;
- analizzare il sistema organizzativo e di controllo nel suo complesso.

In sintesi l'analisi delle predette componenti si è incentrata:

- sulla verifica dell'adeguatezza del sistema organizzativo;
- sulla verifica dell'esistenza dei protocolli e delle procedure formalizzate per regolamentare le attività svolte dalle strutture nelle aree potenzialmente a rischio, tenendo conto delle fasi di istruzione e formazione delle decisioni aziendali;
- sulla verifica dell'esistenza di poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate e/o concretamente svolte;
- sulla verifica, per le singole attività potenzialmente a rischio reato, dell'esistenza di protocolli, procedure e di regole di comportamento, individuando le integrazioni necessarie per una maggior aderenza ai principi espressi dal D.Lgs. n. 231/2001;
- sulla verifica dell'adeguatezza del sistema disciplinare vigente diretto a sanzionare l'eventuale violazione dei principi e delle disposizioni volte a prevenire la commissione dei reati, sia da parte dei dipendenti dell'Ente – dirigenti e non – sia da parte di Amministratori e collaboratori esterni;
- sulla verifica dell'esistenza di forme di comunicazione e formazione per il personale, in considerazione della necessità che, iniziative dirette a dare attuazione al D.Lgs n. 231/2001, debbano essere programmate e finalizzate alla comunicazione del Modello organizzativo.

I risultati ottenuti dalla suddetta analisi hanno costituito la base per la progettazione del presente Modello organizzativo.

Fase 3: Progettazione

Tale fase si è articolata nello svolgimento della *As is analysis* sui protocolli, procedure e/o strumenti di controllo esistenti allo scopo di verificare la ragionevole efficacia degli *existing controls* a prevenire le irregolarità. Tale attività si è fondata sulla comprensione del livello di proceduralizzazione delle attività aziendali risultate esposte a rischio, nonché del grado di conoscenza, applicazione, comunicazione, aggiornamento e controllo delle eventuali procedure, protocolli esistenti poste al loro presidio.

Più in particolare e coerentemente con quanto emerso nella "mappatura" aziendale dei rischi, tale fase ha riguardato:

- la verifica/censimento di protocolli, procedure operative e/o strumenti di controllo già esistenti per ciascuna area potenzialmente a rischio. In particolare:
    i. sono stati rilevati gli aspetti di criticità e di carenza nei sistemi di controllo esistenti nell'ottica di prevenire ragionevolmente le ipotesi di reato previste dal Decreto;
    ii. sono state formulate raccomandazioni, suggerimenti e linee guida sulle integrazioni e miglioramenti da apportare in modo da superare ragionevolmente le criticità rilevate.

Questa attività di verifica, in coerenza con i criteri metodologici sopra individuati, è stata svolta attraverso una preliminare richiesta alle strutture coinvolte di avviare una autoanalisi sulle possibili e potenziali aree di rischio nell'ambito delle attività svolte da ciascuna di esse ed una verifica delle procedure, protocolli interni esistenti nelle aree individuate.

La progettazione del sistema di *reporting* informativo consente all'Organismo di Vigilanza di ricevere informazioni ed aggiornamenti sullo stato delle attività risultate potenzialmente esposte a rischio.

Fase 4: Predisposizione

Tale fase ha condotto alla redazione del Modello organizzativo mediante la materiale predisposizione e/o adattamento degli strumenti organizzativi di cui si compone, ritenuti più opportuni a valorizzare l'efficacia dell'azione di prevenzione dei reati, come nella:

- redazione e revisione delle procedure operative per le aree/attività ritenute potenzialmente a rischio in quanto prive di presidi di controllo;
- elaborazione del codice etico e quindi di principi etici per le aree/attività ritenute potenzialmente a rischio in quanto prive di presidi di controllo;
- elaborazione del sistema disciplinare interno graduato secondo la gravità delle violazioni;
- definizione dei poteri, compiti e responsabilità dell'Organismo di vigilanza e suoi rapporti con le strutture aziendali;
- progettazione delle iniziative in tema di comunicazione e di formazione etica e prevenzione dei reati.

Fase 5: Implementazione

In tale fase l'attività condotta ha l'obiettivo di rendere operativo il Modello nel suo complesso, mediante:

- la sua formale adozione a mezzo approvazione da parte del Consiglio di Amministrazione;
- la definitiva attuazione e comunicazione degli elementi di cui esso si compone: codice etico, procedure operative, organismo di vigilanza, piano di comunicazione e formazione, sistema disciplinare.

Risulta evidente che sarà compito dell'Organismo di Vigilanza nella conduzione dei suoi primi interventi e nella gestione dinamica del Modello di controllo, individuare i criteri cui ispirarsi nella:

- conduzione delle verifiche periodiche di controllo del Modello e dei suoi elementi costitutivi;
- aggiornamento della "mappa" delle aree a rischio-reato e le azioni necessarie a conservare nel tempo l'efficacia del Modello nella prevenzione dei reati;

- attività di reporting informativo agli organi sociali per la modifica o integrazione degli elementi sostanziali di rischio.

2.2 Il Modello ed il Codice Etico a confronto

Il Modello risponde all'esigenza di prevenire, per quanto possibile, la commissione di reati previsti dal Decreto attraverso la predisposizione di regole di comportamento specifiche.
Da ciò emerge chiaramente la differenza con il Codice Etico, che è strumento di portata generale, finalizzato alla promozione di un'etica aziendale, ma privo di una specifica proceduralizzazione.

Tuttavia, anche in considerazione di quanto contenuto nelle Linee Guida di CONFINDUSTRIA, si tende a realizzare una stretta integrazione tra Modello e Codice Etico, in modo da formare un *corpus* di norme interne con lo scopo di incentivare la cultura dell'etica e della trasparenza aziendale.

I comportamenti di dipendenti e amministratori ("Dipendenti"), di coloro che agiscono, anche nel ruolo di consulenti o comunque con poteri di rappresentanza della Ente ("Consulenti") e delle altre controparti contrattuali di ESEB, quali ad esempio eventuali partner in joint venture, ATI etc ("partner"), devono conformarsi alle regole di condotta – sia generali sia specifiche – previste nel Modello e nel Codice Etico.

In particolare:

- I Dipendenti, i Consulenti e i Partner non devono porre in essere quei comportamenti:
  - che integrano le fattispecie di reato previste dal Decreto;
  - che ESEB bene non costituiscano di per sé un'ipotesi di reato, possano potenzialmente diventarlo;
- I Dipendenti, i Consulenti e i Partner devono evitare di porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione;
- È fatto divieto di effettuare elargizioni in denaro a pubblici funzionari;
- È obbligatorio il rispetto della prassi aziendale per la distribuzione di omaggi e regali;
- I rapporti nei confronti della Pubblica Amministrazione devono essere gestiti in modo unitario, intendendosi con ciò che le persone che rappresentano la Ente nei confronti della Pubblica Amministrazione devono aver ricevuto un esplicito mandato da parte dell'Ente;
- Coloro che svolgono una funzione di controllo e supervisione verso i Dipendenti che operano con enti pubblici devono seguire con attenzione e con le modalità più opportune l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- I compensi dei Consulenti e dei Partner devono essere determinati solo per iscritto;
- Nessun tipo di pagamento può essere effettuato in contanti o in natura se superiore a 5.000 euro;
- Devono essere rispettati, da parte degli Amministratori, i principi di trasparenza nell'assunzione delle decisioni aziendali che abbiano diretto impatto sui soci e su terzi;
- Devono essere istituite, da parte degli Amministratori, e immediatamente comunicate all'Organismo di Vigilanza apposite procedure per consentire l'esercizio del controllo nei limiti previsti (ai soci, agli altri organi, alle società di revisione) e il rapido accesso alle informazioni attribuite da leggi e regolamenti, con possibilità di riferirsi al Collegio Sindacale in caso di ostacolo o rifiuto.

I destinatari del Modello

Le regole contenute nel Modello si applicano a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo dell'Ente, ai dipendenti, nonché a coloro i quali, pur non appartenendo all'Ente, operano su mandato della medesima o sono legati all'Ente stesso da rapporti aventi carattere di continuità.

ESEB comunica il presente Modello attraverso modalità idonee ad assicurarne l'effettiva conoscenza da parte di tutti i dipendenti.
I soggetti ai quali il Modello si rivolge sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con l'Ente.

ESEB condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse dell'Ente ovvero con l'intenzione di arrecare ad essa un vantaggio.

3 L'Organismo di Vigilanza

Nel caso in cui si verifichino fatti integranti i reati previsti il Decreto[3] pone come condizione per la concessione dell'esimente dalla responsabilità amministrativa che sia stato affidato a un organismo dell'Ente (dotato di autonomi poteri di iniziativa e di controllo) il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

A Identificazione dell'Organismo di Vigilanza interno

In attuazione di quanto previsto dal decreto, l'organismo cui affidare tale compito è stato individuato nelle figura di avvocato in qualità di membro esterno e Presidente dell'organismo stesso, nella figura di un commercialista in qualità di altro membro esterno e nella figura di responsabile amministrativo in qualità di membro interno, con delibera del Consiglio di Amministrazione del 22 dicembre 2010 e successive, sentito il Collegio Sindacale.

B) Funzioni e poteri

All'Organismo di Vigilanza è affidato il **compito di vigilare** sull':

- **Effettività** del Modello: ossia vigilare affinché i comportamenti posti in essere all'interno dell'Ente corrispondano al modello predisposto;
- **Efficacia** del Modello: ossia verificare che il Modello predisposto sia concretamente idoneo a prevenire il verificarsi dei reati previsti dal Decreto e dai successivi provvedimenti che modifichino il campo di applicazione;
- **Opportunità di aggiornamento** del Modello al fine di adeguarlo ai mutamenti ambientali e alle modifiche della struttura aziendale.

Su di un piano più operativo è affidato all'Organismo di Vigilanza il compito di:

- Verificare periodicamente la mappa delle aree di rischio reato (o attività sensibili) al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Ente a rischi di reato. Tutte le comunicazioni devono essere esclusivamente in forma scritta;
- Effettuare periodicamente, anche utilizzando professionisti esterni, verifiche volte all'accertamento di quanto previsto dal Modello, in particolare assicurare che le procedure, i protocolli e i controlli previsti siano posti in essere e documentati in maniera conforme e che i principi etici siano rispettati. Si osserva, tuttavia, che le attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale;
- Verificare l'adeguatezza e l'efficacia del Modello nella prevenzione dei reati di cui al Decreto;
- Effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere, soprattutto, nell'ambito delle attività sensibili i cui risultati vengano riassunti in un apposito rapporto il cui contenuto sarà esposto nel corso delle comunicazioni agli organi societari;
- Coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per uno scambio di informazioni per tenere aggiornate le aree a rischio reato per:
  - Tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;
  - Verificare i diversi aspetti attinenti l'attuazione del Modello (definizione di clausole standard, formazione del personale, cambiamenti normativi ed organizzativi, etc);

[3] Art. 6, lett. b).

    - Garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace siano intraprese tempestivamente;
- Raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute nel rispetto del Modello, nonché aggiornare la lista delle informazioni che allo stesso devono essere trasmesse. A tal fine l'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale rilevante e deve essere costantemente informato dal management;
    - Sugli aspetti dell'attività aziendale che possono esporre l'Ente al rischio conseguente alla commissione di uno dei reati previsti dal decreto;
    - Sui rapporti con Consulenti e Partner;
- Promuovere iniziative per la formazione e la comunicazione del Modello e predisporre la documentazione necessaria a tal fine;
- Interpretare la normativa rilevante e verificare l'adeguatezza del sistema di controllo interno in relazione a tali prescrizioni normative;
- Riferire periodicamente al Consiglio di Amministrazione e al Collegio Sindacale in merito all'attuazione delle politiche aziendali per l'attuazione del Modello.

La struttura così identificata deve essere in grado di agire nel rispetto dell'esigenza di recepimento, verifica e attuazione dei Modelli richiesti dall'art. 6 del decreto, ma anche, necessariamente, rispetto all'esigenza di costante monitoraggio dello stato di attuazione e della effettiva rispondenza degli stessi modelli alle esigenze di prevenzione che la legge richiede. Tale attività di costante verifica deve tendere in una duplice direzione:

- Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente, è compito dell'Organismo di Vigilanza adottare tutte le iniziative necessarie per correggere questa situazione. Si tratterà allora, a seconda dei casi e delle circostanze, di:
    - Sollecitare i responsabili delle singole unità organizzative al rispetto del Modello di comportamento;
    - Indicare direttamente quali correzioni e modificazioni debbano essere apportate alle ordinarie prassi di attività;
    - Segnalare i casi più gravi di mancata attuazione del Modello ai responsabili e agli addetti ai controlli all'interno delle singole funzioni;
- Qualora,invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento, che pertanto risulti integralmente e correttamente attuato, ma si riveli non idoneo allo scopo di evitare il rischio di verificarsi di taluno dei reati previsti dal decreto, sarà proprio l'Organismo di Vigilanza a doversi attivare per garantire l'aggiornamento nonché i tempi e le forme dell'adeguamento.[4]

A tal fine, come anticipato, l'Organismo di Vigilanza deve avere libero accesso alle persone e a tutta la documentazione aziendale e la possibilità di acquisire dati e informazioni rilevanti dai soggetti responsabili. Infine all'Organismo di Vigilanza devono essere segnalate tutte le informazioni come di seguito specificato.

C) Reporting dell'Organismo di Vigilanza agli Organi Societari

L'Organismo di Vigilanza ha la responsabilità nei confronti dell'organo amministrativo di comunicare:

- All'inizio di ciascun esercizio il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
- Periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;
- Immediatamente eventuali problematiche significative scaturite dalle attività;
- Almeno annualmente in merito all'attuazione del modello da parte dell'Ente.

L'Organismo di Vigilanza potrà essere invitato a relazione periodicamente al Collegio Sindacale e al Consiglio di Amministrazione in merito alle proprie attività.

L'Organismo di Vigilanza deve inoltre, valutando le singole circostanze:

[4] Tempi e forme, naturalmente, non predeterminati. I tempi devono comunque intendersi come i più solleciti possibile e il contenuto sarà quello imposto dalle rilevazioni che hanno determinato l'esigenza di adeguamento.

1. Comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per le attività suscettibili di miglioramento, nonché le specifiche delle modifiche necessarie per realizzare l'implementazione;
2. Segnalare eventuali comportamenti/azioni non in linea con il Codice Etico e con le procedure e/o protocolli aziendali, al fine di:
    a. Acquisire tutti gli elementi per effettuare comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
    b. Evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.

Le attività indicate al punto 2) dovranno essere comunicate dall'Organismo di Vigilanza al Consiglio di Amministrazione nel più breve tempo possibile, richiedendo anche il supporto di altre strutture aziendali, che possano collaborare nell'attività di accertamento e nell'individuazione delle azioni volte a impedire il ripetersi di tali circostanze.
L'Organismo di vigilanza ha l'obbligo di informare immediatamente il Collegio Sindacale qualora la violazione riguardi i vertici dell'Ente e/o il Consiglio di Amministrazione.

Le copie dei relativi verbali saranno custodite dall'Organismo di Vigilanza e dagli organismi di volta in volta coinvolti.

D) Reporting: prescrizioni generali e prescrizioni specifiche obbligatorie

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei soggetti tenuti all'osservanza del Modello, in merito a eventi che potrebbero ingenerare responsabilità della Ente ai sensi del Decreto.

Prescrizioni di carattere generale
Valgono al riguardo le seguenti prescrizioni di carattere generale:

- Devono essere raccolte da ciascun Responsabile di Funzione eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal Decreto o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello;
- Ciascun dipendente deve segnalare la violazione (o presunta violazione) del Modello contattando il proprio diretto superiore gerarchico e/o l'Organismo di Vigilanza (con disposizione dell'Organismo di Vigilanza sono istituiti eventualmente "canali informativi dedicati" per facilitare il flusso di segnalazioni / informazioni ufficiose);
- I consulenti, i collaboratori ed i partner, per quanto concerne la loro attività svolta nei confronti di ESEB, effettuano le segnalazioni direttamente all'Organismo di Vigilanza mediante "canali informativi dedicati" che sarà compito dell'Organismo di Vigilanza stessa definire;
- L'Organismo di Vigilanza valuta le segnalazioni ricevute e le attività da porre in essere; gli eventuali provvedimenti conseguenti sono definiti e applicati in conformità a quanto infra previsto in ordine al sistema disciplinare.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione e, in ogni caso, sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti di ESEB o delle persone accusate in mala fede.

Prescrizioni specifiche obbligatorie
Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza le notizie relative:

- Ai procedimenti penali e disciplinari azionati in relazione a notizia di violazione del Modello;
- Alle sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- Alle ispezioni o iniziative di qualsivoglia autorità pubblica di vigilanza.

Reporting da parte di esponenti aziendali o di terzi

In ambito aziendale dovrà essere portata a conoscenza dell'Organismo di Vigilanza, oltre alla documentazione prescritta nella Parte Speciale del Modello secondo le procedure ivi contemplate, ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi e attinente all'attuazione del Modello nelle aree di attività a rischio.

Valgono al riguardo le seguenti prescrizioni:

- Devono essere raccolte eventuali segnalazioni relative alla commissione di reati previsti dal Decreto in relazione alle attività aziendali o, comunque, a comportamenti non in linea con le linee di condotta adottate da ESEB;
- L'afflusso di segnalazioni, incluse quelle di natura ufficiosa, deve essere canalizzato verso l'Organismo di Vigilanza che valuterà le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti a procedere a un'indagine interna;
- Le segnalazioni, in linea con quanto previsto dal Codice Etico, potranno essere in forma scritta ed avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'Organismo di Vigilanza prenderà in considerazione anche le segnalazioni anonime, intendendosi per segnalazione anonima qualsiasi segnalazione in cui le generalità del segnalante non siano esplicitate, né siano rintracciabili, fatta eccezione per quelle segnalazioni di contenuto generico e/o confuso. In ogni caso, l'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione e penalizzazione, assicurando altresì la riservatezza e l'anonimato del segnalante, fatti salvi obblighi di legge e la tutela dei diritti degli Enti o delle persone accusate in mala fede;
- È prevista l'istituzione di "canali informativi dedicati" con duplice funzione: quella di facilitare il flusso di segnalazioni e informazioni verso l'Organismo di Vigilanza e quella di risolvere velocemente casi di dubbio.

E) Raccolta, conservazione e archiviazione delle informazioni

Ogni informazione, segnalazione, report previsti dal Modello viene conservata dall'Organismo di Vigilanza stesso.

4 Formazione e diffusione del Modello

A) Dipendenti

Formazione dei dipendenti
ESEB riconosce e ritiene che, ai fini dell'efficacia del presente Modello, sia necessario garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute sia nei confronti dei Dipendenti di sede che dei c.d. "esterni". Tale obiettivo riguarda tutte le risorse aziendali che rientrano nelle due categorie anzidette – comprendendo altresì nella seconda categoria tutte quelle risorse che operano in stretta collaborazione con ESEB – sia che si tratti di risorse già presenti c/o l'Ente sia che si tratti di risorse da inserire.

A tal fine ESEB si impegna ad effettuare (destinando a ciò risorse umane e finanziarie) programmi di formazione ed informazione attuati con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle "attività sensibili".

La formazione del personale è pertanto considerata da ESEB condizione indispensabile per una efficace attuazione del Modello. Tale formazione sarà da effettuarsi periodicamente e con modalità che garantiscano l'obbligatorietà della partecipazione ai corsi, controlli di frequenza e controlli di qualità sul contenuto dei programmi.

La formazione è gestita dall'Organismo di Vigilanza in stretta collaborazione con il vertice aziendale e con il RAQ.
La formazione potrà essere articolata con seminari; occasionali e-mail di aggiornamento; informativa con la lettera di assunzione per i neo-assunti; con nota informativa interna o, in ogni caso, mediante modalità che saranno ritenute idonee in base al livello ed al ruolo ricoperto dal singolo Dipendente, nonché in relazione al differente coinvolgimento dello stesso nelle "attività sensibili".

B) Collaboratori Esterni e partner

Informativa a Collaboratori Esterni e Partner
Potranno essere altresì forniti a soggetti esterni a ESEB apposite informative sulle politiche e le procedure adottate sulla base del presente Modello organizzativo, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

5 Il sistema disciplinare

A) Principi generali

Ai sensi degli artt. 6, comma 2, lett. e) e 7, comma 4, lett. b) del Decreto il Modello può ritenersi efficacemente attuato solo qualora preveda un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso indicate.

Tale sistema disciplinare si rivolge ai dipendenti ed ai dirigenti, prevedendo adeguate sanzioni di carattere disciplinare.
La violazione delle regole di comportamento del Codice Etico e delle misure previste dal Modello, da parte di lavoratori dipendenti dell'Ente e/o dei dirigenti dello stesso, costituisce un inadempimento alle obbligazioni del rapporto di lavoro, ai sensi dell'art. 2104 c.c. e dell'art. 2106 c.c. .
Le infrazioni dei principi sanciti nel Codice Etico e delle misure previste dal Modello, le relative sanzioni irrogabili e il procedimento disciplinare sono descritti nella sezione specifica del Codice Etico, approvato dal Consiglio di Amministrazione in data 22 dicembre 2010.
L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta, i protocolli e le procedure interne sono vincolanti per i destinatari, indipendentemente dall'effettiva realizzazione di un reato quale conseguenza del comportamento commesso.

B) Misure nei confronti dei Dipendenti

L'art. 2104 c.c. , individuando il dovere di "obbedienza" a carico del lavoratore, dispone che il prestatore di lavoro deve osservare nello svolgimento del proprio lavoro le disposizioni di natura sia legale che contrattuale impartite dal datore di lavoro. In caso di inosservanza di dette disposizioni il datore di lavoro può irrogare sanzioni disciplinari, graduate secondo la gravità dell'infrazione, nel rispetto delle previsioni contenute nel CCNL applicabile.

Il sistema disciplinare deve in ogni caso rispettare i limiti concessi al potere sanzionatorio imposti dalla Legge n. 300 del 1970 (cd "Statuto dei Lavoratori") e dalla contrattazione collettiva di settore, sia per quanto riguarda le sanzioni irrogabili che per quanto riguarda le forme di esercizio di tale potere.

In particolare il sistema disciplinare deve risultare conforme ai seguenti **principi**:

- Il sistema deve essere debitamente pubblicizzato mediante affissione in luogo accessibile ai dipendenti ed eventualmente oggetto di specifici corsi di aggiornamento e di informazione;

- Le sanzioni non possono comportare mutamenti definitivi del rapporto di lavoro e devono essere conformi al principio di proporzionalità rispetto all'infrazione, la cui specificazione è affidata, ai sensi dell'art. 2106 c.c. alla contrattazione collettiva di settore;
- La multa non può essere di importo superiore a 3 ore della retribuzione base;
- La sospensione dal servizio e dalla retribuzione non può superare i 3 giorni o, nel caso di violazioni di particolare gravità, 6 giorni;
- Deve essere assicurato il diritto di difesa al lavoratore cui sia stato contestato l'addebito.

C) Misure nei confronti degli Amministratori

In caso di violazione della normativa vigente, del Modello o del Codice Etico da parte degli Amministratori di ESEB, l'Organismo di Vigilanza informa il Consiglio di Amministrazione e il Collegio Sindacale, i quali provvedono ad assumere le opportune iniziative previste dalla vigente normativa.

D) Misure nei confronti di soggetti esterni

Ogni comportamento posto in essere da collaboratori, consulenti o altri terzi collegati a ESEB da un rapporto contrattuale non di lavoro dipendente, in violazione delle previsioni del Modello e/o del Codice Etico, potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o anche in loro assenza, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni all'Ente, anche indipendentemente dalla risoluzione del rapporto contrattuale.

Parte Speciale

Introduzione

Nella Parte Speciale, che segue, saranno analizzate le attività considerate come “sensibili” ai fini del Decreto in relazione al tipo di attività di ESEB. Saranno in particolare analizzate le attività che presentano profili di rischiosità in relazione alle seguenti tipologie di reato:

1. Reati contro la Pubblica Amministrazione;
2. Reati di ricettazione, riciclaggio ed impiego di denaro, beni o altre utilità di provenienza illecita;
3. Reati societari e corruzione tra privati;
4. Delitti informatici e trattamento illecito di dati;
5. Reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro;
6. Reati commessi in violazione dei diritti d’autore;
7. Attività strumentali alla commissione dei reati.

6 Reati contro la Pubblica Amministrazione

6.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione

Con specifico riferimento ai reati di cui agli artt. 24 e 25 del Decreto, si elencano di seguito le fattispecie del Decreto identificate quali rilevanti, in relazione all'operatività dell'Ente, nell'ambito della presente Parte Speciale:

- Malversazione a danno dello Stato (art. 316 bis c.p.) – art. 24 Decreto;

Tale ipotesi di reato si configura nel caso in cui, dopo aver ricevuto finanziamenti o contributi da parte dello Stato o di altro ente pubblico o delle Comunità Europee, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.) – art. 24 Decreto;

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.
La fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio, comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.) – art. 24 Decreto;

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità Europee.

- Truffa ai danni dello Stato (art. 640 c. 2 c.p.) – art. 24 Decreto;

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore o da arrecare un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea).Tale reato può realizzarsi, ad esempio, qualora nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere supportate da documentazione artefatta al fine di ottenere l'aggiudicazione della gara stessa.

- Frode informatica (art. 640 ter c.p.) – art. 24 Decreto;

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informativo o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o a un altro ente pubblico.
Il reato può essere integrato, ad esempio, qualora una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

- Concussione (art. 317 c.p.) – art. 25 Decreto;
- Corruzione per l'esercizio della funzione (artt. 318, 320 c.p.) – art. 25 Decreto;
- Corruzione per un atto contrario ai doveri d'ufficio (artt. 319, 319 bis, 320 c.p.) – art. 25 Decreto;
- Corruzione in atti giudiziari (art. 319 ter c.p.) – art. 25 Decreto;
- Pene per il corruttore (art. 321 c.p.) – art. 25 Decreto;
- Istigazione alla corruzione (art. 322 c.p.) – art. 25 Decreto;
- Induzione indebita a dare o promettere utilità (art. 319 quater c.p.) – art. 25 Decreto;
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) – art. 25 Decreto.

- Corruzione tra privati (Art. 25-*ter*, comma 1, lettera s-*bis*), nei casi di cui al nuovo terzo comma dell'art. 2635 codice civile.

---

1 Ai fini del presente documento, per Pubblica Amministrazione si intende qualsiasi persona fisica o giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autorizzativi.

In relazione all'operatività dell'Ente, a titolo esemplificativo e non esaustivo, si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione i seguenti:

- Amministrazioni dello Stato, anche a ordinamento autonomo, Comuni, Regioni e Province;
- i Ministeri, i Dipartimenti e le Commissioni;
- Aziende municipalizzate e gli Enti pubblici trasformati in S.p.A. (ad es.:Poste Italiane, FS, ecc.);
- Camere di commercio, industria, artigianato, agricoltura e l'Ufficio del Registro;
- gli enti pubblici economici e gli enti pubblici non economici nazionali, regionali e locali (INPS, ENASARCO, INAIL, ISTAT);
- le amministrazioni, le aziende e gli enti del Servizio Sanitario regionale;
- Banca d'Italia, Consob, Agenzia delle Entrate, Guardia di Finanza, Autorità Garante della Privacy, etc.

Per le finalità previste dal presente documento, si considerano non solo i rapporti "diretti", ma anche quelli "indiretti" con soggetti che - notoriamente - intrattengono rapporti di qualsivoglia natura (parentela, affinità, coniugo, convivenza, ecc.) con Pubblici Ufficiali o Incaricati di Pubblico Servizio.

6.2 Destinatari della Parte Speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dai dirigenti e dai dipendenti "esponenti aziendali" di ESEB nelle aree di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella Parte Generale (qui di seguito tutti denominati "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

6.3 Principi generali di comportamento

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

1. Mantenere una stretta osservanza di tutte le leggi e i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione e alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
2. Instaurare e mantenere qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza;
3. Instaurare e mantenere qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi.

La presente Parte Speciale prevede, conseguentemente, l'**espresso divieto** a carico degli Esponenti Aziendali in via diretta e a carico dei Collaboratori Esterni e Partner, di:

1. agire comportamenti tali da integrare le fattispecie di reato sopra considerate (Artt. 24 e 25 del Decreto);
2. agire comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra elencate possano potenzialmente diventarlo;
3. creare qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti, in particolare, anche per il tramite di collaboratori:

1. è vietato tenere rapporti con la Pubblica Amministrazione se non da parte dei soggetti a ciò deputati secondo l'organigramma dell'Ente (indicante da MAQ anche le funzioni svolte), ordini di servizio o eventuali deleghe;
2. è fatto divieto di offrire o effettuare, direttamente o indirettamente, pagamenti indebiti e promesse di vantaggi personali, di qualsiasi natura, ai rappresentanti della Pubblica Amministrazione italiana e straniera. Tale divieto include l'offerta, diretta o indiretta, di gratuita disponibilità di servizi, finalizzata a influenzare decisioni o transazioni;
3. è vietato distribuire ai rappresentanti della Pubblica Amministrazione omaggi o regali, salvo che si tratti di piccoli omaggi di modico (inferiore a 50 Euro) o simbolico valore e, in ogni caso, tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici;
4. è vietato presentare ad organismi pubblici nazionali o stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici e, in ogni caso, compiere qualsivoglia atto che possa trarre in inganno l'ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;
5. è fatto divieto destinare somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento a scopi diversi da quelli cui erano destinati;
6. è vietato ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;
7. è vietato versare a chiunque, a qualsiasi titolo, somme o dare beni o altre utilità finalizzati a facilitare e/o rendere meno onerosa l'esecuzione e/o la gestione di contratti con la Pubblica Amministrazione rispetto agli obblighi in essi assunti;
8. è vietato riconoscere compensi a consulenti, collaboratori o partner commerciali dell'Ente che non trovino giustificazione nelle attività effettivamente prestate;
9. è vietato alterare in qualsiasi modo i sistemi informatici e telematici della Ente o manipolarne i dati.

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

1. effettuare elargizioni in denaro a pubblici funzionari;
2. distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali e di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'Ente. Come previsto dal Codice Etico, gli omaggi consentiti si caratterizzano sempre per esiguità del valore o perché volti a promuovere l'immagine ed il marchio dell'Ente. Tutti i regali offerti – salvo quelli di modico valore – devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo;
3. accordare altri vantaggi di qualsiasi natura (promesse di assunzione etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto 2);
4. effettuare prestazioni in favore dei partner che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con i partner stessi;
5. riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
6. ricevere o sollecitare elargizioni in denaro, omaggi o vantaggi di altra natura, nell'ambito dell'esercizio di pubbliche funzioni o di pubblico servizio; chiunque riceve omaggi o vantaggi di altra natura non compresi nelle fattispecie consentite è tenuto, secondo le procedure stabilite, a darne comunicazione all'Organismo di Vigilanza, che ne valuta l'appropriatezza e provvede a far notificare a chi ha elargito tali omaggi la politica di ESEB in materia;
7. presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
8. destinare somme ricevute da organismi pubblici e nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopo diversi da quelli cui erano destinati;
9. conferire incarichi di consulenza a soggetti segnalati dalla Pubblica Amministrazione.

I presenti principi devono essere integrati con quelli indicati in relazione alle singole aree/processi a rischio di cui al seguente paragrafo 6.4

6.4 Aree di attività a rischio ("attività sensibili")

Processo Rischio Reato 1
Gestione Accreditamento Istituzionale

Funzioni coinvolte

- Presidente
- Comitato di Presidenza
- Direttore
- Responsabile qualità

PP.AA. interessate

- Regione Lombardia

Fattispecie di reato rilevanti nei rapporti con la P.A.

- Truffa ai danni della P.A.
- Corruzione e collegati

Attività sensibili

a. Monitoraggio dei requisiti necessari a mantenere l'accreditamento
b. Predisposizione della documentazione per il mantenimento/rinnovo dell'accreditamento
c. Gestione delle ispezioni/accertamenti/controlli/sopralluoghi da parte della Regione Lombardia sul possesso dei requisiti necessari per l'accreditamento
d. Consegna dei documenti in sede di ispezioni sul rispetto dei requisiti
e. Gestione dei rapporti con la Regione in costanza di accreditamento per comunicazioni relative alla variazione dei requisiti o risposte in merito a richieste di chiarimenti

Modalità di attuazione dei reati astrattamente ipotizzabili

CORRUZIONE E COLLEGATI

-Il personale della Ente potrebbe in astratto corrispondere o promettere di corrispondere al pubblico ufficiale denaro o altra utilità al fine di mantenere l'accreditamento in mancanza dei requisiti. In particolare, si potrebbe ipotizzare un patto corruttivo in sede di modifiche (esterne o interne) dei requisiti necessari a mantenere l'accreditamento ovvero i soggetti coinvolti nelle verifiche potrebbero astrattamente erogare o promettere di erogare al personale della P.A. (ad es. ispettori regionali) denaro o altra utilità al fine di 1)far ritenere adempiuti o parzialmente adempiuti, essendo invero inevasi o aggirati, gli obblighi di legge 2)omettere rilievi o non irrogare sanzioni a seguito della violazione di norme 3)indurre, in genere, i pubblici ufficiali a compiere, omettere o ritardare un atto del loro ufficio o compiere un atto contrario ai doveri del loro ufficio.

TRUFFA AI DANNI DELLA P.A.

Potrebbero ipotizzarsi falsità nelle dichiarazioni che attestano il possesso dei requisiti necessari ad ottenere il mantenimento dell'accreditamento, ovvero si potrebbe omettere di comunicare la perdita del possesso dei requisiti per l'accreditamento sia per ragioni interne che per intervenuta modifica normativa. In particolare, il personale della Ente potrebbe in via astratta alterare o contraffare della documentazione o dei dati da predisporre e trasmettere alla P.A., o rilasciare dichiarazioni non veritiere finalizzate al mantenimento dell'accreditamento in assenza dei presupposti.

Principi di controllo rilevanti

I protocolli che intervengono nella regolamentazione delle attività sensibili sono ispirati ai seguenti principi di controllo:

- il sistema interno di ripartizione dei poteri (procure, deleghe, e mansionari) deve essere coerente con le attività e i compiti effettivamente svolti dal personale. Particolare cura deve essere dedicata alla regolamentazione puntuale delle attribuzioni degli operatori dell'Ente che si interfacciano con esponenti della Regione per il mantenimento della struttura accreditata e per l'assistenza durante le operazioni ispettive e di controllo;
- devono essere ricostruibili a posteriori la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- i documenti relativi alla procedura devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;

- l'accesso ai documenti già archiviati deve sempre essere motivato e consentito solo alle persone autorizzate in base alle norme interne e per i rispettivi ambiti di competenza, al Collegio Sindacale, ai Revisori e all'Organismo di Vigilanza;
- i processi relativi alle verifiche di completezza e veridicità della documentazione da presentare alla P.A. per il mantenimento dell'accreditamento devono essere formalizzati;
- devono essere previsti processi di *audit* interno, su base periodica, relativi al mantenimento dei requisiti per l'accreditamento.

Processo Rischio Reato 2
Gestione Finanziamenti Sistema Dote

Funzioni coinvolte
- Presidente
- Comitato di Presidenza
- Amministrazione
- Direttore
- Responsabile DDIF
- Responsabile apprendistato
- Responsabili Doti comunque nominate (garanzia giovani, dote lavoro..)

PP.AA. interessate
- Regione Lombardia
- Provincia

Fattispecie di reato rilevanti
- Corruzione e collegati
- Truffa e frode ai danni della P.A.

Attività sensibili
a. Presentazione offerta formativa
b. Prenotazione dote
c. Scelta dei docenti
d. Svolgimento dei corsi /tenuta e controllo dei registri delle presenze
e. Inserimento dati rilevanti per ottenere il finanziamento nel sistema informatico interno ed esterno
f. Rendicontazione e invio richiesta liquidazione alla P.A.

Modalità di attuazione del reato astrattamente ipotizzabile
CORRUZIONE E COLLEGATI:
Astrattamente si potrebbe ipotizzare la corresponsione al pubblico ufficiale o incaricato di pubblico servizio di somme di denaro o altre utilità al fine di omettere rilievi nel corso delle visite di controllo sulla corretta gestione del sistema dote e, in generale, di indurre i pubblici ufficiali a compiere, omettere e/o ritardare uno più atti del loro ufficio ovvero compiere un atto contrario ai doveri del loro ufficio.
Si potrebbe anche ipotizzare la corruzione dei funzionari della Provincia in sede di individuazione delle priorità territoriali che condizionano la Regione nella concessione dei finanziamenti.

TRUFFA E FRODE AI DANNI DELLA P.A.:
Il personale della Ente potrebbe astrattamente indurre la P.A..in errore mediante artifici e raggiri posti in essere al fine di ottenere un ingiusto profitto con altrui danno ed in particolare,
- comunicando alla P.A. lo svolgimento di corsi in realtà mai svolti o erogati in misura inferiore a quanto dichiarato, con falsificazione di firme o in accordo con gli utenti. Indipendentemente dalla falsificazione delle firme sui registri potrebbero essere comunicate alla P.A. maggiori presenze di quelle realmente registrate nei registri cartacei.

Principi di controllo rilevanti
I protocolli e le procedure che intervengono nella regolamentazione delle attività sensibili sono ispirati ai seguenti principi di controllo:
- il sistema interno di ripartizione dei poteri (procure, deleghe, e mansionari) deve essere coerente con le attività e i compiti effettivamente svolti dal personale. Particolare cura deve essere dedicata alla regolamentazione puntuale delle attribuzioni degli operatori della Ente che si interfacciano con la P.A. per l'invio dei dati rilevanti e per l'assistenza durante le operazioni ispettive e di controllo;

- deve essere previsto un adeguato sistema di controlli sullo svolgimento dei corsi, sulla tenuta dei registri, sulla comunicazione dei dati rilevanti da inviare alla P.A.;
- devono essere ricostruibili a posteriori la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- i documenti relativi alla procedura devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- l'accesso ai documenti già archiviati deve sempre essere motivato e consentito solo alle persone autorizzate in base alle norme interne e per i rispettivi ambiti di competenza, al Collegio Sindacale, ai Revisori e all'Organismo di Vigilanza;
- i processi relativi alle verifiche di completezza e veridicità della documentazione da presentare alla P.A. devono essere formalizzati prevedendo la separazione delle funzioni e la presenza di controlli gerarchici sulle attività che presentano un maggior rischio di commissione dei reati;
- devono essere previsti processi di *audit* interno , su base periodica, relativi all'effettivo svolgimento dei servizi finanziati.

Processo rischio reato 3
Gestione progetti finanziati

Funzioni interessate
- Presidente
- Comitato di Presidenza
- Amministrazione
- Direttore
- Aree operative coinvolte nel progetto finanziato

P.P.A.A. interessate
- Regione Lombardia
-Enti Pubblici eroganti finanziamenti
-Altri enti anche privati auli Fondimpresa, Cassa edile

Fattispecie di reato rilevanti nei rapporti con la P.A.
- Corruzione e collegati
- Truffa e frodi a danno della P.A.

Attività sensibili
a. Preparazione e presentazione del progetto
b. Preparazione e presentazione documentazione di accompagnamento
c. Apertura buste
d. Scelta dei docenti
e. Svolgimento dei corsi formativi/tenuta e controllo dei registri delle presenze
f. Inserimento dati nel sistema informatico
g. Rendicontazione
h. Invio richiesta di finanziamento

Modalità di attuazione dei reati astrattamente realizzabili

CORRUZIONE E COLLEGATI:
Astrattamente si potrebbe ipotizzare la corresponsione al pubblico ufficiale o incaricato di pubblico servizio di somme di denaro o altre utilità al fine di ottenere il finanziamento o di omettere rilievi nel corso delle visite di controllo sulla corretta gestione dei corsi e, in generale, di indurre i pubblici ufficiali a compiere, omettere e/o ritardare uno più atti del loro ufficio ovvero compiere un atto contrario ai doveri del loro ufficio.

TRUFFA E FRODE AI DANNI DELLA P.A.:
Il personale della Ente potrebbe astrattamente indurre la PA in errore mediante artifici e raggiri posti in essere al fine di ottenere un ingiusto profitto con altrui danno ed in particolare attestando lo svolgimento di corsi mai tenuti o attestando la presenza ai corsi da parte di persone assenti.

La Ente, inoltre, potrebbe essere coinvolta ex d.lvo 231/2001 nella responsabilità connessa al reato di cui all'art. 316-*ter* c.p. (indebita percezione di erogazioni pubbliche) qualora utilizzi o presenti dichiarazioni o documenti falsi o attestanti cose non vere, ovvero ometta informazioni dovute nelle fasi di istruttoria, attuazione del progetto e relativa rendicontazione.
La violazione del vincolo di destinazione del finanziamento ottenuto a scopi diversi da quelli concordati con la P.A., come ad esempio qualora un finanziamento ottenuto per la realizzazione di corsi formativi venga utilizzato per altre finalità aziendali o per ottenere un profitto personale degli esponenti della Ente, integra invece il reato di malversazione (art. 316 bis c.p.).

Principi di controllo rilevanti
- il processo di gestione dei finanziamenti deve essere formalizzato sia nella fase di partecipazione al bando, attraverso la presentazione del progetto, che nelle fasi successive di rendicontazione, indicando precisamente le funzioni coinvolte e le attività che devono essere svolte;
-deve essere sempre previsto un controllo gerarchico sulla completezza e veridicità della documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali della Ente), nonché sulla veridicità e correttezza dei dati relativi alla rendicontazione (es. definizione dei criteri contabili per il calcolo del rendiconto, corretta allocazione dei costi, stato di avanzamento del progetto…);
-deve essere garantita la separazione funzionale tra chi gestisce e coordina le attività di realizzazione del progetto e chi predispone e presenta la documentazione sull'esistenza e avanzamento dei lavori;
-deve essere previsto un adeguato sistema di controlli sullo svolgimento dei corsi, sulla tenuta dei registri, sulla comunicazione dei dati rilevanti da inviare alla P.A.;
-deve essere ricostruibile a posteriori la formazione degli atti e i relativi livelli autorizzativi, a garanzia delle scelte effettuate. Ogni comunicazione interna relativa al finanziamento deve avvenire per iscritto;
-l'accesso ai documenti archiviati deve essere possibile solo in presenza di motivazione alle persone autorizzate in base alle norme interne e per i rispettivi ambiti di competenza, al Collegio Sindacale, ai Revisori e all'O.d.V;

Processi Strumentali
Seguendo la metodologia e la mappatura utilizzata per la individuazione dei processi "a rischio", sono state identificati alcuni processi considerati "strumentali", ossia che possono supportare funzionalmente la commissione degli illeciti nelle aree a rischio reato.

Rispetto ai reati contro la P.A., nella Ente i principali processi strumentali sono i seguenti.

I processi di acquisto di beni e servizi
Sul piano dei principi di controllo recepiti nei relativi protocolli sono rilevanti:
1) Una regolamentazione puntuale dell'albo fornitori/docenti ed il monitoraggio delle relative performance;
2) Sistemi di segregazione delle responsabilità in relazione alla manifestazione dei fabbisogni, scelta del fornitore/docente, autorizzazioni agli acquisti e relativi pagamenti;
3) Le verifiche di merito che precedono la fase di pagamento delle fatture di acquisto;
4) La formalizzazione di sistemi di autocertificazione circa eventuali rapporti di collegamento dei fornitori con esponenti della P.A.;
5) La richiesta di accettazione esplicita del Codice Etico tra le condizioni di contratto;
6) La formalizzazione del processo di scelta dei Fornitori/docenti che garantisca un elevato grado di professionalità.

Gestione risorse umane
Sul piano dei principi di controllo recepiti nei relativi protocolli sono rilevanti:
1) La formalizzazione del processo di selezione e valutazione del personale dipendente/consulenti con una chiara e documentata segregazione di funzioni e responsabilità tra i diversi soggetti che intervengono nei processi selettivi;
2) Una documentata azione di monitoraggio sulla presenza e permanenza dei requisiti professionali del personale/consulenti;
3) La formalizzazione dei sistemi di autocertificazione circa eventuali rapporti di parentela-colleganza dei candidati/dipendenti/consulenti con esponenti della P.A.;
4) L'accettazione esplicita tra le condizioni di assunzione-avvio della collaborazione del Codice Etico della Ente;
5) Qualora si voglia introdurre un sistema premiante, previsione di un sistema legato non esclusivamente al fatturato, bensì al gradimento degli utenti e delle aziende datori di lavoro dei partecipanti;

6) La formalizzazione della procedura di conferimento di incarichi di consulenza con previsione chiara dell'oggetto della prestazione e individuazione di un compenso in linea con gli standard di mercato, con allegata notazione interna che indichi le motivazioni in base alle quali è necessario per la Ente avvalersi di un professionista esterno.

I processi di contabilità, finanza e bilancio
Sul piano dei principi di controllo recepiti nei relativi protocolli sono rilevanti:

1) La presenza di processi di budget e di contabilità industriale;
2) Lo stringente monitoraggio di eventuali scostamenti rispetto a quanto pianificato;
3) Un sistema di verifica puntuale nel merito che preceda la fase di registrazione delle fatture passive;
4) La formalizzazione dei livelli di autorizzazione per disporre i pagamenti;
5) La limitazione delle operazioni effettuate in contanti e mediante la piccola cassa;
6) La presenza di sistemi interni per l'attestazione formale della veridicità dei dati inviati dalle diverse funzioni aziendali all'Ufficio contabilità e che confluiscono nella bozza di bilancio;

La gestione delle visite ispettive
Relativamente alla gestione delle visite ispettive/controlli della P.A.:

1) devono essere attribuiti formalmente i poteri interni e le relative responsabilità attraverso deleghe di funzione ai soggetti che devono presenziare alle ispezioni;
2) deve essere sempre prevista la presenza alle verifiche di almeno due soggetti del'Ente;
3) devono essere date chiare indicazioni sul comportamento da mantenere al fine di assicurare la massima trasparenza e collaborazione;
4) in caso di rilevazioni di criticità deve essere prevista la redazione di un report a cura dei soggetti della Ente che hanno presenziato alla verifica da inviare al superiore gerarchico e all'OdV insieme con il verbale redatto dal personale della P.A.

6.5 Principi di attuazione dei comportamenti prescritti

Ai fini dell'attuazione dei comportamenti di cui sopra, ESEB definisce dei principi di attuazione dei comportamenti prescritti all'interno delle attività sensibili che devono trovare precisa attuazione nelle procedure di prevenzione.

I principi di attuazione dei comportamenti prescritti sono di seguito riportati:

(I) Rapporti con i rappresentanti della Pubblica Amministrazione
I rapporti con i rappresentanti della Pubblica Amministrazione nello svolgimento delle operazioni attinenti le attività sensibili, sono tenuti dal Presidente oppure da un soggetto da questi delegato.

(II) Rapporti con consulenti e collaboratori
Non vi deve essere identità di soggetti, all'interno della Ente, tra chi richiede la consulenza e/o collaborazione, chi autorizza e chi esegue il pagamento. Ne consegue, in considerazione dell'organizzazione aziendale di ESEB, che gli incarichi di consulenza di particolare rilevanza devono essere deliberati dal Consiglio di Amministrazione o, se costituito, dal Comitato Esecutivo.
Consulenti e collaboratori devono essere scelti sulla base di precisi requisiti di onorabilità, professionalità e competenza ed in relazione alla loro reputazione e affidabilità.
I contratti con consulenti e collaboratori devono essere definiti per iscritto in tutte le loro condizioni e termini.
I compensi dei consulenti e collaboratori devono trovare adeguata giustificazione nell'incarico conferito e devono essere congrui, in considerazione delle prassi esistenti sul mercato e/o delle tariffe vigenti.
Nessun pagamento a consulenti e collaboratori può essere effettuato in contanti.
E' fatto divieto affidare ai consulenti e collaboratori qualsiasi attività che non rientri nel contratto di consulenza.

(III) Gestione delle erogazioni pubbliche
Per ogni contributo, finanziamento, sovvenzione ottenuti dallo Stato, dagli enti pubblici o dalla Unione Europea deve essere predisposto un apposito rendiconto che dia atto degli scopi per i quali l'erogazione pubblica è stata richiesta e concessa e della sua effettiva utilizzazione.

(IV) Rapporti con organi ispettivi

Nel caso di ispezioni giudiziarie, tributarie e amministrative (ad esempio relative al D. Lgs n. 81/2008, verifiche tributarie, INPS, NAS, ASL, ecc) i rapporti con gli organi ispettivi devono essere tenuti dal responsabile della funzione o da soggetto da questi delegato.

Il responsabile della funzione o il soggetto da questi delegato è tenuto a verificare che gli organi ispettivi redigano verbale delle operazioni compiute e richiederne una copia, in tutti i casi in cui ve ne sia il diritto; tale copia dovrà essere adeguatamente conservata. Nel caso in cui non fosse stato possibile ottenere il rilascio di una copia del verbale ispettivo, il responsabile della funzione o il soggetto da questi delegato a partecipare all'ispezione provvederà a redigere un verbale ad uso interno. Il personale della Ente, nell'ambito delle proprie competenze, deve prestare piena collaborazione, nel rispetto della legge, allo svolgimento delle attività ispettive.

Il responsabile della funzione deve informare con una nota scritta l'Organismo di Vigilanza qualora, nel corso o all'esito della ispezione, dovessero emergere profili critici.

(V) Gestione del personale

Il delegato alla gestione del personale è tenuto a garantire l'applicazione di criteri di valutazione dei candidati che risponda alle esigenze di obiettività e trasparenza:

a) l'assunzione dei candidati deve avvenire nel rigoroso rispetto delle procedure standard definite dall'Ente per la selezione del personale;
b) l'esito del processo valutativo dei candidati sia formalizzato in apposita documentazione, accuratamente archiviata dal Responsabile competente secondo le prestabilite procedure interne.

6.6 Procedure di prevenzione

ESEB adotta un sistema di controlli interno diretto a prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione.

7 Reati di ricettazione, riciclaggio ed impiego di denaro, beni o altre utilità di provenienza illecita

7.1 Le fattispecie di reato

Nei paragrafi successivi vengono descritti i reati rilevanti sul piano della responsabilità della Ente ex d.lvo n. 231/2001, segue una descrizione dei processi sensibili con relativa evidenza delle fattispecie di reato che potrebbero essere astrattamente rilevanti nell'interesse e a vantaggio del'Ente, nonché la formalizzazione dei principi di controllo finalizzati alla prevenzione del rischio penale di impresa.

Tipologie di reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o altre utilità cui è associabile la responsabilità aziendale ex D.Lgs. n. 231/2001.

Ricettazione (art. 648 c.p.)

"Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve o occulta denaro o cose provenienti da qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due a otto anni e con la multa da euro 516 a 10.329.
La pena è della reclusione sino a sei anni e della multa sino a euro 516 se il fatto è di particolare tenuità.
Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile ovvero manchi una condizione di procedibilità riferita a tale delitto".
Lo scopo della incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell'evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.
Per "acquisto" deve intendersi l'effetto di una attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.
Il termine "ricevere" sta ad indicare ogni forma di conseguimento di possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.
Per "occultamento" deve intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.
La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento del bene. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico, tra l'autore del reato principale e il terzo acquirente.
Il reato di ricettazione può essere realizzato in particolare in alcune aree aziendali.

Riciclaggio (art. 648 bis)

"Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.
La pena è aumentata quando il fatto è stato commesso nell'esercizio di una attività professionale.
La pena è diminuita se il denaro, i beni o le altre attività provengono da delitto per il quale è stata stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'art. 648".
Lo scopo della incriminazione del reato di riciclaggio è quello di impedire che gli autori del reato possano far fruttare i capitali illegittimamente acquisiti, rimettendoli in circolazione come capitali ormai "ripuliti" e perciò investibili anche in attività economiche produttive lecite. In questo modo, la norma incriminatrice persegue anche un ulteriore obiettivo finale, vale a dire scoraggiare la stessa commissione dei reati principali, mediante l'apposizione di barriere frapposte alla possibilità di sfruttare i proventi illeciti.
Per "sostituzione" si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.
Il "trasferimento" consiste nella condotta tendente a ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.
Le "operazioni" idonee ad ostacolare l'identificazione della illecita provenienza potrebbero essere considerate quelle in grado di intralciare l'accertamento da parte della Autorità Giudiziaria della provenienza delittuosa dei valori provenienti dal reato.

Impiego di denaro, beni o altre utilità di provenienza illecita (art. 648 ter c.p.)

"Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio di una attività professionale.

La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648. Si applica l'ultimo comma dell'art. 648.

L'inserimento nel codice del delitto in esame nasce dal rilievo che i profitti della criminalità organizzata debbono essere contrastati tenendo conto di una duplice prospettiva: mentre in un primo momento occorre impedire che il c.d. "denaro sporco", frutto della illecita accumulazione, venga trasformato in denaro "pulito", in un secondo momento è necessario fare in modo che il capitale non possa trovare un legittimo impiego.

La condotta, espressa dall'inciso "impiega in attività economiche o finanziarie", consente due rilievi. Da un lato, il riferimento specifico alle attività finanziarie

intende con evidenza coinvolgere la vasta cerchia di intermediari, bancari e non, i quali operano in questo campo. D'altro lato tale coinvolgimento, a titolo di concorso nel reato, è favorito dal verbo "impiegare" la cui accezione è per certo più ampia rispetto al termine "investire", che suppone un impiego finalizzato a particolari obiettivi, ed esprime il significato di "usare comunque".

Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente di escludere la funzione meramente professionale (sanitaria, educativa), dove ha assoluta prevalenza l'aspetto intellettuale (es. costituzione di uno studio medico o impartizione di lezioni individuali); non naturalmente quando essa si accompagni ad una struttura di tipo imprenditoriale (per esempio il denaro di illecita provenienza è impiegato nella costituzione di una clinica privata o di una ente privata). Il termine in essere consente del pari di non comprendere nella sfera di operatività della norma gli impieghi di denaro o altre utilità che abbiano carattere occasionale o sporadico.

Autoriciclaggio (art. 648 ter)

Il reato previsto dall'art. 648-ter.1, e introdotto dall'art. 3, comma 3, L. 15 dicembre 2014, n. 186, disciplina due distinte ipotesi:

a) la prima, più grave, riguarda chi, avendo commesso o concorso a commettere un delitto non colposo punito con la reclusione pari o superiore nel massimo a cinque anni, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare *concretamente* l'identificazione della loro provenienza delittuosa (art. 648-ter.1 co. 1 c.p.);

b) la seconda, meno grave, punisce le medesime attività ove poste in essere in relazione ad utilità provenienti da delitti non colposi puniti con la reclusione inferiore nel massimo a cinque anni (art. 648-ter.1 co. 2 c.p.). La pena è però più grave se il denaro, i beni o le altre utilità provengono da un delitto commesso avvalendosi delle condizioni previste dall'art. 416-bis c.p. (associazioni di tipo mafioso anche straniere) ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo (art. 648-ter.1 co. 3 c.p.).

Presupposto dell'autoriciclaggio è una condotta che ostacola *concretamente* l'identificazione della provenienza delittuosa. Questo significa che per la configurazione di questo delitto non sono sufficienti le condotte che determinano solo un semplice ritardo nell'identificazione della provenienza: non sono cioè rilevanti ai fini dell'autoriciclaggio quelle operazioni le cui modalità esecutive sono facilmente superabili con la normale diligenza degli organi accertatori.

È inoltre da ritenere che il semplice trasferimento delle somme non configuri il reato di autoriciclaggio in quanto occorrerebbe la prova che si sia trattato di un trasferimento avvenuto con modalità anomale (ad esempio, attraverso plurimi passaggi, taluni dei quali inutili; oppure mediante il transito su conti esteri, soprattutto se siti in banche di Paradisi fiscali; con la collaborazione amichevole di terze persone aventi la natura di mere "*teste di legno*", ecc.).

Tra le condotte non punibili si segnala, inoltre, quanto indicato al quarto comma dell'art. 648-ter.1 c.p., che prevede che "*fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale*".

Infine, sotto il profilo sanzionatorio, il legislatore ha previsto un aumento di pena quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale e, per converso, una diminuzione di pena (fino alla metà) per chi si sia efficacemente adoperato per

evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

7.2 Destinatari della Parte Speciale

Destinatari della presente Parte Speciale sono i soggetti di volta in volta individuati dalla fattispecie incriminatrice (amministratori, direttori generali, sindaci, dipendenti, liquidatori, ecc) "soggetti apicali" di ESEB, nonché i dipendenti sottoposti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, questi soggetti saranno di seguito denominati "Destinatari".

7.3 Aree di attività a rischio

La mappatura delle aree operative di ESEB, svolta attraverso la documentazione aziendale ed una serie di interviste e sessioni di rilevazione su operatori "chiave" risultanti dall'organigramma aziendale, ha consentito di individuare i processi sensibili ove può essere astrattamente presente il rischio di commissione di alcuni dei reati previsti dall'art. 25 ter del d.lvo 231/2001.
Nella trattazione che segue per ciascun processo sensibile vengono sintetizzate le principali evidenze dell'analisi.

Descrizione dei processi a rischio
Processo n. 1
Amministrazione Aziendale e Controllo Di Gestione

Funzioni coinvolte
- Presidente
- Vicepresidente
- Direttore
- Amministrazione

Fattispecie di reato rilevanti ed ipotesi sulle relative modalità di attuazione
RICETTAZIONE:
La fattispecie potrebbe in astratto configurarsi qualora vengano disposti pagamenti relativi a fatture passive per acquisti di beni provenienti da attività illecite.
RICICLAGGIO:
La fattispecie potrebbe in astratto configurarsi nel caso in cui siano autorizzati incassi di denaro proveniente da attività illecita, oppure nel caso in cui operatori aziendali procedano consapevolmente all'apertura di conti bancari in favore della Ente utilizzando finanziamenti in denaro che siano provento di delitto non colposo (ad es. truffa ai danni della P.A., frode fiscale, false comunicazioni sociali).

IMPIEGO DI DENARO, BENI O ALTRA UTILITA' DI PROVENIENZA ILLECITA:
il reato potrebbe essere astrattamente integrato nel caso in cui operatori aziendali, consapevolmente, utilizzino fondi di provenienza illecita per effettuare, anche tramite intermediari finanziari, investimenti a favore del'Ente. La fattispecie potrebbe concretizzarsi nell'impiego dei capitali di provenienza illecita in attività economiche o finanziarie attraverso rapporti con soggetti terzi.

AUTORICICLAGGIO:
il reato potrebbe configurarsi qualora, ottenuto un indebito finanziamento, si compiano operazioni per ostacolarne la tracciabilità.

Attività sensibili
- Finanza e tesoreria
- Gestione dei flussi finanziari
- Adempimenti contabili per la gestione dei flussi finanziari e di transazioni finanziarie
- Registrazioni di contabilità generale
- Registrazione delle fatture passive
- Controlli sulla regolarità delle fatture
- Archiviazione della documentazione a supporto delle fatture
- Gestione contratti con controparti di acquisto e/o vendita
- Investimenti

Processo n. 2
Acquisti di Beni e Servizi

Funzioni coinvolte
- Presidente
- Vicepresidente
- Comitato di Presidenza
- Direttore
- Amministrazione
- Logistica
- Coordinatori didattici

Fattispecie di reato rilevanti ed ipotesi sulle relative modalità di attuazione
RICETTAZIONE:
la fattispecie potrebbe essere astrattamente integrata nel caso in cui operatori aziendali consapevolmente acquistino, nell'interesse della Ente, beni ad un prezzo notevolmente inferiore a quello di mercato in quanto provenienti da un precedente illecito penale (ad es. furto) commesso dal venditore o da terzi.

IMPIEGO DI DENARO; BENI OD ALTRE UTILITA' DI PROVENIENZA ILLECITA:
la fattispecie potrebbe concretizzarsi nel successivo impiego nella attività aziendale dei beni acquistati di provenienza delittuosa

Attività sensibili
- Ricerca e selezione fornitori
- Gestione del sistema di valutazione e qualifica dei fornitori
- Gestione Ordini di acquisto
- Gestione contratti con controparti

7.4 Principi di controllo rilevanti
I protocolli e le procedure che intervengono nella regolamentazione delle attività sensibili sono ispirati ai seguenti principi di controllo:
- Il sistema interno della ripartizione interna (procure, deleghe e mansionari) deve essere coerente con le attività e i compiti effettivamente svolti dal personale;
- deve essere verificata l'attendibilità commerciale e professionale dei fornitori, con particolare riferimento ai fornitori più importanti per la Ente;
- deve essere garantito il monitoraggio periodico delle prestazioni dei fornitori;
- deve essere verificata la regolarità dei pagamenti, con riferimento alla piena corrispondenza tra destinatari/beneficiari e controparti effettivamente coinvolte nella transazione;
- devono essere rispettate le limitazioni legali all'uso del contante e dei titoli al portatore, nonché del divieto di apertura/utilizzo di conti o libretti di risparmio anonimi o con intestazione fittizia,
- deve essere controllata la corrispondenza quantitativa e qualitativa tra beni effettivamente ricevuti, risultanze del documento di trasporto e quantità/unità di prodotto richieste nell'ordine di acquisto;
- deve essere verificata l'esatta riconciliazione contabile tra corrispettivi pagati, fatture passive e beni/servizi ricevuti;
- deve essere sempre eseguita la riconciliazione di magazzino tra la merce effettivamente ordinata e la merce acquisita in magazzino;
- deve essere garantita la regolarità delle transazioni in entrata, con particolare riferimento alla corretta registrazione degli incassi;
- deve essere effettuata l'esatta riconciliazione tra incassi da estratto conto bancario, fatture attive e prestazioni realmente eseguite;
- i documenti riguardanti l'attività di impresa devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale, ed all'organismo di vigilanza;
- i sistemi informativi devono garantire la riservatezza dell'accesso e la tracciabilità delle azioni mediante sistemi di autenticazione (user id e password)

- in tutti i casi è comunque obbligatorio attenersi alle regole del codice etico della Ente che rappresentano parte integrante dei protocolli che indirizzano le attività sensibili.

8 Reati societari

8.1 La tipologia dei reati societari (art. 25 ter del Decreto)

Rispetto alla categoria dei reati contro la Pubblica Amministrazione, i reati societari hanno, in linea generale e di massima, una incidenza minore ai fini della responsabilità aziendale *ex* D.Lgs. 231/2001 a causa di:

- esclusione delle sanzioni interdittive a carico dell'azienda nel cui interesse sia commesso l'illecito societario ed applicazione delle sole sanzioni pecuniarie (art. 25-*ter* del D.Lgs. 231/2001);
- qualificazione dei reati societari come c.d. reati "propri", rispetto ai quali la commissione è ipotizzabile esclusivamente ad opera di coloro che siano titolari della qualificazione soggettiva indicata dal legislatore (in linea di massima: amministratori, sindaci, revisori e liquidatori), salva la rilevanza delle qualifiche soggettive di fatto di cui all'art. 2639 c.c.;
- tendenziale perseguibilità "a querela" (e non d'ufficio) della gran parte delle fattispecie.

Tuttavia, ai fini della costruzione del presente Modello Organizzativo, l'impatto di tali reati sulla Ente Sistema Edilizia Brescia non può essere sottovalutata in quanto, dall'analisi condotta sulla stessa, sono emerse delle aree di rischio potenziale in relazione a talune fattispecie riconducibili ai reati societari.

Nei paragrafi successivi vengono descritti i reati in materia societaria, rilevanti sul piano della responsabilità aziendale *ex* D.Lgs. 231/2001.

False comunicazioni sociali (art. 2621 c.c.) [modificato dalla L. n. 69/2015]
- Fatti di lieve entità (art. 2621-bis c.c.) [aggiunto dalla L. n. 69/ 2015]
- False comunicazioni sociali delle società quotate (art. 2622 c.c.) [modificato dalla L. n. 69/2015]
- Falsità nelle relazioni o nelle comunicazioni della Società di revisione (art. 2624, commi 1 e 2, c.c.)6
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla L. n. 262/2005]
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla L. n. 190/2012]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.)

8.2 Aree di attività a rischio

Tenuto conto della peculiarità dell'attività della Ente Sistema Edilizia Brescia, le attività considerate più specificamente a rischio, in relazione ai reati descritti nella presente Parte Speciale, sono ritenute le seguenti:

1) redazione del bilancio, di situazioni contabili periodiche infrannuali e di qualsivoglia comunicazione, prevista o non prevista dalla legge, nei confronti di terzi, anche se effettuata in via indiretta, ma tale da incidere su detti documenti;
2) gestione di documenti utili all'esercizio delle attività di controllo o di revisione e rendicontazione e/o redazione ed invio di relazioni e comunicazioni agli organi sociali;
3) rapporti ed operazioni con i creditori, atti di disposizione dei beni sociali;
4) rapporti e comunicazioni, di qualsiasi genere, con le autorità di pubblica vigilanza.

Per quanto riguarda la fattispecie relativa alla corruzione tra privati sono da considerarsi a rischio, in

analogia con quanto previsto riguardo Corruzione nei confronti della Pubblica Amministrazione, le seguenti aree dell'Ente che, pur non implicando direttamente l'instaurazione di rapporti con i terzi oggetto di attività corruttiva, gestiscono strumenti o rapporti di tipo finanziario e simili che potrebbero essere impiegati per attribuire vantaggi e utilità a ai vari soggetti coinvolti nella commissione di reati di corruzione privata:
Gestione Accreditamento istituzionale
Gestione Finanziamenti sistema dote
Gestione Finanziamenti a bando
Ed i relativi processi definiti come strumentali.
Si segnala che la gestione amministrativa dell'Ente è affidata ad un Consiglio di Amministrazione, supportato da un consulente esterno.
Eventuali integrazioni delle suddette attività a rischio reato potranno essere proposte al Consiglio di Amministrazione dall'Organismo di Vigilanza dell'espletamento dei propri compiti, per effetto dell'evoluzione dell'attività dell'Ente in conseguenza di eventuali modifiche dell'attività svolta dalle singole funzioni aziendali.

8.3 Destinatari della parte speciale

Destinatari della presente Parte Speciale sono i soggetti di volta in volta individuati dalla fattispecie incriminatrice (amministratori, direttori generali, sindaci, dipendenti, liquidatori, ecc) "soggetti apicali" di ESEB, nonché i dipendenti sottoposti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, questi soggetti saranno di seguito denominati "Destinatari".
In merito agli amministratori, al dirigente preposto, ai direttori generali, ai sindaci e ai liquidatori, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 c.c., infatti, dei reati societari previsti dal codice civile risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Obiettivo della presente Parte Speciale è che al fine di impedire il verificarsi dei reati previsti nel Decreto:

- tutti i Destinatari come sopra descritti siano precisamente consapevoli della valenza dei comportamenti censurati e
- adottino quindi regole di condotta conformi a quanto prescritto dalla stessa.

8.4 Principi generali di comportamento

Nello svolgimento delle proprie attività i componenti degli organi interni, i dirigenti e i dipendenti dell'Ente Sistema Edilizia Brescia nonché i Consulenti e i Partner nell'ambito delle attività da essi svolte conoscono e rispettano:

1) la normativa applicabile;
2) il Codice Etico;
3) il sistema dei controlli interni e quindi le procedure interne, la documentazione e le disposizioni inerenti la struttura organizzativa e il sistema di controllo della gestione;
4) le norme relative al sistema amministrativo, contabile, finanziario della Ente Sistema Edilizia Brescia ;
5) i principi contabili nazionali ed internazionali;
6) le leggi, norme e regolamenti degli enti di controllo dei mercati.

È fatto divieto ai componenti degli organi interni ed ai Dipendenti e Consulenti (nell'ambito delle attività da essi svolte) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; è fatto altresì divieto di porre in essere comportamenti in violazione dei principi e delle procedure interne.
Conseguentemente, i soggetti sopraindicati hanno l'espresso obbligo di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria dell'ente;
2. tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei

dati e delle informazioni relative agli eventuali strumenti di debito emessi dalla Ente Sistema Edilizia Brescia , necessari per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'Ente, sull'evoluzione della sua attività, nonché sui suoi strumenti di debito e relativi diritti;
3. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del patrimonio sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
4. salvaguardare il regolare funzionamento dell'Ente e degli organi interni garantendo ed agevolando ogni forma di controllo interno sulla gestione previsto dalla legge, nonché la libera e corretta formazione della volontà consiliare;
5. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

→ **con riferimento al precedente punto 1:**

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Ente;

b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Ente;

→ **con riferimento al precedente punto 2:**

a) alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi;

b) illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria dell'Ente e sull'evoluzione della sua attività, nonché sugli strumenti di debito e relativi diritti;

c) inficiare la comprensibilità del prospetto accrescendo oltremisura la massa dei dati, delle informazioni e delle parti descrittive contenute nel prospetto rispetto a quanto richiesto dalle effettive esigenze informative dei creditori.

→ **con riferimento all'obbligo di cui al precedente punto 3:**;

a) effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;

b) distrarre i beni sociali, in sede di liquidazione dell'Ente, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli.

→ **con riferimento al precedente punto 4:**

a) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino, lo svolgimento dell'attività di controllo e di revisione da parte dei soggetti incaricati;

b) determinare o influenzare l'assunzione delle deliberazioni del Consiglio di Amministrazione, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà consiliare;

→ **con riferimento al precedente punto 5:**

a) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle autorità di vigilanza cui è soggetta l'attività dell'Ente Sistema Edilizia Brescia , nonché omettere la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;

b) esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie dell'Ente;

c) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti.

8.5 Principi di controllo

Il sistema di controllo a presidio delle regole di comportamento sopra descritte si deve basare sui seguenti fattori.

8.5.1 Principi di attuazione dei comportamenti prescritti

Le regole generali di organizzazione sono di seguito riportate:

5.1.1 Redazione di bilanci, scritture contabili, relazioni ed altri documenti di impresa

Le operazioni di rilevazione e registrazione delle attività di impresa devono essere effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.
Tutti i dati e le informazioni che servono alla redazioni dei bilanci (bilancio d'esercizio) e degli altri documenti contabili dell'Ente devono essere chiari, completi e rappresentare in modo veritiero la situazione economica, finanziaria e patrimoniale dell'Ente.
I dati e le informazioni sono raccolti tempestivamente, sotto la supervisione del Presidente, ed elaborati da soggetti da questo delegati ai fini della predisposizione della bozza di bilancio. A richiesta, insieme ai dati e alle informazioni devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni.
La rilevazione, la trasmissione e l'aggregazione dei dati e delle informazioni contabili per la redazione del bilancio d'esercizio, deve avvenire con modalità tali (anche per il tramite di un sistema informativo) da assicurare che vi sia sempre evidenza dei passaggi del processo di formazione dei dati, e sia sempre individuabile il soggetto che ha inserito i dati nel sistema. I profili di accesso a tale sistema sono identificati dal Presidente o da soggetto da lui delegato, nel rispetto del principio di separatezza delle funzioni e di coerenza dei livelli autorizzativi.
Il Presidente, inoltre, cura che la bozza di bilancio e tutti i documenti contabili, relativi agli argomenti indicati nell'ordine del giorno delle riunioni del Consiglio di Amministrazione, siano completi e messi a disposizione degli amministratori con ragionevole anticipo rispetto alla data della riunione.
La redazione del bilancio d'esercizio deve essere effettuata sulla base della prassi consolidata e, periodicamente, verificata e aggiornata di concerto con il Collegio Sindacale. Eventuali variazioni non giustificate dei principi contabili stabiliti dalle procedure, devono essere tempestivamente segnalate all'Organismo di Vigilanza.

5.1.2 Tutela del patrimonio sociale

Tutte le operazioni relative alla destinazione degli utili, alla costituzione di società, all'acquisto e cessione di partecipazioni, alle fusioni e scissioni nonché tutte le operazioni che possono ledere l'integrità del patrimonio sociale devono essere effettuate nel rispetto dello Statuto, del Codice Etico e delle procedure aziendali a tale scopo predisposte.

5.1.3 Rapporti con i Sindaci

Il Presidente, il Vice Presidente, il Direttore o un suo delegato, incaricato della raccolta ed elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale deve garantire la completezza, inerenza e correttezza della documentazione trasmessa.
Le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale, devono essere documentate e conservate a cura del Presidente o da suo delegato.
Il Presidente assicura che tutti i documenti relativi ad operazioni all'ordine del giorno delle riunioni del Consiglio di Amministrazione o, comunque, relativi a operazioni sulle quali il Collegio Sindacale debba esprimere parere, siano messi a disposizione di questi ultimi con ragionevole anticipo rispetto alla data della riunione.

5.1.4 Rapporti con consulenti e collaboratori

Si applicano le regole generali indicate nell'apposita Parte Speciale (gestione risorse umane) del presente Modello.

5.1.5 Interessi degli amministratori nelle operazioni della Società

Nel rispetto della norma di cui all'art. 2391 c.c., gli amministratori devono dare notizia al Consiglio di Amministrazione ed al Collegio Sindacale di ogni interesse che essi, per conto proprio o di terzi (incluso ogni soggetto con cui gli amministratori intrattengano, direttamente o indirettamente, relazioni economiche o di cui siano dipendenti o amministratori), abbiano in una determinata operazione dell'Ente,

precisandone la natura, i termini, l'origine e la portata. In conformità a quanto previsto nel Codice Etico dell'Ente, gli amministratori devono astenersi dal votare tale operazione o transazione.
Le segnalazioni concernenti gli interessi degli amministratori nelle operazioni dell'Ente devono essere inviate all'Organismo di Vigilanza, che ne cura l'archiviazione e l'aggiornamento.

8.5.2 Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica della procedura
In particolare, i rapporti con il Consiglio di Amministrazione ed il Collegio Sindacale, sono intrattenuti dal Direttore o dai soggetti dal medesimo appositamente incaricati e/o delegati, così come specificamente individuati dalle procedure aziendali interne.

8.5.3 Separazione dei compiti
La separazione tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Consiglio di Amministrazione ed il Collegio Sindacale deve garantire, per tutte le fasi della procedura, un meccanismo costituito da soggetti addetti alla fase di esecuzione e soggetti addetti alla fase di verifica e controllo della medesima.

8.5.4 Partecipazione regolare e continua del Collegio Sindacale alle riunioni del Consiglio di Amministrazione
Il Collegio Sindacale deve garantire la partecipazione regolare e continua alle riunioni del Consiglio di Amministrazione, a garanzia dell'effettiva conoscenza da parte del Collegio Sindacale in merito alle scelte di gestione dell'Ente.

8.5.5 Tempestiva e completa evasione delle richieste di documentazione
Le sedi territoriali dell'Ente Sistema Edilizia Brescia interessate e le cinque macro aree evidenziate nell'organigramma dell'Ente (Rendicontazione, Amministrazione, Formazione, Orientamento, Logistica), devono evadere in maniera completa, esaustiva e tempestiva le richieste di documentazione specifica avanzate dal Consiglio di Amministrazione e dal Collegio Sindacale nell'espletamento delle proprie attività di vigilanza e controllo.
Allo stesso modo, le strutture competenti devono evadere in maniera completa, esaustiva e tempestiva le richieste di documentazione specifica avanzate dall'organo incaricato della revisione legale nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili. Pertanto ciascuna struttura ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori.
Tempestiva e completa deve anche essere la messa a disposizione del soggetto incaricato della revisione legale, da parte delle strutture interessate, della documentazione disponibile relativa alle attività di controllo ed ai processi operativi seguiti, sui quali i revisori effettuano le proprie attività di verifica.
Infine tempestiva e completa deve parimenti essere la messa a disposizione della documentazione necessaria alla rendicontazione delle attività didattiche espletate o all'esibizione dei documenti ai soggetti che, per legge, hanno il potere / dovere di controllo su tali attività.

8.5.6 Tracciabilità delle fasi di attività sia a livello di sistema informativo sia in termini documentali
È importante che siano osservate le seguenti direttive:

1) Sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo del Consiglio di Amministrazione e del Collegio Sindacale;
2) Verifica e conservazione delle dichiarazioni di supporto per la predisposizione della situazione economica e finanziaria dell'Ente, con firma delle stesse da parte del dirigente preposto alla redazione dei documenti contabili societari e dei consiglieri muniti dei necessari poteri;
3) Al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate da ogni funzione della Ente Sistema Edilizia Brescia sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla gestione dei rapporti con il Consiglio d'Amministrazione e il Collegio Sindacale.

8.5.7. Rimando ai principi di controllo previsti al punto
Inoltre per quanto riguarda il reato di "Corruzione tra privati" si rimanda a quanto sopra riportato al paragrafo **6** con riferimento ai punti:

1) Principi generali di comportamento (punto 6.3);
2) Principi di attuazione dei comportamenti prescritti (punto 6.5);

estendendo anche alla sfera dei rapporti con il privato i medesimi meccanismi di prevenzione ed ostacolo nei confronti delle attività strumentali alla commissione di azioni corruttive già in essere nell'ambito della sfera della Pubblica Amministrazione.

9 Delitti informatici e trattamento illecito di dati

9.1 La fattispecie di reato

Per quanto concerne la presente Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24 bis del Decreto.

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

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

Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* cod. penale)

" *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:*

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* cod. penale)

"*Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617quater*".

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* cod. penale)

"*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro*".

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. penale)

" *Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:*

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato".

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. penale)

" *Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater."

Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cod. penale)

"*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
Se ricorre una o più delle circostanze di cui al numero 1 del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno quattro anni e si procede d'ufficio."

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* cod. penale)

"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione, o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata.*"

Danneggiamento di sistemi informatici e telematici (art. 635-*quater* cod. penale)

"*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*
Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- *quinquies* cod. penale)

"*Se il fatto di cui all'art.635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cod. penale)

"*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00*".

9.2 Aree di attività a rischio

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24- *bis* del D.Lgs. 231/2001, sono relative alla gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

- Gestione dei sistemi informativi e trattamento illecito delle informazioni
- Gestione del profilo utente e del processo di autenticazione
- Gestione e protezione della postazione di lavoro
- Utilizzo di firma elettronica
- Predisposizione ed invio telematico di scritture private e/o attestazioni e/o dichiarazioni sostitutive di certif. o atto di notorietà DPR 445/2000

- Gestione degli output di sistema e dei sistemi di memorizzazione
- Gestione e protezione delle reti

Con specifico riguardo alle problematiche connesse al rischio informatico, ESEB, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso (*i*) la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e (*ii*) la garanzia della massima continuità del servizio.

9.3 Destinatari della Parte Speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dai dirigenti e dai dipendenti "esponenti aziendali" di ESEB nelle aree di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella Parte Generale (qui di seguito tutti denominati "Destinatari").
Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

9.4 Principi generali di comportamento

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.
Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che ESEB si pone sono i seguenti:
- **Riservatezza**: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità**: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- **Disponibilità**: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.
Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di ESEB (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-*bis* del D.Lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente parte speciale.
Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:
a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le

informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
h) istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
Pertanto, i soggetti sopra indicati devono:
1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare c/o l'Ente (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
5. evitare di trasferire all'esterno e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Ente, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc…);
7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Ente solo prodotti ufficialmente acquisiti dall'Ente stesso;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Ente;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

9.5 Procedure di prevenzione

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

- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Esistenza di procedure/norme/circolari**: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma**: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno dell'Ente.

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

Ai fini dell'attuazione delle regole elencate, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo, nel disciplinare la fattispecie di attività sensibile descritta, dovranno essere osservati anche i seguenti principi di riferimento.
Gestione e monitoraggio degli accessi ai sistemi informatici e telematici.

1) Esistenza di una normativa aziendale relativa alla gestione del rischio informatico che individui le seguenti fasi:
- identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
- individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
- individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
- identificazione delle possibili contromisure;
- effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
- definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
- documentazione e accettazione del rischio residuo.

2) Esistenza di una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:
- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un polo di competenza interno che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

3) Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
4) Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.
5) Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.
6) Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichi attraverso la verifica e la gestione dei diritti d'accesso.
7) Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
8) Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
9) Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).
10) Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.

11) Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.
12) Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'Ente oggetto di protezione (risorse tecnologiche e informazioni).
13) Predisposizione e attuazione di una policy aziendale che stabilisce (*i*) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (*ii*) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.
L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.
I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.
A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di attività sensibili.
Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste nella Parte Generale del presente Modello.

10 Reati di omicidio colposo e lesioni colpose gravi o gravissime

10.1 La fattispecie di reato

La presente sezione della Parte Speciale si riferisce ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro, richiamati dall'art.25-septies del Decreto e di seguito riportati.
A differenza delle altre ipotesi di reato presupposto previste nel Decreto che richiedono la sussistenza del dolo (coscienza e volontarietà dell'azione criminosa), i delitti di cui alla presente Parte Speciale sono puniti a titolo di colpa.

Omicidio colposo (art. 589 c.p.)
E' punita la condotta di chiunque cagiona per colpa la morte di una persona con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro.

Lesioni colpose gravi o gravissime (art. 590 c.p.)
E' punita la condotta di chiunque cagioni ad altri per colpa una lesione personale grave o gravissima con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro.

La lesione è grave se:
1. dal fatto deriva una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai 40 giorni;
2. il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è gravissima se dal fatto deriva:
1. una malattia certamente o probabilmente insanabile;
2. la perdita di un senso;
3. la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
4. la deformazione ovvero lo sfregio permanente del viso.

10.2 Aree di attività a rischio

L'attività che la Ente ha individuato al proprio interno come sensibile, nell'ambito dei reati e dei corrispondenti illeciti amministrativi, di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro è:

ATTIVITA'	DIREZIONE	PRESIDI
Nomina del RSPP	PRESIDENTE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Nomina Medico competente	PRESIDENTE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Acquisizione documentazione per le Certificazioni obbligatorie	DIREZIONE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81

Valutazione dei Rischi e elaborazione del relativo documento con conseguenti aggiornamenti	PRESIDENTE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Elaborazione delle Procedure in materia di sicurezza, prevenzione incendi, primo soccorso e verifiche periodiche delle stesse	RSPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Individuazione ed elaborazione delle Misure preventive e protettive e dei DPI	RSPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Individuazione fattori a rischio	RSPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Informazione ai lavoratori sui rischi per la salute e misure di prevenzione e protezione adottate	RSPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Assegnazione mansioni	DIRETTORE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Conservazione ed aggiornamento Registro Infortuni Raccolta e gestione dei quasi-infortuni, non-conformità e situazioni pericolose	DIRETTORE	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Controllo corretto utilizzo delle attrezzature	PREPOSTI: DOCENTI E ISTRUTTORI	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Controllo utilizzo delle dotazioni di sicurezza (guanti, tappi, mascherine, tuta, scarpe, ecc)	PREPOSTI: DOCENTI E ISTRUTTORI	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Informazione, Formazione ed addestramento dei lavoratori	DIREZIONE RSPP ASPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Vigilanza sulle procedure adottate e delle istruzioni impartite alle ditte appaltatrici presso le sedi di ESEB	DIREZIONE RSPP ASPP	_ Codice Etico _ PRO.01 – PRO.02 _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Invio informazioni al RSPP, al datore di lavoro e all'Organismo di Vigilanza	PREPOSTI DIREZIONE	_ Codice Etico _ Procedure implementate ai fini del D. Lgs n. 81/2008 _ PG Verifica degli adempimenti in

		materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Ispezioni per prevenzione incendi e presidi di primo soccorso	PREPOSTI	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Programmazione riunioni periodiche sulla sicurezza e coinvolgimento RLS	RSPP	_ Codice Etico _ PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81
Vigilanza sulle procedure adottate e delle istruzioni date ai lavoratori presso ESEB e presso attività di stage/apprendistato	PREPOSTI: DOCENTI E ISTRUTTORI	_ Codice Etico _ PRO.03 _ MOG di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81

Eventuali integrazioni della suddetta area di attività a rischio potranno essere disposte dal Presidente della Ente di concerto con l'Organismo di Vigilanza, a cui è dato mandato di definire gli opportuni provvedimenti operativi.

10.3 Destinatari della Parte Speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dirigenti, RSPP e dipendenti "esponenti aziendali" della Ente nell'area di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella parte Generale (di seguito tutti denominati "Destinatari").
Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati adottino regole di condotta conformi a quanto prescritto dalla stessa, al fini di impedire il verificarsi dei reati previsti nel Decreto.

10.4 Principi generali di comportamento

Nello svolgimento delle attività, tutti i Destinatari del Modello sono tenuti ad osservare i principi generali di comportamento che la Ente ha individuato in conformità anche a quanto previsto dal Codice Etico e alle regole dettate dalla normativa in materia di tutela della salute e della sicurezza sul posto di lavoro.

In particolare la Ente adotta le seguenti misure generali:

1. attenta valutazione dei rischi e completa trasposizione degli stessi nel Documento di Valutazione dei rischi;
2. eliminazione dei rischi per la salute e la sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non possibile, loro riduzione al minimo;
3. riduzione dei rischi alla fonte;
4. programmazione della prevenzione mirando ad un complesso che integra in modo coerente nella prevenzione le condizioni tecniche produttive ed organizzative dell'Ente nonché l'influenza dei fattori dell'ambiente di lavoro;
5. sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
6. rispetto dei principi ergonomici nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, anche per attenuare il lavoro monotono e quello ripetitivo;
7. priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;
8. limitazione al minimo dei lavoratori che sono, o che possono essere esposti al rischio;
9. utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;
10. controllo sanitario dei lavoratori in funzione dei rischi specifici;
11. allontanamento del lavoratore dall'esposizione a rischio, per motivi sanitari inerenti la sua persona;
12. misure igieniche;
13. misure di protezione collettiva e individuale;

14. misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;
15. uso di segnali di avvertimento e di sicurezza,
16. regolare manutenzione di ambienti, attrezzature, macchine ed impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;
17. informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro;
18. istruzioni adeguate ai lavoratori.

10.5 Procedure di prevenzione

L'Alta Direzione di ESEB ha deciso di procedere all'implementazione di un modello di organizzazione e di gestione (MOG) per la sicurezza nei luoghi di lavoro di cui all'articolo 30 del d.lgs. 9 aprile 2008, n.81 idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche di cui al d.lgs. 8 giugno 2001, n.231.
L'Alta Direzione di ESEB ha scelto di applicare le indicazioni del Ministero del Lavoro contenute all'interno di procedure semplificate per l'adozione dei modelli di organizzazione e gestione nelle piccole e medie imprese (PMI) di cui all'articolo 30 comma 5 del d.lgs. 9 aprile 2008, n.81.

Il modello di gestione di cui al precedente paragrafo si integra con il presente documento andando a definire in modo più specifico le procedure, i processi e le figure aziendali responsabili.

L' ESEB ha implementato un sistema di controlli volto alla creazione di un canale informativo nei confronti dell'Organismo di Vigilanza al fine di prevenire la commissione dei reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza sul posto di lavoro.

11 Reati in materia di violazione dei diritti d'autore

11.1 La fattispecie di reato

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES, D.LGS. 231/01)
Si riporta di seguito una breve descrizione dei reati contemplata dall'art. 25-novies del Decreto e che possono riguardare potenzialmente l'Ente.

• Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis);
• Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3);
• Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1);
• Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2);
• Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941);
• Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941);
• Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).

11.2 Aree di attività a rischio

I reati sopra indicati sono caratterizzati dalla previsione che l'attività illecita abbia ad oggetto la violazione del diritto d'autore ad opera di un soggetto operante all'interno dell'Ente.
In particolare, si considerano a rischio tutte le aree della Ente che potenzialmente nell'esercizio delle proprie funzioni potrebbero violare il diritto di autore di un altro soggetto, legalmente tutelato. In particolare, possiamo individuare un maggior rischio in quelle aree, come le Unità Operative Gestione, Amministrazione, Segreteria, Qualità e Comunicazione che utilizzano sistemi informatici, i quali, generalmente sono protetti da un copyright e poiché la loro attività si esplica proprio attraverso la stipula di accordi con soggetti terzi che potrebbero prevedere l'utilizzo di documenti protetti dal diritto d'autore. Inoltre, si sottolinea, come anche nell'erogazione dei servizi agli utenti l'Ente è a rischio di commissione reato.

11.3 Destinatari della Parte Speciale

Questa Parte Speciale si riferisce a comportamenti posti in essere da chiunque operando nelle aree di attività a rischio, violi il diritto d'autore legalmente tutelato esponendo la Ente ad un rischio legale, oltre che reputazionale.

11.4 Principi generali di comportamento

Nell'espletamento della propria attività, tutti i dipendenti/collaboratori di ESEB sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati del Modello e, in particolare, dal Codice Etico.
È inoltre necessario:
• che sia garantito il rispetto del Codice Etico;
• che tutte le attività svolte siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
• che sia rispettato il principio di separazione dei ruoli e responsabilità nelle fasi dei processi aziendali.

A tutti i dipendenti/collaboratori dell'Ente è fatto divieto di:
• porre in essere, collaborare o dare causa alla realizzazione dei comportamenti tali da integrare le fattispecie di delitti relativi al diritto d'autore sopra richiamati;
• porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, ESEBbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

11.5 Procedure di prevenzione

L'Ente ha implementato un sistema di controlli volto alla creazione di un canale informativo nei confronti dell'Organismo di Vigilanza al fine di prevenire la commissione dei reati commessi con violazione delle norme a tutela dei diritti d'autore.
Per la prevenzione dei reati previsti nella presente Parte Speciale, l'Organismo di Vigilanza dovrà effettuare controlli nei confronti dei Destinatari della presente Parte Speciale, al fine di verificare l'osservanza delle prescrizioni ivi previste.

12 Reati ambientali

12.1 Reati ambientali (art. 25-*undecies*, D.lvo n. 231/01) - Fattispecie di reato rilevanti

Inquinamento idrico (art. 137 D.lvo 152/2006)
Gestione di rifiuti non autorizzata (art. 256 D.lvo 152/2006)
Omessa bonifica (art. 257 D.lvo 152/2006)
Violazioni in materia di formulari e certificati (artt.258 e 260 bis D.lvo 152/2006)

12.2 Attività sensibili

a. Scarico di acque reflue industriali, in particolare scarico delle acque di lavaggio degli utensili del cantiere
b. Attività di selezione e gestione dei fornitori di servizi di analisi
c. Prelievo di acque superficiali e/o sotterranee nell'ambito della sede e del cantiere
d. Scarico di acque sul suolo, sul sottosuolo e nelle acque sotterranee
e. Deposito dei rifiuti provenienti dalle lavorazioni del cantiere
f. Attività di miscelazione di rifiuti
g. Attività di raccolta, trasporto e smaltimento dei rifiuti, in particolare materiali provenienti dalle lavorazioni del cantiere
h. Gestione degli adempimenti e delle dichiarazioni obbligatorie per legge in materia ambientale
i. Gestione delle ispezioni/controlli/accertamenti della P.A. sul rispetto della normativa ambientale

12.3 Modalità di attuazione dei reati astrattamente ipotizzabili

INQUINAMENTO IDRICO

- Scarico non autorizzato (autorizzazione assente, sospesa o revocata) di acque reflue industriali contenenti sostanze pericolose (art. 137 c.2). In particolare, il reato potrebbe realizzarsi qualora le acque provenienti dal lavaggio degli strumenti di cantiere venissero scaricate nella rete fognaria in assenza di autorizzazione amministrativa e si accertasse la presenza delle sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 al decreto legislativo. A prescindere dalla applicazione del D.lvo 231, che si verifica solo in presenza di scarico di acque contenenti sostanze inquinanti, si segnala che le acque provenienti dalle lavorazioni di cantiere sono sempre classificate come "acque reflue industriali", con la conseguenza che il loro scarico necessita di autorizzazione amministrativa, pena l'applicazione di una sanzione penale.
- Scarico di acque reflue industriali contenenti sostanze pericolose in violazione delle prescrizioni imposte con l'autorizzazione o da autorità competenti (art. 137 c. 3).
- Scarico di acque reflue industriali contenenti sostanze pericolose in violazione dei limiti tabellari o dei limiti più restrittivi indicati nell'autorizzazione della P.A.
- Violazione dei divieti di scarico sul suolo, nelle acque sotterranee e nel sottosuolo (art. 137 c. 11). Il reato si potrebbe configurare qualora le acque provenienti dal cantiere venissero scaricate sul terreno.

GESTIONE DI RIFIUTI NON AUTORIZZATA

-raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione (art. 256 c.1). In particolare al personale della Ente potrebbe essere addebitato il reato in esame, in concorso con il trasportatore, qualora il trasportatore non abbia regolare autorizzazione.
-Realizzazione o gestione di una discarica non autorizzata destinata allo smaltimento di rifiuti pericolosi e non pericolosi (art. 256 c. 3). Il reato potrebbe astrattamente verificarsi qualora, a prescindere dall'effettuazione di interventi di predisposizione dei luoghi, si verificasse un ripetitivo accumulo di materiali oggettivamente destinati all'abbandono, ovvero un unico conferimento di ingenti quantità di rifiuti che faccia però assumere alla zona

interessata l'inequivoca destinazione a ricettacolo di rifiuti, con conseguente trasformazione del territorio. Si segnala inoltre che, a prescindere dalla possibile applicazione del d.lvo 231, l'abbandono di rifiuti costituisce reato.

OMESSA BONIFICA
-inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (sempre che non si provveda a bonifica, in conformità al progetto approvato dalla autorità competente) e omissione della relativa comunicazione agli enti competenti
VIOLAZIONI IN MATERIA DI FORMULARI E CERTIFICATI DI ANALISI
-Predisposizione di un certificato di analisi dei rifiuti falso (per quanto attiene alle informazioni relative a natura, composizione e caratteristiche chimico-fisiche dei rifiuti) e uso di un certificato falso durante il trasporto (art. 258 c.4, secondo periodo)
-predisposizione di un certificato di analisi falso, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti –SISTRI; inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (art. 260-bis, c. 6)
-trasporto di rifiuti pericolosi senza copia cartacea della scheda SISTRI-Area movimentazione o del certificato analitico dei rifiuti, nonché uso di certificato di analisi contenente false indicazioni circa i rifiuti trasportati in ambito SISTRI (art. 260 bis c. 7)
-trasporto di rifiuti pericolosi e non con copia cartacea della scheda SISTRI –Area movimentazione fraudolentemente alterata (art. 260 bis c. 8)

12.4 Procedure di prevenzione

Principi di controllo rilevanti

I protocolli che intervengono nella regolamentazione delle attività sensibili sono ispirati ai seguenti principi di controllo:
-**Esistenza di disposizioni** aziendali/regolamenti interni/procedure formalizzate/prassi operative relative all'attività di smaltimento dei rifiuti (dalla raccolta all'avvio verso lo smaltimento, tenuta dei registri cartacei ed eventuale tracciabilità SISTRI, ivi comprese modalità di archiviazione della documentazione)
- **Esistenza di disposizioni** aziendali/regolamenti interni/procedure formalizzate/prassi operative relative alla gestione degli scarichi delle acque reflue industriali
- **Tracciabilità della documentazione per la verificabilità ex post**
- **Segregazione dei compiti** al fine di separare le responsabilità tra chi autorizza, chi esegue e chi controlla il processo
- **Definizione delle modalità di selezione dei fornitori** di servizi di autotrasporto dei rifiuti (iscrizione all'apposito Albo, conferimento in discariche autorizzate)
- **Audit interni periodici** volti alla verifica del rispetto della normativa ambientale
- **Attività di monitoraggio** finalizzata alla verifica e aggiornamento periodico/tempestivo del sistema dei controlli di processo, del sistema di deleghe, procure, responsabilità, in coerenza con il modello di governance e organizzativo.

In particolare l'Ente deve:
a. **individuare una funzione aziendale** con il compito e la responsabilità di coordinare il personale coinvolto nelle operazioni di gestione e prevenzione dei rischi ambientali;
b. **prevedere programmi per il monitoraggio degli scarichi** in modo da poter intervenire tempestivamente in occasione di eventi (guasti, sversamenti, ecc.) che possono determinare la commissione di reati ambientali;
c. **prevedere programmi per la periodica revisione** interna dei metodi di raccolta, stoccaggio, separazione, ecc. dei rifiuti ed adempimenti consistenti nella verifica delle autorizzazioni dei soggetti cui affidare i propri rifiuti, nella corretta gestione dei formulari, nelle comunicazioni obbligatorie agli enti nei tempi previsti dalla legge;
d. **prevedere specifiche procedure per la gestione delle comunicazioni con l'esterno**
, soprattutto con le Autorità di vigilanza in materia ambientale.

Funzioni coinvolte
- C.d.A.
- Direttore
- Responsabile per l'ambiente

PP.AA. interessate
- Regione Lombardia
- ASL
- Arpa
- Carabinieri nucleo ambientale
- Comune
- Provincia

13 Reati di impiego di cittadini terzi il cui soggiorno è irregolare

13.1) La tipologia del reato

L'articolo 25 duodecies del D. Lgs. 231/01 individua il così detto "reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

13.2) Destinatari della parte speciale

Destinatari della presente Parte Speciale sono gli amministratori ed il direttore generale della Ente Sistema Edilizia Brescia ed il responsabile dell'ufficio gestione del personale

13.3) Aree a rischio

Le aree di attività ritenute a rischio definibile come potenzialmente basso in relazione al reato sopracitati in relazione al fatto che le assunzione avvengono **mediante concorso (?)** sono considerate le seguenti:

- Selezione ed assunzione del Personale nel caso in cui sia assunta una persona il cui permesso di soggiorno non è regolare.
- Gestione del personale nel caso in cui nel corso del rapporto di lavoro al dipendente extracomunitario venga revocato il permesso di soggiorno oppure che questi non provveda al suo rinnovo alla scadenza.

E 4) Misure per la prevenzione

I presidi organizzativi e di controllo in essere all'interno della Ente Ediel Bresciana sono formalizzati nella procedura:

- Protocollo "Selezione, assunzione e gestione del personale"

14 Attività strumentali alla commissione dei reati

14.1 Attività strumentali alla commissione dei reati

ESEB adotta un sistema di controlli interni con lo scopo di monitorare tutte quelle attività che potrebbero costituire un supporto per la commissione dei reati nei processi aziendali in cui si intrattengono relazioni con la Pubblica Amministrazione.

In particolare la seguente tabella elenca i processi sensibili ed i relativi standard di controllo organizzativo su cui è stata condotta l'analisi.
Le seguenti aree di attività sono state ritenute più specificatamente a rischio a conclusione dell'attività di valutazione. Di seguito sono elencate tutte le attività sensibili mappate durante le fasi di diagnosi:

PROCESSO	STANDARD DI CONTROLLO ORGANIZZATIVO
Finanza dispositiva	a. Esistenza di regole chiare e formalizzate che suddividano tra attori, responsabilità e livelli autorizzativi per la richiesta dell'ordine di pagamento o di messa a disposizione, l'effettuazione del pagamento e il controllo consultivo; b. Esistenza di un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi residenti nei sistemi informativi.
Selezione ed assunzione del personale	a. Tracciabilità delle fonti di reperimento dei c.v. , del processo di assunzione e della relativa documentazione; b. Assegnazione della responsabilità della valutazione attitudinale e tecnica del candidato a soggetti distinti.
Gestione di omaggi	a. Identificazione dei soggetti titolati a rilasciare omaggi e a provvedere alla loro fornitura; b. Esigenza per ciascuna tipologia di bene/servizio di un catalogo e di uno specifico range economico; c. Tracciabilità del processo.
Spese di rappresentanza	a. Chiara definizione delle categorie di spesa effettuabili, dei soggetti aziendali abilitati a sostenere le spese, dei livelli di autorizzazione per il rimborso delle spese effettuate, delle regole di registrazione delle spese sostenute a favore di pubblici dipendenti e amministratori.
Incarichi a professionisti	a. Chiara definizione di attori diversi e di differenti livelli autorizzativi operanti nelle fasi di richiesta della consulenza, autorizzazione, definizione contrattuale, certificazione dell'esecuzione dei servizi, effettuazione del pagamento; c. Esistenza di requisiti professionali, economici e organizzativi a garanzia degli standard qualitativi richiesti, d. Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati; d. Espletamento di adeguata attività selettiva e di obiettiva comparazione delle offerte.
Approvvigionamento di beni e servizi	a. Chiara definizione di attori diversi e di differenti livelli autorizzativi operanti nelle fasi di richiesta della fornitura, effettuazione dell'acquisto, certificazione della consegna, effettuazione del pagamento; b. Esistenza di criteri tecnico-economici per la selezione di potenziali fornitori e la validazione della fornitura, c. Espletamento di adeguata attività selettiva e di obiettiva comparazione delle offerte; d. Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati.