

ESTRACOM S.p.A.

MODELLO 231
Modello di organizzazione e controllo
ex D. Lgs. 231/2001

PARTE GENERALE

LUGLIO 2009

Sommario

1. Aspetti generali	3
1.1. Obiettivi	4
1.2. Principi	5
1.3. Destinatari	5
1.4. La normativa di riferimento	5
1.5. I reati	6
1.6. Organizzazione	12
1.7. Obbligatorietà	13
1.8. Struttura del modello	13
2. Codice Etico	14
3. Mappatura delle aree a rischio	15
4. Organismo di Vigilanza	21
4.1. Composizione	21
4.2. Funzioni e poteri	23
4.3. Poteri di accesso	25
4.4. Raccolta e conservazione delle informazioni	26
4.5. Regolamento di funzionamento	26
5. Flussi informativi	27
5.1. Flussi informativi dall'Organismo di Vigilanza verso i vertici societari	27
5.2. Flussi informativi dalle aree aziendali verso l'Organismo di Vigilanza	27
5.3. Altri flussi informativi	28
6. Sistema disciplinare	30
6.1. Funzioni del sistema disciplinare	30
6.2. Sanzioni a carico dei dipendenti	30
6.3. Sanzioni a carico dei dirigenti	34
6.4. Sanzioni a carico degli amministratori e dei sindaci	34
6.5. Misure a carico dei terzi (consulenti e partners)	34
6.6. Pubblicazione del sistema disciplinare	34
7. Applicazione, diffusione e aggiornamento del modello	36
7.1. Parti speciali	36
7.2. Comunicazione e formazione	36
7.3. Aggiornamento del modello	37

1. ASPETTI GENERALI

Il Decreto Legislativo 8 giugno 2001 n. 231 ha introdotto l'istituto della responsabilità amministrativa delle persone giuridiche. Il Decreto prevede la possibilità che, nel caso di commissione di determinati reati, la Società possa essere chiamata a risponderne se questi sono stati commessi **nel suo interesse o a suo vantaggio** dai propri amministratori o dipendenti.

Le sanzioni previste a carico della Società possono essere:

- **pecuniarie**, da € 25.800 fino ad € 1.549.000;
- **interdittive**, che possono consistere: nella interdizione totale o parziale dall'esercizio dell'attività; nella sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; nel divieto di contrattare con la Pubblica Amministrazione; nell'esclusione da agevolazioni, finanziamenti, contributi e nell'eventuale revoca di quelli già concessi.

Gli art. 6 e 7 dello stesso decreto dispongono che l'azienda possa essere esonerata da tale responsabilità se, in sede di giudizio di uno dei reati previsti, prova di avere adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a prevenire la commissione del reato della specie verificatosi.

In particolare, il D. Lgs. 231/01 prevede che l'organizzazione non risponda per i reati commessi dai soggetti aziendali se prova che:

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

Le aree d'intervento sono quelle inerenti i reati societari, i reati sulla sicurezza ed igiene sul lavoro, i reati di riciclaggio e ricettazione, i reati contro la Pubblica Amministrazione, i reati transnazionali, quelli contro la personalità individuale, quelli per abusi di mercato, quelli con finalità terroristiche.

1.1. OBIETTIVI

L'attuazione del Modello 231 di organizzazione, gestione e controllo risponde alla convinzione dell'azienda che ogni elemento utile al fine di ricercare condizioni di correttezza e trasparenza nella gestione delle attività aziendali è meritevole di attenzione sia per l'immagine della società sia per la piena tutela degli interessi degli stakeholders aziendali.

La scelta di adozione del Modello si ritiene che possa costituire, un potente strumento di sensibilizzazione nei confronti di tutti i soggetti che operano per conto di ESTRACOM S.p.A. affinché, nell'espletamento delle loro attività, siano indotti a comportamenti ispirati dall'etica della responsabilità e conseguentemente corretti ed in linea con le diverse disposizioni di legge.

Obiettivo del presente documento è definire il Modello 231 di ESTRACOM S.p.A., ossia il modello organizzativo, gestionale e di controllo e le iniziative regolamentari da adottare per il rispetto della disciplina specifica sulla responsabilità amministrativa delle persone giuridiche (D. Lgs. 231/2001) e la limitazione dei rischi correlati.

In particolare, mediante la mappatura dei rischi e la formalizzazione dei processi a rischio reato, il modello si propone le finalità di:

- determinare, in tutti coloro che operano in nome e per conto della società, una piena consapevolezza di poter incorrere, in caso di violazione di alcune disposizioni normative, in un illecito passibile di sanzioni sul piano penale e amministrativo;
- rendere tali soggetti consapevoli che tali comportamenti illeciti potrebbero comportare sanzioni pecuniarie ed interdittive nei confronti dell'azienda;
- sottolineare come i comportamenti illeciti siano fortemente condannati e contrari agli interessi di ESTRACOM S.p.A., anche quando apparentemente essa potrebbe trarne un vantaggio, poiché sono comportamenti contrari ai principi etico-sociali della società oltre che alle disposizioni di legge;
- consentire a ESTRACOM S.p.A., grazie ad un monitoraggio costante dei processi sensibili e quindi dei rischi di commissione di reato, di reagire tempestivamente al fine di prevenire e contrastare la commissione dei reati stessi.

1.2. PRINCIPI

Ai sensi di quanto esplicitamente previsto dal Decreto, i Principi cardine a cui il Modello si ispira sono:

- ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua;
- nessuno deve poter gestire in autonomia un intero processo, ovvero deve essere rispettato il principio della separazione delle funzioni;
- i poteri autorizzativi devono essere assegnati coerentemente con le responsabilità assegnate;
- il sistema di controllo deve documentare l'effettuazione dei controlli, compresa la supervisione.

1.3. DESTINATARI

I principi e i contenuti del presente modello di organizzazione, gestione e controllo sono destinati ai componenti degli organi sociali, del management e ai dipendenti di ESTRACOM S.p.A. nonché a tutti coloro che operano in Italia e all'estero per lo svolgimento di attività e per il conseguimento degli obiettivi di ESTRACOM S.p.A.

1.4. LA NORMATIVA DI RIFERIMENTO

La normativa di interesse include la L. 300/2000 ed il D. Lgs. 231/2001, oltre a recenti norme che hanno esteso l'applicazione dei reati previsti dal Decreto 231. Di seguito se ne traccia di ciascuna un breve profilo.

Legge 29 settembre 2000 n. 300. Ratifica ed esecuzione dei seguenti Atti internazionali elaborati in base all'articolo K. 3 del Trattato dell'Unione europea: Convenzione sulla tutela degli interessi finanziari delle Comunità europee, fatta a Bruxelles il 26 luglio 1995, del suo primo Protocollo fatto a Dublino il 27 settembre 1996, del Protocollo concernente l'interpretazione in via pregiudiziale, da parte della Corte di Giustizia delle Comunità europee di detta Convenzione, con annessa dichiarazione, fatto a Bruxelles il 29 novembre 1996, nonché della Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, fatta a Bruxelles il 26 maggio 1997 e della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali, con annesso, fatta a Parigi il 17 dicembre 1997. Delega al Governo per la disciplina della responsabilità amministrativa

Decreto Legislativo 8 giugno 2001 n. 231 e successive modifiche ed integrazioni. Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell'articolo 11 della legge 29 settembre 2000 n. 300

Per ciascuno dei reati previsti dal D. Lgs. 231/2001 sono previste specifiche sanzioni sia di tipo pecuniario che interdittivo (oltre alla confisca ed alla pubblicazione della sentenza). Al momento sono stati presentati molti progetti di legge per ampliare ulteriormente il novero dei reati presupposto per la responsabilità amministrativa della persone giuridiche.

La **Legge 3 agosto 2007 n. 123** ha esteso la responsabilità amministrativa delle persone giuridiche anche ai reati di "omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro". Questa riforma appare particolarmente penalizzante sotto il profilo sanzionatorio.

Il **Decreto Legislativo 9 aprile 2008, n. 81** riunisce e armonizza le disposizioni contenute in numerose precedenti normative in materia di sicurezza e salute nei luoghi di lavoro, congiuntamente abrogate dal decreto stesso, e riordina anche l'impianto sanzionatorio previsto dal D. Lgs. 231/2001.

Il **Decreto Legislativo 21 novembre 2007, n. 231** introduce nuove disposizioni per reprimere il riciclaggio ed il finanziamento del terrorismo. Nell'ambito 231/2001 viene quindi inserito il nuovo art. 25-octies che, ai fini della responsabilità amministrativa d'impresa, include anche i reati di ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita.

La **Legge 18 marzo 2008, n. 48** ratifica e dà esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23/11/2001) che estende la portata del reato informatico includendo tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica. L'adeguamento dell'ordinamento interno ha ricompreso i reati informatici nell'alveo del D. Lgs. 231/2001.

1.5. I REATI

Nella tabella 1 che segue si riportano le fattispecie penali rilevanti ai fini del decreto 231/2001 con le relative sanzioni pecuniarie ed interdittive previste.

Tabella 1 - Reati e sanzioni

Norma di riferimento nel decreto 231/01	Reato presupposto	Sanzioni pecuniarie		Sanzioni interdittive				
		Quote (min –max)	Somme (min – max) in euro	Interdizione dall'esercizio dell'attività	Sospensione o revoca autorizzazioni, licenze o permessi (art 9 comma 2 lett. b)	Divieto di contrarre con la PA (art 9 comma 2 lett. c)	Esclusione da agevolazioni, finanziamenti contributi (art 9 comma 2 lett. d)	Divieto di pubblicizzare beni o servizi (art 9 comma 2 lett. e)
Art 24	Art 316 bis c.p (Malversazione a danno dello Stato)	100-500 Con aggravante: 200-600	258.00,00-774.500,00 Con aggravante 51.600,00-929.400,00	-	-	Si	Si	Si
Art 24	Art 316 ter c.p.(Indebita percezione di erogazioni da parte dello stato)	100-500 Con aggravante: 200-600	258.00,00-774.500,00 Con aggravante 51.600,00-929.400,00	-	-	Si	Si	Si
Art 24	Art. 640, comma 2 n. 1 c.p. (Truffa a danni dello Stato)	100-500 Con aggravante: 200-600	258.00,00-774.500,00 Con aggravante 51.600,00-929.400,00	-	-	Si	Si	Si
Art 24	Art. 640 bis c.p. (Truffa aggravata per il conseguimento di erogazioni pubbliche)	100-500 Con aggravante: 200-600	258.00,00-774.500,00 Con aggravante 51.600,00-929.400,00	-	-	Si	Si	Si
Art 24	Art. 640 ter c.p. (Frode informatica)	100-500 Con aggravante: 200-600	258.00,00-774.500,00 Con aggravante 51.600,00-929.400,00	-	-	Si	Si	Si
Art. 25 c. 1	Art. 318, 321 e 322 c.p. corruzione impropria ed istigazione alla corruzione impropria	100-200	258.00,00- 309.800,00	-	-	-	-	-
Art. 25 c. 2	Art. 319, 319 ter c. 1, 321, 322 c. 2 e 4. Corruzione propria, corruzione in atti giudiziari e istigazione alle corruzioni	200-600	51.600,00- 929.400,00	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)
Art. 25 c. 3	317,319 aggravato ex 319 bis, 319 ter c.2, 321 c.p. (concussione, corruzione propria aggravata, corruzione in atti giudiziari aggravata)	300-800	77.400,00- 1.239.200,00	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)
Art. 25 bis	Reati di falsi in monete, in carte di credito e in valori di bollo	50-500	12.900,00-774.500,00	Si (max 1 anno)	Si (max 1 anno)	Si (max 1 anno)	Si (max 1 anno)	Si (max 1 anno)

Norma di riferimento nel decreto 231/01	Reato presupposto	Sanzioni pecuniarie		Sanzioni interdittive				
		Quote (min –max)	Somme (min – max) in euro	Interdizione dall'esercizio dell'attività	Sospensione o revoca autorizzazioni, licenze o permessi (art 9 comma 2 lett. b)	Divieto di contrarre con la PA (art 9 comma 2 lett. c)	Esclusione da agevolazioni, finanziamenti contributi (art 9 comma 2 lett. d)	Divieto di pubblicizzare beni o servizi (art 9 comma 2 lett. e)
25 ter	Reati societari (art 2621 e seguenti cod. civ.)	100-500 Con aggravante: 300-1500	25.800,00-774.500,00 con aggravante: 77.400,00- 2.323.500,00	-	-	-	-	-
25 quater1	Delitti con finalità di terrorismo	200-1000	51.600,00- 1.549.000,00	Si (min 1 anno) + interdizione definitiva se aggravante 25 c. 3	Si (min 1 anno) + interdizione definitiva se aggravante 25 c. 3	Si (min 1 anno) + interdizione definitiva se aggravante 25 c. 3	Si (min 1 anno) + interdizione definitiva se aggravante 25 c. 3	Si (min 1 anno) + interdizione definitiva se aggravante 25 c. 3
25 quater 2	Pratiche di mutilazione degli organi genitali femminili	300-700	77.400,00-1.084.300,00	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)	Si (min 1 anno)
25 quinquies	Reati contro la libertà individuale	200-1000	51.600,00- 1.549.000,00	Si (min 1 anno) + interdizione definitiva se aggravante	Si (min 1 anno) + interdizione definitiva se aggravante	Si (min 1 anno) + interdizione definitiva se aggravante	Si (min 1 anno) + interdizione definitiva se aggravante	Si (min 1 anno) + interdizione definitiva se aggravante
25 sexes	Abusi di mercato (TU 58/1998)	400-1000 se aggravato: fino a 100 volte il prodotto o il profitto	103.200,00- 1.459.000,00	-	-	-	-	-
25 septies commi 1 e 2	589 cp aggravata violazione norme antinfortunistiche	Minimo 1000 per aziende primo comma 27 septies Da 250 a 500 quote per tutti altri casi	258.000,00 - 1.549.000,00 64.500 – 774.500	Si (min 3 mesi, max 1 anno)	Si (min 3 mesi, max 1 anno)	Si (min 3 mesi, max 1 anno)	Si (min 3 mesi, max 1 anno)	Si (min 3 mesi, max 1 anno)
25 septies comma 3	590 comma 3 cp (lesioni sup 40 giorni con violazione norme antinfortunistiche)	100 – 250	25.800 – 387.250	Si (max 2 mesi)	Si (max 2 mesi)	Si (max 2 mesi)	Si (max 2 mesi)	Si (max 2 mesi)
25 octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	200-1000	51.600,00- 1.549.000,00	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)

Norma di riferimento nel decreto 231/01	Reato presupposto	Sanzioni pecuniarie		Sanzioni interdittive				
		Quote (min –max)	Somme (min – max) in euro	Interdizione dall'esercizio dell'attività	Sospensione o revoca autorizzazioni, licenze o permessi (art 9 comma 2 lett. b)	Divieto di contrarre con la PA (art 9 comma 2 lett. c)	Esclusione da agevolazioni, finanziamenti contributi (art 9 comma 2 lett. d)	Divieto di pubblicizzare beni o servizi (art 9 comma 2 lett. e)
Art. 10 c. 2 L. 146/2006	Reati associativi transnazionali	400-1000	103.200,00- 1.459.000,00	Si (min 1 anno) + interdizione definitiva se aggravato	Si (min 1 anno) + interdizione definitiva se aggravato	Si (min 1 anno) + interdizione definitiva se aggravato	Si (min 1 anno) + interdizione definitiva se aggravato	Si (min 1 anno) + interdizione definitiva se aggravato
Art 10 c.7 L. 146/2006	Traffico di migranti transnazionale	200-1000	51.600,00- 1.549.000,00	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)	Si (max 2 anni)
Art. 10 c. 9 L. 146/2006	Intralcio alla giustizia transnazionale	Max 500	25.800,00-774.500,00	-	-	-	-	-
Art. 192 D.Lvo 152/2006	Abbandono di rifiuti	-	105,00 – 620,00 (?) Art. 255 D.Lvo 152/2006 (?)	-	-	-	-	-
24 bis c. 1	615 ter c.p. (accesso abusivo a sistema informatico)	100 – 500	2.580,00 - 774.500,00	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)	no	no	Si (3 mesi a 2 anni)
24 bis c. 1	617 quater, 617 quinquies c.p. (intercettazione flussi informatici e installazione apparecchiature atte ad intercettare)	100 – 500	2.580,00 - 774.500,00	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)	no	no	Si (3 mesi a 2 anni)
24 bis c. 1	635 bis, ter, quater, quinquies (danneggiamenti sistemi informatici e informazioni informatiche.)	100 – 500	2.580,00 - 774.500,00	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)	no	no	Si (3 mesi a 2 anni)
24 bis c. 2	615 quater c.p. (Detenzione di programmi atti a interrompere un sistema informatico).	100 – 300	2.580,00 - 464.700,00	No	Si (3 mesi a 2 anni)	no	no	Si (3 mesi a 2 anni)
24 bis c. 2	615 quinquies c.p. (diffusione virus)	100 – 300	2.580,00 - 464.700,00	No	Si (3 mesi a 2 anni)	no	no	Si (3 mesi a 2 anni)

Norma di riferimento nel decreto 231/01	Reato presupposto	Sanzioni pecuniarie		Sanzioni interdittive				
		Quote (min –max)	Somme (min – max) in euro	Interdizione dall'esercizio dell'attività	Sospensione o revoca autorizzazioni, licenze o permessi (art 9 comma 2 lett. b)	Divieto di contrarre con la PA (art 9 comma 2 lett. c)	Esclusione da agevolazioni, finanziamenti contributi (art 9 comma 2 lett. d)	Divieto di pubblicizzare beni o servizi (art 9 comma 2 lett. e)
24 bis c. 3	491 bis (salvo art. 24) Falsità in documenti informatici aventi efficacia probatoria.	100 – 400	2.580,00 - 619.600,00	No	no	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)
24 bis c. 3	640 quinquies c.p. (salvo art. 24) Truffa informatica commesso da soggetto che presta servizi di certificazione di firma elettronica	100 – 400	2.580,00 - 619.600,00	No	no	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)	Si (3 mesi a 2 anni)

Nell'ambito dell'analisi ci si è concentrati su alcuni reati-presupposto, mentre altri - tenuto conto sia dell'attività svolta dall'azienda, e quindi della non pertinenza dei reati con essa, sia dell'assoluta carenza di interesse o vantaggio dalla commissione dei suddetti illeciti - non sono stati presi in considerazione.

In particolare è stato rivolto un focus su:

- Corruzione, malversazione, indebite percezioni di contributi e truffe a danni dello Stato (art. 24 e 25),
- Concussione (art. 24 e 25);
- Reati societari (art. 25 ter),
- Reati di omicidio colposo e lesioni personali colpose gravissime con violazione delle norme anti-infortunistiche (art. 25 septies),
- Reati informatici (art. 24 bis);
- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies).

Non sono stati considerati quali possibili presupposti per la responsabilità della Società i seguenti illeciti:

- Falsità in monete, in carte di credito e in valori di bollo (art. 25 bis), delitti con finalità di terrorismo ed eversione dell'ordine democratico (25 quater1), delitti di pratiche di mutilazione di organi genitali femminili (art. 25 quater 2), delitti contro la personalità individuale (art. 25 quinquies), reati ed illeciti amministrativi di abusi di mercato (art. 25 sexies);
- Reati transnazionali di riciclaggio e altri.

Con riferimento a queste esclusioni non sono emersi elementi tali da far presupporre un potenziale rischio di commissione dei relativi reati o illeciti amministrativi.

In taluni casi, infatti, non paiono ragionevolmente ipotizzabili comportamenti illeciti connessi all'attività imprenditoriale (si pensi, ad esempio, ai reati d'infibulazione, di eversione dell'ordinamento democratico, di tratta dei migranti ecc..).

In altri casi, ove si sia ravvisata una possibile connessione teorica tra i reati-presupposto e l'attività imprenditoriale (esempio, la riduzione in schiavitù), si è trattato di una pertinenza meramente scolastica, senza però ragionevoli motivi per poterne supporre una possibile, ancorché teorica, realizzazione.

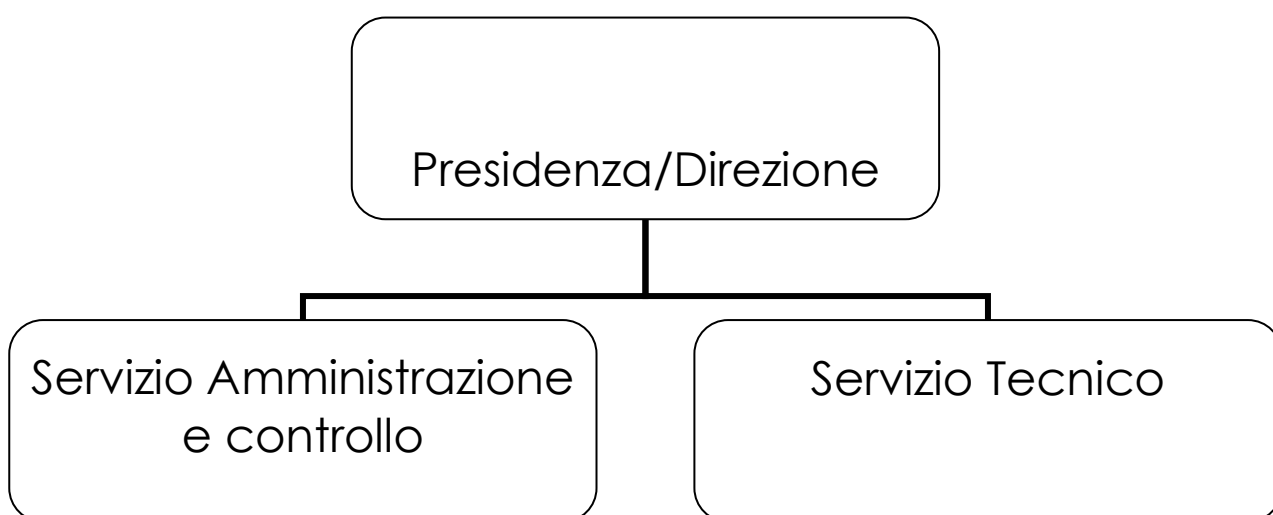
Per gli illeciti in materia di abbandono di rifiuti, stanti le incertezze sull'effettiva applicabilità del Decreto 231/01, non sono state svolte valutazioni approfondite, fermo restando l'opportunità cautelativa di tenerne conto e comunque in attesa di prevedibili evoluzioni normative.

Per alcuni reati, infine, non è nemmeno teoricamente ipotizzabile un interesse o vantaggio dell'ente alla loro realizzazione.

1.6. ORGANIZZAZIONE

Sotto l'aspetto organizzativo si riporta qui sotto la rappresentazione grafica della struttura organizzativa di ESTRACOM S.p.A. nella forma di organigramma sintetico.

ESTRACOM S.p.A. - Organigramma aziendale sintetico



1.7. OBBLIGATORIETÀ

E' fatto obbligo agli Amministratori, al Direttore e a tutto il personale di osservare scrupolosamente le norme e le disposizioni che compongono il presente modello organizzativo e gestionale.

1.8. STRUTTURA DEL MODELLO

Il Modello 231 di organizzazione e controllo di ESTRACOM S.p.A. è strutturato in una parte generale e quattro parti speciali.

La parte generale è costituita dal presente documento che riporta: gli aspetti generali del modello, il codice etico, la mappatura dei rischi aziendali, la composizione ed i poteri dell'Organismo di Vigilanza, i flussi informativi aziendali per un efficace funzionamento del modello, il sistema disciplinare per le violazioni del modello, la diffusione ed aggiornamento del modello.

Le quattro parti speciali fanno riferimento alle categorie di reato su cui si concentra l'attenzione dell'Azienda e, per ciascuna categoria di reati, mettono in evidenza le fattispecie di reato, le attività aziendali a rischio, i principi aziendali di comportamento strettamente connessi.

2. CODICE ETICO

Il Codice etico è un documento ufficiale adottato dal Consiglio di Amministrazione di ESTRACOM S.p.A. in data 10 dicembre 2009 contenente l'insieme dei diritti e dei doveri dei soggetti aziendali e delle responsabilità aziendali (principi di comportamento) nei confronti dei soggetti portatori di interesse.

Il Codice etico costituisce parte integrante del Modello 231 di organizzazione, gestione e controllo di ESTRACOM S.p.A. e viene allegato al presente documento.

Tutti i soggetti aziendali sono chiamati ad uniformarsi ai comportamenti prescritti dal Codice etico.

3. MAPPATURA DELLE AREE A RISCHIO

Sotto l'aspetto del rischio, per una più efficace valutazione e graduazione dello stesso, sono stati considerati due aspetti: in primo luogo l'attinenza dell'ipotetico reato con l'attività d'impresa (pertinenza) e i relativi interessi o vantaggi che l'azienda può trarre dall'illecito, in secondo luogo il grado di impatto sull'azienda in termini di sanzioni.

Nella figura 1 si riportano in forma matriciale tali due aspetti considerati; i quadranti che derivano mettono in evidenza in basso a sinistra i rischi aziendali che, pur presenti, sono di livello basso, mentre in alto a destra sono riportati i maggiori rischi aziendali su cui occorre prestare particolare attenzione.

Tale valutazione ha natura meramente indicativa, poiché le variabili sono molteplici e non tutte pronosticabili con sufficiente certezza, posto che molte dipendono dalla valutazione soggettiva altrui.

Figura 1 - Mappa per il livello di rischio

		Impatto sull'azienda in termini di sanzioni		
		Basso	Medio	Alto
Attinenza dell'illecito con l'attività di impresa	Alta			
	Media			
	Bassa			

Sulla definizione del grado di rischio contribuisce anche il livello di formalizzazione delle procedure aziendali, infatti un elevato livello di formalizzazione delle stesse generalmente assicura una minore probabilità di verificarsi del rischio.

Di seguito si riporta la sintesi della mappatura dei rischi ai sensi del D. Lgs. 231/2001.

Va premesso che, in generale, sotto l'aspetto delle responsabilità di processo emerge che gli aspetti operativi vengono sempre curati da soggetti differenti rispetto a chi è deputato ai controlli ed alla supervisione, tenuto conto del fatto che molte funzioni amministrative (finanza, contabilità, bilanci, approvvigionamenti, legale, relazioni interne ed esterne, sistemi qualità, ecc.) ed informatiche sono gestite nelle parti operative dalla capogruppo CONSIAG S.p.A., direttamente o avvalendosi della Società controllata Sinergie S.r.l., fermi restando i poteri decisionali di ESTRACOM.

Il reato di **malversazione ai danni dello stato** si concretizza nel caso in cui l'azienda ottenga correttamente contributi o finanziamenti da parte di amministrazioni pubbliche ma non li destini alle finalità per cui sono stati erogati. In ESTRACOM S.p.A. si presenta tale problematica relativamente a contributi

erogati dal FSE relativamente a corsi di formazione. Trattasi di contributi di importo complessivo non rilevante e le procedure sono gestite secondo il sistema Qualità certificato ISO 9001:2000 della capogruppo, peraltro l'ente erogatore impone specifici adempimenti formali ed il tutto è gestito tramite un ente terzo di formazione che è titolare dei progetti finanziati. Pertanto si presenta un rischio ex 231 molto basso.

Per quel che concerne l'**indebita percezione di erogazioni a danni dello stato**, che si concretizza con l'ottenimento di contributi o finanziamenti in modo fraudolento (nel caso specifico si fa sempre riferimento a contributi del FSE), vale quanto detto al paragrafo precedente.

Il reato di **truffa ai danni dello Stato** o di altro ente Pubblico si realizza mediante qualsiasi condotta che, inducendo taluno in errore con artifici e raggiri, procura per sé o ad altri un ingiusto profitto con altrui danno. Nel caso di specie, ESTRACOM fa richiesta di autorizzazioni rivolte a Ministeri, Provincia, comuni, Vigili del fuoco, ecc. per lo svolgimento della propria attività. Tali attività vengono poste in essere dall'azienda sulla base delle specifiche esigenze, quindi generalmente senza una precisa periodicità e non sono soggette a specifica regolamentazione aziendale, ma si attengono comunque alle disposizioni degli enti pubblici cui si rivolge l'azienda. Pertanto il livello di rischio è considerato basso.

Il reato di **truffa aggravata per il conseguimento di erogazioni pubbliche** è una forma aggravata di truffa, caratterizzata per il fatto che la condotta è finalizzata al conseguimento di contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee (codice penale articolo 640 bis). I rischi connessi a tutte le fattispecie di truffa ai danni degli enti pubblici sono direttamente correlati allo stretto rapporto esistente tra la società, i Comuni ed altri Enti Pubblici territoriali. Pertanto il processo e le funzioni interessate in questo caso sono le stesse dei reati di malversazione ed indebita percezione di erogazione a danno dello Stato, e, al riguardo, si confermano le stesse valutazioni di rischio sopra formulate per i contributi per attività formative.

Il reato di **frode informatica a danno dello Stato** si configura allorché chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno (codice penale, articolo 640 ter). In ESTRACOM tale problematica non si presenta in termini significativi, in quanto, nello svolgimento del proprio core business (servizi telecomunicazioni per i clienti), il personale aziendale può avere accesso a dati ed informazioni di terze parti e della Pubblica Amministrazione, ma, nel settore in cui opera l'azienda, esistono specifiche prescrizioni Ministeriali finalizzate all'impedimento del reato in oggetto. Invece, sul fronte del supporto informatico gestionale "interno", si rileva che tutte le aziende del Gruppo hanno

un sistema informatico relativamente valido in termini di autorizzazioni agli accessi e di tracciabilità delle operazioni, in considerazione delle dimensioni del Gruppo societario e dell'articolazione e complicità del sistema informativo, nonché in funzione del DPS adottato ai sensi del D. Lgs. 196/03. Va però considerato che, in questo secondo caso, mancano specifiche prescrizioni aziendali finalizzate all'impedimento della commissione del reato in questione.

Il reato di **concussione** è quello commesso dal pubblico ufficiale o l'incaricato di un pubblico servizio, che, abusando della sua qualità o dei suoi poteri, costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità (codice penale, articolo 317). In ESTRACOM non si presenta tale tipo di problematica.

In merito al reato di **corruzione impropria** (ed istigazione alla corruzione impropria), che si concretizzano con l'erogazione (o la promessa di erogazione) di denaro o altro da parte di un soggetto aziendale ad un pubblico ufficiale per il compimento di un atto dovuto, le funzioni ed i processi sensibili sono quelli che gestiscono i casi di richieste di autorizzazione inoltrate alla P.A. Il relativo rischio è stato valutato medio.

Il reato di **corruzione propria** (ed istigazione alla corruzione propria) evidenzia qualche rischio in più rispetto a quello precedente di corruzione impropria in quanto è relativo all'erogazione (o la promessa di erogazione) di denaro o altro da parte di un soggetto aziendale ad un pubblico ufficiale per il compimento di un atto contrario ai doveri di ufficio (omissione o ritardo). Poiché potenzialmente sono numerose le occasioni aziendali di contatto con pubblici ufficiali per motivi di visite ispettive (Ministero, Guardia di finanza, Vigili del fuoco, ecc.) e può essere di rilevante importanza economica la partecipazione a gare e a trattative per concessione di servizi e la stipula contratti con la P.A., così potrebbe essere molto sensibile il momento in cui l'autorità giudiziaria chiede la fornitura di informazioni sui clienti, a questi aspetti è stato attribuito un grado di rischio elevato. Invece è stato considerato medio il rischio per la gestione dei contratti di servizio stipulati con la P.A.

Per il reato di **corruzione in atti giudiziari**, considerato il rilievo economico che possono avere le risoluzioni di contenziosi giudiziari e stragiudiziali, non proceduralmente regolamentate, anche se non frequenti, il livello di rischio è stato valutato medio.

Per quel che concerne i **reati societari**, ed in particolare le false comunicazioni sociali (falso in bilancio), potenzialmente si presentano rischi ex 231/01, sebbene l'azienda predisponga annualmente il bilancio attraverso il coinvolgimento di diversi organi aziendali (Consiglio di Amministrazione, Presidente, Direttore, collegio sindacale), di funzioni amministrative di CONSIAG S.p.A., che sviluppano il service operativo in queste materie. Sulla base di quanto emerso nel corso delle interviste, nel bilancio aziendale sono presenti alcune voci oggetto di valutazioni discrezionali (ammortamenti, partite sospese di fine esercizio, ecc.). Pertanto il rischio non può essere trascurato, ma risulta comunque di livello

medio, tenuto altresì conto del fatto che le uniche sanzioni previste a carico dell'ente hanno natura pecuniaria.

I **reati di omicidio colposo e lesioni personali colpose gravissime con violazione delle norme antinfortunistiche**, inseriti nell'ambito 231 con la recente L. 123/2007 e successivamente meglio precisate dal Testo Unico sulla Sicurezza D. Lgs. 81/08, costituiscono la principale area di rischio per quanto riguarda ESTRACOM S.p.A., soprattutto sotto il profilo dell'impatto economico delle sanzioni. I soggetti direttamente coinvolti dalla problematica sono il datore di lavoro ed il delegato per la sicurezza, che hanno affrontato con molta serietà ed impegno le problematiche degli infortuni sul lavoro, ma devono ancora rendere efficaci le attività di monitoraggio del rispetto delle disposizioni aziendali, che peraltro si presentano valide. In ultima analisi, in tale materia, si configura per ESTRACOM un significativo rischio ex 231.

I reati di **riciclaggio e riutilizzo** costituiscono in teoria una medio/bassa area di rischio da monitorare attraverso specifici controlli sui flussi finanziari e sui rapporti con i fornitori. I reati consistono nel sostituire o trasferire denaro o altra utilità di natura illecita ovvero nell'utilizzare in attività imprenditoriali detti beni. La rilevanza ai fini del Decreto 231 del 2001 era subordinata alla natura "transnazionale" dell'operazione finanziaria, vale a dire a condotte che esplicano i loro effetti in un territorio ultranazionale, mentre ora - a decorre dal 29/12/2007 - valgono anche in ambito nazionale.

ESTRACOM intrattiene rapporti solo in ambito nazionale con fornitori e clienti, che, se inaffidabili, potrebbero originare problematiche di riciclaggio e riutilizzo. L'alienazione dei cespiti aziendali potrebbe raggiungere valori significativi, ma è attività eccezionale; mentre è sicuramente importante la gestione complessiva dei flussi finanziari, ma al riguardo va sottolineato che molte procedure aziendali sono regolamentate dal sistema Qualità aziendale ISO 9001:2000 certificato e vedono il coinvolgimento operativo delle funzioni amministrative della capogruppo sia per i "cicli attivi" sia per i "cicli passivi", per questo motivo il rischio è valutato medio.

Reati informatici. Con il termine di reati informatici si comprendono una serie di illeciti previsti da varie norme del codice penale e recentemente modificate dalla legge 48 del 2008 che ha recepito una direttiva sopranazionale (c.d. Convenzione di Budapest).

Tra essi si annoverano i reati di: accesso abusivo ad un sistema informatico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche; danneggiamento di dati o sistemi informatici utilizzati dallo Stato o da altro ente di pubblica utilità; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un

sistema informatico o telematico; frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Relativamente ai reati informatici se ne ravvisa un rischio potenziale basso, con le stesse motivazioni sopra espresse per i reati di frode informatica ai danni dello Stato.

Altri reati. Per numerosi altri reati, vista l'attività aziendale e la conseguente scarsa (spesso nulla) attinenza dell'illecito con l'attività d'impresa, non emergono possibili o potenziali responsabilità in capo all'azienda. I reati che non evidenziano rischi ex 231 sono costituiti da: falsità in monete, in carte di credito e in valori di bollo, delitti con finalità di terrorismo ed eversione dell'ordine democratico, delitti di pratiche di mutilazione di organi genitali femminili, delitti contro la personalità individuale, reati ed illeciti amministrativi di abusi di mercato, intralcio alla giustizia, reati transnazionali diversi dal riciclaggio e riutilizzo.

Sinteticamente si può riassumere nella figura 2 un indice di "significatività" dell'impatto sull'azienda di eventuali illeciti commessi da soggetti apicali o dipendenti.

I reati legati agli infortuni sul lavoro ed alla corruzione costituiscono l'ambito di maggior rischio per l'Azienda, si ritiene che comunque occorra prestare attenzione in particolare anche ai reati relativi ricettazione e riciclaggio e ai reati societari.

Figura 2 - Matrice di significatività

		Impatto sull'azienda in termini di sanzioni		
		Basso	Medio	Alto
Attinenza dell'illecito con l'attività di impresa	Alta			Infortunistica - Corruzione
	Media	Reati societari		
	Bassa	Truffe – Frode informatica		Ricettazione e riciclaggio – Malversazione - Indebita percezione di erogazioni pubbliche

(Nota: nella figura non è stato riportato il reato di abbandono dei rifiuti stante l'attuale ambiguità nella definizione delle sanzioni)

In conclusione, per ESTRACOM il principale rischio ex 231/01 è attribuibile al reato di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il rischio assume rilevanza sia sotto il profilo delle sanzioni pecuniarie, per un minimo di 1000 quote cui corrisponde una **sanzione (minima) di 258 mila €**, sia sotto il profilo delle seguenti **sanzioni interdittive applicabili per un minimo di 3 mesi ed un massimo di un anno**:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

4. ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza definisce e svolge le attività di competenza in modo **collegiale** ed è dotato ai sensi dell'art. 6, comma 1, lett. b), del D. Lgs. n. 231 del 2001 di “**autonomi poteri di iniziativa e controllo**”.

L'autonomia e l'indipendenza dell'Organismo di Vigilanza sono garantite dal posizionamento organizzativo, dai requisiti dei membri e dalle linee di riporto:

- nel contesto della struttura organizzativa l'organismo di Vigilanza si posiziona in staff del Consiglio di Amministrazione;
- ai membri dell'Organismo di Vigilanza sono richiesti requisiti di indipendenza, onorabilità e professionalità;
- l'Organismo di Vigilanza riporta direttamente al Consiglio di Amministrazione.

Per lo svolgimento delle attività operative di competenza ed al fine di consentire la massima adesione al requisito di continuità di azione ed ai compiti di legge, l'Organismo di Vigilanza si avvarrà del personale aziendale ritenuto necessario ed idoneo e/o di professionisti esterni specificatamente individuati.

L'Azienda metterà a disposizione dell'Organismo di Vigilanza le risorse umane e finanziarie necessarie allo svolgimento delle attività. Eventuali dinieghi del Consiglio di Amministrazione nel mettere a disposizione dell'Organismo di Vigilanza tali risorse dovranno essere adeguatamente motivate in forma scritta.

4.1. COMPOSIZIONE

L'Organismo di Vigilanza è composto da tre membri nominati dal Consiglio di Amministrazione per garantire competenza multidisciplinare.

Almeno uno dei membri è esterno all'azienda e alle Società del Gruppo societario di appartenenza, in quanto, oltre ad avere i requisiti di idonea professionalità, è in grado di garantire maggiore indipendenza di giudizio nelle valutazioni dell'Organismo.

Dell'Organismo di Vigilanza in ogni caso non faranno parte il datore di lavoro ed i soggetti delegati per la sicurezza.

La durata in carica dei membri coincide con quella del Consiglio di Amministrazione che li ha nominati.

Fatta salva l'ipotesi di una rivisitazione del ruolo dell'Organismo di Vigilanza sulla base dell'esperienza maturata, costituirà motivo di sostituzione o integrazione della composizione dell'Organismo di Vigilanza:

- l'attribuzione di compiti, ruoli e/o responsabilità all'interno della struttura organizzativa aziendale non compatibili con i requisiti di "autonomia e indipendenza" e/o "continuità di azione" propri dell'Organismo di Vigilanza;
- la cessazione o rinuncia del membro dell'Organismo di Vigilanza alla funzione aziendale e/o alla carica ricoperta;
- la cessazione o rinuncia del membro dell'Organismo di Vigilanza dettata da motivazioni personali.

Costituiscono motivi di ineleggibilità e/o di decadenza dei singoli membri dell'Organismo di Vigilanza:

- a)** relazioni di parentela, coniugio o affinità entro il IV grado con: componenti del Consiglio di Amministrazione; persone che rivestono funzioni di rappresentanza o di amministrazione o di direzione della Società; sindaci della Società; collaboratori della società di revisione;
- b)** conflitti di interesse, anche potenziali, con la Società o con società controllate, che ne compromettano l'indipendenza;
- c)** titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza sulla Società o su società controllate;
- d)** funzioni di amministratore ricoperte, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese sottoposte a procedure concorsuali;
- e)** rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'Organismo di Vigilanza;
- f)** condanna, anche non passata in giudicato, ovvero sentenza di "patteggiamento", in Italia o all'estero, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D. Lgs n. 231 del 2001;
- g)** condanna, anche non passata in giudicato, ovvero sentenza di "patteggiamento" a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di sostituzione o integrazione o di ineleggibilità e/o decadenza dovesse configurarsi a carico di un membro, questi dovrà darne notizia immediata agli altri membri dell'Organismo di Vigilanza e decadrà automaticamente dalla carica. L'Organismo di Vigilanza comunica la notizia al Presidente della Società.

In casi di particolare gravità il Consiglio di Amministrazione potrà disporre – sentito il parere del Collegio Sindacale – la sospensione delle funzioni e/o dei poteri dell'Organismo di Vigilanza e la nomina di un interim o la revoca dei poteri. Costituirà motivo di sospensione o di revoca:

- omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del D. Lgs. n. 231 del 2001 ovvero da sentenza di applicazione della pena su richiesta (c.d. patteggiamento);
- grave inadempimento delle funzioni dell'Organismo di Vigilanza.

4.2. FUNZIONI E POTERI

L'Organismo di Vigilanza opera con autonomi poteri di iniziativa e di controllo.

I compiti dell'Organismo di Vigilanza sono così definiti:

- a) vigilanza sull'effettività del Modello 231, ossia sull'osservanza delle prescrizioni da parte dei destinatari;
- b) monitoraggio delle attività di attuazione e aggiornamento del Modello 231;
- c) verifica dell'adeguatezza del Modello 231, ossia dell'efficacia nel prevenire i comportamenti illeciti;
- d) analisi circa il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del Modello 231 e promozione del necessario aggiornamento;
- e) approvazione ed attuazione del programma annuale delle attività di vigilanza nell'ambito delle strutture e funzioni della Società (di seguito "Programma di Vigilanza");
- f) cura dei flussi informativi di competenza con il Consiglio di Amministrazione e con le funzioni aziendali.

E' demandato all'Organismo di Vigilanza di definire:

- a) le risorse necessarie e le modalità operative per svolgere con efficacia le attività al fine di garantire che non vi sia omessa o insufficiente vigilanza (art. 6 comma 1 lettera d) del D. Lgs. citato);
- b) i provvedimenti necessari per garantire all'Organismo di Vigilanza ed alle altre risorse di supporto operativo i richiesti autonomi poteri di iniziativa e di controllo (art. 6 comma 1 lettera b) del D. Lgs. citato)

Sotto l'aspetto più operativo sono affidati all'Organismo di Vigilanza di ESTRACOM S.p.A. gli incarichi di:

- attivare le procedure di controllo, tenendo presente che una

responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al management operativo e forma parte integrante del processo aziendale ("controllo di linea");

- condurre ricognizioni dell'attività aziendale ai fini della mappatura aggiornata delle aree di attività a rischio nell'ambito del contesto aziendale;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di attività a rischio;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del modello e verificare la presenza della documentazione organizzativa interna necessaria al fine del funzionamento del modello stesso;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del modello, nonché aggiornare la lista delle informazioni che devono essere trasmesse obbligatoriamente allo stesso Organismo di Vigilanza;
- coordinarsi con le altre funzioni aziendali per il migliore monitoraggio delle attività nelle aree a rischio;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione prevista dalle procedure aziendali inerenti le attività a rischio reato;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- verificare che gli elementi del Modello per le diverse tipologie di reati siano adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, ad un aggiornamento degli elementi stessi.

L'Organismo di Vigilanza non assume responsabilità diretta per la gestione delle attività a rischio che devono essere oggetto di verifica ed è quindi indipendente dalle Aree, Funzioni e Staff cui fa capo detta responsabilità.

Qualunque problema che possa interferire nelle attività di vigilanza viene comunicato al Presidente ed al Direttore al fine di risolverlo.

L'Organismo di Vigilanza non ha l'autorità o la responsabilità di cambiare politiche e procedure aziendali, ma di valutarne l'adeguatezza per il raggiungimento degli obiettivi indicati nel D. Lgs 231/2001. E' responsabilità dell'Organismo di Vigilanza proporre gli aggiornamenti al modello ritenuti necessari per prevenire comportamenti che possano determinare la commissione dei reati, fornendo a tal fine al management raccomandazioni e suggerimenti per rafforzarlo laddove questo risulti essere inadeguato.

L'Organismo di Vigilanza ha comunque l'autorità e la responsabilità di raccomandare al management gli aggiornamenti del modello e di essere informato prima che una procedura riguardante un'attività ritenuta a rischio venga definita.

All'Organismo di Vigilanza sono attribuite:

- la facoltà, con autonomi poteri di rappresentanza, di stipulare, modificare e/o risolvere incarichi professionali a soggetti terzi in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico.
- la disponibilità delle risorse umane e finanziarie per lo svolgimento delle attività di competenza dell'Organismo di Vigilanza.

4.3. POTERI DI ACCESSO

Nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni aziendali per le attività di indagine, analisi e controllo.

L'Organismo di Vigilanza ha l'autorità di accedere a tutti gli atti aziendali, riservati e non, pertinenti con l'attività di controllo, ed in particolare:

- a)** documentazione societaria;
- b)** documentazione relativa a contratti attivi e passivi;
- c)** informazioni o dati relativi al personale aziendale e più in generale qualunque tipo di informazione o dati aziendali anche se classificati "confidenziale", fermo rimanendo il rispetto della normativa di legge in materia di "privacy";
- d)** dati e transazioni in bilancio;
- e)** procedure aziendali;
- f)** piani strategici, budget, previsioni e più in generale piani economico-finanziari a breve, medio, lungo termine.

Nel caso di controlli inerenti la sfera dei dati personali e/o sensibili, l'Organismo di Vigilanza individua le migliori modalità per la salvaguardia della riservatezza degli stessi.

Per conseguire le proprie finalità l'Organismo di Vigilanza può coordinare la propria attività con quella svolta dal collegio sindacale ed accedere ai risultati da questi ottenuti, utilizzando la relativa documentazione.

L'Organismo di Vigilanza ha l'autorità di accedere fisicamente alle aree che sono oggetto di verifica, intervistando quindi direttamente il personale aziendale e, ove necessario, conducendo accertamenti dell'esistenza di determinate informazioni o del patrimonio aziendale.

4.4. RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI

Ogni informazione, segnalazione, rapporto previsti nel Modello 231 è conservato dall'Organismo di Vigilanza in un apposito archivio cartaceo e/o informatico.

Fatti salvi gli ordini legittimi delle Autorità, i dati e le informazioni conservate nell'archivio sono posti a disposizione di soggetti esterni all'Organismo di Vigilanza solo previa autorizzazione dell'Organismo stesso e del responsabile della funzione aziendale cui le informazioni si riferiscono.

4.5. REGOLAMENTO DI FUNZIONAMENTO

L'Organismo di Vigilanza disciplina il proprio funzionamento mediante apposito regolamento.

Il regolamento include:

- compiti del Presidente;
- convocazione delle sedute;
- decisioni;
- segreteria e verbali;
- audizioni e comitati tecnici;
- contenuto dei rapporti al Consiglio di Amministrazione;
- contenuto degli altri rapporti da/verso l'Organismo di Vigilanza;
- risorse finanziarie;
- modalità organizzative di gestione dei supporti documentali;
- modalità di contatto con l'Organismo di Vigilanza.

5. FLUSSI INFORMATIVI

5.1. FLUSSI INFORMATIVI DALL'ORGANISMO DI VIGILANZA VERSO I VERTICI SOCIETARI

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello 231, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati.

L'Organismo di Vigilanza riporta al Consiglio di Amministrazione le attività svolte secondo le tempistiche specificamente previste nel modello di organizzazione, gestione e controllo e nel suo regolamento di funzionamento.

Sono previste le linee di riporto seguenti:

- a) **continuativa**, nei confronti del Presidente del Consiglio di Amministrazione, il quale informa il Consiglio stesso nell'ambito dell'informativa sull'esercizio delle deleghe conferite;
- b) **semestrale**, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale; a tale proposito viene predisposto uno specifico rapporto semestrale relativo all'attività svolta con segnalazione dell'esito delle verifiche e delle innovazioni legislative in materia di responsabilità amministrativa degli enti;
- c) **immediata**, nei confronti del Presidente del Consiglio di Amministrazione, ove risultino accertati fatti di particolare materialità o significatività.

In particolare l'Organismo di Vigilanza è tenuto a comunicare periodicamente al Consiglio di Amministrazione le seguenti informazioni:

- Rendicontazione delle attività svolte nel corso del periodo e dei risultati conseguiti, con la segnalazione di eventuali problematiche emerse;
- Necessità di modifiche al modello che si rendono necessarie per cambiamenti organizzativi, per modifiche nelle modalità operative gestionali, per modifiche nel sistema delle deleghe o per adeguamenti normativi.

5.2. FLUSSI INFORMATIVI DALLE AREE AZIENDALI VERSO L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza deve essere informato da parte dei soggetti tenuti all'osservanza del Modello 231 in merito a eventi che potrebbero ingenerare responsabilità di ESTRACOM S.p.A. ai sensi del D. Lgs. n. 231 del 2001.

Al riguardo:

- Ciascuna figura apicale comunica all'Organismo di Vigilanza una

informativa semestrale sullo stato di attuazione del Modello 231 nelle attività e strutture della Funzione e con la segnalazione delle situazioni maggiormente significative emerse nel periodo con riferimento alle problematiche inerenti il D. Lgs. 231/2001 (es. gare con la PA di importo elevato)

- almeno una volta l'anno la funzione preposta alla gestione dei dati finanziari mette a disposizione dell'Organismo di Vigilanza il verbale del soggetto deputato al controllo contabile (ex art. 2409-bis/ter c.c.) in cui è stato effettuato il controllo sulla procedura di gestione dei flussi finanziari
- ciascuna figura apicale aziendale segnala tempestivamente all'Organismo di Vigilanza cambiamenti nella struttura, nelle modalità operative di gestione, nel sistema di deleghe e negli altri aspetti che possono richiedere modifiche al modello di organizzazione, gestione e controllo
- ciascun figura apicale aziendale predisponde report periodici semestrali relativi alle attività di controllo poste in essere nell'ambito della funzione per il monitoraggio della gestione ("controllo in linea")
- ciascun responsabile o dipendente deve segnalare comportamenti non in linea con i principi e i contenuti del Modello 231, contattando l'Organismo di Vigilanza.

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 della società o delle persone accusate erroneamente o in mala fede.

5.3. ALTRI FLUSSI INFORMATIVI

a) Flussi dall'Organismo di Vigilanza alle risorse deputate ai controlli

L'Organismo di Vigilanza, al termine di ogni riunione periodica dello stesso, comunica in forma scritta alle risorse deputate ad effettuare i controlli operativi le attività di controllo da svolgere nel successivo periodo.

b) Flussi dalle risorse deputate ai controlli all'Organismo di Vigilanza

Le eventuali risorse aziendali o esterne, individuate dall'organismo di Vigilanza per effettuare i controlli operativi, riportano all'Organismo di Vigilanza trimestralmente, e comunque prima di ogni rapporto dell'Organismo di Vigilanza al Consiglio di Amministrazione, le seguenti informazioni:

- Report periodici relativi all'attività svolta con riferimento alle specifiche richieste di controllo formulate in precedenza dall'Organismo di Vigilanza

- Segnalazione delle problematiche riscontrate
- Segnalazione delle esigenze di modifica del modello di organizzazione, gestione e controllo

c) Flussi dall'Organismo di Vigilanza alle funzioni aziendali ed ai dipendenti

All'adozione del modello organizzativo ex D. Lgs.231/2001 l'Organismo di Vigilanza si attiva affinché venga diffuso a livello aziendale:

- un documento informativo relativo alle prescrizioni della normativa vigente in tema di responsabilità amministrativa aziendale ex D. Lgs. 231/2001
- il modello di organizzazione, gestione e controllo
- il codice etico
- il sistema disciplinare

Le singole funzioni aziendali dovranno tempestivamente distribuire ad ogni dipendente aziendale la documentazione ricevuta dall'Organismo di Vigilanza.

Successivamente, ogni modifica della documentazione di cui al punto precedente dovrà essere diffusa a livello aziendale secondo le medesime modalità.

d) Flussi dal Responsabile per la Sicurezza alle funzioni aziendali

Permane in capo al Responsabile per la Sicurezza aziendale l'obbligo di fornire indicazioni sui nuovi adempimenti normativi inerenti la tutela della sicurezza e dell'igiene sul lavoro.

e) Flussi dalle singole funzioni aziendali al Responsabile per la Sicurezza

Le funzioni aziendali che intendano proporre modifiche ai loro processi organizzativi-produttivi, che potrebbero avere impatto sulla tutela della salute, sull'igiene e sulla sicurezza dei lavoratori, sono tenute a richiedere l'autorizzazione preventiva delle innovazioni proposte al responsabile per la Sicurezza aziendale. Quest'ultimo valuterà se dare o meno l'autorizzazione per la modifica dei processi ed, eventualmente, aggiornare il piano di valutazione dei rischi.

6. SISTEMA DISCIPLINARE

6.1. FUNZIONI DEL SISTEMA DISCIPLINARE

Il sistema disciplinare, vale a dire l'insieme delle sanzioni previste per la violazione delle norme del Modello Organizzativo e del Codice Etico, costituisce uno strumento indispensabile per garantire l'effettività e l'attuazione del Modello Organizzativo stesso.

L'articolo 6, comma 2, lett. E) del decreto 231 del 2001 prevede espressamente la necessità di creare un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo.

Le sanzioni disciplinari si applicano a prescindere dall'esito del procedimento penale eventualmente instaurato per il fatto che costituisce anche violazione delle misure del Modello Organizzativo e del Codice Etico.

La sanzione disciplinare deve essere proporzionata all'addebito tenendo a tal fine conto sia delle circostanze oggettive che delle modalità soggettive della condotta del responsabile. Si ha altresì riguardo, nell'irrogare la sanzione, all'entità del pregiudizio arrecato all'azienda.

6.2. SANZIONI A CARICO DEI DIPENDENTI

I comportamenti tenuti dai lavoratori dipendenti in violazione delle regole comportamentali contenute nel presente Modello Organizzativo e nel Codice Etico, nonché la violazione dei doveri relativi alla prevenzione degli infortuni e delle malattie sul luogo di lavoro, sono definiti come illeciti disciplinari.

Le sanzioni irrogabili nei riguardi di detti lavoratori dipendenti rientrano tra quelle previste dal vigente CCNL, nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili.

In relazione a quanto sopra, il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui al vigente CCNL.

Tali categorie descrivono i comportamenti sanzionati a seconda del rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti stessi, a seconda della loro gravità.

In particolare, si prevede che:

- a) incorre nei provvedimenti di rimprovero verbale o scritto il lavoratore che violi le procedure interne previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una "lieve trasgressione dei regolamenti aziendali" (cfr. art. 21 punto 1) del CCNL vigente;
- b) incorre nel provvedimento della multa il lavoratore che violi più volte le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento più volte non conforme alle prescrizioni del Modello stesso, prima ancora che dette mancanze siano state singolarmente accertate e contestate, dovendosi ravvisare in tali comportamenti la ripetuta effettuazione della mancanza della "lieve trasgressione dei regolamenti aziendali" prima ancora che la stessa sia stata singolarmente accertata e contestata, ai sensi di quanto previsto all'art. 21 punto 2) del CCNL vigente;
- c) incorre nel provvedimento della sospensione dal servizio e dalla retribuzione da 1 a 10 giorni il lavoratore che, nel violare le procedure interne previste dal presente Modello o adottando, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, nonché compiendo atti contrari all'interesse di ESTRACOM S.p.A., arrechi danno alla Società o la esponga a una situazione oggettiva di pericolo alla integrità dei beni dell'azienda, dovendosi ravvisare in tali comportamenti la determinazione di un danno o di una situazione di pericolo per l'integrità dei beni dell'Azienda o il compimento di atti contrari ai suoi interessi derivanti da una "grave trasgressione dei regolamenti aziendali", ai sensi di quanto previsto all'art. 21 punti 4) e 5) del CCNL vigente.
- d) incorre nel provvedimento del licenziamento senza preavviso il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento il compimento di "azioni che costituiscono delitto a termine di legge" ai sensi di quanto previsto all'art. 21 punto 7) del CCNL vigente.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, saranno applicate, ai sensi di quanto previsto dal codice disciplinare vigente in ESTRACOM in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;

- al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- alle mansioni del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, alla Direzione aziendale.

Il datore di lavoro non potrà adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

Salvo che per il richiamo verbale, la contestazione dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere comminati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

Se il provvedimento non verrà comminato entro i 6 giorni successivi a tali giustificazioni, queste si riterranno accolte.

Il lavoratore potrà presentare le proprie giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'Associazione sindacale cui aderisce, ovvero, di un componente la Rappresentanza sindacale unitaria.

La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto. I provvedimenti disciplinari di cui sopra alle lettere b), c) e d) potranno essere impugnati dal lavoratore in sede sindacale, secondo le norme contrattuali relative alle vertenze.

Il licenziamento per mancanze di cui ai punti A) e B) dell'art. 25 potrà essere impugnato secondo le procedure previste dall'art. 7 della legge n. 604 del 15 luglio 1966 confermate dall'art. 18 della legge n. 300 del 20 maggio 1970.

Non si terrà conto a nessun effetto dei provvedimenti disciplinari decorsi due anni dalla loro comminazione.

Il licenziamento, con o senza preavviso, potrà essere irrogato allorché la violazione delle misure del Modello Organizzativo o del Codice Etico abbia anche determinato una mancanza prevista dai vigenti Contratti Collettivi di Lavoro.

Agli effetti della salute e della sicurezza sul lavoro, l'art. 20 del D. Lgs. 81/2008 – Obblighi dei lavoratori – dispone che:

1. *Ciascun lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione ed alle istruzioni e ai mezzi forniti dal datore di lavoro*
2. *I lavoratori devono in particolare:*
 - a) *Contribuire, insieme al datore di lavoro, ai dirigenti ed ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;*
 - b) *osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;*
 - c) *utilizzano correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;*
 - d) *utilizzano in modo appropriato i dispositivi di protezione messi a loro disposizione;*
 - e) *segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;*
 - f) *non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;*
 - g) *non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;*
 - h) *partecipare ai programmi di formazione ed addestramento organizzati dal datore di lavoro;*
 - i) *si sottoporre ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.*
3. *I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in caso ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto.*

6.3. SANZIONI A CARICO DEI DIRIGENTI

La violazione delle misure previste dal Modello Organizzativo e dal Codice Etico possono costituire, in proporzione alla gravità del fatto e all'entità del danno cagionato alla Società, causa di applicazione di provvedimento disciplinare previsto dalle leggi e dai contratti vigenti, nonché di licenziamento per giusta causa allorché venga meno il rapporto fiduciario.

Per quanto attiene alla responsabilità verso terzi derivante da violazione delle misure previste dal Modello Organizzativo e dal Codice Etico, resta salva la responsabilità della Società secondo quanto previsto dalle leggi e dai contratti collettivi vigenti.

6.4. SANZIONI A CARICO DEGLI AMMINISTRATORI E DEI SINDACI

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, oppure da parte di uno o più membri del Collegio Sindacale, l'Organismo di Vigilanza informa il Collegio Sindacale e l'intero Consiglio di Amministrazione i quali prendono gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea al fine di adottare le misure più idonee previste dalla legge.

6.5. MISURE A CARICO DEI TERZI (CONSULENTI E PARTNERS)

La violazione da parte dei Terzi (Consulenti o Partners esterni, non legati da vincolo di subordinazione con l'Impresa, ma sottoposti per il singolo incarico a controllo e vigilanza da parte dell'Impresa) delle regole di cui al presente Modello costituisce inadempimento degli obblighi contrattuali che può comportare, nei casi più gravi, alla risoluzione del contratto.

A tal proposito nei singoli contratti stipulati di volta in volta con i Terzi dovranno essere istituite clausole ad hoc per disciplinare le conseguenze derivanti dalla violazione del Modello Organizzativo e del Codice Etico.

In ogni caso resta salvo il diritto al risarcimento dei danni cagionati alla Società conseguenza della violazione delle misure previste dal Modello Organizzativo e dal Codice Etico.

6.6. PUBBLICAZIONE DEL SISTEMA DISCIPLINARE

Il sistema disciplinare previsto dal Modello Organizzativo deve essere opportunamente pubblicizzato, in modo tale da renderlo conoscibile a chiunque vi sia sottoposto.

Per i lavoratori dipendenti dovranno essere rispettate le modalità di pubblicazione previste dalle leggi e dai contratti collettivi di lavoro vigenti, mediante affissione in luoghi accessibili liberamente ai lavoratori.

Per gli altri soggetti saranno individuate, a cura del Consiglio di Amministrazione o dell'Organismo di Vigilanza, specifiche modalità di comunicazione ritenute più adatte alle concrete peculiarità del caso concreto.

7. APPLICAZIONE, DIFFUSIONE E AGGIORNAMENTO DEL MODELLO

7.1. PARTI SPECIALI

Per l'applicazione del Modello 231 di ESTRACOM S.p.A. vengono individuate quattro parti speciali nell'ambito delle quali sono riportate: le fattispecie di reato, le attività aziendali a rischio, i principi aziendali di comportamento.

Le parti speciali riguardano i reati:

- a) nei rapporti con la Pubblica Amministrazione
- b) societari
- c) in materia di sicurezza del lavoro
- d) in materia di riciclaggio e ricettazione

Tenuto conto dell'attuale mappatura dei rischi, al momento non si rende necessario attivare parti speciali inerenti i reati contro la fede pubblica, contro la personalità dello stato, contro la personalità individuale, per gli abusi di mercato, di frode informatica.

7.2. COMUNICAZIONE E FORMAZIONE

La comunicazione e la formazione del personale sono importanti requisiti dell'attuazione del Modello 231. ESTRACOM S.p.A. si impegna a facilitare e promuovere la conoscenza del Modello 231 da parte del management e dei dipendenti, con grado di approfondimento diversificato secondo posizione e ruolo, in un'ottica di personalizzazione dei percorsi e di reale rispondenza ai bisogni delle singole risorse.

Il Modello 231 è comunicato formalmente dall'Organismo di Vigilanza a ciascun componente degli organi sociali ed a ciascun dirigente. Ciascun componente sottoscrive una dichiarazione di conoscenza e adesione ai principi e ai contenuti del Modello 231. La dichiarazione viene archiviata e conservata dall'Organismo di Vigilanza.

I principi e i contenuti del D. Lgs. n. 231 del 2001 e del Modello 231 sono, inoltre, divulgati mediante corsi di formazione. La partecipazione ai corsi è obbligatoria. La struttura dei corsi di formazione è approvata dall'Organismo di Vigilanza su proposta delle funzioni aziendali competenti. Gli interventi formativi vengono periodicamente rinnovati in occasione di nuove assunzioni.

Il Modello 231 è comunicato e reso disponibile a ciascun dipendente attraverso:

- affissione nelle bacheche aziendali;
- invio di una lettera a tutto il personale da distribuirsi attraverso la busta paga, riportante i principali contenuti del decreto e le modalità per prenderne visione dei contenuti e per riceverne copia su richiesta;
- la pubblicazione sulla intranet aziendale.

Il Modello 231 è reso disponibile a tutti gli utenti sul sito internet di ESTRACOM S.p.A.

I principi e i contenuti del Modello 231 sono portati a conoscenza di tutti coloro con i quali ESTRACOM S.p.A. intrattiene relazioni contrattuali. L'impegno all'osservanza della legge e dei principi di riferimento del Modello 231 da parte dei terzi aventi rapporti contrattuali con ESTRACOM S.p.A. è previsto da apposita clausola del relativo contratto ed è oggetto di accettazione da parte del terzo contraente.

7.3. AGGIORNAMENTO DEL MODELLO

La revisione ed aggiornamento del Modello 231 è funzionale al mantenimento nel tempo dell'efficacia del modello e si rende necessaria in occasione:

- a) di novità legislative con riferimento alla disciplina della responsabilità degli enti per gli illeciti amministrativi dipendenti da reato
- b) di cambiamenti significativi della struttura organizzativa o dei settori di attività della Società
- c) di significative violazioni del Modello 231 che evidenzino l'inefficacia del modello
- d) di verifiche o controlli che evidenzino la necessità di adeguamenti.

La necessità di revisione ed aggiornamento del Modello 231 viene segnalata in forma scritta dall'Organismo di Vigilanza al Consiglio di Amministrazione e sarà compito di quest'ultimo avviare la procedura di revisione ed aggiornamento.