"IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO D.LGS. 231/2001"

ApiServizi Varese S.r.l.

PARTE SPECIALE

PARTE SPECIALE A	**Reati contro la pubblica amministrazione**
PARTE SPECIALE B	**Reati contro la criminalità informatica**
PARTE SPECIALE C	**Reati Societari**
PARTE SPECIALE D	**Reati di violazione del diritto d'autore**
PARTE SPECIALE E	**Reati colposi in materia di tutela della sicurezza e della salute nei luoghi di lavoro**

Documento: *Modello di Organizzazione, Gestione e Controllo*
File: *Modello organizzativo_APISRV_VARESE parte Speciale.doc*
Approvazione: *Consiglio di Amministrazione* **Verbale riunione del:** *30-3-2011*

Sommario

INTRODUZIONE: I DESTINATARI DELLA PARTE SPECIALE PRINCIPI DI COMPORTAMENTO E ATTUAZIONE

Questa Parte Speciale definisce i comportamenti a cui i Destinatari come già definiti nella Parte Generale si atterranno nello svolgimento delle attività rientranti nelle c.d. Aree Sensibili o a Rischio e in considerazione delle diverse posizione e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente così come prescritto in questa Parte Speciale al fine di prevenire e impedire il verificarsi di reati.

Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nel codice etico e nelle procedure operative interne.

Si precisa inoltre che destinatari del presente Allegato sono anche i membri delle Associazione Temporanee di Scopo di cui l'Ente è membro o ne diventerà membro.

In particolare, la presente Parte Speciale ha la funzione di:

a) fornire un elenco dei principi generali e dei principi procedurali specifici cui i Destinatari, in relazione al tipo di rapporto in essere con l'Ente, sono tenuti ad attenersi per una corretta applicazione del Modello;

b) fornire al O.d.V. e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

PARTE SPECIALE - A

I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE
(artt. 24, 25 e 25-novies del D.Lgs. 231/2001)

A.1 ELENCO REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

A.1.1 Definizione di Pubblica Amministrazione e di incaricati di Pubblico Servizio

La nozione di Pubblica Amministrazione considerata ai fini della individuazione delle aree a rischio è stata quella dedotta dagli artt. 357 e 358 c.p., in base ai quali sono pubblici ufficiali e incaricati di pubblico servizio 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 certificativi o autorizzativi.
ai sensi dell'art. 357, comma 1 del Codice Penale, è considerato pubblico ufficiale colui il quale esercita una pubblica funzione legislativa, giudiziaria o amministrativa (disciplinata da norme di diritto pubblico);
ai sensi dell'art. 358 del Codice Penale, "sono incaricati di un pubblico servizio (disciplinato da norme di diritto pubblico ma senza i poteri di natura certificativa autorizzativa e deliberativa propri della pubblica funzione) coloro i quali, a qualunque titolo, prestano un pubblico servizio.
Per giurisprudenza consolidata ai fini della individuazione di pubblico ufficiale o incaricato di pubblico servizio occorre verificare se la relativa attività sia disciplinata da norme di diritto pubblico e sia volta in concreto al perseguimento di interessi collettivi.
La figura di pubblico ufficiale o incaricato di pubblico servizio può attribuirsi anche ad Enti che anche se regolati da norme di diritto privato, svolgano di fatto o prestino servizi nell'interesse della collettività con funzione pubblicistica o comunque nel soddisfacimento di bisogni di interesse generale, quali: Poste Italiane S.p.A., RAI – Radiotelevisione Italiana, Ferrovie dello Stato, Enel S.p.A., Eni S.p.A., Telecom Italia S.p.A., Hera S.p.A., etc., andrà prestata quindi massima attenzione nel rapportarsi a questi enti ed in particolare con i loro dipendenti, collaboratori, dirigenti ed amministratori.
Per quanto concerne la presente parte Speciale –A si elencano di seguito la descrizione dei reati come segue:

A.1.2 art. 24. indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico.

Rientrano tra questi reati:
art. 316 bis c.p. malversazione a danno dello stato
art. 316 ter c.p. indebita percezione di erogazioni a danno dello stato
art. 640 com. 2°, n.1 c.p. truffa a danno dello stato o di altro ente pubblico
art. 640-bis c.p. truffa a danno dello stato o di altro ente pubblico
art. 640-ter c.p. frode informatica in danno dello stato o di altro ente pubblico
Rischio reato: l'ente risulta esposto ad alcune di queste tipologie di reati e si è tutelato dal loro compimento come indicato nella presente parte speciale del Modello Organizzativo.

Articolo 316-*bis* codice penale (Malversazione a danno dello Stato)
Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire

iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.
Commento-
Il delitto consiste nell'effettuare un mutamento di destinazione di contributi, sovvenzioni o finanziamenti ottenuti dallo Stato, da altri enti pubblici o dalle Comunità europee, per il fine di impiegarli nella realizzazione di opere o nello svolgimento di attività di pubblico interesse.
Il delitto si consuma anche se solo una parte dei fondi viene distratta ed anche nel caso in cui la parte correttamente impiegata abbia esaurito l'opera o l'iniziativa cui l'intera somma era destinata.
La condotta criminosa prescinde dal modo in cui sono stati ottenuti i fondi e si realizza solo in un momento successivo all'ottenimento dei fondi stessi.
Esemplificazioni di condotte illecite
Utilizzo di finanziamenti o erogazioni pubbliche per la formazione del personale a scopi diversi rispetto a quelli per i quali erano destinati.

Articolo 316-*ter* codice penale (Indebita percezione di erogazioni a danno dello Stato)
Salvo che il fatto costituisca il reato previsto dall'articolo 640-*bis*, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni.
Quando la somma indebitamente percepita è pari o inferiore a e 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da e 5.164,00 a e 25.822,00. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Fattispecie
La fattispecie di delitto si realizza qualora la società - tramite chiunque (anche un soggetto esterno alla società stessa) - consegua per sé o per altri erogazioni dallo Stato, da altri enti pubblici o dalle Comunità europee, mediante una condotta consistente in qualsiasi tipo di utilizzo (ad es. presentazione) di dichiarazioni (scritte o orali), o di altra documentazione materialmente e/o ideologicamente falsa ovvero attraverso l'omissione di informazioni dovute.
La fattispecie si consuma con l'avvenuto ottenimento delle erogazioni (che costituisce l'evento tipico del reato).
Il reato qui in esame (art. 316-ter c.p.) si configura come ipotesi speciale anche nei confronti dell'art. 640, comma 2, n. 1, c.p. (truffa aggravata in danno dello Stato), rispetto al quale l'elemento "specializzante" è dato non più dal tipo di artificio o raggiro impiegato, bensì dal tipo di profitto conseguito ai danni dell'ente pubblico ingannato. Profitto che nella fattispecie più generale, testé richiamata, non consiste nell'ottenimento di una erogazione ma in un generico vantaggio di qualsiasi altra natura.

Esemplificazioni di condotte illecite
Produzione di documentazione non veritiera per l'ottenimento di finanziamenti erogati da un ente pubblico (es. INAIL).

Articolo 640 codice penale (Truffa)
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da e 51,00 a e 1.032,00.
La pena è della reclusione da uno a cinque anni e della multa da e 309,00 a e 1.549,00:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;
2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità.
2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

Fattispecie
La norma fa riferimento alla generica ipotesi di truffa (art. 640 c.p.), aggravata dal fatto che il danno economico derivante dall'attività ingannatoria del reo ricade sullo Stato o su altro ente pubblico.
La condotta consiste, sostanzialmente, in qualsiasi tipo di menzogna (compreso l'indebito silenzio su circostanze che sono rese note) tramite la quale si ottiene che taluno cada in errore su qualcosa e compia, di conseguenza, un atto di disposizione che non avrebbe compiuto se avesse conosciuto la verità.
Per la consumazione del reato occorre che sussista, oltre a tale condotta, il conseguente profitto di qualcuno (chiunque esso sia, anche diverso dall'ingannatore) e il danno dello Stato o dell'ente pubblico.

Esemplificazioni di condotte illecite
Indebito conseguimento di rimborsi, conguagli o altre elargizioni previdenziali da parte dell'INPS.

Articolo 640-*bis* codice penale (Truffa aggravata per il conseguimento di erogazioni pubbliche)
La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda 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.

Fattispecie
La fattispecie si realizza se il fatto previsto dall'art. 640 c.p. (ossia la truffa) riguarda 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.

Esemplificazioni di condotte illecite
Questa ipotesi è applicabile solo quando la fraudolenta captazione di una pubblica sovvenzione sia riferibile a un'opera o a un'attività di interesse pubblico altrimenti si incorre nell'art. 640, co. 2 n.1.
Si ricordi inoltre che quando le somme siano erogate in più rate si entra in ipotesi di reato a consumazione prolungata, che inizia con la percezione della prima rata e si conclude con la ricezione dell'ultima. Es. La realizzazione di un corso di formazione non effettuato.

Articolo 640-*ter* codice penale (Frode informatica)
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 ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da e 51,00 a e 1.032,00. La pena è della reclusione da uno a cinque anni e della multa da e 309,00 a e 1.549,00 se ricorre una delle circostanze previste dal numero 1) del secondo comma

dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Fattispecie
Questa fattispecie delittuosa si realizza quando un soggetto, 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.
Il reato presenta elementi costitutivi pressoché identici a quelli della truffa, salvo il fatto che l'attività fraudolenta non investe una persona, ma un sistema informatico attraverso la sua manipolazione.
Il reato colpisce gli interventi che consistono nell'adibire l'apparato informatico a scopi diversi da quelli per cui era stato destinato o nel manipolarne arbitrariamente i contenuti.
Il dolo consiste nella volontà di alterare il funzionamento dei sistemi o di intervenire su dati, programmi, informazioni, con la previsione del profitto ingiusto e dell'altrui danno, senza che sia necessaria alcuna volontà di indurre altri in errore o di ingannare.
Poiché sia integrata la circostanza aggravante dell'abuso della qualità di operatore del sistema, non rileva un'astratta qualifica del soggetto attivo, ma la legittimazione per motivi di prestazione d'opera.
Il reato si consuma con la realizzazione dell'ingiusto profitto in danno dello Stato o di altro ente pubblico.
Costituisce fattispecie del reato, quale esempio, la frode realizzata attraverso collegamenti telematici o trasmissione di dati su supporti informatici a pubbliche Amministrazioni o ad enti pubblici o ad Autorità di vigilanza.

Esemplificazioni di condotte illecite
Questa condotta consiste o nella alterazione del funzionamento di un sistema informatico o telematico o in ipotesi di un interventi non autorizzato su dati, informazioni, programmi e questo porti al conseguimento di un profitto con un danno altrui, con l'ulteriore aggravante quando l'abuso è effetuato da un operatore di sistema preposto all'utilizzo del sistema informatico o telematico.

A.1.3 art. 25 concussione e corruzione

Rientrano tra questi reati:
art. 317 c.p. concussione
art. 318 c.p. corruzione per un atto d'ufficio
art. 319 c.p. corruzione per un atto contrario ai doveri d'ufficio
art. 319 bis c.p. circostanze aggravanti
art. 319 ter c.p. corruzione in atti giudiziari
art. 320 c.p. corruzione di persona incaricata di un pubblico servizio
art. 321 c.p. pene per il corruttore
art. 322 commi 2° e 4° c.p. istigazione alla corruzione
art. 322 bis c.p. peculato, concussione corruzione e istigazione alla corruzione di membri degli organi delle comunità europee e di funzionari delle comunità europee e di stati esteri
Rischio reato: l'ente risulta esposto ad alcune di queste tipologie di reati e si è tutelato dal loro compimento come indicato nella presente parte speciale del Modello Organizzativo.

317 c.p. Concussione

Il 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, è punito con la reclusione da quattro a dodici anni.

318 c.p. Corruzione per un atto d'ufficio

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni. Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino ad un anno.

319 c.p. Corruzione per un atto contrario ai doveri d'ufficio

Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per se o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da due a cinque anni.

319 bis c.p. Circostanze aggravanti

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi.

Fattispecie

La fattispecie prevista dall'art. 318 c.p. (corruzione per un atto d'ufficio) si realizza quando il pubblico ufficiale per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. La nozione di pubblico ufficiale è quella definita dall'art. 357 c.p. Qui, come è chiaro, si tratta di atti che non contrastano con i doveri d'ufficio. Il reato può essere integrato anche quando il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto.

La fattispecie prevista dall'art. 319 c.p. si realizza, invece, quando il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

Si ha circostanza aggravante se il fatto di cui all'art. 319 c.p. ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene (art. 319-bis c.p.).

L'attività delittuosa del funzionario pubblico può, dunque, estrinsecarsi sia in un atto conforme ai doveri d'ufficio (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia, e soprattutto, in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Esemplificazioni di condotte illecite

Selezione di dipendenti con finalità corruttive.

Creazione di fondi neri da utilizzare a scopo corruttivo mediante l'acquisto di consulenze fittizie.

319 ter c.p. Corruzione in atti giudiziari

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da tre a otto anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni.

Fattispecie
Tale fattispecie si realizza se i fatti indicati negli articoli 318 e 319 c.p. siano commessi dal pubblico ufficiale per favorire o danneggiare una parte in un processo civile, penale o amministrativo. La norma si applica, senza distinzione, a tutti i pubblici ufficiali e non soltanto ai magistrati (un magistrato, un cancelliere un funzionario).

Esemplificazioni di condotte illecite
Versamento di denaro ad un cancelliere del Tribunale affinché accetti delle memorie o altre produzioni documentali fuori termine, consentendo quindi di superare i limiti temporali previsti dai codici di procedura.
Pagamento di una parcella maggiorata o alterazione dell'incarico dei legali in contatto con Organi giudiziari affinché condizionino favorevolmente l'esito di un processo a carico dell'Ente.

Art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
Le disposizioni dell'art. 319 si applicano anche all'incaricato di un pubblico servizio; quelle di cui all'articolo 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato.
In ogni caso, le pene sono ridotte in misura non superiore ad un terzo.

Fattispecie
Le disposizioni dell'articolo 319 c.p. si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio; quelle di cui all'articolo 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, quale definito dall'art. 358 c.p., ma solo qualora rivesta la qualità di pubblico impiegato.

Art. 321 c.p. Pene per il corruttore
Le pene stabilite nel primo comma dell'art. 318, nell'articolo 319, nell'articolo 319-bis, nell'articolo 319-ter e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al Pubblico Ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

Fattispecie
Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'articolo 319-ter e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche, per disposizione della norma qui in esame, a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.
In altri termini, colui che corrompe commette una autonoma fattispecie di reato rispetto a quella compiuta dal pubblico ufficiale (o dall'incaricato di pubblico servizio) che si è lasciato corrompere nei modi e ponendo in essere le condotte contemplate negli articoli sopra richiamati.

Art. 322 commi 2° e 4° c.p. istigazione alla corruzione
Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena

stabilita nell'art. 319, ridotta di un terzo". La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate nell'art. 319

322 bis c.p. Peculato, concussione corruzione e istigazione alla corruzione di membri degli organi delle comunità europee e di funzionari delle comunità europee e di stati esteri
Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche: 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee; 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee; 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle di funzionari o agenti delle Comunità europee; 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee; 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio. Le disposizioni degli articoli 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso: 1) alle persone indicate nel primo comma del presente articolo; 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali. le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

Fattispecie
Questa fattispecie delittuosa si configura allorché il privato tiene il comportamento incriminato dal sopra illustrato art. 321 c.p. (e cioè svolge attività corruttiva), ma il pubblico ufficiale (o l'incaricato di pubblico servizio) rifiuta l'offerta illecitamente avanzatagli.

A.1.4 art. 25-novies induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Rientrano tra questi reati:
art. 377-bis c.p. induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
Salvo che il fatto non costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.
Rischio reato: l'ente risulta esposto a questa tipologia di reati e si è tutelato dal loro compimento come indicato nella parte speciale allegata al presente Modello Organizzativo.

Fattispecie
Tale fattispecie si realizza con violenza o minaccia o promessa di denaro od altra utilità per il fine tratteggiato dalla disposizione.

Esemplificazioni di condotte illecite

Minaccia a un dipendente dell'Ente per non rendere dichiarazioni all'autorità giudiziaria su un procedimento in corso in cui l'Ente è parte.

A.2 LE AREE A RISCHIO

I reati sopra descritti trovano come presupposto l'instaurazione di rapporti con la P.A., in relazione alle condotte criminose sopra evidenziate, le aree di attività dell'Ente nel cui si possa nel concreto avere il rischio di commissione dei reati previsti sono:

- ✓ per il Servizio Formazione accreditata presso Regione Lombardia o di altri enti pubblici
- ✓ per il Servizio Formazione in ATS
- ✓ per il Servizio Finanza agevolata su progetti con Contributi Pubblici (diversi dall'area formazione)
- ✓ per il Servizio Ambiente e Sicurezza
- ✓ per il Servizio Innovazione Energia
- ✓ per il Servizio Commercio Estero
- ✓ per il Servizio Progetti Europei

I servizi si devono intendere rivolti anche a terzi, in particolare per l'area Formazione si evidenziano

1)Processo di accreditamento dell'ente presso la Pubblica Amministrazione:
- a)creazione della domanda di accreditamento;
- b)ispezione ed eventuali contestazioni;
- c)mantenimento dell'accreditamento.

2)Organizzazione attività formative finanziate dalla Pubblica Amministrazione:
- a)richiesta e gestione di finanziamenti, contributi o altre agevolazioni;
- b)creazione del progetto e della predisposizione della documentazione;
- c)firma e inoltro della domanda di partecipazione;
- d)rapporti con l'ente pubblico nella fase di attribuzione;
- e)fase di ricevimento dei fondi;
- f)rendicontazione anche via informatica;
- g)ispezione ed eventuali contestazioni.

3)Ottenimento di autorizzazioni, licenze, permessi da parte della Pubblica Amministrazione
- a)certificati di prevenzione incendi;
- b)verifica ASL adeguatezza immobile;
- c)altre autorizzazioni proprie dell'Ente verso la P.A.

Per gli Altri servizi sopraindicati

1)Generalmente
- a)richiesta e/o creazione di domande di finanziamento agevolato;
- b)richiesta e/o creazione di domande per contributi pubblici;
- c)richiesta e/o creazione di domande/dichiarazione con rilevanza pubblica in generale;
- d)firma ed inoltre delle domande di cui ai punti a), b) e c) di cui sopra;
- e)rapporto con gli enti pubblici delle domande di cui ai punti a), b) e c) di cui sopra;
- f)fase di ricevimento dei fondi delle domande di cui ai punti a), b) e c) di cui sopra;
- g)rendicontazione anche via informatica delle domande di cui ai punti a), b) e c)

di cui sopra.

Per i terzi in ipotesi di verifica o ispezione si possono evidenziare inoltre:

a)fase di accompagnamento all'ispezione;
b)messa a disposizione di dati e documenti;
c)fase di firma dei relativi verbali;
d)fase di esecuzione delle eventuali prescrizioni.

Per il Servizio Gestione del personale dipendente dell'Ente (compreso Paghe e Contributi), Amministrazione e gestione del personale, rapporti con enti previdenziali e assistenziali, nonché la sicurezza e l'igiene sul lavoro;

a) amministrazione e gestione degli aspetti retributivi e previdenziali connessi al personale e ai collaboratori con enti previdenziali ed assistenziali (INPS, INAIL, ecc.);
b) adempimenti connessi alla normativa della sicurezza nei luoghi di lavoro relativi rapporti con autorità preposte al controllo, anche in caso di ispezioni.

Per il Servizio Fiscale Tributario interno all'Ente
Amministrazione e gestione di documentazione fiscale, rapporti con uffici di accertamento quali agenzia Entrate, Guardia di Finanza, Agenzia delle Dogane;

a)amministrazione e gestione degli aspetti fiscali connessi all'Ente;
b)rapporti con autorità preposte al controllo, anche in caso di ispezioni.

Per il Servizio API – CAF
E quindi intrattenuti per conto di terzi in ambito previdenziale in ambito assistenza API – CAF;

a)richiesta e gestione di dichiarazioni fiscali per conto di terzi;
b)firma e inoltro di dichiarazioni di cui al punto a) sopra;
c)rapporti con Enti pubblici per quanto al punto a) sopra;
d) rapporti con autorità preposte al controllo, anche in caso di ispezioni per quanto al punto a) sopra;

In relazione alle verifiche ed ispezioni e in generale di Autorità Pubbliche di Vigilanza possono essere ricomprese una elevato numero di autorità ispettive, in ambito fiscale, amministrativo e previdenziale comprese anche la gestione contenziosi Giudiziari e Stragiudiziari, e Banca d'Italia, ASL, Guardia di Finanza, Garante Privacy, ecc.

Si ricorda inoltre che, possono presentare in via astratta profili di rischio (corruzione/truffa aggravata ai danni dello Stato/ostacolo all'esercizio delle Autorità Pubbliche di vigilanza) anche la predisposizione delle dichiarazioni funzionali alla liquidazione di tributi e, più in generale, l'invio e la ricezione di documenti alla/dalla Pubblica Amministrazione.

Inoltre in generale per qualsiasi tipo di Servizio o attività ricordiamo i reati che si possono commettere utilizzando la Gestione del Software della Pubblica Amministrazione

A.2.1 LE AREE A RISCHIO INDIRETTO:

Costituiscono Aree a rischio indiretto:
A)L'Area Acquisti;
B)L'Area Finanziaria;
C)Selezione del Personale (assunzione, valutazione e sviluppo);

D)Nomina di dirigenti o di membri di organi sociali (rappresentanza della società);
E)Incarichi di consulenza o prestazione professionale;
F)Area Omaggi e spese di Rappresentanza.
In dettaglio i rischi evidenziabili sono:

A) Area Acquisti

Il processo di gestione degli acquisti di beni e servizi (o di consulenze), con la relativa liquidazione delle fatture, costituisce una delle potenziali modalità attraverso la quale potrebbe essere commesso il reato di corruzione. Il reato di corruzione, infatti, potrebbe essere commesso attraverso una gestione poco trasparente della selezione dei fornitori o dei professionisti. Ad esempio, attraverso la creazione di fondi in seguito a servizi contrattualizzati a prezzi superiori a ai prezzi di mercato o, ancora, per mezzo dell'assegnazione di incarichi a persone o Società vicine o gradite ai soggetti pubblici, così da ottenere favori nell'ambito delle attività aziendali.
Per tali ragioni, l'emissione di ordini di ordini (così come il conferimento di consulenze) può anzitutto risultare strumentale alla corresponsione di indebite utilità a favore di pubblici ufficiali o incaricati di pubblico servizio: ad esempio, potrebbe darsi il caso dell'attribuzione di un fittizio contratto di consulenza (con riconoscimento del relativo compenso) a favore di un pubblico agente (o di suoi congiunti o Enti allo stesso riconducibili) al fine di compensare indebiti favori o per ottenere un indebito vantaggio.
In aggiunta, attraverso l'emissione di ordini di acquisto di beni fittizi (o con il conferimento di consulenze), la Società può costituire indebite provviste finanziarie da utilizzare per la corruzione di pubblici agenti; inoltre, tali procedimenti essere altresì utilizzati quale forma di retribuzione di prestazioni indebite erogate da pubblici funzionari (ad esempio, potrebbe darsi la stipulazione di un contratto di consulenza a favore di un familiare di un pubblico funzionario, quale corrispettivo dell'interessamento da parte del medesimo in una pratica relativa alla Società).

B) L'area Finanziaria

E' previsto che il Modello (art. 6,2 lett.c) del Decreto) debba evidenziare sistemi/procedure di gestione delle risorse finanziarie al fine di impedire la commissione dei reati, tutelando in particolare tutte quelle operazioni che assumono particolare rilievo per valore, modalità, rischiosità, atipicità: tra queste si possono indicare, a titolo di esempio, l'accessibilità a fondi "extra contabili" o la gestione della "liquidità", il cui utilizzo potrebbe portare alla commissione di reati di corruzione.

L'ente già utilizza delle procedure standardizzate per rilevare:
- l'intero iter dei flussi finanziari dal momento iniziale a quello finale;
- l'individuazione esatta del titolo giustificativo del flusso di pagamento attraverso la registrazione della forma e del contenuto del pagamento, identificando con particolare attenzione i soggetti incaricati, tenendo il più possibile separate le attività di chi esegue, chi controlla e chi autorizza.

C) Selezione del personale (assunzione, valutazione e sviluppo)

Il processo di selezione, reclutamento e assunzione del personale costituisce una delle modalità strumentali per mezzo della quale, in linea di principio, può essere commesso il reato di corruzione. L'attività di selezione del personale presenta profili di rischio in quanto possibile

via di retribuzione indiretta a favore di pubblici funzionari, quale corrispettivo dell'interessamento in una pratica relativa alla Società. Si potrebbe prospettare, ad esempio, l'assunzione di un congiunto del
pubblico funzionario (o, eventualmente, dello stesso pubblico funzionario) presso la Società, in relazione al compimento di atti in suo favore.
Anche i processi di valutazione ed incentivazione del personale (e, più in generale, dell'intera attività di gestione del personale) possono rappresentare profili di rischio, nelle seguenti ipotesi:
- riconoscimento ad un familiare (o ad una persona gradita) di un pubblico funzionario di privilegi o vantaggi professionali indebiti o non dovuti e collegati all'interessamento del pubblico funzionario medesimo in una pratica d'interesse dell'Ente;
- assegnazione a dipendenti di bonus/incentivi non proporzionati alla parte fissa del loro compenso (o legati al raggiungimento di uno specifico obiettivo, quale l'ottenimento di un determinato contratto), potendo tali incentivi spingere il lavoratore dipendente a compiere atti di corruzione per raggiungere i propri scopi;
- riconoscimento di bonus/incentivi "ingiustificati" con la finalità di rendere disponibili somme di denaro in seguito utilizzabili per fini corruttivi, sia direttamente attraverso l'accreditamento da parte del lavoratore dipendente di una somma, o di una parte di essa, su un conto intestato ad una Società estera facente capo al pubblico funzionario, sia indirettamente.

D) Nomina di dirigenti o di membri di organi sociali (rappresentanza della società);

La nomina di dirigenti o l'attribuzioni di incarichi a organi sociali di rappresentanza o di controllo dell'Ente, può rappresentare profili di rischio rappresentati analogamente a quelli indicati nel capitolo che precede.

E) Incarichi di consulenza o prestazione professionale

Particolare attenzione deve essere inoltre rivolta al conferimento di contratti di consulenza/prestazione professionale a favore di soggetti terzi che potrebbero, con la finalità di avvalorare la propria attività, utilizzare una parte dei compensi pattuiti per attribuire indebiti vantaggi a favore di pubblici funzionari e nell'interesse della Società.
Va evidenziato, infine, che i contratti di consulenza o prestazione professionale sono particolarmente a rischio in quanto, rispetto alla fornitura di beni, presentano una maggiore difficoltà sia nell'individuare valore che nel determinare lo specifico contenuto della prestazione.

G) Area Omaggi e spese di Rappresentanza

I processi di gestione degli omaggi (sponsorizzazioni, donazioni, liberalità) rappresentano delle possibili modalità strumentali attraverso cui potrebbe essere commesso il reato di corruzione. La gestione anomala di tali attività potrebbe costituire un potenziale strumento per la commissione del reato di corruzione verso dipendenti e rappresentanti della PA, al fine di ottenerne favori nell'ambito dello svolgimento delle attività aziendali (ad esempio, per l'acquisizione di ordini/contratti, per l'ottenimento di licenze, ecc.).

La gestione delle prestazioni gratuite, erogate in qualsiasi forma dalla Società a titolo di omaggio a favore della clientela o di terzi, si presenta a rischio in quanto possibile strumento di corresponsione di utilità non dovute a pubblici funzionari o a soggetti collegati. Ad esempio, potrebbe darsi l'invio ad un pubblico funzionario, in occasione della conclusione di un contratto,

di un omaggio (non di esiguo valore) quale corrispettivo all'interessamento di tale funzionario nella pratica relativa alla Società.

Facendo poi riferimento ai contratti di sponsorizzazioni, si evidenzia che, in via astratta, un contratto per la fornitura di sponsorizzazioni può essere utilizzato dalla Società quale strumento per creare disponibilità occulte. Si potrebbe citare, a titolo d'esempio, il caso della sponsorizzazione di manifestazioni/iniziative sportive nelle quali viene fatto figurare come versato dalla Società un corrispettivo superiore a quello effettivamente destinato alla sponsorizzazione, con la sottostante intesa che il soggetto sponsorizzato restituirà, in forma occulta, parte del corrispettivo alla Società sponsorizzante. L'insidiosità di tale condotta appare particolarmente marcata data la natura immateriale della prestazione oggetto del contratto e, quindi, la difficoltà di quantificare l'effettivo valore economico della prestazione resa.
I processi in analisi possono, inoltre, presentare profili di rischio nell'ipotesi in cui siano sponsorizzati eventi e manifestazioni su indicazione del funzionario pubblico, finalizzati a:
- ottenere privilegi/vantaggi indebiti o non dovuti per la Società;
- effettuare donazioni/liberalità a soggetti riconducibili a funzionari pubblici;
- effettuare donazioni/liberalità "falsate" al fine di rendere disponibili somme di denaro/beni utilizzabili per fini corruttivi.

Anche le spese di rappresentanza, infine, costituiscono una delle modalità strumentali attraverso cui può essere commesso il reato di corruzione (ovvero una modalità attraverso cui la Società può creare disponibilità occulte). Si pensi al caso della corruzione di un pubblico funzionario mediante il sostenimento di costi ed oneri che la Società indica quali spese di rappresentanza (al fine di giustificare il connesso esborso finanziario). Tali spese potrebbero in tal modo costituire il potenziale strumento attraverso cui commettere reati di corruzione verso pubblici dipendenti o incaricati di pubblico servizio.

A.3 LE MISURE PER LA PREVENZIONE

A.3.1. Divieti

I Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti di API nell'ambito dell'espletamento delle attività considerate a rischio, l'espresso divieto di:

- ✓ porre in essere comportamenti previsti dagli artt. 24 e 25 e 25-novies del D.Lgs. 231/2001, senza limitazione alcuna ai reati di corruzione, istigazione alla corruzione, che si realizzano attraverso l'offerta o la promessa di denaro o altra utilità agli interlocutori dell'ente che indìce il bando per ottenere, indebitamente, l'aggiudicazione di fondi o l'accelerazione indebita di un atto dovuto, ovvero nel caso di presentazione di documentazione, l'allegazione di fatti volutamente falsi e/o lacunosi per ottenere l'aggiudicazione di bandi;
- ✓ porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

è fatto divieto di:

- ✓ adottare comportamenti contrari alle leggi e al Codice Etico, in tutte le fasi del
- ✓ effettuare elargizioni in denaro a pubblici ufficiali o incaricati di pubblico servizio;
- ✓ distribuire omaggi e regali al di fuori di quanto previsto dalla prassi dell'Ente;
- ✓ esibire alla Pubblica Amministrazione documenti, dati falsi o alterati;
- ✓ chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore;

- ✓ omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione.
- ✓ accordare altri vantaggi di qualsiasi natura (come, a puro titolo di esempio, promesse di assunzioni o consulenze dirette o di prossimi congiunti) in favore di rappresentanti della Pubblica Amministrazione, finalizzate comunque ad ottenere illeciti vantaggi;
- ✓ riconoscere compensi in favore di consulenti e collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o che, addirittura, non corrispondano ad alcuna prestazione;
- ✓ ricevere o sollecitare elargizioni in denaro, omaggi, regali, o vantaggi di altra natura da pubblici funzionari ove eccedano le normali pratiche commerciali e di cortesia; chiunque riceva omaggi o vantaggi di altra natura non compresi nelle c.d. "regalie d'uso" è tenuto a darne immediata comunicazione all'O.d.V.;
- ✓ assumere personale e/o attribuire incarichi (ad es. di consulenza) nei casi in cui l'assunzione o l'incarico siano (o possano apparire) finalizzati allo scambio di favori con soggetti pubblici;
- ✓ effettuare pagamenti di parcelle maggiorate ai legali o di altri soggetti coinvolti in processi di rappresentanza legale al fine di costituire fondi per comportamenti corruttivi;
- ✓ i consulenti esterni eventualmente coinvolti nelle aree a rischio della presente Parte Speciale A devono sottoscrivere, in sede di contratto, una dichiarazione nella quale affermino:
  i)di conoscere il contenuto del D.Lgs 231/01, del Codice Etico e dei principi del Modello dell'Ente e di impegnarsi ad osservarne il contenuto;
  ii) di segnalare tempestivamente all'O.d.V. di API eventuali violazioni delle prescrizioni contenute nel Modello e nel Codice Etico o di comportamenti comunque contrari a quanto previsto dal D.Lgs 231/01 dei quali siano venuti a conoscenza nell'ambito dei rapporti con la Pubblica Amministrazione.

A.3.2. Principi procedurali

Ai fini dell'attuazione dei comportamenti di cui sopra:

1) nessun tipo di pagamento potrà esser effettuato in denaro contante o in natura;

2) le dichiarazioni rese a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, dovranno contenere solo elementi assolutamente veritieri, completi e corretti;

3) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti dovranno porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente ai propri superiori o all'O.d.V. eventuali situazioni di irregolarità o di sospetto di irregolarità;

4) per i rapporti intrattenuti con la la Pubblica Amministrazione attraverso supporti informatici, l'idoneità dell'operatore, che immette dati e dichiarazioni deve essere sempre individuabile; (attraverso password o firma digitale)

5) i soggetti che interloquiscono con la Pubblica amministrazione siano a ciò autorizzati ad e se del caso muniti di apposita procura;

6) in caso di ispezione presso la Sede Legale o una delle Unità Locali si deve tempestivamente avvertire il Direttore Generale o un Procuratore dotato del potere di rappresentare la società. In caso di assenza di uno dei suddetti si convocherà un responsabile di funzione che rappresenterà la società finché una persona dotata dei necessari poteri sarà presente;

7) Segregazione delle funzioni e dei compiti, la struttura competente attribuisce a ciascun ufficio le attività operative e di controllo, al fine di garantire la contrapposizione dei ruoli tra i

soggetti che gestiscono le fasi istruttorie e realizzative e i soggetti deputati alle attività di verifica.
8)Tracciabilità del processo e delle informazioni sia a livello di sistema informativo sia in termini documentali per ciascuna fase rilevante degli accordi con la Pubblica Amministrazione le procedure dell'Ente prevedono che la documentazione prodotta venga, archiviata dalla struttura competente in apposito fascicolo da tenere aggiornato, con modalità formalizzata, nel corso dello svolgimento dell'attività. Si provvede inoltre alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;

A.3.3. La Valutazione sul grado di pericolo della commissione del Rischio Reato

La valutazione del grado di pericolo della commissione del reato per questa sezione speciale può essere valutato rischio 2, su una scala da 0 a 3 dove 0 rappresenta un rischio remoto, 1 un rischio basso, 2 un rischio medio e 3 un rischio alto.
La valutazione di posizionare rischio 2 quindi medio, non è relativa alla ipotesi di accadimento per l'Ente in quanto tale, ma parte dal presupposto che l'ipotesi di rischio basso ci sia se non si ponesse in essere l'attività di ricezione di finanziamenti pubblici, per il fatto quindi di ricevere finanziamenti pubblici il rischio stimato è 2 cioè medio.
Quanto sopra vale per le ipotesi di reato di cui agli articoli 24, indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico e per quanto all' art. 25 concussione e corruzione, mentre per quanto all'art. 25-novies induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria si possa ipotizzare un rischio 1 e quindi un rischio basso, questo per la peculiarità del fatto che si possa ipotizzare media di per se la commissione dell'illecito in quanto tale da parte dell'Ente.

A.4 I PROTOCOLLI LE PROCEDURE E I REGOLAMENTI

Al fine di poter dare compiutezza tramite protocolli, procedure e regole comportamentali alle misure di prevenzione di cui al capitolo precedente ed in generale a tutto quanto dettagliato nella presente sezione speciale si definiscono i seguenti protocolli che formano parte integrante della seguente parte speciale come segue:

1)Approvazione di un regolamento definito come Regolamento e codice di condotta in caso di Ispezioni e Controlli da parte di Autorità di Vigilanza Pubbliche denominato anche R.I.C.A.V.P. – riferimento procedura del Sistema Qualità Apiservizi: **SP018**

2)Approvazione di un regolamento protocollo Omaggi, Spese di Rappresentanza e Sponsorizzazioni – riferimento procedura del Sistema Qualità Apiservizi: **SP019**

3)Approvazione di un protocollo Incarichi di Consulenza, Assunzione personale, Amministratori e Verifica soci/associati – riferimento procedura del Sistema Qualità Apiservizi: **SP020**

4)Approvazione di un protocollo Amministrazione, Conservazione Documenti, Area Contabile e Finanziaria – riferimento procedura del Sistema Qualità Apiservizi: **SP023**

5)Approvazione di un protocollo per la costituzione di Associazione Temporanee di Scopo – riferimento procedura del Sistema Qualità Apiservizi: **SP021**

A.5 LE ISTRUZIONI E LE VERIFICHE DELL'ODV

Compiti dell'O.D.V., in riferimento all'osservanza e all'efficace applicazione del Modello in materia di reati con la PA, sono:

a)il puntuale riscontro del rispetto dei Protocolli, delle Procedure e dei Regolamenti così come individuato nel capitolo precedente;
b)la somministrazione di Check list con cadenza stabilita dall'O.D.V. circa il puntuale rispetto di quanto indicato nella presente parte speciale;
c)la risoluzione di eventuali dubbi interpretativi posti dai destinatari sul Modello e sui principi previsti dalla Parte Speciale;
d)la conservazione e l'archiviazione della documentazione relativa all'attività di controllo svolta nelle aree di rischio segnalate nella Parte Speciale per almeno 10 anni.
Qualora emergessero, dagli accertamenti posti in essere dall'O.D.V., elementi tali da far risalire alla violazione dei principi e dei protocolli contenuti nella Parte Speciale, alla commissione del reato o al tentativo di commissione del reato, l'O.D.V. dovrà riferire al Consiglio Direttivo e al Collegio dei Revisori, in modo tale che vengano adottati gli opportuni provvedimenti di competenza.

L'O.d.V. dovrà inoltre tenere in evidenza e verificare:
1) le Segnalazioni, da parte di soggetti destinatari o c.d. soggetti terzi, riguardano in genere tutte le notizie relative alla presumibile commissione dei reati previsti dal Decreto in relazione all'attività dell'Ente o a comportamenti non in linea con le regole di condotta adottate dall'Ente stesso.

Rientrano nella tipologia di segnalazioni:
a) ordini ricevuti da un superiore e ritenuti in contrasto con la legge, o il codice Etico;
b) eventuali richieste o offerte di denaro o beni (eccedenti il modico valore) e destinati a pubblici ufficiali o incaricati di pubblico servizio;
c) eventuali scostamenti significativi del budget o anomalie di spesa emerse in fase di controllo di gestione o in altre attività similari;
d) omissioni, falsità o trascuratezze nella tenuta della contabilità o nella conservazione della documentazione dei registri contabili;
e) qualsiasi scostamento riscontrato nel processo di valutazione delle offerte rispetto a quanto previsto dalle procedure dell'ente o a criteri predeterminati.

2)Le Informazioni, relative ad atti ufficiali, riguardano notizie utili per l'attività dell'O.d.V. (quali a titolo esemplificativo criticità o anomalie riscontrare nell'attuazione del Modello, notizie relative a mutamenti nell'organizzazione aziendale).

Rientrano nella tipologia di segnalazioni:
a) i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o a qualsiasi altra autorità, relative allo svolgimento di indagini, anche nei confronti di ignoti, comunque concernenti l'Ente per i reati previsti dal Decreto;
b) le richieste di assistenza legale inoltrate dagli amministratori e/o dagli altri dipendenti in caso di avvio di procedimento penale a carico degli stessi;
c) le notizie relative ai procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
d) le decisioni relative alla richiesta di erogazioni di finanziamento pubblico;
e) gli aggiornamenti del sistema dei poteri (deleghe e procure);
f) i rapporti preparati nell'ambito delle proprie funzioni dai responsabili interni;

g) i report trimestrali delle gare pubbliche, bandi e convenzioni con Enti Pubblici cui l'Ente ha partecipato, nonché il prospetto riepilogativo delle commesse ottenute a seguito di trattativa privata;
h) le informazioni dalle quali possano emergere eventi con profili di criticità rispetto all'osservanza delle norme del Decreto e del Modello.
i) il bilancio annuale corredato dei relativi allegati;
l) le comunicazioni da parte del Collegio Sindacale e dell'Organo di Revisione relative alle criticità emerse anche se risolte;

A.6 QUESTIONARIO RELATIVO AI REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Si allega questionario di verifica al fine della evidenza delle attività espletate e dei puntuali riscontri all'interno delle procedure e dei regolamenti adottati e delle rispondenze ed integrazioni anche del sistema Qualità ai corretti principi di comportamento della presente parte speciale dei reati contro la P.A.

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE
Artt. 24. – 25 – 25 novies del D.Lgs. 231 / 2001

CORRUZIONE E CONCUSSIONE	
TIPO DI REATO	**CONTROLLI CAUTELATIVI**
• Vendere beni, fornire servizi e realizzare opere per la Pubblica Amministrazione. •Ottenere concessioni, licenze ed autorizzazioni da parte della P.A. • Ottenere trattamenti di favore (ad esempio in sede di conciliazione amministrativa) da parte della Pubblica Amministrazione. • Ottenere trattamenti di favore da parte di Autorità di controllo e/o di vigilanza.	• Esplicita previsione tra i principi etici del divieto di pratiche corruttive. • Controllo dei flussi finanziari aziendali. • Controllo della documentazione aziendale e, in particolare, delle fatture passive (la pratica più diffusa per procurarsi la provvista per corrompere è l'utilizzazione di fatture per operazioni inesistenti). • Controlli dei collaboratori esterni (ad esempio agenti) e della congruità delle provvigioni pagate rispetto a quelle praticate nell'area geografica di riferimento.
TRUFFA AGGRAVATA AI DANNI DELLO STATO	
TIPO DI REATO	**CONTROLLI CAUTELATIVI**
• Produzione alla P.A. di documenti falsi attestanti l'esistenza di condizioni essenziali per partecipare ad una gara, per ottenere licenze, autorizzazioni, ecc.	• Specifiche previsioni nel sistema aziendale di programmazione e di controllo. • Puntuali attività di controllo gerarchico (incluso sistema di deleghe).
FRODE INFORMATICA	
TIPO DI REATO	**CONTROLLI CAUTELATIVI**

Alterazione di registri informatici della PA per far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.) ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali / previdenziali di interesse dell'azienda (es. mod. 770), già trasmessi all'Amministrazione.	Sistema di controlli interni all'azienda che prevedano ai fini del corretto e legittimo accesso ai Sistemi informativi della Pubblica Amministrazione; • un adeguato riscontro delle password di abilitazione per l'accesso ai Sistemi Informativi della PA possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche Funzioni/Strutture aziendali; • la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dall'Ente; • il rispetto della normativa sulla privacy a tutela del dipendente. Questi meccanismi assumono maggiore pregnanza per quegli enti che, sulla base di un rapporto di appalto/concessione con un'Amministrazione pubblica o in qualità di Società miste partecipate da un'Amministrazione/Ente locale e da un privato imprenditore, si assumono l'incarico di realizzare, sviluppare e gestire un Sistema Informativo pubblico o un Sistema Informativo di interesse pubblico.
REATI IN TEMA DI EROGAZIONI PUBBLICHE	
TIPO DI REATO	**CONTROLLI CAUTELATIVI**
• Settore finanziario • Investimenti ambientali • Investimenti produzione • Ricerca ed innovazione tecnologica	• Specifica previsione del codice etico. • Diffusione del Codice Etico verso tutti i dipendenti. • Programma di informazione/formazione periodica del dipendente. responsabilizzazione esplicita, riportata in ordine di servizio della Funzione competente e nel contesto delle relative procedure aziendali, delle funzioni competenti alla predisposizione dei progetti e delle relative istanze. • Separazione funzionale fra chi gestisce le attività realizzative e chi presenta la documentazione di avanzamento. • Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali

	dell'azienda che presenta il progetto). • Coerenza delle procure verso l'esterno con il sistema delle deleghe. • Esclusione esplicita, nel sistema delle procure, della "richiesta di denaro o altra utilità a terzi". • Meccanismi di pubblicità verso gli interlocutori esterni delle procure. Puntuali attività di controllo gerarchico, previste altresì in sede di Ordine di servizio delle Funzioni competenti che partecipano al processo di acquisizione di beni e servizi per l' Ente.

Descrizione	Sì	No	N/A	Note
La presente *check list* dispone a carico degli Esponenti Aziendali, dei Consulenti, dei Partner e parti terze in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti del Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, **di attenersi ai seguenti principi generali di condotta:**				
1. astenersi dal porre in essere comportamenti tali da integrare i Reati sopra descritti (artt. 24 e 25 del Decreto);	**Sì**			**Previsto nel Codice Etico**
2. porre in essere, promuovere, collaborare, o dare causa a comportamenti tali da integrare le fattispecie rientranti tra i Reati ed Illeciti di cui agli artt. 24 e 25 del Decreto;	**Sì**			**Previsto nel Codice Etico**
3. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte possano potenzialmente diventarlo;	**Sì**			**Previsto nel Codice Etico**
4. utilizzare anche occasionalmente l'Ente o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati di cui agli artt. 24 e 25 del Decreto;	**Sì**			**Previsto nel Codice Etico**

<u>Gestione del rapporto :</u> **<u>Assumere o mettere in atto comportamenti</u>** **1)** che nell'esercizio delle attività oggetto delle autorizzazioni/licenze, possano essere finalizzati ad evitare, anche in parte, l'osservanza degli adempimenti di legge/amministrativi o, comunque, a poter disporre di indebiti privilegi;	**Sì**			**Previsto nel Codice Etico**
2) che in sede di adempimenti conseguenti agli obblighi di legge/normativi e di attività di gestione in genere, possano essere diretti a rappresentare alla Pubblica Amministrazione dati/informazioni non corretti, con la finalità di perseguire "posizioni privilegiate" nell'interesse dell'Ente o di eludere obblighi di legge/normativi;	**Sì**			**Previsto nel Codice Etico**
3) che in sede di ispezioni/controlli/verifiche da parte di Autorità Indipendenti/Organismi di Vigilanza/Ministeri/Rappresentanti delle Istituzioni, possano essere finalizzati a influenzare indebitamente, nell'interesse dell'Ente, il giudizio/parere di tali Organismi;	**Sì**			**Previsto nel Codice Etico**
4) nell'espletamento delle rispettive attività e funzioni oltre alle regole di cui al presente Modello, gli Esponenti Aziendali sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti: • il Codice etico; • le procedure operative volte a garantire la trasparenza nel processo di approvvigionamento; •le regole di affidamento delle docenze e la continuazione del rapporto medesimo;	**Sì** **Sì** **Sì** **Sì**			**Previsto nel Codice Etico** **Previsto nel Codice Etico e nel sistema qualità Sez. MGQ 04 paragrafo 2.4** **Previsto nel sistema qualità Sez. MGQ 04 paragrafo 2.4 e nella procedura PT 001 processo area formazione e nelle specifiche SP 001 capitolato per la fornitura di servizi di formazione e SP 002 linea guida doveri comportamentali del docente** **Previsto nel sistema documentale della Qualità**

• ogni altra documentazione relativa al sistema di controllo interno in essere presso l'Ente;	**Sì**			**e in particolare nel Manuale Qualità e nelle procedure in esso richiamate.**
• le procedure informative per l'assunzione e la formazione del personale interno	**Sì**			**Previsto nel Codice Etico** **Previsto nel sistema qualità Sez. MGQ 03 paragrafo 2.2 risorse umane**
Ai Consulenti, Partner, Fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice etico da parte del Ente/Gruppo.				**Previsto nel Codice Etico** **Sono state previste le modalità di trasmissione e divulgazione del Codice Etico e Modello Organizzativo 231.**
Si prevede a carico dei Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente/Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, **l'espresso divieto di:**	**Sì**			**Previsto nel Codice Etico**
a)effettuare elargizioni in denaro a pubblici funzionari italiani o esteri (o a loro familiari, parenti, affini , amici ecc.);				
b)distribuire omaggi e regali o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della P.A. (o loro parenti, affini, amici, ecc.), al di fuori di quanto previsto dalla prassi aziendale (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). Gli omaggi consentiti nell'ambito del Gruppo/Ente si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte ad es. non sono di modico valore viaggi e soggiorni, iscrizioni	**Sì**			**Previsto nel Codice Etico**

a circoli, ecc.) o la *brand image* del Gruppo/Ente medesimo. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;	**Sì**			**Previsto nel Codice Etico**
c)promettere od offrire a rappresentanti della Pubblica Amministrazione (o loro parenti, affini, amici, ecc.) la prestazione di consulenze e/o altri servizi che possano avvantaggiarli a titolo personale;	**Sì**			**Previsto nel Codice Etico**
d)effettuare prestazioni in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;	**Sì**			**Previsto nel Codice Etico**
e)riconoscere compensi in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.	**Sì**			**Previsto nel Codice Etico**
f)presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari a qualsiasi livello, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;	**Sì**			**Previsto nel sistema Qualità nel manuale qualità sez. MGQ 04 paragrafo 2.2 e 2.3 e PT 001**
<u>Ai fini dell'attuazione dei comportamenti di cui sopra:</u> **1.** i rapporti nei confronti della P.A. per le suddette Aree a Rischio devono essere gestiti in modo unitario, procedendo alla nomina di uno o più Responsabili Interni per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse);	**Sì**			**Previsto nel sistema Qualità nel manuale qualità sez. MGQ 04 paragrafo 2.4**
2. gli accordi di associazione con i Partner devono essere definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura – e devono essere proposti o verificati o approvati da almeno due soggetti	**Sì**			

appartenenti all'Ente;				
3. gli incarichi conferiti ai Consulenti/Docenti devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito e devono essere proposti o negoziati o verificati o approvati da almeno due soggetti appartenenti all'Ente;	**Sì**			**Previsto nel sistema Qualità nel manuale qualità sez. MGQ 04 paragrafo 2.4**
4. i contratti stipulati con i Fornitori nell'ambito delle Aree a Rischio devono essere redatti per iscritto con l'indicazione del compenso pattuito e devono essere proposti o negoziati o verificati o approvati da almeno due soggetti appartenenti all'Ente;	**Sì**			**Previsto nel sistema Qualità nel manuale qualità sez. MGQ 04 paragrafo 2.4**
5. nessun tipo di pagamento può essere effettuato in contanti o in natura;	**Sì**			**Prevista in apposita disposizione di servizio .**
6. le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;	**Sì**			**Previsto nel Codice Etico nel sistema Qualità PT 001 Processo Area formazione e nelle linee guida alle spese ammissibili della Regione Lombardia e manuale di gestione del FAPI o dell'Ente erogatore del Finanziamento**
7. coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi l'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire tempestivamente all' ODV eventuali situazioni di irregolarità.				**Previsto nel Codice Etico Previsto nel Regolamento Interno dell'ODV distribuito ai dipendenti e ai collaboratori coinvolti in tali attività.**

PARTE SPECIALE – B

REATI DI CRIMINALITA' INFORMATICA
(art. 25-bis del D.Lgs. 231/2001)

Questa Parte Speciale definisce i comportamenti a cui i Destinatari come già definiti nella Parte Generale si atterranno nello svolgimento delle attività rientranti nelle c.d. Aree Sensibili o a Rischio e in considerazione delle diverse posizione e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente così come prescritto in questa Parte Speciale al fine di prevenire e impedire il verificarsi di reati.
Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nel codice etico e nelle procedure operative interne.
Si precisa inoltre che destinatari del presente Allegato sono anche i membri delle Associazione Temporanee di Scopo di cui l'Ente è membro o ne diventerà membro.
In particolare, la presente Parte Speciale ha la funzione di:
a) fornire un elenco dei principi generali e dei principi procedurali specifici cui i Destinatari, in relazione al tipo di rapporto in essere con l'Ente, sono tenuti ad attenersi per una corretta applicazione del Modello;
b) fornire al O.d.V. e ai responsabili delle altre funzioni dell'Ente chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

B.1 ELENCO REATI CONTRO LA CRIMINALITA' INFORMATICA

B.1.1 Definizione di Reati di Criminalità Informatica

Con la nozione di reato informatico o crimine informatico intendiamo i comportamenti previsti dal codice penale o da leggi speciali nel quale lo strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione del fatto di reato.
Può essere considerato reato informatico sia la frode commessa tramite l'utilizzo di un computer sia il danneggiamento del sistema informatico.
Ci troviamo quindi di fronte a un crimine informatico quando un sistema di elaborazione o ciò che viene prodotto dall'elaboratore, è usato come mezzo per compiere frodi, sabotaggi, falsificazioni, e l'elaboratore ha almeno uno dei seguenti ruoli:
a)oggetto, manipolazione, distruzione dell'elaboratore, o dei relativi programmi ivi contenuti;
b)soggetto, l'elaboratore è luogo, motivo o fonte del crimine;
c)strumento quando ad esempio serve a commettere un reato es. intercettazione.
L' art. 24-bis del Decreto, articolo introdotto dalla L. 18 marzo 2008, n. 48, art. 7, recepisce l'art. 491-bis c.p. che, a sua volta, estende le ipotesi di falsità in atti di cui al Libro II, Titolo VII, Capo III c.p. a tutte le fattispecie delittuose in cui una o più delle suddette falsità abbia ad oggetto un c.d. "documento informatico"; introduce all'interno del Decreto alcune ipotesi di reato in materia di criminalità informatica, già disciplinate all'interno del Codice Penale.
Articolo 491-bis codice penale
(Documenti informatici)
Se alcuna 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.
Si evidenzi inoltre che diversi reati contro la Pubblica Amministrazione sono stati introdotti sempre dalla L. 18 marzo 2008, n. 48, a tutela proprio dello Stato e degli Enti Pubblici, quali

l'art. 635-ter c.p. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità, l'art. 635-quater c.p. danneggiamento di sistemi informatici o telematici, l'art. 635-quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilità.
Per una definizione di Pubblica Amministrazione considerata ai fini della individuazione delle aree a rischio dobbiamo dedurla dagli artt. 357 e 358 c.p., in base ai quali sono pubblici ufficiali e incaricati di pubblico servizio 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 certificativi o autorizzativi.

B.1.2 art. 24-bis delitti informatici e trattamento illecito di dati

Rientrano tra questi reati:
art. 491-bis c.p. documenti informatici di cui poi all'estensione degli articoli del c.p. 476/7/8/9, 480/1/2/3/4/5/6/7/8/9, 490, 492 , 492.
art. 615-ter c.p. accesso abusivo ad un sistema informatico o telematico
art. 615-quater c.p. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
art. 615-quinquies c.p. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
art. 617-quater c.p. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
art. 617-quinquies c.p. installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
art. 635-bis c.p. danneggiamento di informazioni, dati e programmi informatici
art. 635-ter c.p. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilita'
art. 635-quater c.p. danneggiamento di sistemi informatici o telematici
art. 635-quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilita'
art. 640-quinquies c.p. frode informatica del soggetto che presta servizi di firma elettronica
Rischio reato: l'ente risulta esposto ad alcune di queste tipologie di reati e si è tutelato dal loro compimento come indicato nella parte speciale allegata al presente Modello Organizzativo.

<u>art. 491-bis c.p. documenti informatici</u>
Se alcuna 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.
Si veda più avanti nel prosieguo del capitolo

<u>art. 615-ter c.p. accesso abusivo ad un sistema informatico o telematico</u>
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 qualita' 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.

Fattispecie
Commette il delitto 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.

Esemplificazioni di condotte illecite
Accesso abusivo agli archivi di un ente pubblico, al fine di acquisire informazioni per l'ottenimento di un finanziamento.

art. 615-quater c.p. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, e'punito con la reclusione sino ad un anno e con la multa sino a euro 5.164,00.
La pena e' della reclusione da uno a due anni e della multa da euro 5.164,00 a euro 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater.

Fattispecie
Il delitto è commesso da chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

Esemplificazioni di condotte illecite
Procurare i mezzi di accesso ad un sistema informatico in modo abusivo per cancellare un finanziamento di altri soggetti.

art. 615-quinquies c.p. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
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 fino a due anni e con la multa sino a euro 10.329,00.

Fattispecie
Commette il delitto 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.

Esemplificazioni di condotte illecite
Procurare un programma al fine di favorire il rallentamento di una banca dati pubblica.

art. 617-quater c.p. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
Chiunque fraudolentamente 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.

Fattispecie
Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.
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.

Esemplificazioni di condotte illecite
Accedere ad un account di posta protetta da password al fine di leggere la corrispondenza del proprietario dell'account medesimo.

art. 617-quinquies c.p. installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
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 piu' sistemi, e' punito con la reclusione da uno a quattro anni.
La pena e' della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater.

Fattispecie
Compie il delitto 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.
Esemplificazioni di condotte illecite
Utilizzazione di apparecchi capaci di copiare i codici di accesso degli utenti ovvero di intercettarli.

art. 635-bis c.p. danneggiamento di informazioni, dati e programmi informatici
Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi, informazioni altrui e' punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se ricorre la circostanza 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 a quattro anni e si procede d'ufficio.
Fattispecie
Il delitto, salvo che il fatto costituisca più grave reato, consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, da chiunque posta in essere.

art. 635-ter c.p. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilita'
Salvo che il fatto costituisca piu' 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'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Fattispecie
Il delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di 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.

art. 635-quater c.p. danneggiamento di sistemi informatici o telematici
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) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Fattispecie
Il delitto, salvo che il fatto costituisca più grave reato, è commesso da chiunque, mediante le condotte di cui all'articolo 635 - bis c.p., 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.

art. 635-quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilita'
Se il fatto di cui all'articolo 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) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Fattispecie
Il delitto è commesso se il fatto di cui all'art. 635-quater c.p. 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.

Esemplificazioni di condotte illecite
In relazione agli Art. 635 bis, 635 ter, 635 quater, 635 quinquies la condotta consiste nell'alterazione del funzionamento di un sistema informatico o telematico dello Stato o di altro Ente Pubblico, al fine di ottenere un vantaggio per l'Ente es. nella fase di ottenimento di un finanziamento.

art. 640-quinquies c.p. frode informatica del soggetto che presta servizi di certificazione di firma elettronica
Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a se´ 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 a 1.032 euro.
Nota
Il soggetto attivo che può compiere il reato può essere solo il certificatore di firma elettronica e quindi è da escludere perché estraneo alle finalità dell'Ente.

B.1.2.1 il comma 3 art. 24-bis del d.lgs. 231/2001

Recita:" 3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote."
L' Articolo 491-bis codice penale (Documenti informatici) recita "se alcuna 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."
Devono essere quindi ricompresi anche se non citate direttamente ma indirettamente nell'elenco dei reati informatici i seguenti reati come segue:

Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)
Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)
Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Falsità materiale commessa da privato (art. 482 c.p.)
Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)
Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

Falsità in registri e notificazioni (art. 484 c.p.)
Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

Falsità in scrittura privata (art. 485 c.p.)
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.

Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)
Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480".

Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)
Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private.

Uso di atto falso (art. 489 c.p.)
Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.

Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)
Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente.

Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)
Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)
Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

B.2 LE AREE A RISCHIO

I reati informatici possono potenzialmente essere commessi da ogni Servizio dell'Ente, per questo motivo i principi di comportamento espressi nella presente Parte Speciale devono essere conosciuti e rispettati da tutti i Dipendenti e i Collaboratori dell'Ente, in particolare comunque si evidenziano attività potenzialmente a rischio per i seguenti:

- ✓ per il Servizio Formazione accreditata presso Regione Lombardia o di altri enti pubblici
- ✓ per il Servizio Formazione in ATS

1)Gestione informatica delle attività legate al Processo di accreditamento dell'ente presso la Pubblica Amministrazione:

a) invio della domanda di accreditamento;
b) invio documentazione per mantenimento dell'accreditamento;

2)Gestione informatica, organizzazione del processo di rendicontazione alla Pubblica Amministrazione delle attività formative erogate:

a)inizio del progetto, richiesta e gestione di finanziamenti;
b)firma e inoltro della domanda di partecipazione;
c)rapporti con l'ente pubblico nella fase di attribuzione;
d)fase di ricevimento dei fondi;
e)rendicontazione anche via informatica;
f)gestione registro presenze;
g)ispezione ed eventuali contestazioni.

3)Gestione informatica relativa alle autorizzazioni, licenze, permessi da parte della Pubblica Amministrazione

a)richieste per via informatica;
b)firma e inoltro della domanda;
e)rendicontazione anche via informatica;
g)ispezione ed eventuali contestazioni.

4)Rischio di accesso abusivo a un sistema informatico

Alcune delle attività di cui sopra possono avvenire anche con firma digitale del legale rappresentante dell'Ente.

Le Funzioni preposte alla trasmissione di dati o informazioni alla Pubblica Amministrazione tramite i Sistemi Informatici potrebbero inviare virus diretti a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente Pubblico allo scopo di procurare all'Ente un ingiusto vantaggio (ad esempio ritardare l'informativa o le dichiarazioni rispetto alla scadenza prevista).

- ✓ per il Servizio Finanza agevolata su progetti con Contributi Pubblici (diversi dall'area formazione)
- ✓ per il Servizio Ambiente e Sicurezza
- ✓ per il Servizio Innovazione Energia
- ✓ per il Servizio Commercio Estero
- ✓ per il Servizio Progetti Europei

I servizi si devono intendere rivolti anche a terzi, in particolare per l'area Formazione si evidenziano

Per gli Altri servizi sopraindicati relativamente agli adempimenti informatici:

1)Generalmente
- a)richiesta e/o creazione di domande di finanziamento agevolato;
- b)richiesta e/o creazione di domande per contributi pubblici;
- c)richiesta e/o creazione di domande/dichiarazione con rilevanza pubblica in generale;
- d)firma ed inoltre delle domande di cui ai punti a), b) e c) di cui sopra;
- e)rapporto con gli enti pubblici delle domande di cui ai punti a), b) e c) di cui sopra;
- f)fase di ricevimento dei fondi delle domande di cui ai punti a), b) e c) di cui sopra;
- g)rendicontazione anche via informatica delle domande di cui ai punti a), b) e c) di cui sopra;
- h)ispezione ed eventuali contestazioni delle domande di cui ai punti a), b) e c) di cui sopra.

Per i terzi in ipotesi di verifica o ispezione si possono evidenziare inoltre:
- a)fase di accompagnamento all'ispezione;
- b)messa a disposizione di dati e documenti;
- c)fase di firma dei relativi verbali;
- d)fase di esecuzione delle eventuali prescrizioni.

2)Rischio di accesso abusivo a un sistema informatico.

Alcune delle attività di cui sopra possono avvenire anche con firma digitale del legale rappresentante dell'Ente.

Le Funzioni preposte alla trasmissione di dati o informazioni alla Pubblica Amministrazione tramite i Sistemi Informatici potrebbero inviare virus diretti a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente Pubblico allo scopo di procurare all'Ente un ingiusto vantaggio (ad esempio ritardare l'informativa o le dichiarazioni rispetto alla scadenza prevista).

- ✓ Per il Servizio Gestione del personale dipendente interno all'Ente (compreso Paghe e Contributi).

1) Amministrazione e gestione del personale, rapporti con enti previdenziali e assistenziali, nonché la sicurezza e l'igiene sul lavoro;
a) invio informatico di dichiarazioni previdenziali

- ✓ Per il Servizio Fiscale Tributario interno all'Ente

1) Amministrazione e gestione di documentazione fiscale, rapporti con uffici di accertamento quali agenzia Entrate, Guardia di Finanza, Agenzia delle Dogane;
a) invio informatico di dichiarazioni fiscali;

- ✓ Per il Servizio API – CAF

Servizi intrattenuti per conto dei terzi in ambito assistenza API – CAF;
1)richiesta e gestione di dichiarazioni fiscali informatiche per conto di terzi;

2)firma informatica e inoltro di dichiarazioni di cui al punto 1 sopra;
3)rapporti con Enti pubblici per quanto al punto 1 sopra;
4)rapporti con autorità preposte al controllo, anche in caso di ispezioni per quanto al punto 1 sopra;

- ✓ Per il servizio Informatico dell'Ente:

1) gestione dei Sistemi informatici e Telematici dell'Ente.
2) accesso alla rete internet.

1) Gestione dei Sistemi informatici e Telematici dell'Ente
Le Funzioni dell'Ente abilitate all'utilizzo dei Sistemi Informatici e Telematici interni, nell'ambito delle proprie mansioni, potrebbero, potenzialmente, occultare, modificare o cancellare dati o informazioni disponibili sul Sistema Informatico e Telematico interno per procurare alla Società un ingiusto vantaggio (es. eludere le ispezioni delle Autorità di Vigilanza).

2) Accesso alla rete internet
Tutti i dipendenti abilitati all'uso della rete internet, potenzialmente potrebbero:
-introdursi abusivamente in un Sistema Informatico o Telematico;
-deteriorare o rendere inservibili Sistemi Informatici e Telematici;
-diffondere, comunicare o consegnare virus o altri programmi dannosi;

Si ricorda inoltre che, possono presentare in via astratta profili di rischio (corruzione/truffa aggravata ai danni dello Stato/ostacolo all'esercizio delle Autorità Pubbliche di vigilanza) anche la predisposizione delle dichiarazioni funzionali alla liquidazione di tributi e, più in generale, l'invio e la ricezione di documenti alla/dalla Pubblica Amministrazione, anche con l'utilizzo di sistemi informatici.

Inoltre in generale per qualsiasi tipo di Servizio o attività ricordiamo i reati che si possono commettere utilizzando la Gestione del Software della Pubblica Amministrazione.

B.3 LE MISURE PER LA PREVENZIONE

B.3.1. Divieti

Premesso che nell'espletamento di tutte le attività operative attinenti la gestione informatica della rete oltre alle regole del presente Modello, dipendenti, collaboratori e fornitori informatici dovranno conoscere e rispettare:
1. le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
2. le procedure dell'Ente vigenti, la documentazione e gli ordini di servizio inerenti la struttura gerarchico funzionale ed organizzativa dell'Ente;
3. le procedure e i comportamenti individuati nel Documento Programmatico sulla Sicurezza, formalmente adottato in ossequio a quanto disposto dal D.Lgs. 196/2003;
4. i divieti imposti dall'Ente sono indicati nei seguenti Regolamenti individuati al cap B.4 ai punti da 1) a 3) .

B.3.2. Principi procedurali

Premesso che nell'espletamento di tutte le attività procedurali attinenti la gestione informatica della rete oltre alle regole del presente Modello, dipendenti, collaboratori e fornitori informatici dovranno conoscere e rispettare:
1. Ruoli e responsabilità definiti:
la gestione delle abilitazioni avviene tramite la definizione di profili a ai quali corrispondono le necessarie abilitazioni in ragione delle funzioni svolte all'interno dell'Ente.
2. Segregazione dei compiti e delle attività:
a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi da parte degli utenti.
3. Attività di controllo:
le attività di gestione ed utilizzo di sistemi informativi sono soggette ad attività di controllo a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche.
4. Tracciabilità del processo:
sia a livello di sistema informativo sia in termini documentali tutte le operazioni correttive effettuate tramite sistema (ad esempio rettifiche contabili, variazioni dei profili utente, etc.) sono tracciabili attraverso sistematica registrazione degli eventi.

B.3.3. La Valutazione sul grado di pericolo della commissione del Rischio Reato

La valutazione del grado di pericolo della commissione del reato per questa sezione speciale può essere valutato rischio 2, su una scala da 0 a 3 dove 0 rappresenta un rischio remoto, 1 un rischio basso, 2 un rischio medio e 3 un rischio alto.
La valutazione di posizionare rischio 2 quindi medio, non è relativa alla ipotesi di accadimento per l'Ente in quanto tale, ma parte dal presupposto che l'ipotesi di rischio basso ci sia se non si ponesse in essere l'attività di ricezione di finanziamenti pubblici, per il fatto quindi di ricevere finanziamenti pubblici il rischio stimato è 2 cioè medio.

B.4 I PROTOCOLLI LE PROCEDURE E I REGOLAMENTI

Al fine di poter dare compiutezza tramite protocolli, procedure e regole comportamentali alle misure di prevenzione di cui al capitolo precedente ed in generale a tutto quanto dettagliato nella presente sezione speciale si definiscono i seguenti protocolli che formano parte integrante della seguente parte speciale come segue:

1)Approvazione di un regolamento definito come Regolamento R.S.I. - Regolamento e codice di condotta per l'utilizzo di Strumenti Informatici telefonici e fax - riferimento procedura del Sistema Qualità Apiservizi: **SP016**

2)Approvazione di un protocollo per la costituzione di Associazione Temporanee di Scopo - riferimento procedura del Sistema Qualità Apiservizi: **SP021**

3)Approvazione di un regolamento definito come R.R.I. 231 - Regolamento e codice di condotta per la prevenzione dei Reati Informatici - riferimento procedura del Sistema Qualità Apiservizi: **SP017**

B.5 LE ISTRUZIONI E LE VERIFICHE DELL'ODV

Compiti dell'O.D.V., in riferimento all'osservanza e all'efficace applicazione del Modello in materia di reati Informatici, sono:
a)il puntuale riscontro del rispetto dei Protocolli, delle Procedure e dei Regolamenti così come individuato nel capitolo precedente;
b)la somministrazione di Check list con cadenza stabilita dall'O.D.V. circa il puntuale rispetto di quanto indicato nella presente parte speciale;
c)la risoluzione di eventuali dubbi interpretativi posti dai destinatari sul Modello e sui principi previsti dalla Parte Speciale;
d)verifica della ricezione dell'aggiornamento almeno annuale del Documento Programmatico sulla Sicurezza;
e)la risoluzione di eventuali dubbi interpretativi posti dai destinatari sul Modello e sui principi previsti dalla Parte Speciale;

Qualora emergessero, dagli accertamenti posti in essere dall'O.D.V., elementi tali da far risalire alla violazione dei principi e dei protocolli contenuti nella Parte Speciale, alla commissione del reato o al tentativo di commissione del reato, l'O.D.V. dovrà riferire al Consiglio di Amministazione e al Collegio dei Revisori, in modo tale che vengano adottati gli opportuni provvedimenti di competenza.

L'O.d.V. dovrà inoltre tenere in evidenza e verificare:
1) le Segnalazioni, da parte di soggetti destinatari o c.d. soggetti terzi, riguardano in genere tutte le notizie relative alla presumibile commissione dei reati previsti dal Decreto in relazione all'attività dell'Ente o a comportamenti non in linea con le regole di condotta adottate dall'Ente stesso.

Rientrano nella tipologia di segnalazioni:
a) ordini ricevuti da un superiore e ritenuti in contrasto con la legge, o il codice Etico;
b) eventuali richieste o offerte di denaro o beni (eccedenti il modico valore) e destinati a pubblici ufficiali o incaricati di pubblico servizio;
c) eventuali scostamenti significativi del budget o anomalie di spesa emerse in fase di controllo di gestione o in altre attività similari;
d) omissioni, falsità o trascuratezze nella tenuta della contabilità o nella conservazione della documentazione dei registri contabili;
e) qualsiasi scostamento riscontrato nel processo di valutazione delle offerte rispetto a quanto previsto dalle procedure dell'ente o a criteri predeterminati.

2)Le Informazioni, relative ad atti ufficiali, riguardano notizie utili per l'attività dell'O.d.V. (quali a titolo esemplificativo criticità o anomalie riscontrare nell'attuazione del Modello, notizie relative a mutamenti nell'organizzazione dell'Ente).

Rientrano nella tipologia di segnalazioni:
a) i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o a qualsiasi altra autorità, relative allo svolgimento di indagini, anche nei confronti di ignoti, comunque concernenti l'Ente per i reati previsti dal Decreto;
b) le richieste di assistenza legale inoltrate dagli amministratori e/o dagli altri dipendenti in caso di avvio di procedimento penale a carico degli stessi;
c) le notizie relative ai procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
d) le decisioni relative alla richiesta di erogazioni di finanziamento pubblico;

e) gli aggiornamenti del sistema dei poteri (deleghe e procure);
f) i rapporti preparati nell'ambito delle proprie funzioni dai responsabili interni;
g) i report trimestrali delle gare pubbliche, bandi e convenzioni con Enti Pubblici cui l'Ente ha partecipato, nonché il prospetto riepilogativo delle commesse ottenute a seguito di trattativa privata;
h) le informazioni dalle quali possano emergere eventi con profili di criticità rispetto all'osservanza delle norme del Decreto e del Modello.
i) il bilancio annuale corredato dei relativi allegati;
l) le comunicazioni da parte del dell'Organo di Revisione relative alle criticità emerse anche se risolte;

B.6 QUESTIONARIO RELATIVO AI REATI INFORMATICI

Si allega questionario di verifica al fine della evidenza delle attività espletate e dei puntuali riscontri all'interno delle procedure e dei regolamenti adottati e delle rispondenze ed integrazioni anche del sistema Qualità ai corretti principi di comportamento della presente parte speciale dei reati Informatici.

REATI INFORMATICI
Art. 24. bis D.Lgs. 231 / 2001

Descrizione	Sì	No	Rif. Flow chart	Note
La presente check list prevede a carico dei Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell' Ente nell'ambito dell'espletamento delle attività considerate a rischio, **l'espresso divieto di:**				**Vedi:** **Regolamento R.S.I.** **Regolamento e codice di condotta per l'utilizzo di strumenti informatici telefonici e fax** **Regolamento R.R.I.231** **Regolamento e codice di condotta per la prevenzione dei reati informatici ex D.lgs. 231/2001**
1. porre in essere, promuovere, collaborare, o dare causa a comportamenti tali da integrare le fattispecie rientranti tra i Reati informatici come richiamati dall'art 24 bis del D.Lgs. 231/2001;	Sì			**Previsto nel Codice Etico** **Previsto nei Regolamenti R.S.I. e R.R.I. 231**
2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte, possano potenzialmente diventarlo;	Sì			**Previsto nel Codice Etico** **Previsto nei Regolamenti R.S.I. e R.R.I. 231**

3. utilizzare anche occasionalmente l'Ente o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati di cui a quello esaminando.	Sì			**Previsto nel Codice Etico** **Previsto nei Regolamenti R.S.I. e R.R.I. 231**
PRINCIPI PROCEDURALI SPECIFICI Principi procedurali da osservare nelle singole operazioni a rischio Si indicano di seguito i principi procedurali che in relazione ad ogni singola Area a Rischio gli Esponenti Aziendali sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del ODV:				
1. si deve richiedere l'impegno dei Partner. Fornitori e parti terze al rispetto degli obblighi di legge in tema di Reati Informatici;	Sì			**Già prevista in apposita modulistica in uso presso l'Ente.**
2. la selezione dei fornitori dei servizi **I.T.** (*Information Thecnology*), siano essi Partner, Fornitori o parti terze deve essere svolta con particolare attenzione e in base ad apposita procedura interna. In particolare, l'affidabilità di tali Partner o Fornitori e parti terze deve essere valutata, ai fini della prevenzione dei Reati di cui a quello esaminando, anche attraverso specifiche indagini *ex ante*;	Sì			**Previsto nel Codice Etico e nel sistema qualità Sez. MGQ 04 paragrafo 2.4** **Già prevista in apposita modulistica in uso presso l'Ente.**
3. deve essere rispettata da tutti gli Esponenti Aziendali la previsione del Codice etico diretta a vietare comportamenti tali che siano in contrasto con la prevenzione dei Reati informatici ;	Sì			**Previsto nel Codice Etico** **Già prevista in apposita modulistica in uso presso l'Ente.**
4. nel caso in cui si ricevano segnalazioni di violazione delle norme del Decreto 231, da parte dei propri Esponenti Aziendali e/o Collaboratori Esterni, la direzione è tenuta ad intraprendere le iniziative più idonee per acquisire ogni utile informazione al riguardo.	Sì			**Previsto nel Codice Etico** **Già prevista in apposita modulistica in uso presso l'Ente.**
Rapporti con parti terze Nei contratti con i Consulenti, i Partner i Fornitori e parti terze deve essere contenuta apposita clausola che regoli le conseguenze				

della violazione da parte degli stessi delle norme di cui al Decreto 231, nonché del Modello. Gli Organi di *Governance* devono aver adottato e fatto adottare da tutte le Unità Operative le necessarie procedure per prevenire la commissione dei reati sotto elencati: Accesso abusivo a un sistema informatico o telematico (art. 615- ter c.p.) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - quater c.p.) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 - quinquies c.p.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 – quater c.p.) Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 - quinquies c.p.) Danneggiamento di informazioni, dati e programmi informatici (art. 635 - bis c.p.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 - ter c.p.) Danneggiamento di sistemi informatici e telematici (art. 635 - quater c.p.) Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 - quinquies c.p.) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 - quinquies c.p.) Articolo 491-bis codice penale (Documenti informatici) Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.) Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.) Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.) Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.) Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni				**Tutti i Reati sono Previsti nel Regolamento R.R.I. 231**

amministrative (art. 480 c.p.) Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.) Falsità materiale commessa da privato (art. 482 c.p.) Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.) Falsità in registri e notificazioni (art. 484 c.p.) Falsità in scrittura privata (art. 485 c.p.) Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.) Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.) Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.) Uso di atto falso (art. 489 c.p.) Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.) Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.) Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)	Sì			

PARTE SPECIALE - C

I REATI SOCIETARI
(art. 25-ter del D.Lgs. 231/2001)

C.1. INTRODUZIONE: I DESTINATARI DELLA PARTE SPECIALE PRINCIPI DI COMPORTAMENTO E ATTUAZIONE

Questa Parte Speciale definisce i comportamenti a cui i Destinatari, come già definiti nella Parte Generale, si atterranno nello svolgimento delle attività rientranti nelle c.d. Aree Sensibili o a Rischio, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente, così come prescritto in questa Parte Speciale al fine di prevenire e impedire il verificarsi di reati.
Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nel codice etico e nelle procedure operative interne.
Si precisa inoltre che destinatari del presente Allegato sono anche i membri delle Associazione Temporanee di Scopo di cui l'Ente è membro o ne diventerà membro.
In particolare, la presente Parte Speciale ha la funzione di:
a) fornire un elenco dei principi generali e dei principi procedurali specifici a cui i Destinatari, in relazione al tipo di rapporto in essere con l'Ente, sono tenuti ad attenersi per una corretta applicazione del Modello;
b) fornire al O.d.V., e ai responsabili delle altre funzioni dell'Ente chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

C.2 ELENCO REATI SOCIETARI

C.2.1 Definizione di Reati Societari

Il D. Lgs. 28 marzo 2002 n. 61 ha integrato il D. Lgs. 231/2001 con l'articolo 25-ter, (Reati societari), che introduce specifiche sanzioni a carico dell'ente "in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica".

C.2.2 art. 25-ter Reati societari

Rientrano tra questi reati:

art. 2621 false comunicazioni sociali
art. 2622 commi 1 e 3 c.c. false comunicazioni sociali in danno della società, dei soci o dei creditori
art. 2623 c.c. falso in prospetto abrogato dall'articolo 34, comma 2, della legge 28 dicembre 2005, n. 262
art. 2624 c.c. falsità nelle relazioni o nelle comunicazioni delle società di revisione abrogato dall'articolo 37, comma 34, del decreto legislativo 27 gennaio 2010, n. 39
art. 2625 c.c. com. 2 impedito controllo
art. 2626 c.c. indebita restituzione dei conferimenti
art. 2627 c.c. illegale ripartizione degli utili e delle riserve
art. 2628 c.c. illecite operazioni sulle azioni o quote sociali o della societa' controllante
art. 2629 c.c. operazioni in pregiudizio dei creditori
art. 2629 bis c.c. omessa comunicazione del conflitto di interessi
art. 2391 c.c. interessi degli amministratori
art. 2632 c.c. formazione fittizia del capitale
art. 2633 c.c. indebita ripartizione dei beni sociali da parte dei liquidatori
art. 2636 c.c. illecita influenza sull'assemblea
art. 2637 c.c. aggiotaggio
art. 2638 c.c. ostacolo alle funzioni delle autorità pubbliche di vigilanza

L'Ente, dopo attente valutazioni ed analisi, ha ritenuto opportuno evidenziare, tra gli articoli dei Reati Societari sopra esposti l'art. 2638, che ha come oggetto l'ostacolo alle funzioni delle autorità pubbliche di vigilanza, di seguito riportato:

<u>art. 2638 c.c. ostacolo alle funzioni delle autorità pubbliche di vigilanza</u>
Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima sono puniti con la reclusione da uno a quattro anni.
La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

Premessa

Con "autorità pubblica di vigilanza" dell'art. 2638 cod. civ. si identifica qualsiasi ente che disponga di controlli di tipo ispettivo, preventivo o successivo, come, oltre a CONSOB, anche Banca d'Italia, ISVAP, COVIP Commissione di Vigilanza sui Fondi Pensione, Autorità Garante per la concorrenza del Mercato ANTITRUST, Autorità per le garanzie nelle telecomunicazioni, Autorità per l'energia elettrica e il Gas, Garante per la protezione dati personali. ecc..

Fattispecie

Esposizione nelle comunicazioni alle autorità di vigilanza di fatti non rispondenti al vero su: situazione economica, situazione patrimoniale e situazione finanziaria dell'Ente ovvero occultamento di fatti sulla suddetta situazione che si sarebbero dovuti comunicare od omissioni di comunicazioni obbligatorie.
La norma individua due distinte ipotesi di reato.
La prima si realizza attraverso l'esposizione, nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni di vigilanza, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero, allo stesso fine, attraverso l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima (comma I); la punibilità è estesa anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.
La seconda punisce la condotta dei soggetti che, consapevolmente, ostacolano l'esercizio delle funzioni di vigilanza, in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza (comma II).
Soggetti attivi di entrambe le ipotesi di reato sono gli amministratori, i direttori generali, i sindaci ed i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza; è prevista la pena della reclusione da uno a quattro anni. In relazione alla commissione, nelle forme del tentativo, dei delitti sopra descritti, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà; la Società, poi, non risponde se volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.
Questa figura di reato risponde all'esigenza di coordinare ed armonizzare le fattispecie riguardanti le numerose ipotesi, esistenti nella disciplina previgente, di falsità nelle comunicazioni agli organi di vigilanza, di ostacolo allo svolgimento delle funzioni, di omesse comunicazioni alle autorità medesime. Viene così completata secondo il legislatore la tutela penale dell'informazione societaria, in questo caso nella sua destinazione alle autorità di vigilanza settoriali.

Esemplificazioni di condotte illecite

Gli Amministratori di società trasmettono all'ufficio ispezioni della Regione Lombardia o di altri enti pubblici un prospetto riportando notizie false o comunque notizie incomplete e frammentarie relativamente a determinate rilevanti operazioni su un determinato progetto finanziato.

C.3 LE AREE A RISCHIO

I reati societari così come individuati dall'Art. 2638, possono potenzialmente essere commessi dai sottoelencati Servizi dell'Ente. Per questo motivo i principi di comportamento espressi nella presente Parte Speciale devono essere conosciuti e rispettati da tutti i Dipendenti e i Collaboratori dell'Ente che collaborano con le aree potenzialmente a rischio:

- ✓ Per il Servizio Formazione accreditato presso Regione Lombardia o di altri enti pubblici;
- ✓ Per il Servizio Formazione in ATS:

1)Gestione delle attività legate al Processo di accreditamento dell'ente presso la Pubblica Amministrazione:

a) trasmissione di documentazione non veritiera su specifiche domande fatte dalla vigilanza;

b) non risposta a questionari inviati dalle autorità di vigilanza.

2)Gestione informatica del processo di rendicontazione alla P.A. delle attività formative erogate:

a) trasmissione di documentazione non veritiera su specifiche domande fatte dalla vigilanza;

b) non risposta a questionari inviati dalle autorità di vigilanza.

C.4 LE MISURE PER LA PREVENZIONE

C.4.1. Divieti

Nell'espletamento di tutte le attività operative attinenti la gestione dei rapporti con le autorità di vigilanza, i dipendenti, collaboratori e fornitori dovranno conoscere e rispettare:

1. le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
2. le procedure dell'Ente vigenti, la documentazione e gli ordini di servizio inerenti la struttura gerarchico funzionale ed organizzativa dell'Ente;
3. i divieti imposti dall'Ente indicati nei Regolamenti individuati al cap C.5 ai punti da 1) a 3).

Inoltre dovranno:

4. omettere le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività dell'Ente, nonché la trasmissione dei dati e documenti previsti dalla normativa o specificatamente richiesti dalle predette autorità;
5. 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, quali espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti;
6. esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società.

C.4.2. Principi procedurali

Nell'espletamento di tutte le procedure attinenti la gestione delle attività di Vigilanza, oltre alle regole del presente Modello, dipendenti, collaboratori e fornitori dovranno conoscere e rispettare i seguenti principi fondamentali:

1. Ruoli e responsabilità definiti all'interno del sistema di deleghe relative alle ispezioni delle attività di vigilanza.

2. Puntualità dei compiti e delle attività attraverso l'effettuazione delle segnalazioni periodiche, con la puntualità dovuta, alle autorità previste da leggi e regolamenti, oltre alla tempestività e alla qualità delle comunicazioni alle autorità di vigilanza;
3. Attività di controllo. Attuazione di tutti gli interventi di natura organizzativo contabile necessari per estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni e puntuale invio all'autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa di settore;
4. Tracciabilità del processo. Trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza, evidenziando chi ha autorizzato la relativa trasmissione dei documenti previsti in leggi e regolamenti in materia.
5. Correttezza, professionalità e trasparenza nella condotta da tenere nel corso degli accertamenti ispettivi, in particolare con la messa a disposizione, con tempestività e completezza, dei documenti che gli incaricati ritengano necessario acquisire;

C.4.3. La Valutazione sul grado di pericolo della commissione del Rischio Reato

La valutazione del grado di pericolo della commissione del reato per questa sezione speciale può essere valutato rischio 1, su una scala da 0 a 3 dove 0 rappresenta un rischio remoto, 1 un rischio basso, 2 un rischio medio e 3 un rischio alto.

C.5 I PROTOCOLLI LE PROCEDURE E I REGOLAMENTI

Al fine di poter dare compiutezza tramite protocolli, procedure e regole comportamentali alle misure di prevenzione di cui al capitolo precedente, ed in generale a tutto quanto dettagliato nella presente sezione, si definiscono i seguenti protocolli che formano parte integrante della parte speciale, come segue:

1)Approvazione di un regolamento definito come Regolamento R.I.C.A.V.P., Regolamento di comportamento da adottare in caso di Ispezione e Controllo da parte di Autorità di Vigilanza Pubbliche - riferimento procedura del Sistema Qualità Apiservizi: **SP018**

2)Approvazione di un protocollo Amministrazione, Conservazione Documenti, Area Contabile e Finanziaria – riferimento procedura del Sistema Qualità Apiservizi: **SP023**

3)Approvazione di un protocollo per la costituzione di Associazione Temporanee di Scopo – riferimento procedura del Sistema Qualità Apiservizi: **SP021**

C.6 LE ISTRUZIONI E LE VERIFICHE DELL'ODV

Compiti dell'O.D.V., in riferimento all'osservanza e all'efficace applicazione del Modello in materia di reati di Omessa comunicazione alle autorità di vigilanza, sono:
a)il puntuale riscontro del rispetto dei Protocolli e dei Regolamenti così come individuato nel capitolo precedente;
b)la somministrazione di Check list con cadenza stabilita dall'O.D.V. circa il puntuale rispetto di quanto indicato nella presente parte speciale;
c)la risoluzione di eventuali dubbi interpretativi, posti dai destinatari, sul Modello e sui principi previsti dalla Parte Speciale.

Qualora emergessero, dagli accertamenti posti in essere dall'O.D.V., elementi tali da far risalire alla violazione dei principi e dei protocolli contenuti nella Parte Speciale, alla commissione del reato o al tentativo di commissione del reato, l'O.D.V. dovrà riferire al Consiglio Direttivo e al Collegio dei Revisori, in modo tale che vengano adottati gli opportuni provvedimenti di competenza.

L'O.d.V. dovrà inoltre tenere in evidenza e verificare:
1) le Segnalazioni, da parte di soggetti destinatari o c.d. soggetti terzi, riguardanti in genere tutte le notizie relative alla presumibile commissione dei reati previsti dal Decreto in relazione all'attività dell'Ente o a comportamenti non in linea con le regole di condotta adottate dall'Ente stesso.

Rientrano nella tipologia di segnalazioni:
a) ordini ricevuti da un superiore e ritenuti in contrasto con la legge, o il codice Etico;
b) eventuali scostamenti significativi dal budget o anomalie di spesa emerse in fase di controllo di gestione o in altre attività similari;
c) omissioni, falsità o trascuratezze nella tenuta della contabilità o nella conservazione della documentazione dei registri contabili;

2) le Informazioni, relative ad atti ufficiali, riguardanti notizie utili per l'attività dell'O.d.V. (quali a titolo esemplificativo criticità o anomalie riscontrare nell'attuazione del Modello, notizie relative a mutamenti nell'organizzazione dell'Ente).

Rientrano nella tipologia di informazioni:
a) i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, relative allo svolgimento di indagini, anche nei confronti di ignoti, comunque concernenti l'Ente, per i reati previsti dal Decreto;
b) le richieste di assistenza legale inoltrate dagli amministratori e/o dagli altri dipendenti in caso di avvio di procedimento penale a carico degli stessi;
c) le notizie relative ai procedimenti disciplinari svolti e le eventuali sanzioni irrogate, ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
d) le decisioni relative alla richiesta di erogazioni di finanziamento pubblico;
e) gli aggiornamenti del sistema dei poteri (deleghe e procure);
f) i rapporti preparati nell'ambito delle proprie funzioni dai responsabili interni;
g) i report trimestrali delle gare pubbliche, bandi e convenzioni con Enti Pubblici cui l'Ente ha partecipato, nonché il prospetto riepilogativo delle commesse ottenute a seguito di trattativa privata;
h) le informazioni dalle quali possano emergere eventi con profili di criticità rispetto all'osservanza delle norme del Decreto e del Modello;
i) le comunicazioni da parte dell'Organo di Revisione relative alle criticità emerse anche se risolte;
l) verifiche periodiche sull'espletamento delle comunicazioni alle Autorità di Vigilanza e sull'esito di eventuali ispezioni effettuate dagli incaricati di queste ultime.

PARTE SPECIALE - D

I REATI CONTRO IL DIRITTO D'AUTORE
(art. 25-novies del D.Lgs. 231/2001)

D.1. INTRODUZIONE: I DESTINATARI DELLA PARTE SPECIALE PRINCIPI DI COMPORTAMENTO E ATTUAZIONE

Questa Parte Speciale definisce i comportamenti a cui i Destinatari, come già definiti nella Parte Generale, si atterranno nello svolgimento delle attività rientranti nelle c.d. Aree Sensibili o a Rischio, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente, così come prescritto in questa Parte Speciale al fine di prevenire e impedire il verificarsi di reati.
Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nel codice etico e nelle procedure operative interne.
Si precisa inoltre che destinatari del presente Allegato sono anche i membri delle Associazione Temporanee di Scopo di cui l'Ente è membro o ne diventerà membro.
In particolare, la presente Parte Speciale ha la funzione di:
a) fornire un elenco dei principi generali e dei principi procedurali specifici a cui i Destinatari, in relazione al tipo di rapporto in essere con l'Ente, sono tenuti ad attenersi per una corretta applicazione del Modello;
b) fornire al O.d.V., e ai responsabili delle altre funzioni dell'Ente chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

D.2 ELENCO REATI DIRITTI D'AUTORE

D.2.1 Definizione di Reati per Diritti d'Autore

Questa Parte Speciale definisce una serie di ipotesi di reato attinenti alla violazione del diritto d'autore. Il legislatore le ha introdotte quale reato presupposto della responsabilità degli enti con Legge 23 luglio 2009, n. 99, art. 15.
L'art. 25-novies contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (e, in particolare, dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies) quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'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.

D.2.2 Art. 25-novies Delitti in materia di violazione del diritto d'autore

Rientrano tra questi reati:
Legge 22 aprile 1941, n. 633, art. 171 primo comma, lettera *a-bis)*, e terzo comma, art 171-bis, art. 171-ter, art. 171-septies e art. 171-octies
Rischio reato: l'ente risulta esposto ad alcune di queste tipologie di reati e si è tutelato dal loro compimento come indicato nella parte speciale allegata al presente Modello Organizzativo.

Dopo attenta valutazione si è ritenuto di analizzare i seguenti reati, ai fini della tutela e prevenzione dell'Ente:

Art. 171
a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

Terzo comma:
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Fattispecie

Nella previsione della lettera a-bis) si prende in evidenza la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa, nel terzo comma, la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Nella prima ipotesi la tutela è rivolta all'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi non viene protetta l'aspettativa di guadagno del proprietario dell'opera, ma il suo onore e la sua reputazione.

Esemplificazioni di condotte illecite

Tale reato potrebbe ad esempio essere commesso nell'interesse dell'ente qualora venissero caricati sul sito Internet aziendale dei contenuti coperti dal diritto d'autore.

Art. 171-bis
1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.
2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della

multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

Fattispecie

Questo articolo tutela l'utilizzo di software e banche dati.
Per i software, è tutelata dell'abusiva duplicazione, dell'importazione, distribuzione, vendita e detenzione a scopo sia commerciale che imprenditoriale e locazione di programmi "piratati", quando gli stessi siano. contenuti in supporti non contrassegnati dalla SIAE, oppure ancora se la condotta ha ad oggetto qualsiasi mezzo che consente o facilita la rimozione, o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.
Il secondo comma punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.
Per la configurabilità del reato è sufficiente lo scopo di lucro: in questo modo assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Esemplificazioni di condotte illecite

Tale reato potrebbe ad esempio essere commesso nell'interesse dell'Ente qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un software originale.

Art. 171-ter
1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo

un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.
f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;
h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.
2. È punito con la reclusione da uno a quattro anni e con la multa da da euro 2.582 a euro 15.493 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-*bis*) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.
3. La pena è diminuita se il fatto è di particolare tenuità.
4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.
5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

Art. 171-septies
1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

Art. 171-octies

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi . visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.
2. La pena non è inferiore a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

D.3 LE AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale “F” del Modello, le seguenti:

- ✓ Per il Servizio Formazione accreditata presso Regione Lombardia o di altri enti pubblici;

Distribuzione di materiale soggetto alle disposizioni di cui alla seguente parte speciale rivolta gli utenti dei corsi di formazione messa a disposizione dai docenti dei corsi o dall’Ente.

- ✓ Per il Servizio Informatico dell’Ente

Utilizzo di materiale protetto o comunque sottoposto alle norme di tutela previste dalle norme in oggetto.
1) acquisto di prodotti non autentici;
2) caricamento sul sito Internet di contenuti coperti dal diritto d'autore.

- ✓ Per il servizio aggiornamento dell’Ente

Tale reato potrebbe ad esempio essere commesso nell’interesse dell’ente qualora venissero distribuiti nelle informazioni di aggiornamento rivolte a terzi, contenuti coperti dal diritto d'autore.

D.3.1 Le aree a rischio indiretto:

Costituiscono Aree a rischio indiretto:

A) Area Acquisti

Il processo di gestione degli acquisti di beni, costituisce una delle potenziali modalità attraverso la quale potrebbe essere commesso uno dei reati di cui alla presente parte speciale.

D.4 LE MISURE PER LA PREVENZIONE

D.4.1. Divieti

Premesso che nell’espletamento di tutte le attività operative attinenti la gestione di questa parte speciale oltre alle regole del presente Modello, dipendenti, collaboratori, fornitori, utenti dei servizi, dovranno conoscere e rispettare:
1. le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;

2. le procedure dell'Ente vigenti, la documentazione e gli ordini di servizio inerenti la struttura gerarchico funzionale ed organizzativa dell'Ente;
3. i divieti imposti dall'Ente sono indicati nei seguenti Regolamenti individuati al cap D.5 ai punti 1) e 2) .

La presente Parte Speciale si riferisce inoltre ai comportamenti posti in essere da Collaboratori Esterni e Partners. Per tale motivo occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

D.4.2. Principi procedurali

Premesso che nell'espletamento di tutte le attività procedurali attinenti la gestione di questa parte speciale presente Modello, dipendenti, collaboratori, fornitori, utenti dei servizi, dovranno conoscere e rispettare:
1. Ruoli e responsabilità definiti:
alle quali corrispondono le necessarie abilitazioni in ragione delle funzioni svolte all'interno dell'Ente.
2. Segregazione dei compiti e delle attività:
a garanzia della corretta gestione e del presidio continuativo sul processo di gestione da parte degli utenti.
3. Attività di controllo:
le attività di gestione sono soggette ad attività di controllo a garanzia della tracciabilità delle procedure utilizzate.
4. Tracciabilità del processo:
sia a livello di sistema informativo sia in termini documentali tutte le operazioni sono tracciabili attraverso sistematica registrazione degli eventi.

D.4.3. La Valutazione sul grado di pericolo della commissione del Rischio Reato

La valutazione del grado di pericolo della commissione del reato per questa sezione speciale può essere valutato rischio 1, su una scala da 0 a 3 dove 0 rappresenta un rischio remoto, 1 un rischio basso, 2 un rischio medio e 3 un rischio alto.

D.5 I PROTOCOLLI LE PROCEDURE E I REGOLAMENTI

Al fine di poter dare compiutezza tramite protocolli, procedure e regole comportamentali alle misure di prevenzione di cui al capitolo precedente ed in generale a tutto quanto dettagliato nella presente sezione speciale si definiscono i seguenti protocolli che formano parte integrante della seguente parte speciale come segue:

1)Approvazione di un regolamento definito come Regolamento R.S.I. - Regolamento e codice di condotta per l'utilizzo di Strumenti Informatici telefonici e fax – riferimento procedura del Sistema Qualità Apiservizi:**SP_016**

2)Approvazione di un regolamento protocollo uso materiale didattico e pubblicazioni su sito internet, acquisti informatici – riferimento procedura del Sistema Qualità Apiservizi: **SP_022**

D.6 LE ISTRUZIONI E LE VERIFICHE DELL'ODV

Compiti dell'O.D.V., in riferimento all'osservanza e all'efficace applicazione del Modello in materia di questa sezione speciale, sono:
a)il puntuale riscontro del rispetto dei Protocolli, delle Procedure e dei Regolamenti così come individuato nel capitolo precedente;
b)la somministrazione di Check list con cadenza stabilita dall'O.D.V. circa il puntuale rispetto di quanto indicato nella presente parte speciale;
c)la risoluzione di eventuali dubbi interpretativi posti dai destinatari sul Modello e sui principi previsti dalla Parte Speciale;

Qualora emergessero, dagli accertamenti posti in essere dall'O.D.V., elementi tali da far risalire alla violazione dei principi e dei protocolli contenuti nella Parte Speciale, alla commissione del reato o al tentativo di commissione del reato, l'O.D.V. dovrà riferire al Consiglio Direttivo e al Collegio dei Revisori, in modo tale che vengano adottati gli opportuni provvedimenti di competenza.

L'O.d.V. dovrà inoltre tenere in evidenza e verificare:
1) le Segnalazioni, da parte di soggetti destinatari o c.d. soggetti terzi, riguardano in genere tutte le notizie relative alla presumibile commissione dei reati previsti dal Decreto in relazione all'attività dell'Ente o a comportamenti non in linea con le regole di condotta adottate dall'Ente stesso.

Rientrano nella tipologia di segnalazioni:
a) ordini ricevuti da un superiore e ritenuti in contrasto con la legge, o il codice Etico;
b) eventuali scostamenti significativi del budget o anomalie di spesa emerse in fase di controllo di gestione o in altre attività similari;
c) omissioni, falsità o trascuratezze nella tenuta della contabilità o nella conservazione della documentazione dei registri contabili;
d) qualsiasi scostamento riscontrato nel processo di valutazione delle offerte rispetto a quanto previsto dalle procedure dell'ente o a criteri predeterminati.

2)Le Informazioni, relative ad atti ufficiali, riguardano notizie utili per l'attività dell'O.d.V. (quali a titolo esemplificativo criticità o anomalie riscontrare nell'attuazione del Modello, notizie relative a mutamenti nell'organizzazione dell'Ente).

Rientrano nella tipologia di segnalazioni:
a) i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o a qualsiasi altra autorità, relative allo svolgimento di indagini, anche nei confronti di ignoti, comunque concernenti l'Ente per i reati previsti dal Decreto;
b) le richieste di assistenza legale inoltrate dagli amministratori e/o dagli altri dipendenti in caso di avvio di procedimento penale a carico degli stessi;
c) le notizie relative ai procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
d) gli aggiornamenti del sistema dei poteri (deleghe e procure);
e) i rapporti preparati nell'ambito delle proprie funzioni dai responsabili interni;
f) le informazioni dalle quali possano emergere eventi con profili di criticità rispetto all'osservanza delle norme del Decreto e del Modello;
g) le comunicazioni da parte del dell'Organo di Revisione relative alle criticità emerse anche se risolte.

PARTE SPECIALE - E

I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

(art. 25-septies del D.Lgs. 231/2001)

E.1 TIPOLOGIA REATI PER OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

La Legge 123/2007 ha introdotto l'art. 25 septies del D.Lgs. 231/01 che estende la responsabilità amministrativa degli enti ai reati per omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

L'intera legge 123/2007 è oggi confluita nel TUS ("Testo Unico per la Sicurezza", D.Lgs. 81/2008), che funge da riferimento anche ai fini della regolamentazione della disciplina della responsabilità penale delle imprese. L'art. 30 del TUS funge da raccordo con la precedente normativa, disciplinando il rapporto che deve esistere tra i modelli di organizzazione, gestione e controllo e la prevenzione dei reati per omicidio colposo e lesioni gravi e gravissime.

L'art. 30 del TUS ha inoltre fornito le linee guida per la definizione dei modelli di organizzazione e gestione secondo il D.Lgs. 231/2001, con riferimento alla prevenzione dei reati commessi con violazione delle norme sulla salute e sicurezza sul posto di lavoro, assicurando un modello per il corretto adempimento di tutti gli obblighi giuridici relativi (rispetto standard tecnico-strutturali del luogo di lavoro; valutazione rischi e attività di prevenzione; attività organizzativa, di sorveglianza e vigilanza in merito alla sicurezza dei lavoratori; obblighi di verifica periodica del rispetto e dell'efficacia delle procedure adottate, etc.).

E.2 ELENCO REATI

Si elencano di seguito i testi degli articoli del codice penale, considerati dall'art.25-septies del D.Lgs. 231/01:

Art. 589 c.p. OMICIDIO COLPOSO
Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a cinque anni. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni dodici.

Art. 590, comma 3 c.p. LESIONI PERSONALI COLPOSE
(terzo comma) Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da

euro 500,00 a euro 2.000,00 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

Fattispecie

Rispetto ai criteri di imputazione soggettiva previsti per le altre figure delittuose richiamate dal D.Lgs. 231/2001, tutte punite a titolo di dolo, per la prima volta viene prevista la responsabilità degli enti per reati di natura colposa; infatti, ai fini della configurabilità dei reati ex art. 25 septies, non è necessario che il soggetto attivo abbia agito con intenzione o coscienza di cagionare un evento lesivo, essendo sufficiente: la semplice negligenza, imperizia o imprudenza dello stesso; l'inosservanza di leggi, regolamenti, ordini o discipline; la violazione delle norme sulla prevenzione degli infortuni sul lavoro o relative alla salute e all'igiene sul lavoro, configurandosi in questo modo un interesse o un vantaggio dell'ente.

La fattispecie dei due reati si realizza nel caso l'ente tragga beneficio o vantaggio nel non utilizzo delle necessarie risorse economiche in materia di sicurezza sul lavoro, esponendo i lavoratori a rischi inutili, in quanto facilmente evitabili con l'adozione di misure preventive e precauzionali previste dalla normativa.

È considerata "lesione" il complesso degli effetti patologici costituenti una malattia, nello specifico le alterazioni organiche e funzionali conseguenti all'accadimento di una condotta violenta: è da considerare "grave" se la malattia ha messo in pericolo la vita della vittima, se ha indotto un periodo di convalescenza oltre i 40 giorni, ovvero ha avuto per conseguenza l'indebolimento permanente della potenzialità funzionale di un senso o di un organo. È da considerare "gravissima" se la condotta ha determinato una malattia probabilmente insanabile (con effetti permanenti non curabili) o ha cagionato la perdita totale di un senso, di un arto, della capacità di parlare correttamente o di procreare, la perdita dell'uso di un organo ovvero ha deformato o sfregiato il volto della vittima.

L'evento dannoso (lesione grave o gravissima o dalla morte), può essere perpetrato tramite un comportamento attivo (si pone in essere una condotta lesiva), ovvero mediante un atteggiamento omissivo/passivo (non si interviene a impedire l'evento dannoso che si avrebbe il dovere giuridico di impedire).

Il soggetto risponde della propria condotta colposa nel caso in cui, rispetto alla vittima, si ponga in una posizione di garanzia (se ha, cioè, il dovere giuridico di impedire l'evento lesivo): la legge individua il datore di lavoro come garante "dell'integrità fisica e della personalità morale dei prestatori di lavoro". Tale status è trasferibile ad altri soggetti (apicali e/o a lui subordinati), mediante atto scritto a patto che il prescelto a ricoprire l'incarico abbia le skills necessarie per gestire il trasferimento di responsabilità.
Si conferma quindi che le attività "a rischio" possono riferirsi a chiunque sia tenuto ad osservare o far osservare la norme di prevenzione e protezione del lavoro (datori di lavoro, dirigenti, preposti, soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché in generale nei medesimi lavoratori).

In questa situazione, in caso di evento lesivo, solitamente si individua una condotta attiva nel soggetto delegato che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva è usualmente identificabile nel soggetto delegante che non ottempera agli obblighi di vigilanza e controllo (ad es. datore di lavoro, dirigente, preposto) e in tal modo non interviene ad impedire l'evento.

Esempi:
-Si potrebbe ipotizzare una delibera dell'Ente che comporti l'approvazione di un budget di spesa palesemente insufficiente ai necessari interventi in materia di sicurezza sul lavoro, con l'implicita finalità di trarre un vantaggio illecito mediante il risparmio delle risorse necessarie per la sicurezza.

-Mancata informazione, formazione ed addestramento dei lavoratori sulle procedure e/o istruzioni relative alla sicurezza sul posto di lavoro al fine di risparmiare risorse finanziarie.

E.3 LE AREE E LE ATTIVITÀ A RISCHIO

Sulla base delle analisi condotte, risulta un quadro di APISERVIZI VARESE srl sostanzialmente poco esposto a rischi: considerando i risultati e le conclusioni del documento sulla valutazione dei rischi elaborato dall'Ente, anche in considerazione del fatto che le attività di API consistono essenzialmente in mansioni di concetto (di rappresentanza, amministrative, formative, ecc…), è stato rilevato che la situazione complessiva della sede e degli uffici in cui il medesimo ente opera non presenta particolari rischi e/o carenze tali da mettere a repentaglio la sicurezza e la salute dei lavoratori.

Tale conclusione si riferisce sia ai rischi strutturali, elettrici o di macchinari e servizi, sia a quelli di organizzazione del lavoro, sia a quelli normalmente collegati a fattori come gli agenti biologici, chimici o fisici oppure a fattori ergonomici o psicologici. Con riferimento, poi, all'individuazione delle misure di prevenzione e di protezione, sulla base del predetto documento sulla valutazione dei rischi, risultano pienamente valorizzati i principi ergonomici nella concezione dei posti di lavoro, nella scelta delle attrezzature e, in generale, nella definizione dei metodi di lavoro e produzione, anche per attenuare il lavoro monotono e quello ripetitivo. L'analisi delle misure definite sembra, inoltre, rispettare anche gli ulteriori seguenti criteri: priorità delle misure di protezione collettiva rispetto a quelle di protezione individuale; misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori; uso di segnali di avvertimento e di sicurezza, regolare manutenzione di ambienti, attrezzature, macchine ed impianti.

È stato previsto un "Sistema di registrazione dell'avvenuta effettuazione delle attività di cui ai comma 1 e 2 dell'art. 30 del D.Lgs. 81/08 e s.m.i." per verificarne lo stato di efficienza, adeguatezza e funzionalità, nonché un programma di revisione periodica della valutazione dei rischi effettuata. Infine, è stata anche prevista la messa in opera di un piano di informazione e formazione dei lavoratori. Si riportano per conoscenza i primi due comma dell'art.30 e l'art. 28 del D.Lgs. 81/08.

Art. 30. Modelli di organizzazione e di gestione
1. Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:
a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d) alle attività di sorveglianza sanitaria;
e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

Art. 28.Oggetto della valutazione dei rischi
1. La valutazione di cui all'articolo 17, comma 1, lettera a),anche nella scelta delle attrezzature di lavoro e delle sostanze o dei preparati chimici impiegati, nonchè nella sistemazione dei luoghi di lavoro, deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui anche quelli collegati allo stress lavoro-correlato, secondo i contenuti dell'accordo europeo dell'8 ottobre 2004, e quelli riguardanti lelavoratrici in stato di gravidanza, secondo quanto previsto dal decreto legislativo 26 marzo 2001, n. 151, nonché quelli connessi alle differenze di genere, all'eta', alla provenienza da altri Paesi.
2. Il documento di cui all'articolo 17, comma 1, lettera a), redatto a conclusione della valutazione, deve avere data certa e contenere:
a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa; b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a); c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza; d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio; f) individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.
3. Il contenuto del documento di cui al comma 2 deve altresì rispettare le indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nei successivi titoli del presente decreto.

Con riferimento, quindi, all'individuazione delle attività a rischio astrattamente riscontrabili nel contesto APISERVIZI VARESE srl, si rileva che tali attività, nelle loro specifiche e potenziali modalità attuative dei reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione degli obblighi di tutela della salute e sicurezza sul lavoro, corrispondono, di fatto, a quelle risultanti dalla valutazione dei rischi lavorativi effettuata, ai sensi dell'art. 28 del Testo Unico in materia di sicurezza sul lavoro di cui al D.Lgs. n. 81/2008, da APISERVIZI VARESE srl e contenute nel Documento sulla Valutazione dei Rischi.

L'elemento essenziale ed unificante delle varie e possibili forme di responsabilità e delle relative aree di rischio per l'ente è quindi rappresentato, in estrema sintesi, dalla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili, alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche, nonché nel mancato rispetto delle regole di sicurezza che l'ente si è dato con riferimento alle predette e già valutate situazioni a rischio.

E.4 LE MISURE PER LA PREVENZIONE

L'Ente deve garantire il rispetto della disciplina in tema di salute e sicurezza sul lavoro, assicurando, in generale, un ambiente sano, sicuro e idoneo allo svolgimento dell'attività lavorativa. Quanto sopra con riferimento all'art. 30, comma 1 e 2 del D.Lgs. 81/08 e riassumibile inoltre tramite:

- la valutazione dei rischi per la sicurezza e la salute;
- la definizione di un programma di prevenzione;
- l'eliminazione del rischio o, dove non possibile, la sua riduzione al minimo;
- la valutazione dello stress da lavoro correlato;
- la manutenzione delle attrezzature antincendio;
- prove di evacuazione;
- aggiornamenti formativi per i RLS;
- verifica dell'impianto di messa a terra;
- prevenzione dagli incendi;
- il controllo sanitario dei lavoratori (visite mediche);
- la formazione e l'addestramento adeguato dei Destinatari, attraverso riunioni periodiche;
- l'uso di segnali di avvertimento e sicurezza;
- la regolare manutenzione di ambienti e attrezzature;

Tali misure non devono in alcun caso comportare oneri finanziari per lavoratori.

E.4.1. Principi Generali di Comportamento

In linea generale, ogni soggetto destinatario del Modello dovrà attenersi ai seguenti principi di comportamento:

- tutelare la salute e la sicurezza dei dipendenti e dei terzi eventualmente presenti a prescindere da qualsiasi considerazione economica;
- valutare gli effetti delle proprie condotte in relazione al rischio di infortuni sul lavoro, non adottando comportamenti imprudenti quanto alla salvaguardia della propria salute e della propria sicurezza ed evitando di compiere attività che non siano di propria competenza ovvero suscettibili di compromettere la sicurezza propria, di altri dipendenti, ovvero di soggetti terzi;
- contribuire attivamente all'adempimento degli obblighi previsti a tutela della salute e della sicurezza, partecipando inoltre ai programmi di formazione e di addestramento organizzati dall'Ente e utilizzando in modo appropriato i dispositivi di protezione ricevuti in dotazione;
- rispettare normativa e procedure aziendali interne per la protezione individuale e collettiva, osservando inoltre le disposizioni impartite dal datore di lavoro, dai dirigenti della sicurezza e dai preposti;
- segnalare immediatamente al proprio responsabile, le deficienze dei mezzi e dei dispositivi di sicurezza, adoperandosi direttamente per eliminare o ridurre (nei limiti delle proprie funzioni e competenze e senza incorrere in pericoli) le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- sottoporsi ai controlli sanitari previsti ai sensi di legge o comunque disposti dal medico competente;
- utilizzare correttamente le attrezzature di lavoro;
- non rimuovere e modificare (senza autorizzazione) i dispositivi di sicurezza/segnalazione/ controllo esistenti sulle attrezzature o nei luoghi di lavoro.

E.4.2. Soggetti destinatari e soggetti dedicati a compiti in materia di sicurezza

Devono ritenersi destinatari di tali principi generali:
- tutti i dipendenti;
- tutti i dirigenti e organi sociali;

- tutti i soggetti che ricoprono compiti in materia di tutela della sicurezza (medico competente, RLS, ecc.);
- prestatori esterni di servizi all'interno delle aree aziendali;
- lavoratori di società appaltatrici che operino all'interno delle aree aziendali;
- altri collaboratori occasionali;
- visitatori degli uffici;
- i partecipanti ai corsi di formazione.

I soggetti, che hanno un ruolo di rilievo per la tutela della sicurezza e della salute sul posto di lavoro, sono:
- datore di lavoro, per i compiti da questo non delegabili;
- procuratori del datore di lavoro, per i compiti da questo delegabili;
- l' RLS;
- l'R.S.P.P.;
- il medico competente;
- addetti antincendio;
- addetti primo soccorso;
- O.d.V.

I destinatari sono tenuti in generale, oltre a conoscere le regole generali presenti in tale modello, a rispettare tutti i principi e le direttive contenuti:
- nel Codice Etico;
- nelle attività organizzative di informazione, formazione, sorveglianza riferite alla tutela generale del lavoro;
- nelle procedure operative vote a garantire l'attuazione delle direttive in materia di tutela della sicurezza sul lavoro.

A parti terze, partner, fornitori, consulenti, partecipanti ai corsi di formazione, deve essere nota l'adozione del presente Modello Organizzativo e del Codice Etico da parte dell'Ente.

E.5 I PROTOCOLLI LE PROCEDURE E I REGOLAMENTI

Al fine di poter dare compiutezza tramite protocolli, procedure e regole comportamentali alle misure di prevenzione di cui al capitolo precedente ed in generale a tutto quanto dettagliato nella presente sezione speciale si definiscono i seguenti protocolli che formano parte integrante della seguente parte speciale:

1) Sistema di registrazione dell'avvenuta effettuazione delle attività di cui ai comma 1 e 2 dell'art. 30 del D. Lgs. 81/08 e s.m.i. – riferimento del Sistema Qualità Apiservizi: **ELE_037**

2) Organigramma della Sicurezza, delle persone incaricate della gestione e dell'esecuzione delle differenti attività della sicurezza, con specificazione delle funzioni e dei ruoli – riferimento del Sistema Qualità Apiservizi:**SP_004**

E.6 LE ISTRUZIONI E LE VERIFICHE DELL'ODV

Compiti dell'O.D.V., in riferimento all'osservanza e all'efficace applicazione del Modello in materia di reati di lesioni gravi o omicidio colposo, sono:

a)il puntuale riscontro del rispetto delle protocolli e delle scadenze, così come individuato nel capitolo precedente;
b)la somministrazione di Check list con cadenza stabilita dall'O.D.V. circa il puntuale rispetto di quanto indicato nella presente parte speciale;
c)la risoluzione di eventuali dubbi interpretativi posti dai destinatari sul Modello e sui principi previsti dalla Parte Speciale;
d)la conservazione e l'archiviazione della documentazione relativa all'attività di controllo svolta nelle aree di rischio segnalate nella Parte Speciale per almeno 10 anni.
Qualora emergessero, dagli accertamenti posti in essere dall'O.D.V., elementi tali da far risalire alla violazione dei principi e dei protocolli contenuti nella Parte Speciale, alla commissione del reato o al tentativo di commissione del reato, l'O.D.V. dovrà riferire al Consiglio Direttivo e al Collegio dei Revisori, in modo tale che vengano adottati gli opportuni provvedimenti di competenza.

L'O.d.V. dovrà inoltre tenere in evidenza e verificare:
1) le Segnalazioni, da parte di soggetti destinatari o c.d. soggetti terzi, riguardanti in genere tutte le notizie relative alla presumibile commissione dei reati previsti dal Decreto in relazione all'attività dell'Ente o a comportamenti non in linea con le regole di condotta adottate dall'Ente stesso.

Rientrano nella tipologia di segnalazioni:
a) ordini ricevuti da un superiore e ritenuti in contrasto con la legge, o il codice Etico;
b) eventuali scostamenti significativi del budget o anomalie di spesa emerse in fase di controllo di gestione o in altre attività similari;
c) omissioni, falsità o trascuratezze nella tenuta della contabilità o nella conservazione della documentazione e dei registri anche inerenti la sicurezza sul luogo dilavoro;
d) segnalazioni concernenti inadeguatezze dei luoghi o delle attrezzature di lavoro, ovvero dei dispositivi di protezione individuali o collettivi;

2)Le Informazioni, relative ad atti ufficiali, riguardanti notizie utili per l'attività dell'O.d.V. (quali a titolo esemplificativo criticità o anomalie riscontrare nell'attuazione del Modello, notizie relative a mutamenti nell'organizzazione dell'Ente).

Rientrano nella tipologia di segnalazioni:
a) i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o a qualsiasi altra autorità, relative allo svolgimento di indagini, anche nei confronti di ignoti, comunque concernenti l'Ente per i reati previsti dal Decreto;
b) le richieste di assistenza legale inoltrate dagli amministratori e/o dagli altri dipendenti in caso di avvio di procedimento penale a carico degli stessi;
c) le notizie relative ai procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
d) gli aggiornamenti del sistema dei poteri (deleghe e procure);
e) i rapporti preparati nell'ambito delle proprie funzioni dai responsabili interni;
f) le informazioni dalle quali possano emergere eventi con profili di criticità rispetto all'osservanza delle norme del Decreto e del Modello.
g) le comunicazioni da parte dell'Organo di Revisione relative alle criticità emerse anche se risolte;
h) la reportistica periodica in materia di salute e sicurezza sul lavoro e in particolare il verbale di cui all'art. 35 del D.Lgs. 81/2008;
i) i dati relativi agli infortuni occorsi presso l'Enti.