MODELLO ORGANIZZATIVO

Ai sensi del D. Lgs 231/2001

Parte Generale

INDICE

1. Overview del Decreto e della normativa rilevante.

In data 8 giugno 2001 è stato emanato il Decreto legislativo n. 231 ("D. Lgs. 231/2001"), che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali a cui l'Italia ha già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione del 26 maggio 1997, anch'essa firmata a Bruxelles, sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il D. Lgs. 231/2001, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti per alcuni Reati commessi nell'interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

La nuova responsabilità introdotta dal D. Lgs. 231/2001 mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio delle società che abbiano tratto un vantaggio dalla Commissione del Reato. Per tutti gli illeciti commessi è sempre prevista l'applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione (di seguito P.A.), l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi. Quando si parla di Reati previsti dal D. Lgs. 231/2001 ("Reati"), ci si riferisce sia ai Reati originariamente previsti (Reati nei confronti della P.A.), sia alle ipotesi successivamente introdotte (falsità in monete, in carte di pubblico credito e in valori di bollo e Reati societari).

Gli articoli 6 e 7 del D. Lgs. 231/2001 prevedono, tuttavia, una forma di esonero dalla responsabilità qualora l'azienda dimostri di aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo (i "Modelli") idonei a prevenire la realizzazione degli illeciti penali considerati.

Il sistema prevede, inoltre, l'istituzione di un organo di controllo interno all'azienda con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curarne l'aggiornamento. I suddetti Modelli dovranno rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi Reati previsti dal D. Lgs. 231/2001;
- prevedere specifici protocolli (i.e. procedure) diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai Reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali Reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

E' opportuno specificare che, ove il Reato sia stato commesso da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'azienda o di una sua unità organizzativa dotata di

autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'azienda non risponde se prova che:

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

Nel caso invece in cui il Reato sia stato commesso da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'azienda è responsabile se la commissione del Reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Tale inosservanza è in ogni caso esclusa se l'azienda, prima della commissione del Reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire Reati della specie di quello verificatosi.

1.1. I Reati nei confronti della Pubblica Amministrazione.

Quanto alla tipologia di Reati cui si applica la disciplina in esame, il D. Lgs. 231/2001 si riferisce, innanzitutto, a quelli commessi nei rapporti con la P.A. e precisamente:

- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter c.p.);
- Truffa in danno dello Stato o di altro ente pubblico (art. 640, 2° comma, n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- Corruzione per un atto d'ufficio (art. 318 c.p.);
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- Corruzione in atti giudiziari (art. 319-ter c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Concussione (art. 317 c.p.);
- Malversazione a danno dello Stato o di altro ente pubblico (art. 316- bis c.p.).

Successivamente, l'art. 6 della legge 23 novembre 2001, n. 409 ha inserito nel D. Lgs. 231/2001 l'art. 25-bis, in tema di “falsità in monete, in carte di pubblico credito e in valori di bollo”.

1.2. I Reati societari.

Inoltre, il Consiglio dei Ministri ha approvato in data 28 marzo 2002 il decreto legislativo n. 61, introducendo, con un nuovo articolo del D. Lgs. 231/2001, il 25-ter, la punibilità dei c.d. Reati societari commessi nell'interesse delle società e l'applicazione di sanzioni pecuniarie in capo alle stesse in caso di mancata adozione di modelli organizzativi e gestionali idonei a prevenirli. Di seguito indichiamo le fattispecie previste dal Decreto Legislativo n. 61/2002, che comportano la responsabilità amministrativa dell'azienda nel caso in cui, in seguito alla commissione di uno di detti Reati, l'azienda abbia conseguito una qualsiasi utilità:

- False comunicazioni sociali (art. 2621 c.c.);
- False comunicazioni sociali in danno dei soci o dei creditori (art. 2622 c.c.);
- Falso in prospetto (art. 2623 c.c.);
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.);

- Impedito controllo (art. 2625 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

In relazione ai su menzionati Reati societari si precisa che in caso di responsabilità della società, allo stesso verranno applicate unicamente le sanzioni pecuniarie specificamente previste dal decreto, con esclusione quindi delle sanzioni interdittive previste per le altre ipotesi di Reato.

1.3. Delitti aventi finalità di terrorismo e di eversione dell'ordine democratico (art. 25-quater).

I Reati di azione e di fiancheggiamento materiale non sembrano ipotizzabili. In particolare si fa qui riferimento al Reato di associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.). Ne sono configurabili aree di rischio ascrivibili ai Reati di assistenza agli associati (art. 270 ter c.p.), arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.), addestramento ad attività e condotte con finalità di terrorismo (artt. 270 quinquies e sexies c.p.), né i successivi Reati previsti dagli artt. 280, 280 bis, 289 bis, 302 del c.p.

1.4. Delitti e illeciti finanziari introdotti nel regolamento mercati come allegato V, nel quadro della revisione della normativa finanziaria conseguente all'emanazione della legge comunitaria 2004 (art. 25-sexies)

Si fa riferimento ai Reati di abuso di informazioni privilegiate (art. 184 e 187-bis TUIF) e di manipolazione del mercato (art. 185 e 187-ter TUIF). Anche questa classe di Reati non sembra ipotizzabile. Si descrivono brevemente qui di seguito le fattispecie di Reati contemplate nel quadro della revisione della normativa finanziaria conseguente all'emanazione della legge comunitaria 2004 (TUIF).

Abuso di informazioni privilegiate (art. 184 e 187-bis TUIF)

Il dolo consiste nella coscienza e volontà di utilizzare informazioni privilegiate compiendo operazioni su strumenti finanziari o nel raccomandare ad altri il compimento di tali operazioni, comunicando tali informazioni al di fuori dei propri ordinari compiti professionali.

Manipolazione del mercato (art. 185 e 187-ter TUIF)

Il Reato consiste nella diffusione di notizie false e nella effettuazione di operazioni simulate od altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

1.5. Reati transnazionali ex art. 10, legge n. 146/2006

In riferimento ai Reati di "Associazione per delinquere" (art. 416 c. p.), "Associazione di tipo mafioso" (art. 416 bis c. p.), "Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri" (art. 291 quater, DPR 43/1973), "Associazione finalizzata al traffico di sostanze stupefacenti o psicotrope" (art 74, DPR 309/1990), "Disposizioni contro le immigrazioni clandestine (Art. 12 d.lgs 25 luglio 1998, n.286)", "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria (Art. 377-bis c.p.)", "Favoreggiamento personale (Art.378 c.p.)", "Riciclaggio (Art. 648-bis c.p.)", "Impiego di

denaro, beni o utilità di provenienza illecita (Art. 648-ter c.p.)", è difficilmente ipotizzabile un'ipotesi di Reato.

1.6. Reati di Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, ex art. 25 septies

In relazione al delitto di cui all'articolo 589 del codice penale e all'articolo 590 del c.p., commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, con le eventuali circostanze aggravanti previste dall'art. 583 del c.p.

1.7. Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ex art. 25 octies

In relazione ai Reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648-bis c.p.) ed impiego di denaro, beni e utilità di provenienza illecita (art. 648-ter c.p.).

1.8. Delitti in materia di violazione del diritto d'autore ex art. 25 novies

In relazione alla commissione dei delitti previsti dagli articoli 171, 171-bis, 171-ter, 171-septies e 171-octies, 174, della legge 22 aprile 1941, n. 633, relativi alla protezione del diritto d'autore e di altri diritti connessi al suo esercizio.

1.9. Pratiche di mutilazione degli organi genitali femminili (art. 25-quater. 1).

Il riferimento in tale caso è da ascriversi alla commissione dei delitti di cui all'articolo 583-bis del codice penale.

1.10. Delitti contro la personalità individuale (art. 25- quinquies.).

L'articolo 25-quinquies del decreto 231 "I Delitti contro la personalità individuale" ha recepito la legge 11 agosto 2003, n. 228 - Misure contro la tratta di persone - e, successivamente la Legge 6 febbraio 2006, n. 38 - Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet. Tale tipologia di reati non è ipotizzabile nel caso specifico in esame.

1.11. Delitti in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria ex art. 25 decies

In relazione alla commissione dei delitti previsti dall'art. 377 bis del c.p, relativo all'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

1.12. Reati Ambientali ex art. 25 undecies

In relazione alla commissione dei Reati per la violazione degli articoli 727-bis e 733-bis del codice penale; per la violazione degli articoli 137, 256, 257, 258, 259, 260, 260-bis e 279 previsti dal decreto legislativo 3 aprile 2006, n. 152; per la violazione degli articoli 1 e 3-bis previsti dalla legge 7 febbraio 1992, n. 150; per la violazione dell'articolo 3 della legge 28 dicembre 1993, n. 549; per la violazione degli articoli 8 e 9, del decreto legislativo 6 novembre 2007, n. 202.

1.13. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare Art. 25-duodecies

In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286.

1.14. Corruzione tra privati art. 25 – ter

In relazione ai reati previsti dall'articolo 25 - ter, comma 1, lett. s-bis) del decreto legislativo 231/2001 e dell' art. 2635 c.c.

2. Linee guida.

In data 7 marzo 2002, poi aggiornate a marzo 2008 e marzo 2014, Confindustria ha approvato il testo definitivo delle proprie "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001" che possono essere schematizzate secondo i seguenti punti fondamentali:

- Individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione degli eventi pregiudizievoli previsti dal D. Lgs. 231/2001;
- Predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di appositi protocolli. Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:
  - codice etico;
  - sistema organizzativo;
  - procedure manuali ed informatiche;
  - poteri autorizzativi e di firma;
  - sistemi di controllo e gestione;
  - comunicazione al personale e sua formazione.

Le componenti del sistema di controllo devono essere informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del codice etico e delle procedure previste dal modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione.

E' opportuno evidenziare che il mancato rispetto di punti specifici delle Linee Guida di Confindustria non inficia la validità del Modello. Il singolo Modello infatti, dovendo essere redatto con riferimento alla realtà concreta dell'azienda, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

3. La Fondazione

Il Centro Europeo di Fomazione e Ricerca in Ingegneria Sismica (EUCENTRE), come previsto nell'Articolo 2 dello Statuto, si propone di promuovere, sostenere e curare la formazione e la ricercar nel campo della riduzione dei rischi naturali e antropici, nonché più in generale nel campo della protezione civile, anche attraverso le seguenti azioni:

- lo sviluppo della ricerca applicata, orientata a conseguire concreti obiettivi in ordine alla valutazione ed alla riduzione della vulnerabilità e del rischio;
- lo sviluppo di attività utili alla definizione di specifiche linee di azione pubblica, di atti di indirizzo, di linee guida nonché di documenti a carattere normativo, anche in riferimento allo stato dell'arte internazionale;
- la formazione di operatori aventi spiccate capacità scientifiche e professionali, anche in situazioni di emergenza;
- lo svolgimento di attività di consulenza scientifica e tecnologica, a livello nazionale ed internazionale.

Come indicato nell'Art.6 dello Statuto sono **organi** della Fondazione:

a) il Consiglio di Amministrazione
b) il Presidente
c) il Comitato scientifico
d) il Collegio dei Revisori dei conti

In base all'Art. 7 dello Statuto i componenti del **Consiglio di Amministrazione** sono:

a) il Capo del Dipartimento della protezione civile della Presidenza del Consiglio dei Ministri o persona da lui nominata;
b) il Presidente dell'Istituto Nazionale di Geofisica e Vulcanologia o persona da lui nominata
c) il Rettore dell'Università degli Studi di Pavia o persona da lui nominata
d) il Rettore dell'Istituto Universitario di Studi Superiori di Pavia o persona da lui nominata
e) il Presidente della Fondazione Eucentre.

Spetta al Consiglio di Amministrazione (Art.8):

1) nominare il Presidente
2) nominare i componenti di propria competenza del Comitato scientifico
3) nominare il Responsabile del TREES Lab e il Rettore del CAR College
4) deliberare sul rendiconto economico e finanziario, sul documento finanziario programmatico triennale, sui bilanci preventivi e consuntivi;
5) approvare i regolamenti necesssari al funzionamento della Fondazione, del Laboratorio e del Collegio;
6) approvare le convenzioni tipo che regolano i rapporti con i sostenitori, industriali e professionisti
7) fissare i criteri per l'utilizzo delle apparecchiature del TREES Lab, su proposta del responsabile del laboratorio
8) assumere o licenziare, su proposta del Presidente, il personale della Fondazione e fissarne gli emolumenti.
9) deliberare in ordine ai compensi di cui all'Art.13 dello Statuto

10) deliberare su tutto quanto concerne l'attuazione delle finalità della Fondazione, compiere gli atti di ordinaria e straordinaria amministrazione e adottare in generale tutti i provvedimenti ritenuti necessari per il perseguimento degli scopi della Fondazione

Il **Presidente** ha poteri di firma, rappresenta legalmente la Fondazione, ne sorveglia l'andamento amministrativo e morale, convoca e presiede le riunioni del Consiglio e cura l'esecuzione dei relativi deliberati. Sono compiti specifici del Presidente:

- redigere il rendiconto economico finanziario, il bilancio preventivo ed il documento finanziario programmatico triennale da sottoporre al Consiglio;
- redigere la relazione annuale sull'attività svolta da sottoporre al Consiglio, sentito il Comitato Scientifico;
- redigere gli eventuali regolamenti interni e la convenzione tipo che regola i rapporti con i Sostenitori, da sottoporre all'approvazione del Consiglio;
- attuare le finalità previste dallo statuto e le decisioni del Consiglio;
- deliberare in ordine all'utilizzo delle strutture e delle attrezzature della Fondazione;
- definire le tariffe da applicare per prestazioni esterne di qualsiasi natura.

Il Comitato Scientifico (Art.10) costituisce l'organo principale di riferimento per il Consiglio di Amministrazione, in relazione alle scelte strategiche da operare per il perseguimento degli scopi sociali. Il Comitato si esprime sugli aspetti connessi alle attività scientifiche e formative, anche in relazione all'istituzione di centri di ricerca, corsi di master e corsi di dottorato in convenzione con università italiane e straniere ed in particolare con l'Istituto Universitario di Studi Superiori di Pavia.
E' inoltre istituito il **Comitato dei Sostenitori** (Art.11), costituito dall'insieme degli enti pubblici, imprese e professionisti che si convenzionano con la Fondazione secondo uno o più docuemtni-tipo approvati dal Presidente del Consiglio di Amministrazione, i quali prevedono diritti e doveri dei Sostenitori.

Il **Collegio dei Revisori dei Conti** (Art.12) esamina i bilanci preventivi e consuntivi, predisponendo apposita relazione sulla gestione amministrativa e contabile, effettuando verifiche di cassa, accertano la regolare tenuta delle scritture contabili, vigilano sull'osservanza dello statuto.
La **Direzione Operativa** si occupa della gestione dei progetti in carico alla Fondazione a partire dal'affiancamento nelle proposte, alla presa in carico, al monitoraggio e alla valutazione ex post. Supporta il Presidente in operazioni di marketing e di benchmarking relative all'attività della Fondazione.

La **Direzione Scientifica** si occupa del coordinamento e monitoraggio scientifico delle attività di ricerca ed alta formazione.

4. Funzione e adozione del Modello.

4.1. Dichiarazione programmatica.

EUCENTRE è consapevole dell'opportunità di un sistema di controllo interno per la prevenzione della commissione di Reati da parte dei propri amministratori, dipendenti, collaboratori e partner. A tal fine, sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, EUCENTRE, in conformità con le sue politiche aziendali, ha adottato il presente Modello con la delibera del Consiglio di Amministrazione (di seguito C.d.a.) del 30 settembre 2015 e ha istituito l'Organo di Vigilanza interno ("Organismo di Vigilanza" o anche "OdV") con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento. L'adozione e l'efficace attuazione di tale sistema riduce il rischio di commissione dei Reati contemplati nel D. Lgs. 231/2001. A tal fine, EUCENTRE ha proceduto all'analisi delle proprie aree di rischio tenendo conto, nella stesura del presente Modello, delle prescrizioni del D. Lgs. 231/2001.

4.2. Modalità di modifica/integrazione del Modello.

Essendo il presente Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma I, lettera a del D. Lgs. 231/2001) le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del C.d.a, a cui è peraltro riconosciuta la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

4.3. Funzione del Modello.

Scopo del Modello è la costruzione di un sistema strutturato ed organico di procedure ed attività di controllo preventivo che abbia come obiettivo la prevenzione, per quanto possibile, dei Reati di cui al D.Lgs. 231/2001, mediante l'individuazione delle attività esposte a rischio di Reato e la loro conseguente proceduralizzazione. L'adozione delle procedure contenute nel presente Modello deve condurre, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito, illecito la cui commissione è fortemente condannata e contraria agli interessi della Fondazione anche quando apparentemente essa potrebbe trarne un vantaggio; dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire alla Fondazione di reagire tempestivamente nel prevenire od impedire la commissione del Reato. Punti cardine del Modello, oltre ai principi sopra indicati, sono:

1. la mappa delle attività sensibili della Fondazione, vale a dire delle attività nel cui ambito possono essere commessi i Reati previsti dal D. Lgs. 231/2001, custodita dall'Organismo di Vigilanza;
2. l'attribuzione all'Organismo di Vigilanza dei compiti di vigilanza sull'efficace e corretto funzionamento del Modello, come qui di seguito meglio descritto;
3. la verifica e l'archiviazione della documentazione, cartacea e/o digitale, di ogni operazione rilevante ai fini del D. Lgs. 231/2001 e la sua rintracciabilità in ogni momento;
4. il rispetto del principio della separazione delle funzioni nelle aree ritenute a maggior rischio;
5. la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
6. la messa a disposizione dell'Organismo di Vigilanza di risorse aziendali di numero e valore ragionevole e proporzionato ai risultati attesi e ragionevolmente ottenibili;
7. l'attività di monitoraggio dei comportamenti aziendali, nonché del Modello con conseguente aggiornamento periodico (controllo ex post, anche a campione)
8. l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali (proporzionale al livello di responsabilità) delle regole comportamentali e delle procedure istituite.

5. Attività sensibili.

Per le motivazioni esposte, la Fondazione ha ritenuto opportuno procedere all'attuazione del Modello di Organizzazione e gestione previsto dal D. Lgs. 231/01. Detta iniziativa è stata assunta nella convinzione che tale strumento possa migliorare la sensibilità di coloro che operano per conto della Fondazione sull'importanza di conformarsi non solo a quanto imposto dalla vigente normativa, ma anche ai principi deontologici a cui si ispira la Fondazione, allo scopo di svolgere la propria quotidiana attività ai massimi livelli di correttezza e trasparenza.

5.1. Risk assessment e gap analysis

Il Modello prende spunto e si fonda su un'analisi dei processi e sottoprocessi in cui si articola l'attività della Fondazione al fine di identificare le aree potenzialmente a rischio rispetto alla commissione dei Reati previsti dal D. Lgs. 231/2001 ed individuare, per tale via, quali tra tali Reati possano ritenersi strettamente connessi alle Attività sensibili ("Reati peculiari").

Sulla base dell'analisi svolta, sono stati identificati come peculiari i Reati contro la Pubblica Amministrazione (artt. 24 e 25 D. Lgs. 231/01), considerando che la Fondazione annovera numerosi rapporti con enti o soggetti appartenenti alla sfera pubblica. Rispetto alle funzionalità proprie del Modello, l'attività di analisi dei processi aziendali dovrà essere aggiornata almeno annualmente e comunque in occasione di ogni intervento normativo a modifica delle disposizioni contenute nel D. Lgs. 231/01 che possa aver impatto sulla definizione delle aree di rischio e in occasione di modifica dei processi aziendali.

Rimane facoltà dell'Organismo di Vigilanza richiedere in ogni momento lo svolgimento di specifiche analisi delle attività e dei processi aziendali. Per ciascuna fattispecie di Reato peculiare sono state individuate le attività aziendali nell'ambito delle quali potrebbe essere commesso il Reato stesso (Attività sensibili).

Alla luce di questa analisi, le attività ritenute più sensibili sono quelle in relazione ai Reati contro la P.A. da ricondurre in particolare allo svolgimento delle attività di ricerca che implicano l'uso di risorse pubbliche ed un rapporto con pubblici uffici, organi ispettivi, enti pubblici erogatori di contributi o titolari di poteri autorizzativi, concessori od abilitativi.

Secondariamente sono da evidenziare le attività sensibili afferenti l'area della gestione della Sicurezza del Lavoro con particolare riferimento allo svolgimento di attività presso il laboratorio.

L'attività di analisi dei processi aziendali ha consentito di individuare le attività sensibili in cui possa essere riscontrato il rischio di commissione dei Reati richiamati dal D. Lgs. 231/2001. Per ciascuna attività sensibile sono state identificate, oltre al "referente" attuale del singolo processo aziendale, le modalità operative e gestionali esistenti nonché gli elementi di controllo già presenti. Al fine di rilevare la capacità di rispondere ai requisiti imposti dal D. Lgs. 231/2001 è stata effettuata l'analisi comparativa ("gap analysis") tra il Modello Organizzativo e di controllo esistente e i principi del modello di riferimento definito ai sensi del D. Lgs. 231/2001. Propedeutica all'attività di gap analysis è l'elaborazione di Standard di Controllo (descritti nella Parte Speciale del presente documento) coerenti con i principi del modello organizzativo "a tendere", conforme alle previsioni del D. Lgs. 231/2001. A loro volta, gli Standard di Controllo sono elaborati sulla base delle categorie di attività sensibili individuate dalla metodologia di Progetto. Per quanto riguarda le aree di Reato relative ai Reati societari, "market abuse", Reati transnazionali e ai finanziamenti di attività aventi finalità di terrorismo e di eversione dell'ordine democratico, riciclaggio e ricettazione, nell'ente non sono state rilevate particolari attività sensibili.

In aggiunta, per quanto concerne i reati societari previsti dall'art. 2626 c.c. (indebita restituzione dei

conferimenti) è da rilevare che per le fondazioni alcuni dei reati societari previsti dal decreto 231 non sono direttamente applicabili.
Essendo dunque l'area dei reati contro la PA quella col maggior "rischio 231", per completezza, si riporta di seguito una breve descrizione dei Reati contemplati negli artt. 24 e 25 del Decreto.

Truffa aggravata in danno dello Stato o di altro ente pubblico (art. 640, comma 2 n. 1, c.p.)
Il Reato si configura qualora, utilizzando artifici o raggiri e in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro ente pubblico o dell'Unione Europea. Tale Reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenerne l'aggiudicazione.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)
Il Reato si configura qualora la condotta di truffa sopra descritta abbia ad oggetto finanziamenti pubblici, comunque denominati, erogati dallo Stato, dal altri enti pubblici o dall'Unione Europea. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Malversazione a danno dello Stato (art. 316bis c.p.)
Il Reato punisce il fatto di chi, avendo ottenuto dallo Stato, da altro ente pubblico o dalla Unione Europea, finanziamenti, comunque denominati, destinati a favorire la realizzazione di opere o attività di pubblico interesse, non li destina agli scopi previsti. Poiché il fatto punito consiste nella mancata destinazione del finanziamento erogato allo scopo previsto, il Reato può configurarsi anche con riferimento a finanziamenti ottenuti in passato e che non vengano ora destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni a danno dello Stato (art. 316ter c.p.)
Il Reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316bis), non assume alcun rilievo la destinazione dei finanziamenti pubblici erogati, poiché il Reato si consuma al momento del loro - indebito - ottenimento. Va infine evidenziato che tale Reato, avendo natura residuale, si configura solo qualora la condotta non integri gli estremi del più grave Reato di truffa aggravata ai danni dello Stato (art. 640 bis c.p.).
Frode informatica in danno dello Stato o di altro ente pubblico (art. 640ter, comma 1, c.p.)
Tale ipotesi di Reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico. In concreto, il Reato in esame potrebbe configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto.

Concussione (art. 317 c.p.)
Il Reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio,

abusando della sua qualità o del suo potere, costringa o induca taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità. Il Reato in esame presenta profili di rischio contenuti ai fini del D. Lgs. 231/01, trattandosi infatti di un Reato proprio di soggetti qualificati, la responsabilità della Fondazione potrà ravvisarsi solo nei casi in cui un Dipendente od un Collaboratore, nell'interesse o a vantaggio della stessa, concorra nel Reato del pubblico ufficiale o dell'incaricato di pubblico servizio, che, approfittando della loro posizione, esigano prestazioni non dovute.

Corruzione (artt. 318-319 c.p.)

Il Reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio si faccia dare o promettere, per sé o per altri, denaro o altra utilità per compiere, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri di ufficio. Il Reato si configura altresì nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi o contrari ai doveri d'ufficio – già compiuti dal pubblico agente. Il Reato sussiste dunque sia nel caso in cui il pubblico ufficiale, dietro corrispettivo, compia un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di una gara). Tale ipotesi di Reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio. A norma dell'art. 321 c.p., le pene previste per i pubblici ufficiali e gli incaricati di pubblico servizio si applicano anche ai privati che danno o promettono a quest'ultimi denaro o altra utilità.

Istigazione alla corruzione (art. 322 c.p.)

La pena prevista per tale Reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per indurlo a compiere un atto contrario o conforme ai doveri d'ufficio, qualora la promessa o l'offerta non vengano accettate. Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un'offerta da parte di un privato.

Corruzione in atti giudiziari (art. 319-ter c.p.)

Il Reato si configura nel caso in cui taluno offra o prometta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio denaro o altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo. Potrà dunque essere chiamata a rispondere del Reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario) al fine di ottenerne la positiva definizione.

Turbata libertà degli incanti (art. 353 c.p.)

Il Reato si configura mediante comportamenti fraudolenti volti a falsare il risultato di una procedura ad evidenza pubblica. Il comportamento può essere tenuto con violenza, minaccia, con doni, promesse, collusione od altri mezzi fraudolenti, impedendo o turbando la gara nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni, ovvero allontanandone gli offerenti.

A completamento dell'esame dei Reati previsti dall'art. 24 del decreto (concussione, corruzione, istigazione alla corruzione e corruzione in atti giudiziari), si evidenzia che, a norma dell'art. 322 bis c.p., i suddetti Reati sussistono anche nell'ipotesi in cui essi riguardino pubblici ufficiali stranieri, ossia coloro che svolgano funzioni analoghe a quelle dei pubblici ufficiali italiani nell'ambito di organismi comunitari, di altri Stati membri dell'Unione Europea, di Stati esteri o organizzazioni pubbliche internazionali.

6. Principi generali di comportamento e codice etico.

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte della Fondazione allo scopo di esprimere dei principi di "deontologia aziendale" che essa riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti e Collaboratori;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di Reati (per fatti che, commessi apparentemente a vantaggio della Fondazione, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

I comportamenti dei dipendenti, collaboratori, ed amministratori ("Dipendenti e Collaboratori"), di coloro che agiscono, anche nel ruolo di consulenti o comunque con poteri di rappresentanza della Fondazione ("Consulenti") e delle altre controparti contrattuali della Fondazione quali, ad esempio, partner in ATI, ecc. ("Partner") devono conformarsi alle regole di condotta previste nel Modello, finalizzate ad impedire il verificarsi dei Reati previsti nel D. Lgs. 231/2001 e successive integrazioni. In particolare, le Regole di Condotta prevedono che:

- i Dipendenti, i Collaboratori, i Consulenti e i Partner non devono (i) porre in essere quei comportamenti che integrano le fattispecie di Reato previste dal D. Lgs. 231/2001, (ii) porre in essere quei comportamenti che, sebbene non costituiscano di per sé un'ipotesi di Reato, possano potenzialmente diventarlo;
- i Dipendenti, i Collaboratori, i Consulenti e i Partner devono evitare di porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A.;
- è fatto divieto di elargizioni in denaro a pubblici funzionari;
- è obbligatorio il rispetto della prassi aziendale e del relativo budget per la distribuzione di omaggi e regali. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Fondazione. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire verifiche e autorizzati dal responsabile di funzione. L'Organismo di Vigilanza monitorerà, nell'ambito dei suoi poteri, controlli e verifiche sulla distribuzione di omaggi e regali. I Dipendenti e Collaboratori che ricevono omaggi o benefici non previsti dalle fattispecie consentite, sono tenuti, secondo le procedure stabilite, a darne comunicazione all'Organismo di Vigilanza che ne valuta l'appropriatezza e provvede a far notificare al mittente la politica della Fondazione in materia;
- i rapporti nei confronti della P.A. devono essere gestiti in modo unitario, intendendosi con ciò che le persone che rappresentano la Fondazione nei confronti della Pubblica Amministrazione devono ricevere un esplicito mandato, sia che esso si identifichi con il sistema di deleghe e procure attualmente in essere**,** sia che esso avvenga nell'ambito di sub-deleghe nell'ambito dei poteri conferiti e dell'organizzazione delle mansioni lavorative di chi rappresenta la Fondazione stessa;
- coloro che svolgono una funzione di controllo e supervisione verso i Dipendenti e Collaboratori che operano con gli enti pubblici devono seguire con attenzione e con le modalità più opportune l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di

irregolarità;

- i compensi dei Consulenti e dei Partner devono essere determinati solo per iscritto;
- devono essere rispettati, da parte degli amministratori, i principi di trasparenza nell'assunzione delle decisioni che abbiano diretto impatto sui terzi;
- devono essere rispettate e, qualora non ancora adottate, devono esser istituite, da parte degli amministratori, apposite procedure per consentire l'esercizio del controllo e il rapido accesso alle informazioni attribuite da legge o regolamento.

7. Organismo di Vigilanza.

7.1. Identificazione dell'Organismo di Vigilanza.

In base alle previsioni del D. Lgs. 231/2001 l'organo cui affidare il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei Modelli nonché di curarne l'aggiornamento (nel presente Modello definito Organismo di Vigilanza) deve essere un organismo interno alla Fondazione (art. 6. 1, b del D.Lgs. 231/2001) e diverso dal C.d.a. L'Organismo di Vigilanza è contattabile tramite l'indirizzo odv@eucentre.it di posta piena garanzia di riservatezza e di anonimato per le elettronica con segnalazioni ricevute. Per garantire la sua piena autonomia ed indipendenza nello svolgimento dei compiti che gli sono stati affidati, l'Organismo di Vigilanza riporta direttamente ai vertici della Fondazione. In relazione ai compiti che è chiamato a svolgere, l'Organo di Vigilanza è stato definito in modo da rispondere alle seguenti caratteristiche:

- Autonomia ed indipendenza: questa qualità è stata assicurata collocando l'OdV come unità di staff in elevata posizione gerarchica in modo da non minare l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello;
- Professionalità: questo connotato si riferisce al bagaglio di strumenti e tecniche di cui i componenti dell'OdV sono dotati per poter svolgere efficacemente l'attività assegnata;
- Continuità di azione: per poter dare la garanzia di efficace e costante attuazione di un Modello così articolato e complesso quale é quello delineato, si è ritenuto opportuno dedicare una struttura interna esclusivamente all'attività di vigilanza sul Modello priva, come detto, di mansioni operative che possano portarla ad assumere decisioni con effetti economico-finanziari;
- Poteri di modifica e di iniziativa: l'OdV ha il potere/dovere, nell'assolvimento dei compiti attribuitigli, di esercitare le iniziative necessarie per adeguare il Modello alle esigenze connesse al verificarsi di deviazioni o violazioni rispetto alle norme previste nel Modello stesso o alle esigenze concrete dell'organizzazione.

7.2. Funzioni e poteri dell'Organismo di Vigilanza.

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

a) sull'osservanza del Modello da parte dei Dipendenti, Collaboratori, Consulenti e Partner;
b) sull'effettività ed adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati di cui al D. Lgs. 231/2001;
c) sull'aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali.

A tal fine, all'Organismo di Vigilanza sono altresì affidati i compiti di:

d) attuare le procedure di controllo previste dal Modello. A questo fine l'Organismo di Vigilanza ha il potere di richiedere l'emanazione di apposite procedure secondo le disposizioni attualmente in vigore. Si osserva, tuttavia, che le attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale, da cui l'importanza di un processo formativo del personale;
e) condurre ricognizioni dell'attività aziendale ai fini dell'aggiornamento della mappatura delle attività sensibili;
f) effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere, soprattutto, nell'ambito delle attività sensibili i cui risultati vengono riassunti nel corso delle comunicazioni di reporting agli organi;
g) coordinarsi con il C.d.a. per i programmi di formazione attinenti al D. Lgs. 231/2001;

h) monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisposizione della documentazione interna necessaria al fine del funzionamento del Modello, contenente le istruzioni, chiarimenti o aggiornamenti;
i) raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione;
j) coordinarsi con le altre funzioni aziendali per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale rilevante e deve essere costantemente informato dal management: i) sugli aspetti dell'attività aziendale che possono esporre la Fondazione al rischio conseguente alla commissione di uno dei Reati previsti dal D. Lgs. 231/2001; ii) sui rapporti con Consulenti e Partner; interpretare la normativa rilevante e verificare l'adeguatezza del sistema di controllo interno in relazione a tali prescrizioni normative;
k) verificare le esigenze di aggiornamento del Modello;
l) riferire periodicamente agli organi in merito all'attuazione delle politiche aziendali per l'attuazione del Modello;
m) controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione a supporto dell'attività ex D. Lgs. 231/2001;

7.3. Reporting nei confronti degli organi.

L'Organismo di Vigilanza ha una linea di reporting su base continuativa direttamente con il Presidente del C.d.a Inoltre annualmente l'Organismo di Vigilanza preparerà un rapporto scritto sulla sua attività per il C.d.a. Il reporting avrà ad oggetto:

1) l'attività svolta dall'ufficio dell'Organismo di Vigilanza;
2) le eventuali criticità emerse sia in termini di comportamenti o eventi interni alla Fondazione, sia in termini di efficacia del Modello.

Gli incontri verranno verbalizzati e copie dei verbali verranno custodite dall'Organismo di Vigilanza e dagli organismi di volta in volta coinvolti. Il C.d.a ha la facoltà di richiedere la convocazione in qualsiasi momento dell'Organismo di Vigilanza.

7.4. Altre attività di controllo e reporting previste dalla legge o da regolamenti interni.

L'Organismo di Vigilanza deve coordinarsi, con le funzioni competenti presenti nella Fondazione, per i diversi profili specifici ed in particolare, ma non esclusivamente, con il Responsabile della Funzione Amministrativa.

7.5. Verifiche periodiche.

Le verifiche sul Modello saranno svolte effettuando specifici approfondimenti e test di controllo. Alla fine sarà stipulato un rapporto da sottoporre all'attenzione del C.d.a. che evidenzierà le possibili manchevolezze e suggerirà le azioni da intraprendere.

8. Flussi informativi nei confronti degli organismi deputati al controllo.

L'afflusso di informazioni e segnalazioni relative ad atti, fatti o eventi rilevanti ai fini del D. Lgs. 231/2001, incluse quelle di natura ufficiosa quali quelle provenienti da Dipendenti, Consulenti, Partner, deve essere centralizzato verso l'Organismo di Vigilanza. L'Organismo di Vigilanza valuterà le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

Le segnalazioni potranno essere in forma scritta ed avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti dell'ente o delle persone accusate erroneamente e/o in mala fede.

L'obbligo di informazione grava in genere su tutto il personale che venga in possesso di notizie relative alla commissione dei Reati o a "pratiche" non in linea con le Regole di Condotta adottate. Le informazioni che devono comunque essere obbligatoriamente tenute a disposizione dell'Organismo di Vigilanza dalle funzioni competenti riguardano:

- le decisioni relative alla richiesta, erogazione ed utilizzo di risorse e finanziamenti pubblici;
- i prospetti riepilogativi dei progetti finanziati con fondi pubblici;
- notizie e documentazione relative a progetti finanziati con fondi pubblici affidati da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti e collaboratori nei confronti dei quali la Magistratura procede per i Reati previsti dal D. Lgs. 231/2001;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati di cui al D. Lgs. 231/2001;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- i rapporti preparati dai responsabili delle funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D. Lgs. 231/2001;
- il sistema di deleghe della Fondazione.

Periodicamente l'Organismo di Vigilanza proporrà, se del caso, al C.d.a. eventuali modifiche della lista sopra indicata.

9. Sistema Disciplinare.

9.1. Principi generali.

Aspetto essenziale per l'effettività del Modello è costituito dalla costruzione di un adeguato sistema sanzionatorio per la violazione del codice etico e, in generale, delle procedure interne. L'applicazione di sanzioni disciplinari per violazione delle regole di condotta aziendali prescinde dall'esito del giudizio penale, in quanto tali regole sono assunte dalla Fondazione in piena autonomia ed a prescindere dall'illecito che eventuali condotte possano determinare.

9.2. Sanzioni per i lavoratori subordinati.

I comportamenti tenuti dai lavoratori subordinati in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari. Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori subordinati esse rientrano tra quelle previste dal Regolamento disciplinare aziendale, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori ed eventuali normative speciali applicabili. In relazione a quanto sopra il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui ai Contratti Collettivi applicati dalla Fondazione. Tali categorie descrivono i comportamenti sanzionati, in base al rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

9.3. Sanzioni per i lavoratori subordinati

Ai lavoratori subordinati viene applicato il contratto collettivo nazionale del lavoro ANINSEI per il personale della scuola non statale.

In applicazione dei "Provvedimenti disciplinari" contenuti nel vigente CCNL nel rispetto di ogni regola, procedura e garanzia prevista dalla legge si prevede che:

1. Incorre nei provvedimenti di RIMPROVERO SCRITTO, MULTA O SOSPENSIONE il lavoratore che violi le procedure interne previste dal presente Modello (ad esempio: che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di Attività sensibili, un comportamento non conforme alle prescrizioni del Modello stesso. La sanzione sarà commisurata alla gravità dell'infrazione ed alla reiterazione della stessa (della recidività si terrà conto anche ai fini della commisurazione di una eventuale sanzione espulsiva), e comunque non potrà essere superiore all'importo pari a 4 ore della normale retribuzione in caso di multa, e di 3 giorni nel caso di sospensione dalla retribuzione e dal servizio;
2. Incorre, inoltre, anche nel provvedimento di LICENZIAMENTO CON PREAVVISO, il lavoratore che adotti nell'espletamento delle Attività sensibili un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un Reato sanzionato dal D. Lgs. 231/2001, dovendosi ravvisare in tale comportamento un'infrazione alla disciplina ed alla diligenza del lavoro;
3. Incorre, infine, anche nel provvedimento di LICENZIAMENTO SENZA PREAVVISO il lavoratore che adotti, nell'espletamento delle Attività sensibili un comportamento palesemente in violazione delle prescrizioni del Modello, tale da determinare la concreta applicazione a carico della Fondazione di misure previste dal Decreto, dovendosi ravvisare in tale comportamento un'infrazione alla disciplina ed alla diligenza del lavoro così grave da non consentire la prosecuzione nemmeno provvisoria del rapporto di lavoro, nonché un atto che costituisce delitto a termine di legge.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione

delle sanzioni restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, al C.d.a. Il sistema disciplinare viene costantemente monitorato dal C.d.a. con il supporto, se necessario, dell'Organismo di Vigilanza. Ai lavoratori verrà data un'immediata e diffusa informazione circa l'introduzione delle nuove disposizioni, diramando una circolare interna per spiegare le ragioni che le hanno giustificate e riassumerne il contenuto. Il sistema sanzionatorio farà riferimento ai singoli contratti di categoria e sarà quindi coerentemente applicato anche a lavoratori eventualmente assunti con diverso contratto di lavoro.

9.4. Misure nei confronti di Consulenti e Partner.

Ogni violazione da parte dei Consulenti o dei Partner delle regole di cui al presente Modello o commissione dei Reati di cui al D. Lgs. 231/2001 sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti. Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Fondazione, come nel caso di applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

10. Formazione e comunicazione

10.1. Comunicazione e formazione per i Dipendenti

Ai fini dell'efficacia del Modello, è obiettivo della Fondazione garantire al personale una corretta conoscenza delle procedure e delle regole di condotta adottate in attuazione dei principi di riferimento contenuti nel presente documento, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle aree di attività a rischio. Le procedure, i sistemi di controllo e le regole comportamentali adottati in attuazione dei principi di riferimento contemplati nel presente documento unitamente al Codice Etico, sono comunicati a tutto il personale in relazione all'attività svolta in concreto ed alle mansioni attribuite. Ai dipendenti all'atto dell'accettazione della proposta di assunzione, è richiesto di sottoscrivere una specifica dichiarazione di adesione al Codice Etico e di impegno all'osservanza delle procedure adottate in attuazione dei principi di riferimento per la costruzione del Modello. Il C.d.a, all'atto dell'accettazione della nomina, deve dichiarare e/o sottoscrivere analoga dichiarazione di impegno all'osservanza e di collaborazione all'applicazione del Codice Etico e dei principi di riferimento per la costruzione del Modello di cui al presente documento.

10.2. Informativa per i Collaboratori esterni e Partner

Saranno forniti a soggetti esterni (consulenti e partner) apposite informative sulle politiche e le procedure adottate dalla Fondazione sulla base del presente Modello Organizzativo, nonché i testi delle clausole contrattuali abitualmente utilizzate a riguardo.

10.3. Informativa ai fornitori

La Fondazione comunica l'adozione del Modello e del Codice Etico ai propri fornitori mediante la consegna di una apposita informativa.

11. Allegati – Aggiornamento del Modello Organizzativo

Si riporta di seguito l'elenco degli allegati che costituiscono aggiornamento del piano:

- Reati Informatici;
- Politica Informatica edizione 1 revisione 0 del 19/11/2018;
- Reati di Razzismo e Xenofobia;
- Segnalazioni di illecito, denunce anonime ed accesso agli atti.

I REATI INFORMATICI

Fondazione Eucentre
Via Ferrata, 1 - 27100 Pavia
Tel: 0382 5169811
Fax: 0382 529131
P. IVA: 02009180189

e-mail: info@eucentre.it

Web site: www.eucentre.it

SOMMARIO

REATI INFORMATICI

1. Premessa

Oggigiorno ogni azienda è dotata di diversi computer e gli stessi sono sovente accessibili dall'esterno, costituendo delle reti aperte. La presenza capillare dei computer fa si che in astratto in qualunque impresa possa essere commesso un reato informatico; l'accessibilità dall'esterno rende possibili attacchi da soggetti che non fanno parte dell'organico aziendale e quindi una maggiore difficoltà nella loro individuazione. Colui che decide di commettere un reato di questo tipo, potendolo realizzare a distanza, ha maggiore probabilità di non essere rintracciato.

Vi è poi da considerare che attualmente il patrimonio dell'azienda è totalmente dematerializzato, nel senso che all'interno del computer vengono inserite tutte le informazioni relative all'attività dell'impresa, sia di contenuto economico, che strategico. L'accesso ad un computer aziendale può quindi risultare vantaggioso per il "delinquente informatico" poiché la condotta posta in essere può portare ingenti guadagni per lui ed al contempo determinare ingenti danni all'impresa colpita.

Sotto tale ultimo aspetto rileva come la commissione di un reato informatico all'interno di un'azienda determini un triplice danno per la stessa e segnatamente: un costo per riattivare o sostituire le risorse informatiche colpite; un nocumento, non sempre agevolmente stimabile, riguardante direttamente la diminuzione del patrono aziendale riconducibile all'attacco informatico; un danno, altrettanto difficile da quantificare, relativo all'immagine dell'impresa colpita.

Anche sul piano giuridico si registrano importanti mutamenti visto che nel volgere di pochi anni sono state previste dal legislatore diverse ipotesi di reato informatico, la maggior parte delle quali introdotte dalla L. n. 547/1993. Ne consegue che se l'azienda decidesse di denunciare il delitto subito potrebbe quanto meno contare sull'effettiva possibilità di ottenere soddisfazione all'interno del processo penale cui ha dato impulso.

2. Inside Attack

Normalmente il fronte di attacco outsiders è quello più evidente e si contrasta soprattutto implementando le contromisure tecnologiche, ed insegnando agli impiegati quali sono le negligenze che possono favorire le intrusioni.

Il fronte di attacco interno, invece è quello meno evidente e più insidioso ed in grado di provocare i danni maggiori per l'azienda. Gli attacchi interni detti anche "insiders", rappresentano i principali utilizzatori del patrimonio informativo dell'organizzazione; impiegati infedeli o in contrasto con l'azienda e consulenti disonesti sono coloro che conoscono meglio i sistemi di sicurezza e possono eseguire con facilità operazioni proibite come frodi, furti di informazioni, cancellazioni od alterazioni di dati, utilizzo dei sistemi informatici per scopi privati.

I crimini ad opera dei dirigenti o impiegati della organizzazione difficilmente vengono denunciati all'Autorità Giudiziaria, e questo è dovuto anche al fatto che spesso le aziende vogliono tutelare la loro immagine pubblica. Difatti, le imprese sono molto più propense ad attuare azioni disciplinari nei confronti dei loro impiegati scoperti a commettere delle illegalità.

Questi tipi di reati da "inside attack", sono tanto più sia nelle aziende private che negli uffici delle pubbliche amministrazioni.

I danni che possono derivare dagli attacchi insider possono essere di due livelli:

- Danno primario: questo si presenta in base all'entità della frode ed alla necessità di intervenire sul sistema attaccato e sui dati in esso contenuti per ripristinare le funzionalità;
- Danno secondario: è l'influenza negativa che l'attacco ha sull'immagine aziendale.

3. Le norme penali in ambito informatico

Da un lato, infatti, le nuove norme "tranquillizzano" gli esercenti attività imprenditoriali, poiché, in caso di illecito subito ed accertato, viene offerta la possibilità di far valere i propri interessi in sede giudiziaria. Parimenti, l'effetto "tranquillizzante" troverebbe giustificazione nel carattere generale preventivo delle norme penali, nel senso che l'esistenza di norme specifiche, nonché la previsione di sanzioni detentive, dovrebbe far desistere molti "malintenzionati" dal compimento di attività illecite.

Dall'altro, le nuove disposizioni provocano un forte "stato di agitazione" in coloro che sono investiti della responsabilità di gestione dell'impresa od azienda, in quanto si teme che l'uso dell'informatica possa, anche inconsapevolmente, determinare profili di responsabilità penale, con danni all'immagine talvolta superiori a quelli prodotti dal reato subito.

La preoccupazione aumenta, invero, oggi, atteso che, grazie a quanto statuito dall'art. 7, L. n. 48/2008, viene estesa la responsabilità amministrativa dell'ente, e quindi anche delle aziende, alla maggior parte dei reati informatici commessi dai vertici o dai dipendenti.

L'unica strada che consente di eliminare, o comunque attenuare, tale "stato di agitazione" è quella di utilizzare tutti gli accorgimenti necessari a far fronte alla nuova emergenza rappresentata dal reato informatico.

Trattandosi di fenomeni relativamente nuovi e complessi, occorre individuare i soggetti idonei a predisporre le opportune soluzioni di contrasto.

La necessità di individuare soggetti dotati di specifica competenza è fortemente avvertita in questo settore, stante la novità espressa dai nuovi fenomeni criminali ed in considerazione dei numerosi elementi di conoscenza necessari per studiare strategie adeguate.

A tal riguardo è bene sottolineare come i nuovi fatti previsti dalla legge come reato si caratterizzano sotto diversi profili, ciascuno dei quali può essere compreso solo a seguito di un'adeguata e specifica preparazione, nonché conoscenza dei contesti venutisi a creare grazie all'introduzione su vasta scala dei computers.

Poiché i nuovi reati sono caratterizzati dalla componente tecnologica, in linea di massima, lo studio e la messa in pratica di soluzioni finalizzate ad impedire la commissione di reati all'interno dell'azienda coinvolgono soggetti aventi competenza e background culturale diversi.

Se da un lato, infatti, il tecnico (informatico, esperto della sicurezza) ha le conoscenze per valutare la vulnerabilità delle risorse e per decidere circa le misure di sicurezza necessarie per proteggere i sistemi, il giurista è, almeno sulla carta, colui che più degli altri può, a priori, individuare i rischi che corre l'impresa rispetto ad un'eventuale commissione del reato informatico e, conseguentemente, studiare e proporre tutte le soluzioni idonee ad impedirli o limitarli.

Poiché, per ovvie ragioni, non sempre è agevole ottenere una perfetta collaborazione tra soggetti che hanno una formazione culturale estremamente diversa, e sono per loro natura abituati a vedere i problemi da angolazioni differenti, in questi ultimi anni, grazie anche all'istituzione di specifici corsi universitari e para-universitari, è venuta formandosi una nuova figura di giurista, detto, appunto, "giurista informatico" o "informatico giuridico", in grado di coniugare i due tipi di conoscenza per lungo tempo tenuti separati.

4. Il D.Lgs. n. 231/2001 e la responsabilità dell'azienda

Le aziende hanno, iniziato a porsi seriamente il problema di un loro coinvolgimento per reati commessi al loro interno a partire dal 2001 allorquando è stato approvato il D.Lgs. n. 231/2001.

Tale D.Lgs. ha introdotto, infatti, per la prima volta la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. Secondo questa regolamentazione rientrerebbero, nel concetto di "ente", tutti i soggetti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica, rimanendone esclusi lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici e gli enti che svolgono funzioni di rilevanza costituzionale. Viene prevista la responsabilità amministrativa dell'Ente per i reati-presupposto commessi nel suo interesse o a suo vantaggio da:

- persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente o di sua unità organizzativa dotata di autonomia finanziaria e funzionale;
- persone che esercitano, anche di fatto, la gestione ed il controllo dell'ente o di sua unità organizzativa autonoma;
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui ai punti precedenti.

Viene, tuttavia, esclusa la responsabilità dell'ente nel caso in cui le persone (che ricoprono incarichi "apicali" ovvero soggette "all'altrui direzione") hanno agito nell'interesse esclusivo proprio o di terzi.

Principio generale è quello dell'autonomia della responsabilità dell'ente.

Dispone, infatti, il legislatore che la responsabilità amministrativa sussiste in capo all'ente anche nel caso in cui:

- l'autore del reato non è stato identificato o non è imputabile;
- ovvero il reato si estingue per una causa diversa dall'amnistia.

Conseguenza importante di tale impianto normativo è che in tutte quelle ipotesi in cui, per la complessità dell'assetto organizzativo interno, non sia possibile ricondurre la responsabilità penale in capo ad uno specifico soggetto, e venga comunque accertata la commissione di un delitto, l'ente ne dovrà rispondere sul piano amministrativo, sempre che allo stesso sia imputabile una colpa organizzativa consistente nella mancata adozione ovvero nel carente funzionamento del modello di organizzazione, gestione e controllo.

Per quanto concerne l'ambito di nostro interesse è bene rilevare come secondo l'impostazione originaria del Decreto la responsabilità dell'ente non sarebbe prevista per tutti i reati informatici, ma soltanto per quelli di frode informatica commessa a danno dello Stato o di altro Ente pubblico (art. 24), di assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione(art. 25-*quater*), di distribuzione, cessione e detenzione di materiale pedopornografico (art. 25-*quinquies*, comma 1, lett. c).

Rispetto alla frode informatica si prevede, per l'ente responsabile, la sanzione pecuniaria fino a cinquecento quote; se l'ente ha tratto dal reato un profitto di rilevante entità ovvero, se il reato ha provocato un danno di particolare gravita la sanzione va da duecento a seicento quote.

In caso di condanna, è sempre ordinata la confisca dei beni che costituiscono il profitto o il prezzo del reato (salvo che appartengano a persona estranea al reato), anche per equivalente.

In relazione alla frode informatica commessa nel suo interesse o a suo vantaggio, all'ente possono applicarsi, in aggiunta alla sanzione pecuniaria, alcune tra le sanzioni interdittive previste dall'art. 9 ovvero il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

Rispetto al delitto di assistenza a gruppi terroristici per l'ente responsabile si prevede la sanzione pecuniaria da duecento a settecento quote. Nel caso di condanna si applicano le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non inferiore ad un anno. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di questo delitto si applica la sanzione dell'interdizione definitiva dell'esercizio dell'attività.

Per i reati di distribuzione, cessione e detenzione di materiale pedopornografico si applica la sanzione pecuniaria da duecento a settecento quote. Anche in questo caso si applica la sanzione dell'interdizione definitiva allorquando l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione del reato.

Rispetto a tali delitti, ai sensi dell'art. 26, l'ente risponde anche nell'ipotesi in cui il soggetto qualificato commetta un tentativo, a meno che volontariamente impedisca il compimento dell'azione o la realizzazione dell'evento.

5. Le modifiche apportate dalla L. 18/03/2008, n. 48

A seguito delle modifiche apportate al D.Lgs. n. 231/2001, L. n. 48/2008 le aziende possono essere chiamate a rispondere per la maggior parte dei reati informatici commessi dai suoi vertici e dipendenti.

La L. n. 48, infatti, estende la responsabilità amministrativa degli enti ai seguenti reati informatici:

- falsità in un documento informatico (art. 491-bis c.p.);
- accesso abusivo ad 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 ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
- danneggiamelo di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamelo di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamelo di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

Si tratta di una grande novità atteso che fino ad oggi, come visto, sulla base del D.Lgs. n. 231/2001 tale responsabilità era prevista solo per residuali ipotesi di reato informatico, quali quelli di frode informatica commessa a danno dello Stato o di altro Ente pubblico, di assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione, di distribuzione, cessione e detenzione di materiale pedopornografico.

Ciò che può preoccupare le aziende poi non è solo l'estensione di tale responsabilità a tutti i delitti informatici, ma la circostanza che la stessa possa essere imputata anche nelle ipotesi in cui non venga rintracciato l'autore materiale del reato. Ne consegue che la mancata individuazione del soggetto attivo del reato, non infrequente in materia di criminalità informatica, possa non far comprendere esattamente all'organo giudicante le motivazioni dello stesso e quindi determinare un'attribuzione di responsabilità anche quando l'autore del reato abbia agito per fini esclusivamente personali e non nell'interesse del suo datore di lavoro.

La preoccupazione non può poi che aumentare quando si consideri che l'azienda ritenuta responsabile è soggetta oltre che all'esborso di ingenti somme di danaro a sanzioni interdittive quali:

- l'interdizione dall'esercizio dell'attività;

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

Di fronte a tale nuovo scenario l'azienda è inevitabilmente costretta a studiare delle strategie preventive idonee, da un lato, ad impedire la commissione di reati informatici al suo interno e dall'altro, capaci di escluderne una sua responsabilità nelle ipotesi in cui le misure adottate non siano state in grado di evitare la commissione del reato.

Per limitare al massimo la commissione di reati nel contesto aziendale occorre sicuramente partire da una responsabilizzazione di tutti i soggetti che ivi lavorano, cosa che si può ottenere attraverso strumenti diversi.

Assai utile può rivelarsi la predisposizione di corsi di formazione interna in grado di spiegare ai vertici ed ai dipendenti dell'azienda ciò che si può e ciò che non si deve fare con gli strumenti informatici. Corsi di formazione la cui efficacia dipenderà molto dalla conoscenza preventiva del modo di lavorare e di pensare di ciascuno, conoscenza questa acquisibile attraverso la compilazione di questionari anonimi in grado "di far sentire il polso dell'azienda" a colui che è chiamato a formare.

Altrettanto efficace potrebbe poi rivelarsi la redazione di un vero e proprio codice di comportamento informatico, i cui principi fondamentali potrebbero essere addirittura inseriti all'interno del contratto di lavoro.

Tali soluzioni potrebbero quindi dimostrare in prima battuta che si è fatto tutto ciò che era possibile per impedire che propri dipendenti commettessero un reato informatico e quindi evitare una sorta di responsabilità per culpa in vigilando.

Parimenti, per respingere rimproveri per una forma di culpa in eligendo sarà indispensabile affidare incarichi "delicati" connessi all'uso dei sistemi informatici a soggetti dotati di specifiche competenze.

D'altra parte tali accorgimenti vanno proprio nella direzione del D.Lgs. n. 231/2001, che prevede l'esonero di una responsabilità dell'ente allorquando lo stesso dimostri di aver predisposto modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi.

A tal proposito si distingue a seconda che il reato venga commesso da un vertice o da un dipendente.

Nella prima ipotesi l'ente non risponde del reato commesso quando sia in grado di dimostrare che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

- il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Ovviamente non basta redigere il predetto modello organizzativo essendo necessario che lo stesso risponda alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

Per agevolare il compito delle aziende si prevede che i modelli di organizzazione possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati.

Negli enti di piccole dimensioni il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curarne il loro aggiornamento, può essere svolto direttamente dall'organo dirigente.

Riguardo ai soggetti sottoposti all'altrui direzione, sempre secondo il D.Lgs. n. 231/2001, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.

In ogni caso, è esclusa l'inosservanza di tali obblighi se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il modello, in questo caso, prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio. Ne consegue che l'efficace attuazione del modello richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

EUCENTRE
FOR YOUR SAFETY.

ICT

POLICY SULL'UTILIZZO DELLE DOTAZIONI INFORMATICHE

N. REV.	DATA	MOTIVO DELLA REVISIONE

Fondazione Eucentre
Via Ferrata, 1 - 27100 Pavia
Tel: 0382 5169811
Fax: 0382 529131
P. IVA: 02009180189
e-mail: info@eucentre.it
Web site: www.eucentre.it

REDAZIONE E VERIFICA	EDIZIONE	REVISIONE	APPROVAZIONE
Capo Ufficio Servizi Tecnici Ing. Ettore Festa	Numero: 1 Data: 22/11/2018	Numero: 0 Data: 22/11/2018	Presidente Prof. Riccardo Pietrabissa

EUCENTRE
FOR YOUR SAFETY.

INDICE

1. OBIETTIVO ED AMBITO DI APPLICAZIONE

Il presente documento ha l'obiettivo di definire le linee guida per il corretto utilizzo delle dotazioni informatiche e della rete aziendale, per ridurre il rischio di un loro utilizzo non corretto, intenzionale o involontario, e per assicurare che il sistema informativo ed informatico sia salvaguardato e gestito correttamente. In particolare, giacché qualunque forma di protezione tecnologica può essere vanificata da un non corretto comportamento degli utenti, è necessario garantire:

- la protezione della Fondazione da atti illeciti e da abusi attuati mediante l'uso delle dotazioni informatiche aziendali;
- la prevenzione dei reati di criminalità informatica che possono comportare la responsabilità amministrativa della Fondazione;
- la sicurezza delle informazioni in termini di disponibilità, integrità e riservatezza;
- l'impiego efficiente ed efficace delle risorse affidate;
- l'adozione di una disciplina conforme alle disposizioni del Garante per la protezione dei dati personali (Garante Privacy) ed il rispetto delle leggi vigenti in materia;
- una corretta informativa sulle modalità d'uso degli strumenti.

Quanto definito nel presente documento si applica a coloro che utilizzano le dotazioni informatiche e la rete per conto della Fondazione.

2. RIFERIMENTI

- Decreto legislativo 29 dicembre 1992 n. 518 "Attuazione della Direttiva 91/259/CEE relativa alla tutela giuridica dei programmi per elaboratore";
- Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Legge 18 agosto 2000 n. 248 contenente "Nuove norme di tutela del diritto d'autore";
- Decreto Legislativo 8 giugno 2001 n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica";
- Decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
- Legge 18 marzo 2008 n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno";
- Deliberazione del Garante Privacy n. 13 del 1° marzo 2007;
- Decreto Legislativo 14 settembre 2015 n. 151 contenente "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183" che ha modificato l'articolo 4 della legge 20/05/1970 n.300.

3. DEFINIZIONI E ACRONIMI

Acronimi	Descrizione
Utenti	Dipendenti, collaboratori, consulenti, professionisti, studenti, visitatori ed ospiti a cui è concesso l'accesso alla rete di EUCENTRE
Dotazione informatica	Dispositivo hardware o software reso disponibile dall'azienda Esempi di dotazione informatica sono: computer portatile o fisso, tablet, smartphone e telefono cellulare, badge, posta elettronica aziendale, accesso ad internet, connessione VPN, stampanti, dispositivi di archiviazione di massa (memorie flash, drive esterni, prodotto software, ecc.)
Amministratore di Sistema	Figura professionale finalizzata alla gestione e alla manutenzione dell'impianto di elaborazione dati o dei suoi component
App	Applicazione software dedicata ai dispositivi di tipo mobile (smartphone, tablet)
Attacco informatico	Tentativo di accesso non autorizzato ad un sistema informatico al fine di compromettere la disponibilità e le funzionalità del sistema stesso o anche la riservatezza, l'integrità o la disponibilità dei dati/informazioni in esso contenuti
BYOD	Dispositivo di proprietà del dipendente autorizzato da EUCENTRE per uso aziendale
FTP	File transfer protocol
Password	Sequenza di caratteri alfanumerici o speciali utilizzata come parola chiave necessaria per accedere a risorse informatiche
Phishing	Truffa consistente nel tentativo di indurre con l'inganno a fornire informazioni personali sensibili o comunque riservate attraverso l'uso di strumenti informatici (siti web fasulli, messaggi di posta elettronica con link o allegati dannosi, ecc.)
PIN	Personal Identification Number: codice alfanumerico o password utilizzato per l'autenticazione a servizi, dispositivi o sistemi
Smart card	Dispositivo hardware della dimensione di una carta di credito con potenzialità di elaborazione, memorizzazione dati o interfaccia input/output
Virus Malware	Tipologia di software dannoso in grado di interferire con il corretto funzionamento di altri programmi, di replicarsi e di diffondersi attraverso le reti di comunicazione, provocando, in taluni casi, l'indisponibilità dei sistemi infettati
VPN	(Virtual Private Network). Rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet

4. PRINCIPI GENERALI

Le dotazioni informatiche e l'acesso alla rete sono strumenti aziendali affidati agli utenti per lo svolgimento delle attività assegnate ed il loro utilizzo comporta l'acquisizione di dati sulla prestazione svolta; esse devono essere utilizzate secondo i principi di diligenza e correttezza che sostengono ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

In relazione a quanto sopra, si ritiene necessario adottare comuni regole interne di comportamento, contenute nel presente documento, dirette ad evitare azioni inconsapevoli o non in linea con la politica di EUCENTRE, al fine di minimizzare i rischi di sicurezza informatica e di salvaguardare i livelli di performance dei servizi informatici aziendali.

Al riguardo le dotazioni informatiche devono essere custodite in modo appropriato, adottando tutte le cautele a tutela del loro corretto funzionamento, utilizzate in relazione alle attività assegnate e alle indicazioni aziendali ed in modo coerente con gli obiettivi di EUCENTRE.

I dipendenti sono tenuti a conoscere ed attuare le politiche aziendali in tema di sicurezza delle informazioni al fine di garantirne la riservatezza, l'integrità e la disponibilità, in coerenza con quanto stabilito dalla Privacy Policy.

I destinatari di dotazioni informatiche aziendali sono tenuti a rispettare le regole definite nel presente documento ed in ogni altro documento in vigore che dia ulteriori disposizioni specifiche per la regolamentazione dei singoli dispositivi.

Al fine di garantire la tutela del sistema informativo ed informatico, l'Azienda utilizza accorgimenti tecnici preventivi (quali credenziali di accesso, antivirus, antispam, limitazioni alle autorizzazioni, utilizzo di filtri che prevengono determinate operazioni, ecc.) finalizzati a ridurre il rischio di comportamenti illeciti, dannosi, di situazioni di pericolo o di violazione delle procedure aziendali e dei doveri fondamentali relativi al rapporto di lavoro.

Al termine del rapporto contrattuale con l'azienda, il dipendente è tenuto a restituire le dotazioni individuali assegnate, comprensive anche dei dati aziendali contenuti, avendo cura di eliminare i dati personali eventualmente presenti.

5. REGOLE DI UTILIZZO DELLE DOTAZIONI INFORMATICHE

5.1 Autenticazione ed accesso

- L'accesso alle dotazioni informatiche è protetto, laddove possibile, dall'uso di credenziali di autenticazione strettamente personali e finalizzate al riconoscimento univoco dell'utilizzatore e alla conseguente attribuzione dei profili di accesso e di utilizzo delle stesse.
- Non è consentito fornire il servizio di connettività di rete ad altri.
- Le password di accesso alla rete o ad altri sistemi aziendali devono essere diverse tra loro e non devono mai essere utilizzate per l'autenticazione ad altri servizi.
- Le password per l'accesso via browser alle applicazioni aziendali non devono essere memorizzate attraverso le funzionalità di "remember password", anche se detta memorizzazione non è disattivata per impostazione predefinita.
- Password e badge aziendale devono essere custoditi con attenzione al fine di ridurre il rischio di utilizzi indebiti (es. non scrivere le password su foglietti di carta ed in altri luoghi facilmente accessibili, custodire in luoghi sicuri token, smart card e badge aziendale).
- Non è consentito accedere a sistemi informativi utilizzando le credenziali di accesso altrui e/o comunicare ad altri la password relativa alle proprie credenziali di accesso.

In caso di cessazione dell'attività lavorativa, il Responsabile del Personale lo comunica al Responsabile ICT che provvede a disattivare gli accessi ai sistemi aziendali e la casella di posta elettronica.

Si precisa inoltre che costituiscono reato le seguenti condotte:

- l'accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza ovvero la sua distruzione o il suo danneggiamento costituiscono reato ai sensi del codice penale (art. 615 ter codice penale);
- la detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici costituiscono reato ai sensi del codice penale (art. 615 quater codice penale);
- la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico costituiscono reato ai sensi del codice penale (art. 615 quinquies codice penale);
- L'utilizzo di software in maniera difforme da quanto previsto dalla licenza.

5.2 Posta elettronica

- La casella di posta elettronica assegnata all'utente e contrassegnata dal seguente indirizzo (nome.cognome@eucentre.it) è uno strumento di lavoro e le persone assegnatarie sono responsabili del corretto utilizzo della stessa per le finalità aziendali.
- L'indirizzo di posta elettronica aziendale non deve mai essere utilizzato per registrarsi ed autenticarsi su servizi web esterni all'azienda (es. registrazione a siti internet e social network), a meno che tale registrazione non sia funzionale ad esigenze professionali o per l'adesione ad iniziative/convenzioni aziendali.
- Non scaricare allegati o aprire link presenti in e-mail sospette, ma contattare l'Ufficio ICT per verificare possibili casi di phishing; al riguardo è necessario fare attenzione, per esempio, ad e-mail inviate da mittenti sconosciuti ed a contenuto generalmente di natura commerciale, contenenti richieste di informazioni personali per motivi non ben specificati (scadenza, smarrimento, problemi tecnici), aventi toni intimidatori (minaccia del blocco della carta di credito o del conto corrente in caso di mancata risposta dell'utente).
- Non utilizzare l'indirizzo di posta elettronica aziendale per iscriversi a "mailing list" e/o partecipare a "chat line"/comunità virtuali, a meno che tale registrazione non sia necessaria per esigenze professionali o per l'adesione ad iniziative/convenzioni aziendali.
- Limitare, per quanto possibile, la dimensione degli allegati (anche comprimendo i file più grandi, ricorrendo a formati quali ad esempio *.zip, *.Jpg, ecc.) e l'invio di e-mail ad un numero elevato di destinatari.

- Le mail devono sempre riportare al termine del testo, dopo la firma, la classificazione di riservatezza ed il relativo messaggio che viene fornito dall'Ufficio ICT.

5.3 Accesso ad internet

L'accesso ad internet mediante l'utilizzo delle infrastrutture e delle dotazioni aziendali è consentito secondo le modalità correnti e deve essere effettuato in relazione allo svolgimento delle attività professionali.

L'utente è responsabile dell'uso del servizio di accesso ad internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera, a prescindere dalle misure poste in essere per limitare l'accesso a risorse web (es. sistemi di filtraggio che consentono il blocco totale o parziale di determinati accessi a siti internet).

Nell'uso della rete internet non sono consentiti i seguenti comportamenti:

- accedere utilizzando le credenziali di altro utente;
- porre in essere attacchi informatici o attività intrusive;
- porre in essere attività volte a minare l'integrità, la confidenzialità e la disponibilità del servizio di accesso alla rete internet e dei servizi erogati attraverso di essa;
- effettuare operazioni di trading on line per uso personale, visualizzare in modalità streaming audio e video non inerenti l'attività professionale;
- accedere a siti relativi a giochi e di gaming on line (scommesse).

Eventuali comportamenti attuati in violazione delle disposizioni aziendali in materia di utilizzo della posta elettronica e dell'accesso ad internet potranno dare luogo, in relazione alla loro gravità, all'adozione dei provvedimenti disciplinari previsti dalla contrattazione collettiva applicabile.

5.4 Applicazioni informatiche

Applicazioni informatiche aziendali

Tutte le applicazioni informatiche, ovvero quei sistemi informatici che automatizzano i processi di business (applicativi aziendali di varia utilità) sono rese disponibili ai dipendenti per l'esecuzione delle attività e delle funzioni lavorative assegnate. La loro protezione deve essere effettuata a diversi livelli per evitare il verificarsi di eventi che ne possano bloccare o degradare le prestazioni o minacciarne l'integrità e la riservatezza delle informazioni. I tempi di conservazione dei log sono limitati al tempo necessario rispetto alle specifiche finalità.

Installazione di software

- Non è consentito installare o utilizzare sulle dotazioni informatiche prodotti software non coperti da regolare licenza d'uso oppure prodotti software la cui fruizione è libera per uso personale, ma è a pagamento per uso professionale o aziendale. L'utilizzo di copie pirata di software può essere sanzionato sulla base del Decreto Legislativo n. 518/1992 sulla tutela giuridica del software e della Legge n. 248/2000 contenente norme di tutela del diritto d'autore. Inoltre, l'utilizzo di software privo di licenza d'uso ai fini aziendali espone EUCENTRE a responsabilità dirette, in quanto costituisce reato ai fini del Decreto Legislativo n. 231/2001. Analogamente non è consentito scaricare file musicali (come quelli in formato mp3), foto o video (come quelli in formato jpeg, avi, ecc.) per i quali non si disponga di adeguata licenza. A tal fine il dipendente è tenuto a rimuovere prontamente dalla propria dotazione informatica il materiale eventualmente scaricato senza autorizzazione.
- Il software denominato research deve essere usato esclusivamente per la ricerca e non deve essere utilizzato per impieghi assimilabili a prestazioni professionali.
- Le App per tablet e smartphone la cui installazione è consentita sono esclusivamente quelle acquisite da App store ufficiali (ad esempio Google Play, App Store Apple, Microsoft Store, Amazon Apps, Samsung Apps).
- E' tassativamente vietato l'utilizzo di programmi finalizzati:

  - alla scansione delle reti locali o esterne, alla ricerca di eventuali vulnerabilità dei dispositivi collegati, alla conduzione di tentativi di intrusione e/o all'intercettazione di dati in transito su dette reti, salvo eccezioni derivanti dalla particolare mansione lavorativa che rende necessario l'utilizzo di tale tipologia di strumenti;
  - alla falsificazione, alterazione o rimozione indebite del contenuto di comunicazioni e/o di documenti informatici.
- Nel caso di interventi di assistenza e manutenzione del software richiesti dal dipendente, l'accesso dell'operatore per assumere da remoto il controllo della dotazione informatica potrà avvenire solo previo consenso del dipendente stesso.

5.5 Aree dati aziendali

- Non è consentito utilizzare gli strumenti aziendali di file sharing (cartelle di rete, siti sharepoint, cloud ecc.) per scopi diversi da quelli professionali. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere collocato, nemmeno per brevi periodi, in queste aree dati.
- l'Azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, o acquisiti in violazione di quanto previsto dal presente documento.

5.6 Protezione da virus, phishing ed attacchi informatici ai sistemi aziendali

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo. In relazione a ciò, è necessario:

- non scaricare file eseguibili o immagini da siti Web e/o Ftp di cui non sia certa l'affidabilità;
- segnalare tempestivamente all'Ufficio ICT la presenza sospetta di virus, casi di phishing, guasti, malfunzionamenti sulle dotazioni informatiche e/o sui sistemi aziendali o sospetto furto/compromissione di credenziali;
- porre in essere le cautele necessarie ad evitare l'utilizzo indebito della postazione di lavoro da parte di terzi (bloccare il desktop quando ci si allontana dalla postazione di lavoro, ecc.);
- proteggere l'accesso ai dispositivi mobili (smartphone, tablet, ecc.) utilizzando PIN, password o altri dispositivi di protezione disponibili (lettore di impronte digitali, ecc.);
- non collegare alla postazione di lavoro qualsiasi dispositivo di connessione alla rete telefonica pubblica (Router WiFi, chiavetta internet, ecc.) quando la postazione di lavoro è contemporaneamente connessa alle interfacce cablate o wireless della rete intranet aziendale disponibile presso le sedi di EUCENTRE;
- non modificare indebitamente le configurazioni hardware impostate sulle dotazioni informatiche aziendali;
- non rimuovere i meccanismi di protezione hardware e/o software presenti sulla dotazione informatica (ad esempio non effettuare Jailbreak su dispositivi iOS o Rooting su dispositivi Android).

5.7 Aspetti etici ed immagine aziendale

Premesso che EUCENTRE utilizza strumenti hardware e software quali firewall, antispam, antivirus e altri strumenti di controllo passivo con sistemi di filtraggio che consentono il blocco totale o parziale di determinati accessi a siti internet e garantiscono la sicurezza di eventuali intrusioni illecite dall'esterno non è comunque consentito:

- inviare con qualsiasi mezzo di comunicazione o memorizzare messaggi minatori, offensivi, di natura oltraggiosa e/o discriminatoria (ad esempio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica), esprimersi con linguaggio volgare ed in generale tenere comportamenti che possano recare danno all'immagine aziendale;
- inviare messaggi falsificando il mittente, ossia indicando un mittente diverso da quello reale;
- consultare siti internet eticamente non corretti e non decorosi o partecipare a blog, forum e chat inerenti tematiche contrari alle norme di pubblica sicurezza, anche in assenza di filtri automatici alla navigazione internet installati sui sistemi aziendali.

5.8 Riservatezza delle informazioni

- In caso di consegna di personal computer, tablet e smartphone per interventi di assistenza tecnica e/o al momento della loro dismissione (per riconsegna, rottamazione, ecc.) è necessario segnalare in anticipo all'Ufficio ICT l'eventuale presenza di dati aziendali che richiedano l'adozione di particolari misure di sicurezza e concordare con l'Ufficio ICT le più opportune modalità operative per garantire il livello di protezione richiesto (ad esempio trasferimento su supporti esterni o cartelle di rete).
- I documenti aziendali devono essere memorizzati nei vari dispositivi (PC, Tablet, Smartphone ecc.), inclusi anche quelli esterni (USB flash drive, SD card, hard disk esterni ecc.) in coerenza con il livello di classificazione delle informazioni aziendali contenute nei documenti stessi.

5.9 Furto, smarrimento ed altri atti dolosi

Le dotazioni informatiche portatili devono essere custodite con particolare cura sia durante gli spostamenti che sul luogo di lavoro. Il furto e lo smarrimento di apparati informatici in dotazione, come anche qualsiasi violazione manifesta o tentata alle informazioni aziendali in proprio possesso, contenute su supporti fisici o informatici individuali, devono essere segnalati all'Ufficio ICT e denunciati alle Autorità di Pubblica Sicurezza.

Contestualmente alla segnalazione è necessario modificare tempestivamente le eventuali password che si pensa siano state violate.

6. CONTROLLI

Per ridurre, negli strumenti utilizzati dal dipendente per rendere la prestazione lavorativa, il rischio di comportamenti illeciti o dannosi, di situazioni di pericolo, di eventuali intrusioni illecite o di utilizzi impropri e di violazione delle procedure aziendali ed al fine di garantire l'integrità, la riservatezza e la disponibilità del sistema informativo ed il regolare svolgimento delle attività, EUCENTRE utilizza preventivi accorgimenti tecnici e strumenti hardware e software volti a:

- prevenire la vulnerabilità della strumentazione e della rete (quali ad esempio firewall, antispam, antivirus, e altri strumenti di controllo passivo con sistemi di filtraggio che consentono il blocco totale o parziale di determinati accessi a siti internet o rilevazione e blocco del malware, sia su canali in chiaro che cifrati, senza comunque possibilità di accesso ai contenuti);
- ripristinare i dati in seguito a distruzione o danneggiamento (ad es copie di back up).

Rientrano nei sistemi e nelle misure che consentono il fisiologico e sicuro funzionamento delle strumentazioni informatiche, al fine di garantire un elevato livello di sicurezza della rete aziendale, strumenti quali ad esempio i sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei dati del messaggio e per la connessione ad internet.

L'utilizzo degli strumenti per rendere la prestazione lavorativa comporta la contabilizzazione dei consumi (es., stampanti /fotocopiatrici multifunzione di edificio, connessione internet, traffico telefonico).

Mediante strumenti software viene effettuato il controllo delle applicazioni installate sulle dotazioni informatiche per rilevare la presenza di software privo di licenza d'uso e/o malevolo e per verificare la corretta configurazione dei vari pacchetti installati.

Sono inoltre verificati, attraverso appositi strumenti software e sistemi di filtraggio antivirus che rivelano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete, i tentativi di attacco informatico per accesso fraudolento e/o danneggiamento dei dati e delle applicazioni informatiche centralizzate e delle infrastrutture informatiche aziendali (es. infrastrutture di rete, database, sistemi operativi, Active Directory, ecc.).

Nel caso di eventi a danno di EUCENTRE, o per esigenze tecniche (ad esempio, segnalazioni da soggetti esterni o dalle Autorità, sanzioni amministrative, fuga di informazioni aziendali, anomalie e malfunzionamenti sui sistemi informatici, virus, phishing e attacchi informatici, aggiornamento/sostituzione/implementazione

di software/hardware) o per la verifica sui costi aziendali, la Fondazione si riserva di effettuare controlli nel rispetto delle previsioni di legge.

EUCENTRE privilegerà controlli/verifiche su dati aggregati anonimi riferiti all'area in cui si è verificata l'anomalia. In caso di successive anomalie o, qualora nel corso o a seguito di tali verifiche/controlli, dovessero emergere operazioni ritenute dannose o attività non consentite e non coerenti con la presente procedura, la Fondazione si riserva di effettuare controlli mirati sui sistemi o sui singoli dispositivi.

Tali controlli/verifiche:

- saranno realizzati dall'Ufficio ICT nel pieno rispetto dei diritti e delle libertà fondamentali dei dipendenti e delle previsioni della presente policy;
- verranno eseguiti su dati pertinenti, in coerenza con le finalità del controllo e adottando ogni cautela per tutelare la dignità delle persone e la riservatezza;
- potranno concludersi con un avviso ai dipendenti dell'area in cui è stato rilevato un utilizzo non conforme degli strumenti aziendali con l'invito ad attenersi scrupolosamente alla presente policy.

Qualora, a seguito di tali verifiche, dovessero emergere operazioni ritenute dannose o attività non consentite e non coerenti con la presente procedura, EUCENTRE si riserva di adottare le iniziative atte a salvaguardare la sicurezza del sistema informativo e la tutela aziendale, ivi compresa la rimozione di file/applicazioni ritenuti dannosi e a tutelarla da eventuali conseguenze di tipo legale conseguenti alla violazione delle norme in materia.

Nel caso in cui dovessero rilevarsi comportamenti non conformi alle disposizioni aziendali, troverà applicazione, ove ne ricorrano i presupposti, quanto previsto dal contratto collettivo di lavoro sotto il profilo disciplinare.

7. UTILIZZO DI DISPOSITIVI INFORMATICI PRIVATI (BYOD)

La caratteristica principale di questa sezione della Policy è di stabilire regole comuni per l'utilizzo volontario dei dispositivi portatili privati da parte di utenti quali dipendenti, collaboratori e professionisti - pratica denominata BYOD "Bring Your Own Device" - e fornire linee guida per l'uso sicuro di tali dispositivi, se autorizzati da EUCENTRE.

Per dispositivi personali privati si intendono i computer portatili, gli smartphone ed i tablet, il cui utilizzo è autorizzato da EUCENTRE.

È importante che gli utenti che utilizzano i propri dispositivi personali per EUCENTRE comprendano pienamente gli obblighi a loro carico, pertanto i dipendenti che scelgono questa opzione devono confermare di aver letto, compreso e accettato le condizioni di EUCENTRE.

I dipendenti possono utilizzare il proprio dispositivo mobile per accedere alle seguenti risorse di proprietà dell'azienda: archivi su server, archivi on line, e-mail, calendari, elenchi di contatti. Altri contenuti potrebbero essere forniti attraverso soluzioni specificamente autorizzate.

Prima di utilizzare i servizi aziendali si deve permettere all'ufficio ICT di EUCENTRE di rilevare le informazioni del dispositivo e prendere visione di tutta la documentazione di supporto necessaria, compresa la politica e le linee guida per la configurazione dei dispositivi.

EUCENTRE si aspetta che gli utenti si assumano piena responsabilità in relazione alle informazioni o alle risorse aziendali che potrebbero essere disponibili attraverso il dispositivo.

I dispositivi devono essere utilizzati secondo i regolamenti e le politiche di EUCENTRE e comunque in modo etico.

Gli utenti rimangono gli unici responsabili della configurazione del proprio dispositivo.

Ogni utente è libero di utilizzare qualsiasi software o applicazione, ma ne è anche pienamente responsabile. Quindi EUCENTRE non può essere considerata responsabile per la violazione delle licenze software o app. scaricate sui dispositivi personali.

È totale responsabilità del dipendente assicurarsi che tutto il software installato sia debitamente autorizzato.

Gli utenti sono responsabili del backup di tutte le informazioni personali sui propri dischi rigidi personali o altri sistemi di backup.

I dipendenti e collaboratori devono assicurarsi che il loro dispositivo non contenga dati aziendali se il dispositivo viene trasmesso a terzi per scopi di manutenzione.

Quando si effettua il collegamento alle risorse di EUCENTRE l'accesso deve avvenire in base alle modalità definite dall'ufficio ICT.

Gli utenti sono responsabili per qualsiasi accesso ai dati di EUCENTRE e non devono divulgare i loro codici di accesso a terzi.

Alla cessazione del rapporto di lavoro, gli utenti devono restituire il software di proprietà di EUCENTRE, rimuovere tutte le applicazioni che accedono ai servizi aziendali ed eliminare tutte le informazioni di EUCENTRE dal proprio dispositivo.

Gli ex dipendenti ed ex collaboratori non sono autorizzati a conservare software o App o ripristinare eventuali software o app o dati di cui sono entrati in possesso durante la collaborazione con EUCENTRE.

Qualsiasi tentativo di ripristinare tali informazioni sarà soggetto a un'azione legale contro l'ex dipendente/collaboratore.

Tutti i costi relativi al dispositivo privato sono a carico dell'utente, in particolare EUCENTE non rimborserà i dipendenti per:

- Il costo di componenti del dispositivo.
- Il costo dell'intero dispositivo.
- Le assistenze tecniche o di riparazione.
- L'acquisto di software/app non approvati dal Capo Ufficio / Dipartimento.
- Dispositivi persi o rubati.

EUCENTRE si riserva il diritto di disconnettere qualsiasi dispositivo mobile dalla propria infrastruttura informatica o di disabilitare i servizi senza preavviso.

Gli utenti sono inoltre responsabili di notificare immediatamente l'evento di perdita o furto del dispositivo.

EUCENTRE non è responsabile per eventuali azioni involontarie che potrebbero portare alla perdita di dati personali.

Per quanto riguarda l'utilizzo della casella di posta aziendale e della connessione Wi-Fi aziendali valgono le indicazioni di cui alla presente policy.

REATO DI RAZZISMO E XENOFOBIA

(ART. 25 TERDECIES DEL D.LGS. 231/2001)

SOMMARIO

Reati in tema di razzismo e xenofobia

In data 27 novembre 2017 è stata pubblicata in Gazzetta Ufficiale la Legge 20 novembre 2017 n. 167 *"Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2017".* Il provvedimento amplia il catalogo dei reati presupposto del d.lgs. 231/2001, inserendo l'art. 25 terdecies rubricato come *"razzismo e xenofobia"*con il quale si prevede:

- in relazione alla commissione dei delitti di cui all'art. 3, comma 3 bis, della Legge 13 ottobre 1975 n. 654, si applica all'ente la sanzione pecuniaria da duecento a ottocento quote;
- nei casi di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art. 9 comma 2 per una durata non inferiore a un anno;
- se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dell'esercizio dell'attività ai sensi dell'art. 16, comma 3.

I delitti di cui si fa dunque rimando puniscono i partecipanti di organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali, religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concausa pericolo di diffusione, fondati in tutto o in parte sulla negazione, sulla minimizzazione in modo grave sull'apologia (inciso aggiunto dalla stessa legge Europea) della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

Protocolli e indirizzi operativi di attuazione

Possibili ambiti di commissione del reato

Si tratta di una tipologia di reato che riguarda la discriminazione razziale e xenofoba nei confronti di lavoratori stranieri o italiani presso qualsiasi sede della società, anche se in prova o impiegati a svolgere attività temporanee. In particolare l'area interessata è quella delle Risorse Umane se, a quest'ultima, è stata attribuita la responsabilità delle forze lavoro.

Principi di comportamento

Chi ha la responsabilità della gestione/conduzione del personale deve prestare la massima attenzione per prevenire e nel caso sopprimere episodi di razzismo o xenofobia che potrebbero essere consumati sia da figure apicali che sottoposti. Denunciando i fatti ai superiori interessati e all'Organismo di Vigilanza

Principi organizzativi e di controllo

Devono essere raccolte tutte le informazioni che potrebbero indicare la potenziale presenza di fatti di razzismo o xenofobia.

A mitigazione del potenziale rischio si rimanda al Codice Etico.

Flussi informativi verso l'Organismo di Vigilanza

Ogni informazione circa fatti di razzismo o xenofobia dovrebbe essere inoltrata all'Organismo di Vigilanza.

Chiunque venga a conoscenza di una situazione anomala per quanto sopra indicato è tenuto a comunicarlo in forma scritta all'Organismo di Vigilanza.

EUCENTRE
FOR YOUR SAFETY.

FONDAZIONE EUCENTRE
Centro Europeo di Formazione e Ricerca in Ingegneria Sismica
Via Adolfo Ferrata, 1 - 27100 Pavia, Italia - Tel. 0382.5169811 - Fax 0382.529131
E-mail: info@eucentre.it - Website: www.eucentre.it - P.IVA e C.F. 02009180189

TUTELA DEL DIPENDENTE CHE SEGNALA GLI ILLECITI

Importante misura di prevenzione è quella relativa alla Tutela del dipendente che segnala illeciti. Il dipendente che rileva condotte illecite di cui è venuto a conoscenza, le segnala al Responsabile via e-mail trasparenza@eucentre.it utilizzando l'apposito modulo reperibile nella sezione Amministrazione Trasparente del sito internet di EUCENTRE. Il Responsabile non deve rivelare l'identità del denunciante e deve svolgere attività di riscontro della segnalazione. Ove per effetto della segnalazione scaturisca un procedimento disciplinare contro un dipendente e la segnalazione costituisca elemento fondamentale per incolpare, si procede prima riferendo all'incolpato il solo contenuto della segnalazione e, successivamente svelata l'identità del denunciante.

Il dipendente che, in buona fede, segnala condotte illecite non deve in nessun modo essere discriminato e qualsiasi comportamento contro di lui deve essere sanzionato come grave comportamento disciplinare. Il dipendente segnalante che ritiene di subire discriminazioni o ritorsioni in ragione della segnalazione effettuata, lo riferisce al Responsabile il quale deve prendere immediate misure di protezione e comunicarle al segnalante stesso.

SEGNALAZIONE ESTERNA DEGLI ILLECITI

A chiunque è consentito segnalare eventuali illeciti utilizzando l'apposito modulo pubblicato nella sezione Amministrazione Trasparente del sito da inviare via e-mail trasparenza@eucentre.it o via p.e.c. protocollo@pec.eucentre.it al Responsabile della Prevenzione della Corruzione e della Trasparenza, che valuterà i controlli e/o le misure da intraprendere.

POSTA ELETTRONICA CERTIFICATA

L'utilizzo della Posta Elettronica Certificata (PEC), già introdotta dal D.Lgs. n. 82 del 7 marzo 2005 "Codice dell'Amministrazione Digitale" rientra negli adempimenti richiamati nel Programma in quanto strumentale per l'attuazione dei compiti di anticorruzione e trasparenza. La Fondazione EUCENTRE ha istituito la seguente casella di pec: protocollo@pec.eucentre.it.

La casella PEC è pubblicata sul sito della Fondazione, in Home Page. Poiché tutte le imprese e i professionisti hanno l'obbligo di dotarsi di una casella di posta elettronica certificata, sarà intensificato sempre più l'utilizzo della PEC da parte degli uffici.

ESTRATTO DAL SITO WEB

https://www.eucentre.it/altri-contenuti-segnalazioni-di-illecito/

SEGNALAZIONI DI ILLECITO

È consentito segnalare eventuali illeciti utilizzando il seguente modulo da inviare via e-mail trasparenza@eucentre.it o via p.e.c. protocollo@pec.eucentre.it al Responsabile della Prevenzione della Corruzione e della Trasparenza, che valuterà i controlli e/o le misure da intraprendere.

- Modulo per la segnalazione di presunti illeciti (DOC)

https://www.eucentre.it/altri-contenuti-accesso-civico/

ACCESSO CIVICO

Il Responsabile per la Trasparenza e per la Prevenzione della Corruzione cui inoltrare la richiesta di accesso civico è l'Ing. Ettore Festa, nominato nella funzione dal Consiglio di Amministrazione del 24.10.2017.

email: trasparenza@eucentre.it – pec: protocollo@pec.eucentre.it – Tel. 0382.5169869

La richiesta di accesso civico non è sottoposta ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente e non deve essere motivata. La predetta richiesta la cui presentazione è gratuita deve essere inoltrata al responsabile della trasparenza di Fondazione Eucentre. Quest'ultima, entro 30 giorni, pubblica nel sito il documento, l'informazione o il dato richiesto e lo trasmette, contestualmente, al richiedente.

Per la richiesta di accesso civico si può utilizzare l'allegato modulo.

- Modulo di accesso civico (DOC)