Principi di riferimento per l'adozione del Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/01 della Fondazione Festival dei Due Mondi - Spettacolo dal vivo

PARTI SPECIALI

Indice

1. Prefazione

Nella struttura del presente Modello Organizzativo si distinguono una "Parte Generale" – attinente all'organizzazione sociale nel suo complesso, al progetto per la realizzazione del Modello, all'Organismo di Vigilanza, al sistema disciplinare, alle modalità di formazione e di comunicazione – e le "Parti Speciali", che riguardano l'applicazione nel dettaglio dei principi richiamati nella "Parte Generale" con riferimento alle fattispecie di reato richiamate dal d.lgs. n. 231/2001 che la Fondazione ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività.

Nelle "Parti Speciali" che seguono sono analizzati rispettivamente:

- Parte Speciale "A" – Reati nei rapporti con la Pubblica Amministrazione, delitti con finalità di terrorismo o di eversione dell'ordine democratico, reati transnazionali, delitti di criminalità organizzata, delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria e reato di corruzione tra privati
- Parte Speciale "B" – Delitti commessi con violazione delle norme poste a tutela della salute e della sicurezza nei luoghi di lavoro
- Parte Speciale "C" - Delitti informatici e violazione del diritto d'autore

In considerazione dell'analisi del contesto aziendale, dell'attività svolta dalla Fondazione e delle aree potenzialmente soggette a rischio-reato, sono stati considerati rilevanti e quindi specificamente esaminati nel Modello, solo gli illeciti oggetto delle singole Parti Speciali cui si rimanda per una loro esatta individuazione.

Con riferimento agli altri "reati presupposto" della responsabilità amministrativa degli enti ai sensi del Decreto (Falsità in monete, in carte di pubblico credito, in valori di bollo, delitti contro la personalità individuale, delitti contro la vita e l'incolumità individuale, reati ambientali e contro l'industria e il commercio) si ritiene opportuno precisare che gli stessi, pur presi in considerazione in fase di analisi e anche in seguito all'effettuazione delle interviste con persone chiave, sono solo astrattamente e non concretamente ipotizzabili e comunque gli strumenti di controllo definiti nelle singole Parti Speciali possono costituire, unitamente al rispetto delle disposizioni legislative e del corpo normativo aziendale della Fondazione, un presidio anche per la prevenzione di tali reati.

Considerata la natura della Fondazione non sono stati esaminati i reati societari presupposto della responsabilità ex d.lgs. 231/01.

2. Finalità

La struttura del Modello con la previsione di una "Parte Speciale" consente l'evidenza, nell'ambito di ciascuna delle macro aree elaborate con riferimento ai gruppi di illecito quali previsti dal d.lgs. n. 231/2001, di individuare le Attività Sensibili alle quali vengono, in seguito, associati gli strumenti di controllo adottati per la prevenzione e il tempestivo aggiornamento del Modello.

Nel caso in cui esponenti della Fondazione si trovino a dover gestire Attività Sensibili diverse da quelle indicate nelle singole Parti Speciali, le stesse dovranno comunque essere condotte nel rispetto: a) degli standard di controllo generali; b) di quanto regolamentato dalla documentazione organizzativa interna; c) delle disposizioni di legge.

E' responsabilità delle singole funzioni interessate segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alle Parti Speciali, in accordo a quanto previsto dalla Parte Generale.

La "Parte Speciale" va messa in relazione con i principi comportamentali contenuti nelle procedure aziendali che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive della Fondazione.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- indicare le modalità che gli esponenti aziendali sono chiamati a osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- "Principi di riferimento per l'adozione del Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/01";
- manuali/policy/procedure/istruzioni operative;
- procure e deleghe;
- Codice di comportamento;
- ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

E' inoltre espressamente e ovviamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

3. Il sistema dei controlli

Nello svolgimento delle Attività Sensibili la Fondazione si ispira ai seguenti standard di controllo:

- standard di controllo generali, applicabili a tutte le Attività Sensibili prese in considerazione;
- standard di controllo specifici, applicabili a ciascuna delle Attività Sensibili per la quale sono individuati.

3.1. *Standard* di controllo generali

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

Segregazione delle attività: deve esistere segregazione delle attività tra chi esegue, chi controlla e chi autorizza.

Esistenza di procedure/norme/circolari: devono esistere disposizioni aziendali idonee a fornire almeno i principi di riferimento generali per la regolamentazione dell'attività sensibile.

Poteri di firma e poteri autorizzativi: devono esistere regole formalizzate per l'esercizio dei poteri di firma e poteri autorizzativi interni.

Tracciabilità: i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati devono assicurare l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della Fondazione e le modalità di gestione delle risorse finanziarie.

3.2 *Standard* di controllo specifici

Sulla base degli standard di controllo generali sopra riportati, gli standard di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Fondazione rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle Attività Sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:
   - siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
   - siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
   - la Fondazione adotti strumenti di comunicazione dei poteri di firma conferiti - sistema delle deleghe e procure;
   - l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche;
   - non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
   - l'accesso e l'intervento sui dati della Fondazione sia consentito esclusivamente alle persone autorizzate in conformità al d.lgs. n. 196 del 2003 e successive modifiche e integrazioni, anche regolamentari;
   - sia garantita la riservatezza nella trasmissione delle informazioni;

- i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza.

d) il soggetto che intrattiene rapporti o effettua negoziazioni con la pubblica amministrazione non può da solo e liberamente:

- stipulare i contratti che ha negoziato;
- accedere alle risorse finanziarie e/o autorizzare disposizioni di pagamento;
- conferire incarichi di consulenza / prestazioni professionali;
- concedere qualsivoglia utilità;
- procedere ad assunzioni di personale.

Parte Speciale "A" – Reati nei rapporti con la Pubblica Amministrazione, delitti con finalità di terrorismo o di eversione dell'ordine democratico, reati transnazionali, delitti di criminalità organizzata, delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, reato di corruzione tra privati

1. Le Attività Sensibili ai fini del d.lgs. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Fondazione nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Attraverso l'analisi dei processi della Fondazione sono state individuate le seguenti attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate:

1. **Selezione dei fornitori di beni e servizi, negoziazione e stipula dei relativi contratti (ivi inclusa la negoziazione / stipula di contratti in qualità di ente aggiudicatore)**
2. **Gestione di contratti per l'acquisto di beni e servizi**
3. **Gestione di contenziosi giudiziali, stragiudiziali e procedimenti arbitrali**
4. **Gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari;**
5. **Gestione dei rapporti con soggetti pubblici relativi all'assunzione, gestione e amministrazione del personale, nonché dei relativi accertamenti/ispezioni che ne derivano**
6. **Gestione dei rapporti con Autorità di Vigilanza relativi allo svolgimento di attività regolate dalla legge**
7. **Richiesta / acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici**
8. **Gestione dei rapporti e degli adempimenti con i soggetti pubblici per la richiesta di autorizzazioni/ licenze/ provvedimenti amministrativi / pratiche per l'esercizio delle attività aziendali, e in eventuali verifiche / accertamenti che ne derivano**
9. **Gestione degli adempimenti fiscali e dei relativi rapporti con l'Amministrazione Finanziaria, anche in eventuali verifiche / accertamenti che ne derivano**
10. **Gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici**
11. **Gestione delle operazioni finanziarie**
12. **Gestione dei rimborsi spese a dipendenti, ex dipendenti e cariche sociali**
13. **Selezione, assunzione e gestione amministrativa del personale**
14. **Gestione del credito**

2. *Standard* di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi alle singole Attività Sensibili.

1 Selezione dei fornitori di beni e servizi, negoziazione e stipula dei relativi contratti (ivi inclusa la negoziazione / stipula di contratti in qualità di ente aggiudicatore)

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dell'approvvigionamento di beni, lavori e servizi prevedano:
  a. la predisposizione e autorizzazione delle richieste di acquisto;
  b. i criteri e le modalità di assegnazione del contratto (es. pubblicazione del bando, fornitore unico, short vendor list, assegnazione diretta, acquisto in condizioni di urgenza, ecc.);
  c. il ricorso alla procedura "assegnazione diretta" solo per casistiche limitate e chiaramente individuate, adeguatamente motivato e documentato e sottoposto a idonei sistemi di controllo e sistemi autorizzativi a un adeguato livello gerarchico;
  d. le modalità e i criteri per la predisposizione e l'approvazione del bando di gara;
  e. le modalità di diffusione e pubblicizzazione del bando di gara;
  f. le modalità di definizione e approvazione delle eventuali short vendor list;
  g. i criteri di predisposizione e autorizzazione delle richieste di offerta, inclusa la definizione delle specifiche tecniche e delle condizioni tecnico commerciali;
  h. un modello di valutazione delle offerte (tecniche/economiche) improntato alla trasparenza e alla maggiore limitazione possibile di criteri di soggettività;
  i. i criteri di rotazione delle persone coinvolte nel processo di approvvigionamento ove possibile;
  j. idonei sistemi di monitoraggio al fine di garantire una corretta e fisiologica rotazione dei fornitori inclusi nelle vendor list;
  k. previsioni contrattuali standardizzate in relazione alla natura e tipologia di contratto, ivi incluse previsioni contrattuali finalizzate all'osservanza di principi di controllo/regole etiche nella gestione delle attività da parte del terzo, e le attività da seguirsi in caso di eventuali scostamenti;
  l. l'approvazione del contratto da parte di adeguati livelli autorizzativi.
- deve esistere il divieto di:
  a. intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  b. concessione di utilità a persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  c. assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dell'accreditamento/qualifica dei fornitori di beni e servizi e dei consulenti/professionisti/associazioni di professionisti che prestano attività di opera intellettuale prevedano:

a. la definizione dei requisiti per l'accreditamento/qualifica, ivi incluse le caratteristiche tecnico professionali, di onorabilità e, per quanto opportuno rispetto alla natura e oggetto del contratto, la solidità economico finanziaria;
b. le modalità e i criteri per l'attribuzione, modifica, sospensione e revoca dell'accreditamento/qualifica che tengano conto di eventuali criticità che dovessero verificarsi nel corso dell'esecuzione del contratto;
c. le modalità di aggiornamento dell'accreditamento/qualifica finalizzata alla verifica nel tempo del mantenimento dei relativi requisiti.

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che prevedano in caso di esistenza di relazioni privilegiate[1]/conflitto di interesse tra il rappresentante della Fondazione e la terza parte (ad esempio, fornitori, consulenti, intermediari, partner, clienti, ecc.), l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto delegandola ad altra funzione e, in caso di contratto eccedente determinate soglie di importo, l'obbligo di sottoporlo all'approvazione da parte di un'unità organizzativa diversa da quella del proprio superiore gerarchico.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione di terze parti prevedano:
  a. la definizione delle casistiche in cui sia necessario procedere alla *due diligence*/verifica preventiva sulla terza parte;
  b. le modalità di svolgimento e la formalizzazione, con l'eventuale coinvolgimento delle funzioni competenti della Fondazione, di una *due diligence*/verifica preventiva sulla terza parte in relazione alle caratteristiche tecnico professionali, di onorabilità e, per quanto opportuno, rispetto alla natura ed oggetto del contratto, la solidità economico finanziaria.

2) Gestione di contratti per l'acquisto di beni e servizi

La regolamentazione dell'attività prevede:

- deve esistere il divieto di:
  a. intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  b. concessione di utilità a persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  c. assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dell'accreditamento/qualifica dei fornitori di beni e servizi e dei consulenti/professionisti/associazioni di professionisti che prestano attività di opera intellettuale prevedano:

[1] Per relazioni privilegiate si intendono situazioni di parentela o affinità, o di vincoli di natura personale o patrimoniale che possono influenzare i comportamenti

a. la definizione dei requisiti per l'accreditamento/qualifica, ivi incluse le caratteristiche tecnico professionali, di onorabilità e, per quanto opportuno rispetto alla natura e oggetto del contratto, la solidità economico finanziaria;
b. le modalità e i criteri per l'attribuzione, modifica, sospensione e revoca dell'accreditamento/qualifica che tengano conto di eventuali criticità che dovessero verificarsi nel corso dell'esecuzione del contratto;
c. le modalità di aggiornamento dell'accreditamento/qualifica finalizzata alla verifica nel tempo del mantenimento dei relativi requisiti.
d. devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che prevedano in caso di esistenza di relazioni privilegiate[2]/conflitto di interesse tra il rappresentante della Fondazione e la terza parte (ad esempio, fornitori, consulenti, intermediari, partner, clienti, ecc.), l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto delegandola ad altra funzione e, in caso di contratto eccedente determinate soglie di importo, l'obbligo di sottoporlo all'approvazione da parte di un'unità organizzativa diversa da quella del proprio superiore gerarchico.

- devono essere adottati e attuati uno o più strumenti normativi che annoverino:
  a. l'individuazione della funzione, unità/responsabile dell'esecuzione del contratto ("gestore del contratto") con indicazione di ruolo e compiti assegnati;
  b. l'autorizzazione da parte di posizione abilitata, equivalente o superiore, diversa dal gestore del contratto, in caso di modifiche / integrazioni e/o rinnovi dello stesso;
  c. l'handover[3] del contratto nel caso in cui la funzione che negozia il contratto non coincida con la funzione che lo gestisce.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della gestione dei contratti per l'acquisto di beni e servizi prevedano:
  a. in caso di contratto aperto, la verifica della coerenza tra gli Ordini di Consegna/Ordini di Lavoro rispetto ai parametri previsti nel contratto medesimo;
  b. in caso di contratto aperto, la sottoscrizione degli Ordini di Consegna/Ordini di Lavoro da parte di adeguati livelli autorizzativi;
  c. la verifica della conformità delle caratteristiche dei beni, lavori e servizi oggetto di acquisto, rispetto al contenuto dell'Ordine di Consegna/Ordine di Lavoro/contratto;
  d. la verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti;
  e. le modalità ed i criteri di registrazione delle note di debito o delle note di credito ricevute dai fornitori.

[2] Per relazioni privilegiate si intendono situazioni di parentela o affinità, o di vincoli di natura personale o patrimoniale che possono influenzare i comportamenti

[3] Per *handover* si intende il trasferimento al gestore del contratto di tutte le informazioni utili alla corretta gestione dello stesso

3) Gestione di contenziosi giudiziali, stragiudiziali e procedimenti arbitrali

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dell'accreditamento/qualifica dei fornitori di beni e servizi e dei consulenti/professionisti/associazioni di professionisti che prestano attività di opera intellettuale prevedano:
  a. la definizione dei requisiti per l'accreditamento/qualifica, ivi incluse le caratteristiche tecnico professionali, di onorabilità e, per quanto opportuno rispetto alla natura e oggetto del contratto, la solidità economico finanziaria;
  b. le modalità e i criteri per l'attribuzione, modifica, sospensione e revoca dell'accreditamento/qualifica che tengano conto di eventuali criticità che dovessero verificarsi nel corso dell'esecuzione del contratto;
  c. le modalità di aggiornamento dell'accreditamento/qualifica finalizzata alla verifica nel tempo del mantenimento dei relativi requisiti.
  d. devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che prevedano in caso di esistenza di relazioni privilegiate[4]/conflitto di interesse tra il rappresentante Fondazione e la terza parte (ad esempio, fornitori, consulenti, intermediari, partner, clienti, ecc.), l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto delegandola ad altra funzione e, in caso di contratto eccedente determinate soglie di importo, l'obbligo di sottoporlo all'approvazione da parte di un'unità organizzativa diversa da quella del proprio superiore gerarchico.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che prevedano in caso di esistenza di relazioni privilegiate[5]/conflitto di interesse tra il rappresentante della Fondazione e la terza parte (ad esempio, fornitori, consulenti, intermediari, partner, clienti, ecc.), l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto delegandola ad altra funzione e, in caso di contratto eccedente determinate soglie di importo, l'obbligo di sottoporlo all'approvazione da parte di un'unità organizzativa diversa da quella del proprio superiore gerarchico.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione di terze parti prevedano:
  a. la definizione delle casistiche in cui sia necessario procedere alla *due diligence*/verifica preventiva sulla terza parte;
  b. le modalità di svolgimento e la formalizzazione, con l'eventuale coinvolgimento delle funzioni competenti Fondazione, di una *due diligence*/verifica preventiva sulla terza parte in relazione

[4] Per relazioni privilegiate si intendono situazioni di parentela o affinità, o di vincoli di natura personale o patrimoniale che possono influenzare i comportamenti

[5] Per relazioni privilegiate si intendono situazioni di parentela o affinità, o di vincoli di natura personale o patrimoniale che possono influenzare i comportamenti

alle caratteristiche tecnico professionali, di onorabilità e, per quanto opportuno, rispetto alla natura e oggetto del contratto, la solidità economico finanziaria.

- devono essere adottati e attuati uno o più strumenti normativi che annoverino:
  a. l'individuazione della funzione, unità/responsabile dell'esecuzione del contratto ("gestore del contratto") con indicazione di ruolo e compiti assegnati;
  b. l'autorizzazione da parte di posizione abilitata, equivalente o superiore, diversa dal gestore del contratto, in caso di modifiche / integrazioni e/o rinnovi dello stesso;
  c. l'handover[6] del contratto nel caso in cui la funzione che negozia il contratto non coincida con la funzione che lo gestisce.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della gestione dei contratti per l'acquisto di beni e servizi prevedano:
  a. in caso di contratto aperto, la verifica della coerenza tra gli Ordini di Consegna/Ordini di Lavoro rispetto ai parametri previsti nel contratto medesimo;
  b. in caso di contratto aperto, la sottoscrizione degli Ordini di Consegna/Ordini di Lavoro da parte di adeguati livelli autorizzativi;
  c. la verifica della conformità delle caratteristiche dei beni, lavori e servizi oggetto di acquisto, rispetto al contenuto dell'Ordine di Consegna/Ordine di Lavoro/contratto;
  d. la verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti;
  e. le modalità ed i criteri di registrazione delle note di debito o delle note di credito ricevute dai fornitori.
- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della gestione dei contenziosi giudiziali, stragiudiziali e procedimenti arbitrali, prevedano:
  a. principi di indirizzo per la definizione delle iniziative da intraprendere, tenuto conto della natura, dell'oggetto e del valore della causa, e i relativi livelli approvativi o comunque di condivisione;
  b. flussi informativi in relazione a determinati rapporti con le Autorità Giudiziarie e con loro delegati e/o ausiliari;
  c. il ruolo della funzione legale in relazione alle azioni da intraprendere per ottemperare alle richieste delle Autorità Giudiziarie e dei loro delegati e/o ausiliari, nonché un adeguato processo di verifica da parte delle funzioni aziendali competenti per la materia;
  d. specifici flussi di reporting in relazione a eventi giudiziari di particolare rilevanza.

4) Gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari

La regolamentazione dell'attività prevede che, laddove esponenti aziendali siano stati destinatari di richieste di rendere o produrre davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale

[6] Per handover si intende il trasferimento al gestore del contratto di tutte le informazioni utili alla corretta gestione dello stesso

relative all'esercizio delle proprie funzioni, il divieto di indurre o favorire i medesimi esponenti a non rendere/produrre le suddette dichiarazioni, ovvero a renderle mendaci.

5) Gestione dei rapporti con soggetti pubblici relativi all'assunzione, gestione ed amministrazione del personale, nonché dei relativi accertamenti/ispezioni che ne derivano

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con pubblici ufficiali o incaricati di pubblico servizio prevedano:
  a. l'individuazione dei soggetti incaricati di avere rapporti con pubblici ufficiali o incaricati di pubblico servizio;
  b. l'individuazione delle tipologie di rapporti con pubblici ufficiali o incaricati di pubblico servizio e le relative modalità di gestione
  c. la formalizzazione, per le tipologie di rapporti di cui sopra, di una reportistica relativa al rapporto intercorso, salvo che non sia già predisposta apposita documentazione dalla controparte
  d. le modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali o incaricati di pubblico servizio, con il supporto delle funzioni competenti

6) Gestione dei rapporti con Autorità di Vigilanza relativi allo svolgimento di attività regolate dalla legge

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con pubblici ufficiali o incaricati di pubblico servizio prevedano:
  a. l'individuazione dei soggetti incaricati di avere rapporti con pubblici ufficiali o incaricati di pubblico servizio;
  b. l'individuazione delle tipologie di rapporti con pubblici ufficiali o incaricati di pubblico servizio e le relative modalità di gestione;
  c. la formalizzazione, per le tipologie di rapporti di cui sopra, di una reportistica relativa al rapporto intercorso, salvo che non sia già predisposta apposita documentazione dalla controparte;
  d. le modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali o incaricati di pubblico servizio, con il supporto delle funzioni competenti.

7) Richiesta / acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della richiesta/acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici prevedano:

a. le modalità e i criteri per la selezione dei bandi ai quali partecipare;
b. le modalità di raccolta e verifica delle informazioni necessarie per la predisposizione della documentazione relativa all'istanza;
c. l'approvazione da parte di adeguati livelli autorizzativi della documentazione da trasmettere in relazione alla richiesta di fruizione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie;
d. l'individuazione dell'unità deputata ad intrattenere rapporti con la controparte (ad es. richiesta di chiarimenti alla controparte);
e. le modalità di raccolta e verifica, con il supporto delle funzioni competenti, delle informazioni necessarie per la rendicontazione dei contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie ottenute;
f. l'approvazione da parte di adeguati livelli autorizzativi della documentazione di rendicontazione da trasmettere;
g. l'esistenza di segregazione di ruoli e responsabilità nelle fasi di istanza, gestione e rendicontazione.

8) Gestione dei rapporti e degli adempimenti con i soggetti pubblici per la richiesta di autorizzazioni/ licenze/ provvedimenti amministrativi / pratiche per l'esercizio delle attività aziendali, e in eventuali verifiche / accertamenti che ne derivano

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con pubblici ufficiali o incaricati di pubblico servizio prevedano:
  a. l'individuazione dei soggetti incaricati di avere rapporti con pubblici ufficiali o incaricati di pubblico servizio;
  b. l'individuazione delle tipologie di rapporti con pubblici ufficiali o incaricati di pubblico servizio e le relative modalità di gestione;
  c. la formalizzazione, per le tipologie di rapporti di cui sopra, di una reportistica relativa al rapporto intercorso, salvo che non sia già predisposta apposita documentazione dalla controparte;
  d. le modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali o incaricati di pubblico servizio, con il supporto delle funzioni competenti.

9) Gestione degli adempimenti fiscali e dei relativi rapporti con l'Amministrazione Finanziaria, anche in eventuali verifiche / accertamenti che ne derivano

La regolamentazione dell'attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con pubblici ufficiali o incaricati di pubblico servizio prevedano:

a. l'individuazione dei soggetti incaricati di avere rapporti con pubblici ufficiali o incaricati di pubblico servizio;
b. l'individuazione delle tipologie di rapporti con pubblici ufficiali o incaricati di pubblico servizio e le relative modalità di gestione;
c. la formalizzazione, per le tipologie di rapporti di cui sopra, di una reportistica relativa al rapporto intercorso, salvo che non sia già predisposta apposita documentazione dalla controparte;
d. le modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali o incaricati di pubblico servizio, con il supporto delle funzioni competenti.

10) Gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici

La regolamentazione dell'attività prevede:

- le disposizioni in materia di sicurezza del sistema informatico e telematico adottate dalla Fondazione includono:
  a. la definizione degli obiettivi, delle linee guida e degli strumenti normativi relativamente alla sicurezza informatica e telematica
  b. l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti
  c. i rapporti con gli outsourcer informatici;
  d. le modalità di aggiornamento delle stesse, anche a seguito di cambiamenti significativi;
  e. le esigenze di carattere legale con riferimento alle clausole contrattuali relative alla sicurezza informatica e telematica;
  f. la definizione dell'approccio nell'analisi e valutazione dei rischi e l'identificazione della relativa metodologia;
  g. la definizione dei principi di classificazione dei dati e delle informazioni (confidenzialità, autenticità e integrità);
  h. la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni

11) Gestione delle operazioni finanziarie

La regolamentazione dell'attività prevede:

- deve esistere il divieto di:
  a. intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  b. concessione di utilità a persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  c. assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse.

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito delle operazioni finanziarie prevedano:
    a. il divieto di utilizzo del contante o altro strumento finanziario al portatore (fermo restando eventuali eccezioni dettate da esigenze operative/gestionali oggettivamente riscontrabili, sempre per importi limitati e comunque rientranti nei limiti di legge), per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia
    b. l'obbligo di utilizzare operatori finanziari abilitati per la realizzazione di ciascuna delle operazioni di cui alla precedente lettera a);
    c. la verifica dei destinatari dei pagamenti;
    d. la verifica di corrispondenza tra la transazione finanziaria disposta e la relativa documentazione di supporto disponibile;
    e. il divieto di effettuare pagamenti in paesi diversi da quelli in cui risiede la controparte o in cui ha esecuzione il contratto

    Con riferimento alle operazioni da effettuare tramite piccola cassa preveda:
    a. le modalità di utilizzo della piccola cassa (incluse le tipologie di spese e i limiti di utilizzo);
    b. le riconciliazioni periodiche delle giacenze della piccola cassa con il registro delle movimentazioni di cassa.

    Inoltre, con riferimento ai conti correnti bancari definisca:
    a. le modalità operative di apertura, movimentazione e chiusura dei conti correnti presso banche e istituzioni finanziarie;
    b. le riconciliazioni periodiche dei conti corrente.

12) Gestione dei rimborsi spese a dipendenti, ex dipendenti e cariche sociali

La regolamentazione dell’attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell’ambito della gestione dei rimborsi spese a dipendenti, ex dipendenti e cariche sociali prevedano:
    a. la definizione delle tipologie e dei limiti delle spese rimborsabili e delle modalità di effettuazione e di rimborso delle stesse;
    b. i criteri e le modalità per l’autorizzazione della trasferta;
    c. le modalità di rendicontazione delle spese effettuate, con indicazione dello scopo della spesa;
    d. le verifiche delle spese sostenute e le modalità di autorizzazione al rimborso.

13) Selezione, assunzione e gestione amministrativa del personale

La regolamentazione dell’attività prevede:

- devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione, assunzione e gestione amministrativa del personale prevedano:
  a. un processo di pianificazione delle risorse da assumere che tenga conto del fabbisogno;
  b. l'individuazione dei requisiti minimi necessari (profilo) per ricoprire il ruolo e il relativo livello di retribuzione nel rispetto di quanto previsto dai Contratti Collettivi Nazionali del Lavoro (ove applicabili) e in coerenza con le tabelle retributive di riferimento) la definizione di un processo di selezione del personale che disciplini:
     i) la ricerca di una pluralità di candidature in funzione della complessità del ruolo da ricoprire;
     ii) la gestione dei conflitti di interesse tra il selezionatore e il candidato;
     iii) la verifica, attraverso diverse fasi di screening, della coerenza delle candidature con il profilo definito;
  c. lo svolgimento di verifiche pre-assuntive finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che espongano la Fondazione al rischio di commissione di reati presupposto in tema di responsabilità amministrativa d'impresa (con particolare attenzione all'esistenza di procedimenti penali/carichi pendenti, di conflitto di interesse/relazioni tali da interferire con le funzioni di pubblici ufficiali, incaricati di pubblico servizio chiamati ad operare in relazione ad attività per le quali la Fondazione ha un interesse concreto cosi come con rappresentanti di vertice di società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa che abbiano un particolare rilievo ai fini aziendali);
  d. la definizione di eventuali circostanze ostative nonché delle diverse circostanze che si pongono solo come punto di attenzione all'assunzione a seguito del completamento delle verifiche pre-assuntive;
  e. l'autorizzazione all'assunzione da parte di adeguati livelli;
  f. le modalità di apertura e di gestione dell'anagrafica dipendente;
  g. sistemi, anche automatizzati, che garantiscano la tracciabilità della rilevazione delle presenze in accordo con le previsioni di legge applicabili;
  h. la verifica della correttezza delle retribuzioni erogate.
- deve esistere il divieto di:
  a. intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse
  b. concessione di utilità a persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
  c. assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse.

14) Gestione del credito

La regolamentazione dell’attività prevede che devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che prevedano in caso di esistenza di relazioni privilegiate/conflitto di interesse tra il rappresentante della Fondazione e la terza parte (ad esempio, fornitori, consulenti, intermediari, partner, clienti, ecc.), l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto delegandola ad altra funzione e, in caso di contratto eccedente determinate soglie di importo, l'obbligo di sottoporlo all'approvazione da parte di un'unità organizzativa diversa da quella del proprio superiore gerarchico.

Parte Speciale B- Delitti con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

1. Premessa

L'art. 9 della legge n. 123/2007 ha introdotto nel d.lgs. n. 231/2001 l'art. 25-septies, che estende la responsabilità amministrativa degli enti ai reati di omicidio colposo (art. 589 – 2° comma c.p.) e lesioni personali colpose gravi o gravissime (art. 590 – 3° comma c.p.), commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (quali ad esempio quelle previste dal d.lgs. 9 aprile 2008, n. 81 "Testo unico sulla salute e sicurezza sul lavoro" e successive integrazioni e modificazioni).

Stante la peculiarità della materia da disciplinare, incentrata sull'apprestamento di misure di riduzione del rischio, non già con riguardo a reati dolosi, tipicamente riconducibili a decisioni, bensì a reati colposi, di regola compiuti nello svolgimento dell'attività produttiva, la presente "Parte Speciale" denota una struttura in parte diversa da quella adoperata per disciplinare le precedenti forme di rischio: diversità imposta dal fatto che il settore in esame è, in larga parte, etero normato, vale a dire contraddistinto dalla presenza di una fitta rete di disposizioni normative, che abbracciano sia i meccanismi di individuazione delle posizioni di garanzia, sia la tipologia e i contenuti dei presidi cautelari. La 'specialità' - normativa e criminologia - del 'contesto' rende, dunque, necessaria la costruzione di un sistema di prevenzione autonomamente 'strutturato'.

Quanto ai criteri oggettivi di imputazione della responsabilità all'ente, occorre fare riferimento all'art. 5 del d.lgs. 231/01, laddove stabilisce che i reati-presupposto sono riferibili all'ente solo se commessi (da soggetti apicali e non) nel suo interesse o a suo vantaggio. La riferibilità di tale criterio di imputazione oggettiva ai reati colposi, apprezzabile con una valutazione ex post, fa leva sul cd. risparmio di spesa per l'ente: il vantaggio consisterebbe nel mancato impiego delle risorse economiche necessarie per conformare l'attività aziendale, sia sul terreno della dislocazione dei garanti che su quello dell'adozione e dell'adeguamento delle misure precauzionali, nonché in termini di risparmio di tempo per lo svolgimento dell'attività aziendale.

In merito al il criterio di imputazione soggettiva, l'adozione del Modello di organizzazione, gestione e controllo mantiene una decisiva funzione esimente della responsabilità dell'ente; tanto più che, nel caso di reato commesso dai soggetti apicali, secondo un orientamento dottrinale non sarebbe neppure necessario richiedere la dimostrazione della condotta fraudolenta elusiva, essendo, per contro, sufficiente – ai fini dell'esonero di responsabilità dell'ente – dimostrare l'adozione del modello, la sua idoneità preventiva e che la sua violazione non è dipesa da un difetto di controllo e di vigilanza.

Con riferimento ai delitti dai quali può scaturire la responsabilità amministrativa dell'ente, il d.lgs. n. 81 del 9 aprile 2008 recante il Testo Unico in materia di salute e sicurezza del lavoro stabilisce, all'art. 30 (Modelli di organizzazione e di gestione) che il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa, adottato ed efficacemente attuato, deve assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici individuati dalla norma relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Tale modello organizzativo e gestionale, ai sensi del citato d.lgs. n. 81/2008, deve:

- prevedere anche idonei sistemi di registrazione dell'avvenuta effettuazione delle sopra menzionate attività;
- in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Il medesimo art. 30 dispone che:

- in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti (comma 5);
- la commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali (comma 5-bis).
-

2. La Fondazione e la gestione della salute e sicurezza sui luoghi di lavoro

La Fondazione ha organizzato il proprio personale secondo le seguenti categorie aziendali:· Datore di Lavoro; Dirigenti;· Preposti;· Lavoratori;· Responsabili del Servizio di Prevenzione e Protezione (RSPP);· Medico competente (MC).

Le responsabilità risultano definite come segue:

- il Datore di Lavoro è il responsabile in materia di Ambiente e di Salute e Sicurezza sui luoghi di lavoro.
- i Dirigenti sono le persone che, in ragione delle competenze professionali e dei poteri conferiti, attuano le direttive del Datore di lavoro organizzando l'attività lavorativa e vigilando su di essa.
- i Preposti sono i "capi intermedi", alle dipendenze dei "Dirigenti" suddetti che in ragione delle competenze professionali e nei limiti dei poteri conferiti, sovrintendono alle attività lavorative, garantiscono l'attuazione delle direttive ricevute, controllano la corretta esecuzione delle attività da parte dei lavoratori ed esercitano un funzionale potere di iniziativa.

I documenti in cui sono formalizzate le regole per la gestione della salute e sicurezza sono:

- Manuali
- Procedure Operative;
- DVR.

3. Le Attività Sensibili ai fini del d.lgs. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Fondazione nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 25-*septies* del Decreto, le attività della Fondazione di seguito elencate.

1) ***Pianificazione***: si tratta delle attività di pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro volte a fissare obiettivi coerenti con la politica aziendale, stabilire i processi necessari al raggiungimento degli obiettivi, definire e assegnare risorse.
2) ***Attuazione e funzionamento***: si tratta delle attività volta a definire strutture organizzative e responsabilità, modalità di formazione, consultazione e comunicazione, modalità di gestione del sistema documentale, di controllo dei documenti e dei dati, le modalità di controllo operativo, la gestione delle emergenze che si articola nelle seguenti attività:
   - sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro;
   - individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro;
   - attività di informazione in tema di salute, sicurezza e igiene sul lavoro;
   - attività di formazione in tema di salute, sicurezza e igiene sul lavoro;
   - attività di addestramento;
   - rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
   - gestione degli asset aziendali con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro.
3) ***Controllo e azioni correttive***: si tratta delle attività volte a implementare modalità di misura e monitoraggio delle prestazioni, la registrazione e il monitoraggio degli infortuni, incidenti, non conformità, azioni correttive e preventive, modalità di gestione delle registrazioni, modalità di esecuzione *audit* periodici.
4) ***Riesame della direzione***: si tratta delle attività di riesame periodico del Vertice Aziendale al fine di valutare se il sistema di gestione della salute e sicurezza è stato completamente realizzato e se è sufficiente alla realizzazione della politica e degli obiettivi dell'azienda.

4. *Standard* di controllo specifici

Gli *standard* di controllo specifici, definiti per le singole Attività Sensibili individuate sono quelli di seguito descritti.

Pianificazione

Per le attività di pianificazione del sistema di gestione della salute e sicurezza del lavoratore sono stabiliti i seguenti *standard* di controllo:

- deve essere adottato ed attuato uno strumento normativo che preveda la formalizzazione -della Politica contenente gli indirizzi ed i principi di riferimento generali in tema di ambiente, salute, sicurezza ed igiene sul lavoro. Tale strumento prevede che la Politica:
  a. sia formalmente approvata dalla direzione aziendale;
  b. contenga l'impegno a essere conforme con le vigenti leggi in materia di ambiente, salute, sicurezza e igiene applicabili e con gli altri requisiti sottoscritti;
  c. sia adeguatamente diffusa ai dipendenti e alle parti interessate;
  d. sia periodicamente riesaminata per assicurare che gli indirizzi e i principi di riferimento in esso indicati siano appropriati e adeguati rispetto ai rischi presenti nell'organizzazione (ad es. riesame sulla base delle Linee Guida per l'attuazione del sistema di gestione della sicurezza, dei nuovi regolamenti e delle leggi, etc.).
- deve essere adottato ed attuato uno strumento normativo e/o organizzativo che preveda la definizione di piani in materia di ambiente, salute e sicurezza, approvati dagli organi sociali competenti che:
  a. individuino i soggetti coinvolti, scadenze e risorse necessarie per l'attuazione (finanziarie, umane, logistiche, di equipaggiamento);
  b. siano comunicati al personale interessato al fine di garantirne una adeguata comprensione;
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che:
  a. disciplini ruoli e responsabilità dell'aggiornamento delle informazioni riguardo alla legislazione rilevante e alle altre prescrizioni applicabili in tema di ambiente, salute, sicurezza e igiene sul lavoro;
  b. definisca criteri e modalità da adottarsi per la comunicazione degli aggiornamenti alle area aziendali interessate.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che:
  a. disciplini ruoli e responsabilità nella gestione della documentazione relativa al sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (es. Manuale, Procedure, Istruzioni di lavoro) in coerenza con la Politica e le linee guida aziendali;
  b. definisca le modalità di gestione, archiviazione e conservazione della documentazione prodotta (es: modalità di archiviazione/protocollazione a garanzia di un adeguato livello di tracciabilità /verificabilità).

Attuazione e funzionamento

In merito all'organizzazione della struttura con riferimento alle attività in tema di salute e sicurezza sul lavoro, gli *standard* di controllo specifici sono:

- esistenza di disposizioni organizzative che, tenendo conto della struttura organizzativa della Fondazione e del settore di attività produttiva, siano idonei ad individuare la figura datoriale, con i relativi poteri ed obblighi;
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento al Responsabile del Servizio di Prevenzione e Protezione (RSPP) previsto ai sensi della normativa vigente:
  a. preveda una formale designazione;
  b. definisca, in considerazione dell'ambito di attività, i requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, titoli specifici, specifiche competenze, ecc.);
  c. preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  d. preveda la tracciabilità della formale accettazione dell'incarico da parte del RSPP.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento agli addetti del servizio di prevenzione e protezione (SPP) previsti ai sensi della normativa vigente:
  a. preveda una formale designazione;
  b. definisca, in considerazione dell'ambito di attività, requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, titoli specifici, specifiche competenze, ecc.);
  c. preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  d. preveda la tracciabilità della formale accettazione da parte degli addetti SPP.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento al Medico Competente previsto ai sensi della normativa vigente:
  a. preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  b. definisca la documentazione sanitaria e di rischio da predisporre secondo la normativa vigente (es. Cartella Sanitaria);
  c. preveda la tracciabilità della formale accettazione da parte del medico competente.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento ai soggetti responsabili della sorveglianza sul luogo di lavoro previsti ai sensi della normativa vigente:
  a. preveda una formale designazione;

b. definisca, in considerazione dell'ambito di attività, requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, titoli specifici, specifiche competenze, ecc.);
c. preveda la tracciabilità delle verifiche svolte in ordine al possesso requisiti previsti dalla normativa in materia;
d. preveda la tracciabilità della formale accettazione da parte del Sorvegliante e Direttore Responsabile.

- gli strumenti normativi di disciplina della pianificazione, della gestione e della consuntivazione degli impegni di spesa devono essere applicati anche con riferimento alle spese in materia di ambiente, salute, sicurezza e igiene sul lavoro. In particolare detti strumenti devono regolare:
  a. ruoli, responsabilità e modalità di effettuazione e documentazione delle spese;
  b. modalità di definizione e approvazione del budget di spesa;
  c. modalità di rendicontazione delle spese;
  d. la tracciabilità delle attività effettuate.
- deve esistere un sistema di deleghe di funzioni tale da garantire, in capo al soggetto delegato, la sussistenza:
  a. di poteri decisionali coerenti con le deleghe assegnate;
  b. di potere di spesa adeguato, per l'efficace adempimento delle funzioni delegate;
  c. di un obbligo di rendicontazione formalizzata sui poteri delegati, con modalità prestabilite atte a garantire un'attività di vigilanza senza interferenze.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che identifichi ruoli, responsabilità e modalità per lo svolgimento, approvazione e aggiornamento della valutazione dei rischi aziendali. In particolare tale norma:
  a. identifica ruoli, responsabilità, requisiti di competenza e necessità di addestramento del personale responsabile per condurre l'identificazione dei pericoli, l'identificazione e il controllo del rischio;
  b. identifica le responsabilità per la verifica, l'approvazione e l'aggiornamento dei contenuti dei documenti di valutazione dei rischi;
  c. identifica modalità e criteri per la revisione in tempi o periodi determinati dei processi di identificazione dei pericoli e valutazione del rischio;
  d. prevede, laddove necessario, la tracciabilità dell'avvenuto coinvolgimento del Medico Competente, dei Rappresentanti dei Lavoratori per la Sicurezza e l'Ambiente e delle altre figure previste dalle disposizioni normative vigenti nel processo di identificazione dei pericoli e valutazione dei rischi;
  e. prevede, laddove necessario, la valutazione delle diverse tipologie di sorgenti di rischio: pericoli ordinari o generici, ergonomici, specifici, di processo e organizzativi e una individuazione di aree omogenee in termini di pericolo all'interno dell'azienda;

f. prevede, laddove necessario, l'individuazione delle mansioni rappresentative dei lavoratori;
g. prevede, laddove necessario, il censimento e la caratterizzazione degli agenti chimici e delle attrezzature e macchine presenti;
h. prevede, laddove necessario, esplicita definizione dei criteri di valutazione adottati per le diverse categorie di rischio nel rispetto della normativa e prescrizioni vigenti.

- deve esistere un documento di valutazione dei rischi e la conseguente documentazione redatta secondo le disposizioni vigenti e che contengano almeno:
  a. il procedimento di valutazione, con la specifica individuazione dei criteri adottati;
  b. l'individuazione e formalizzazione delle misure di prevenzione e protezione, e dei dispositivi di protezione individuale, conseguenti alla valutazione;
  c. il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che, con riferimento ai lavoratori incaricati di attuare le misure di emergenza, prevenzione incendi e primo soccorso previsti ai sensi della normativa vigente:
  a. preveda una formale designazione;
  b. definisca, in considerazione dell'ambito di attività, requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, specifiche competenze, ecc.);
  c. preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  d. preveda la tracciabilità della formale accettazione dell'incarico da parte degli incaricati.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento al Coordinatore in materia di salute, sicurezza per la progettazione dell'opera e al Coordinatore in materia di sicurezza e di salute durante la realizzazione dell'opera, previsti ai sensi della normativa vigente:
  a. preveda una formale designazione;
  b. definisca, in considerazione dell'ambito di attività, requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, specifiche competenze, ecc.);
  c. preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa vigente;
  d. preveda la tracciabilità della formale accettazione dell'incarico da parte dei Coordinatori.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che, laddove necessario e con riferimento ai compiti specifici conferiti, individui i criteri e le modalità definite per l'affidamento dei compiti ai lavoratori in tema di ambiente, salute, sicurezza e igiene sul lavoro. In particolare tale norma:

a. definisce ruoli, responsabilità e criteri di affidamento dei compiti ai lavoratori in tema di ambiente, salute, sicurezza e igiene sul lavoro;
b. definisce le misure organizzative per la partecipazione delle funzioni preposte nella definizione di ruoli e responsabilità dei lavoratori;
c. prevede la tracciabilità delle attività di assessment svolte a tale scopo (es. definizione di check list mirate quali elenchi dei compiti critici e/o processi a impatto su ambiente, salute, sicurezza e igiene).

- deve essere adottato e attuato uno strumento normativo e/o organizzativo per la gestione, distribuzione e il mantenimento in efficienza delle misure di prevenzione e protezione atte a salvaguardare l'ambiente e la sicurezza dei lavoratori. In particolare tale norma:
  a. definisce ruoli, responsabilità e modalità per la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buono stato di conservazione nonchè efficienza delle misure di prevenzione e protezione atte a salvaguardare l'ambiente e la sicurezza dei lavoratori;
  b. prevede la tracciabilità delle attività di consegna e verifica sulla funzionalità delle misure di prevenzione e protezione atte a salvaguardare la sicurezza dei lavoratori (es. check list mirate quali elenchi dei dispositivi di protezione individuale da consegnare, condivisi con il responsabile del servizio di prevenzione e protezione)
  c. prevede la tracciabilità della disponibilità e della funzionalità delle misure di prevenzione e protezione atte a salvaguardare l'ambiente.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo per la gestione delle emergenze, atto a mitigarne gli effetti, nel rispetto della salute della popolazione e dell'ambiente. In particolare tale norma:
  a. definisce ruoli, responsabilità e misure per il controllo di situazioni di rischio in caso di emergenza, atte a controllare e circoscrivere gli eventi in modo da minimizzarne gli effetti;
  b. definisce le modalità di abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
  c. definisce le modalità di intervento dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei lavoratori in caso di pericolo grave ed immediato e di pronto soccorso;
  d. individua i provvedimenti atti a evitare rischi per la salute della popolazione o deterioramento dell'ambiente;
  e. definisce le modalità e la tempistica/frequenza di svolgimento delle prove di emergenza;
  f. definisce l'aggiornamento delle misure di prevenzione a seguito dei progressi tecnologici e delle nuove conoscenze in merito alle misure da adottare in caso di emergenze;
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che preveda riunioni periodiche di tutte le figure competenti per la verifica della situazione nella gestione delle tematiche

riguardanti ambiente, salute, sicurezza e igiene e di una adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini la diffusione delle informazioni previste dalla normativa vigente relative all'ambiente, salute, sicurezza e igiene. In particolare tale norma definisce:
  a. ruoli, responsabilità e modalità di informazione periodica delle funzioni competenti verso i lavoratori, in relazione alle tematiche di ambiente, salute, sicurezza e igiene applicabili alle loro attività;
  b. l'informativa del medico competente, laddove necessario, relativamente ai processi e rischi connessi all'attività produttiva.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che regolamenti il processo di formazione in materia di ambiente, salute, sicurezza e igiene dei lavoratori. In particolare tale norma definisce:
  a. ruoli, responsabilità e modalità di erogazione della formazione dei lavoratori su rischi, pericoli, misure, procedure, ruoli e istruzioni d'uso;
  b. i criteri di erogazione della formazione di ciascun lavoratore (es. all'assunzione, trasferimento o cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze pericolose);
  c. l'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa;
  d. i tempi di erogazione della formazione ai lavoratori sulla base delle modalità e dei criteri definiti (definizione di un piano di formazione su base annuale).
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca modalità di qualifica/valutazione/classificazione dei fornitori e dei contrattisti. In particolare tale strumento:
  a. definisce ruoli, responsabilità e modalità di effettuazione della qualifica/ valutazione/ classificazione;
  b. in caso di appalto prevede che si tenga conto oltre che dei requisiti di carattere generale e morale degli appaltatori, anche dei requisiti tecnico-professionali, ivi incluse le necessarie autorizzazioni previste dalla normativa ambientale e di salute e sicurezza;
  c. prevede che si tenga conto della rispondenza di quanto eventualmente fornito con le specifiche di acquisto e le migliori tecnologie disponibili in tema di tutela dell'ambiente, della salute e della sicurezza.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca:
  a. ruoli, responsabilità, modalità e contenuti dell'informazione da fornire alle imprese esterne sui rischi specifici esistenti nell'ambiente in cui le imprese stesse sono destinate a operare e sulle misure da adottare in relazione alla propria attività che un'impresa appaltatrice aggiudicataria deve conoscere, impegnarsi a rispettare e a far rispettare ai propri dipendenti;

b. ruoli, responsabilità e modalità di elaborazione del documento di valutazione dei rischi che indichi le misure da adottare per eliminare i rischi dovuti alle interferenze tra i lavoratori nel caso di diverse imprese coinvolte nell'esecuzione di un'opera;

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca ruoli, responsabilità e modalità di inserimento delle clausole contrattuali standard riguardanti il rispetto delle normative di salute, sicurezza e igiene applicabili, nonché i costi della sicurezza nei contratti di somministrazione dei lavoratori, di appalto e di subappalto.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che identifichi ruoli, responsabilità e modalità di monitoraggio sul rispetto delle normative di salute, sicurezza e igiene da parte dei fornitori nonché sulle attività da questi effettuate nei confronti dei sub-appaltatori in merito al rispetto delle suddette normative.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini le attività di manutenzione/ispezione degli asset aziendali lungo tutto il loro ciclo di vita* (es. stabilimenti, ivi inclusi serbatoi, depositi e tubazioni, nonché attrezzature meccanici, elettrici ed elettromeccanici, etc.) affinché ne sia sempre garantita l'integrità e l'adeguatezza in termini di tutela dell'ambiente, della salute e della sicurezza dei lavoratori. In particolare tale norma:
  a. definisce ruoli, responsabilità e modalità di gestione degli asset;
  b. prevede periodiche verifiche di adeguatezza e integrità degli asset e di conformità ai requisiti normativi applicabili;
  c. prevede la pianificazione, l'effettuazione e la verifica delle attività di ispezione e manutenzione tramite personale qualificato e idoneo.

Controllo e azioni correttive

Per le attività di controllo e azioni correttive sono stabiliti i seguenti *standard* di controllo:

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini:
  a. ruoli, responsabilità e modalità di rilevazione, registrazione e investigazione interna degli infortuni;
  b. ruoli, responsabilità e modalità di tracciabilità e investigazione degli incidenti occorsi e dei "mancati incidenti";
  c. modalità di comunicazione da parte dei responsabili operativi al datore di lavoro e al responsabile del servizio di prevenzione e protezione sugli infortuni/incidenti occorsi;
  d. ruoli, responsabilità e modalità di monitoraggio degli infortuni occorsi (tenendo conto di eventuali controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro) al fine di identificare le aree a maggior rischio infortuni;
  e. ruoli, responsabilità e modalità di comunicazione al datore di lavoro (e/o al suo delegato) degli incidenti ambientali occorsi.

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca ruoli, responsabilità e modalità di registrazione e monitoraggio (anche attraverso l'uso di indicatori) per:
  a. i dati riguardanti la sorveglianza sanitaria;
  b. i dati riguardanti la sicurezza degli impianti (apparecchi di sollevamento e ascensori, impianti elettrici, attrezzature a pressione, serbatoi interrati, apparecchiature laser; macchine);
  c. i dati riguardanti le sostanze e i preparati pericolosi utilizzati in azienda (schede di sicurezza);
  d. altri dati diversi da infortuni e incidenti (tenendo conto di eventuali controversie/contenziosi insorti) al fine di identificare le aree a maggior rischio.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini ruoli, responsabilità e modalità operative riguardo le attività di audit e verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza e dell'ambiente.

  In particolare tale norma definisce:
  a. la tempistica per la programmazione delle attività (piano di audit formalizzato);
  b. le competenze necessarie per il personale coinvolto nelle attività di audit nel rispetto del principio dell'indipendenza dell'auditor rispetto all'attività oggetto di audit;
  c. le modalità di registrazione degli audit;
  d. le modalità di individuazione e applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di gestione dell'ambiente, salute, sicurezza e igiene in azienda o dalle norme e prescrizioni applicabili;
  e. le modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
  f. le modalità di comunicazione dei risultati dell'audit alla Direzione aziendale.
- deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini ruoli, responsabilità e modalità operative delle attività di reporting verso la Direzione. Tale report deve garantire la tracciabilità e la disponibilità dei dati relativi alle attività inerenti al sistema di gestione della sicurezza e dell'ambiente e in particolare l'invio periodico delle informazioni inerenti a:
  a. scostamenti tra i risultati ottenuti e gli obiettivi programmati;
  b. risultati degli audit;
  c. risultati del monitoraggio della performance del sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (infortuni, emissioni, scarichi, rifiuti, bonifiche, etc.);
  d. spese sostenute e risultati di miglioramento raggiunti in relazione alle suddette spese.

Riesame della direzione

Per le attività di riesame della direzione sono stabiliti i seguenti *standard* di controllo:

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca ruoli, responsabilità e modalità di conduzione del processo di riesame da parte della Direzione aziendale in relazione all'efficacia e all'efficienza del sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica in azienda.

Tale norma prevede lo svolgimento delle seguenti attività:

a. analisi delle risultanze del reporting ottenuto;
b. analisi dello stato di avanzamento di eventuali azioni di miglioramento definite nel precedente riesame;
c. individuazione degli obiettivi di miglioramento per il periodo successivo e la necessità di eventuali modifiche ad elementi del sistema di gestione di ambiente, salute, sicurezza e igiene in azienda;
d. tracciabilità delle attività effettuate.

- deve essere adottato e attuato uno strumento normativo e/o organizzativo che identifichi ruoli, responsabilità, modalità operative, criteri e periodicità per la redazione e/o aggiornamento e l'approvazione dei documenti di identificazione:
  a. degli aspetti ambientali in funzione dei beni prodotti, dei servizi resi e delle attività svolte in condizioni operative normali, anomale, in condizioni di avviamento e di fermata e in situazioni di emergenza e di incidenti e la valutazione della loro significatività in funzione degli impatti ambientali diretti e indiretti ad essi correlati (sulla base, anche, del contesto territoriale di riferimento, nel rispetto della normativa vigente e delle prescrizioni previste nei relativi provvedimenti autorizzativi);
  b. delle misure di prevenzione, protezione e mitigazione degli impatti ambientali conseguenti alla valutazione della significatività degli aspetti ambientali.

Parte Speciale C - Delitti informatici e violazione del diritto d’autore

1. Le Attività Sensibili ai fini del d.lgs. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Fondazione nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Attraverso l'analisi dei processi della Fondazione sono state individuate le seguenti attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-*bis* del Decreto:

1) pianificazione generale delle misure da adottare in materia di sicurezza del sistema informatico e telematico, classificazione e trattamento di dati e informazioni;

2) gestione delle modalità di accesso al sistema informatico degli utenti interni ed esterni, gestione dei profili utente e del processo di autenticazione;

3) gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni

4) gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio

5) gestione e protezione della postazione di lavoro;

6) gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni;

7) gestione delle attività di acquisizione e sviluppo di apparecchiature, dispositivi (anche di rilevazione) o programmi informatici e di servizi di installazione, manutenzione, connessione o di altra natura relativi a hardware, software e reti e relative componenti tecniche connesse con il sistema

Le sopra indicate Attività Sensibili 2 e 3 sono state individuate come rilevanti anche nell'ambito della prevenzione dei reati in materia di violazione del diritto d'autore.

2. Il sistema dei controlli

Il sistema dei controlli, perfezionato dalla Fondazione, anche sulla base degli standard di riferimento internazionali per il sistema di sicurezza informatica, prevede principi generali di comportamento, standard di controllo generali e standard di controllo "specifici" applicati alle Attività Sensibili individuate.

Con specifico riguardo alle problematiche connesse al rischio informatico, la Fondazione, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso:

- la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e
- la garanzia della massima continuità del servizio.

2.1. Principi generali di comportamento

I destinatari del Modello sono tenuti a osservare i seguenti principi generali:

- occorre tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e delle procedure interne;
- è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 24 *bis e 25 novies* del d.lgs. 231/2001.

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che la Fondazione si pone sono i seguenti[7]:

- **Integrità**: garanzia che ogni dato aziendale sia realmente e completamente rappresentativo, in maniera oggettiva e senza interpretazioni, dei contenuti a cui si riferisce. Tale obiettivo si persegue tramite l'adozione di opportune contromisure che impediscano alterazioni incidentali o intenzionali che ne possono mutare il significato originale o, in alternativa, forniscano la possibilità di rilevare la suddetta alterazione del dato e di recuperare il dato integro.
- **Riservatezza**: garanzia che un dato aziendale venga reso disponibile solamente alle applicazioni ed agli utenti incaricati e autorizzati al suo utilizzo;

[7] Si veda in merito il capitolo 3 del Documento Programmatico sulla Sicurezza

- **Disponibilità**: garanzia di reperibilità dei dati aziendali in funzione delle esigenze di continuità dei processi aziendali e di rispetto delle norme (di legge e non) che impongono la conservazione storica o determinati livelli di servizio.

In particolare, la presente Parte Speciale prevede, conseguentemente, le seguenti norme di comportamento con riferimento ai soggetti sopra indicati:

a) divieto di alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b) divieto di accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c) divieto di accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;

d) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

e) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

f) divieto di svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

g) divieto di svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

h) divieto di installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

i) divieto di svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

j) divieto di svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

k) divieto di distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

l) divieto di utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore;

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione della Funzione competente;

3. segnalare alla Funzione competente il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla unzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
5. evitare di trasferire all'esterno della Fondazione e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Fondazione stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;
7. evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature della Fondazione solo prodotti ufficialmente acquisiti dall'azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Fondazione;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

2.2Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi alle Attività Sensibili in materia di sicurezza informatica e violazione del diritto d'autore.

1) pianificazione generale delle misure da adottare in materia di sicurezza del sistema informatico e telematico, classificazione e trattamento di dati e informazioni

La regolamentazione dell'attività prevede che le disposizioni in materia di sicurezza del sistema informatico e telematico adottate dalla Fondazione includono:

a) la definizione degli obiettivi, delle linee guida e degli strumenti normativi relativamente alla sicurezza informatica e telematica;
b) l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti;
c) i rapporti con gli outsourcer informatici;
d) le modalità di aggiornamento delle stesse, anche a seguito di cambiamenti significativi;
e) le esigenze di carattere legale con riferimento alle clausole contrattuali relative alla sicurezza informatica e telematica;
f) la definizione dell'approccio nell'analisi e valutazione dei rischi e l'identificazione della relativa metodologia;
g) la definizione dei principi di classificazione dei dati e delle informazioni (confidenzialità, autenticità e integrità);
h) la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni.

2) gestione delle modalità di accesso al sistema informatico degli utenti interni ed esterni, gestione dei profili utente e del processo di autenticazione

La regolamentazione dell'attività prevede che:

- la Fondazione definisce ruoli e responsabilità degli utenti interni ed esterni all'azienda e i connessi obblighi nell'utilizzo del sistema informatico e delle risorse informatiche e telematiche anche con riferimento all'accesso a risorse telematiche in possesso di enti terzi la cui gestione del sistema di sicurezza ricade sulla parte terza stessa;
- l'accesso alle informazioni, al sistema informatico, alla rete, ai sistemi operativi e alle applicazioni viene sottoposto a controllo da parte della Fondazione attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:
    a. l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password od altro sistema di autenticazione sicura (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);
    b. le autorizzazioni specifiche dei diversi utenti o categorie di utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);
    c. procedimenti di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati l'accesso a tutti i sistemi e servizi

informativi, anche di terzi (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

d. la rivisitazione periodica dei diritti d'accesso degli utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);
e. l'accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete, (anche se tali diritti permettono di connettersi a reti e dispositivi di terze parti, la cui gestione del sistema di sicurezza ricade sulla parte terza stessa);
f. la chiusura di sessioni inattive dopo un limitato periodo di tempo (valido per le postazioni di lavoro, come ad esempio screen saver).

3) gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni

La regolamentazione dell'attività prevede che:

- la sicurezza del sistema informatico e telematico viene garantita da parte della Fondazione attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:
  a. le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per le basi dati e i sistemi operativi da esse sottese);
  b. la protezione da software pericoloso (es. worm e virus) (valido, sottoforma di antivirus per gli ambienti microsoft e di patch management per gli altri sistemi e apparati di comunicazione come router, switch e per apparati firewall);
  c. il backup di informazioni di uso centralizzato e del software applicativo ritenuto critico (valido per le applicazioni e basi dati da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;
  d. la previsione di strumenti di protezione idonei a garantire la sicurezza nello scambio di informazioni critiche per il business aziendale e di carattere confidenziale anche con terzi;
  e. gli strumenti per effettuare:
     i) la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;
     ii. la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico http);
     iii. la protezione delle informazioni registrate (log) contro accessi non autorizzati;
  f. una verifica periodica/a evento dei log che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router);

g. il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router) non alterino i livelli di sicurezza;
h. la definizione delle regole per la corretta custodia dei dispositivi di memorizzazione (ad es. pc, telefoni, chiavi USB, CD, hard disk esterni, ecc.).

- deve essere adottato ed attuato uno strumento normativo e/o organizzativo che preveda:
  a. l'obbligo di rispettare le prescrizioni dettate dalla normativa in materia di tutela del diritto morale e patrimoniale d'autore, con specifico riferimento a utilizzo, conservazione e distribuzione di testi, musiche, disegni, immagini, fotografie, programmi per elaboratore e banche di dati protetti dal diritto d'autore (le "Opere"). In particolare, devono essere rispettate le disposizioni di legge applicabili con riferimento all'acquisizione, conservazione, utilizzo, riproduzione, duplicazione, elaborazione, diffusione e distribuzione (anche attraverso reti telematiche) delle Opere o di loro parti. Devono altresì essere osservate le previsioni di legge a tutela della paternità delle Opere nonché le limitazioni previste al diritto di duplicazione di programmi per elaboratore e di riproduzione, trasferimento, distribuzione e/o comunicazione del contenuto di banche dati;
  b. meccanismi autorizzativi per l'utilizzo, la riproduzione, l'elaborazione, la duplicazione e la distribuzione di Opere o di parti delle stesse;
  c. l'adozione di strumenti di protezione (es. diritti di accesso) relativi alla conservazione e all'archiviazione di Opere assicurandone l'inventariazione.

4) gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio

La regolamentazione dell'attività prevede che la Fondazione utilizza controlli crittografici per la protezione delle informazioni e regolamenta la gestione delle chiavi crittografiche al fine di evitare un uso non appropriato della firma digitale.

5) gestione e protezione della postazione di lavoro

La regolamentazione dell'attività prevede che la sicurezza del sistema informatico e telematico viene garantita da parte della Fondazione attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

a. le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per le basi dati e i sistemi operativi da esse sottese);
b. la protezione da software pericoloso (es. worm e virus);
c. il backup di informazioni di uso centralizzato e del software applicativo ritenuto critico (valido per le applicazioni e basi dati da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;

d. la previsione di strumenti di protezione idonei a garantire la sicurezza nello scambio di informazioni critiche per il business aziendale e di carattere confidenziale anche con terzi;
e. gli strumenti per effettuare:
    i. i. la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;
    ii. ii. la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico http);
    iii. iii. la protezione delle informazioni registrate (log) contro accessi non autorizzati;
f. una verifica periodica/a evento dei log che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router);
g. il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router) non alterino i livelli di sicurezza;
h. la definizione delle regole per la corretta custodia dei dispositivi di memorizzazione (ad es. pc, telefoni, chiavi USB, CD, hard disk esterni, ecc.).

6) gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni

La regolamentazione dell'attività prevede che la sicurezza del sistema informatico e telematico viene garantita da parte della Fondazione attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

a. le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per le basi dati e i sistemi operativi da esse sottese);
b. la protezione da software pericoloso (es. worm e virus);
c. il backup di informazioni di uso centralizzato e del software applicativo ritenuto critico (valido per le applicazioni e basi dati da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;
d. la previsione di strumenti di protezione idonei a garantire la sicurezza nello scambio di informazioni critiche per il business aziendale e di carattere confidenziale anche con terzi;
e. gli strumenti per effettuare:
    iv. i. la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;
    v. ii. la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico http);
    vi. iii. la protezione delle informazioni registrate (log) contro accessi non autorizzati;

f. una verifica periodica/a evento dei log che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router);
g. il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router) non alterino i livelli di sicurezza;
h. la definizione delle regole per la corretta custodia dei dispositivi di memorizzazione (ad es. pc, telefoni, chiavi USB, CD, hard disk esterni, ecc.).

7) gestione delle attività di acquisizione e sviluppo di apparecchiature, dispositivi (anche di rilevazione) o programmi informatici e di servizi di installazione, manutenzione, connessione o di altra natura relativi a hardware, software e reti e relative componenti tecniche connesse con il sistema

La regolamentazione dell'attività prevede che la Fondazione identifica i requisiti di sicurezza e di conformità tecnica (ove applicabile) in fase di acquisizione, sviluppo, fornitura e manutenzione del sistema informatico (inclusivo di componente hardware, software e delle componenti tecniche connesse)