MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

EX D.LGS. 231/2001

PARTE SPECIALE

Versione approvata dal Consiglio di Amministrazione del 17 ottobre 2023

INDICE

Sezione II – parte speciale

1. INTRODUZIONE

La *Parte Speciale* del Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/2001 (di seguito anche «Modello 231») ha finalità di prevenzione ai fini della responsabilità amministrativa degli enti ai sensi del D.Lgs. 231/2001, caratterizzata dalla tipicità delle fattispecie di Reato presupposto e dalla necessaria sussistenza di «un interesse o vantaggio» per l'ente come presupposti per l'applicazione delle sanzioni ivi previste, nel caso di commissione dei Reati indicati nel 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, l'individuazione delle cosiddette «aree a rischio», ossia di quelle aree della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei Reati espressamente richiamati dal Decreto.

2. A – AREA A RISCHIO NELL'AMBITO DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E CON SOGGETTI PRIVATI

Per 3-i si sono individuate come applicabili le attività rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui ai seguenti articoli del D.Lgs.231/2001:

- artt. 24 e 25 (Reati nei rapporti con la Pubblica Amministrazione, d'ora in avanti anche «PA»);
- art. 25 ter lett. s) bis (Corruzione tra privati e Istigazione alla corruzione tra privati);
- art. 25 decies (Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria).

Per ragioni prudenziali, è stato valutato il possibile riconoscimento per 3-i della qualifica pubblicistica nell'effettuazione di determinate attività, quali l'approvvigionamento di beni e servizi, ossia il riconoscimento, in capo ai componenti 3-i, della veste di incaricati di un pubblico servizio e, limitatamente ad alcune fasi dell'attività, anche quella di pubblici ufficiali.

Pertanto, nell'individuazione delle aree a rischio e nella definizione degli standard di controllo è stato valutato anche il rischio di commissione dei Reati di corruzione passiva (es. dipendente 3-i quale destinatario della corruzione messa in atto da un fornitore, al fine di ottenere condizioni contrattuali più favorevoli, nel caso di affidamento dei lavori o approvvigionamento di beni) e di concussione (es. dipendente 3-i che, abusando dei suoi poteri o delle sue qualità, costringe o induce altri a corrispondere indebitamente utilità, in vista, ad esempio, dell'assegnazione di un appalto). In tale ottica è stata individuata come attività sensibile l'approvvigionamento di beni, lavori e servizi.

Infine, oltre all'approvvigionamento di beni e servizi, sono state individuate come attività sensibili – da considerarsi come strumentali – quelle aree di attività afferenti alla gestione di strumenti di tipo finanziario o mezzi sostitutivi e che pertanto possono risultare strumentali alla commissione di Reati, quali:

- consulenze e prestazioni professionali;
- transazioni finanziarie (incassi e pagamenti);
- gestione delle spese di rappresentanza e dei beni di rappresentanza;
- selezione, assunzione e politiche di incentivazione del personale.

In tale ambito è ricompreso anche il Reato d'induzione a non rendere dichiarazioni all'autorità giudiziaria (o a renderle mendaci).

Nello schema seguente sono state enucleate le aree di attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione dei Reati di corruzione (tra PA e privati) e di concussione.

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei destinatari, nell'ambito delle aree di attività sensibili in relazione ai Reati commessi nei rapporti con la PA, ai Reati di corruzione e di istigazione alla corruzione tra privati e al Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria è fatto espresso obbligo ai destinatari di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Approvvigionamento di beni, lavori e servizi	Concussione (art. 317 c.p.) Induzione indebita a dare o promettere utilità (art. 319-quater c.p.) Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.) Traffico di influenze illecite (art. 346-bis c.p.)	Pianificazione e programmazione degli Approvvigionamenti Processo di acquisizione Gestione contrattuale
Conferimento di contratti di consulenza o prestazioni professionali	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.) Traffico di influenze illecite (art. 346-bis c.p)	Pianificazione e programmazione degli Approvvigionamenti Processo di acquisizione Gestione contrattuale
Transazioni finanziarie (incassi e pagamenti)	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.) Traffico di influenze illecite (art. 346-bis c.p)	Gestione degli incassi Gestione dei pagamenti
Gestione dei rimborsi spese	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.)	Rimborsi spese
Erogazioni liberali	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.) Traffico di influenze illecite (art. 346-bis c.p)	Cessione a titolo gratuito
Selezione, assunzione e politiche di incentivazione del personale	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.)	Selezione, assunzione e politiche di incentivazione del personale
Negoziazione/stipula/esecuzione di contratti (ivi inclusa la fase di	Corruzione (artt. 318, 319, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.)	Negoziazione e stipula Esecuzione, rendicontazione e fatturazione

Area a rischio	Reati associabili	Attività sensibili
fatturazione) / convenzioni con soggetti pubblici	Truffa aggravata ai danni dello Stato o di altro ente pubblico (art. 640, co. 2, n.1, c.p.) Traffico di influenze illecite (art. 346-bis c.p)	
Gestione dei contenziosi giudiziali e stragiudiziali	Corruzione in atti giudiziari (art. 319-ter c.p.) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (377 bis c.p.) Corruzione tra privati (art.2635 c.3 c.c.) Istigazione alla corruzione tra privati (art.2635-bis c.c.) Traffico di influenze illecite (art. 346-bis c.p)	Gestione contenziosi giuslavoristici Gestione dei contenziosi di altro genere
Gestione dei rapporti con soggetti pubblici	Corruzione (artt. 318, 319-bis, 320, 321 e 322-bis c.p.) Istigazione alla corruzione (art. 322 c.p.) Truffa aggravata ai danni dello Stato o di altro ente pubblico (art. 640, co. 2, n.1)	Gestione dei rapporti con soggetti pubblici per l'ottenimento di provvedimenti amministrativi (quali autorizzazioni, licenze e permessi) necessari per l'esercizio delle attività tipiche aziendali. Gestione di adempimenti, dichiarazioni, deposito atti e documenti, pratiche, verifiche, ispezioni, negli accertamenti/ procedimenti sanzionatori che ne derivano, concernenti le seguenti materie: salute e sicurezza, fiscale, gestione del personale
Acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici	Malversazione (art.316 bis c.p.)	Acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici
Attività che prevedano l'installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici, per trasmissione di dati e comunicazioni	Frode informatica in danno dello Stato o di altro ente pubblico, art. 640 ter c.p.	Sviluppo installazione e manutenzione evolutiva di sistemi software Gestione dei flussi telematici per scambio dati con la PA

2.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI NEI RAPPORTI CON LA PA E CON SOGGETTI PRIVATI

Nell'ambito delle attività operative, i destinatari, con specifico riguardo ai Reati relativi ai rapporti con la PA, in relazione alla corruzione, istigazione, alla corruzione tra privati e al Reato di induzione a non rendere dichiarazioni mendaci all'Autorità Giudiziaria, devono attenersi alle seguenti regole di comportamento e principi generali:

- *non possono accettare o sollecitare* regali, atti di cortesia, quali omaggi o forme di ospitalità, o altre utilità se non nei limiti del modico valore e tali da poter essere considerati usuali in relazione alla ricorrenza e non essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire vantaggi in modo improprio. *Non è consentito offrire, promettere, fare* regali, atti di cortesia, quali omaggi o forme di ospitalità, o altre utilità se non nei limiti del modico valore. In ogni caso, tali spese devono sempre essere autorizzate, documentate e nel rispetto dei limiti di *budget*. Per *«modico valore»* si intende un valore che non eccede i 150,00 euro, non cumulabile, e ripetibile per non più di due volte l'anno, per soggetto destinatario. Ai fini della quantificazione, si fa riferimento al valore di mercato. *In caso di ricevimento* di regali, atti di cortesia, come forme di ospitalità e altre utilità, di valore superiore al citato limite, gli stessi devono essere restituiti o non essere accettati ovvero in caso di impossibilità di restituzione, vige l'obbligo di darne comunicazione al Vertice aziendale;

- nel corso di una trattativa d'affari, richiesta o rapporto commerciale non devono essere intraprese (direttamente o indirettamente) le seguenti azioni:
  - esaminare o proporre opportunità di impiego o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione o soggetti privati a titolo personale;
  - sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti.
- nell'ambito dei rapporti anche di natura non commerciale instaurati tra 3-i e la Pubblica Amministrazione, i pubblici ufficiali, i soggetti incaricati di un pubblico servizio e i soggetti privati, sono tenuti ad astenersi:
  - dall'offrire, promettere, dare, anche per interposta persona, denaro o altra utilità, che può consistere anche in opportunità di lavoro o commerciali, al funzionario pubblico coinvolto o al soggetto privato, ai rispettivi familiari o a soggetti in qualunque modo agli stessi collegati;
  - dall'accettare la richiesta o sollecitazioni, anche per interposta persona, di denaro o altra utilità, che può consistere anche in opportunità di lavoro o commerciali, dal funzionario pubblico coinvolto o dal soggetto privato, dai rispettivi familiari o da soggetti in qualunque modo agli stessi collegati;
  - dal ricercare o instaurare illecitamente relazioni personali di favore, influenza, ingerenza, idonee a condizionare, direttamente o indirettamente, l'esito del rapporto.
- non devono abusare delle loro qualità o dei loro poteri per costringere o indurre taluno a dare o promettere, indebitamente, a loro stessi o a un terzo anche per conto di 3-i, denaro, regali o altra utilità da soggetti che abbiano tratto o possano trarre benefici da attività o decisioni inerenti all'ufficio svolto;
- non devono ricevere o accettare, indebitamente, denaro o una promessa di denaro, regali o altra utilità, per proprio conto, per conto di un terzo o di 3-i, per compiere, omettere o ritardare un atto d'ufficio o per compiere o aver compiuto un atto d'ufficio contrario ai doveri d'ufficio, da soggetti che abbiano tratto o possano trarre benefici da attività o decisioni inerenti all'ufficio;
- non effettuare prestazioni in favore di consulenti che non trovino adeguata giustificazione nel contesto del rapporto costituito con gli stessi;
- non fornire, in qualsiasi forma, informazioni non veritiere o incomplete alla PA;
- non destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- non condizionare in qualsiasi forma e con qualsiasi mezzo la libertà di determinazione di soggetti che, a qualsiasi titolo, siano chiamati a rendere dichiarazioni innanzi all'Autorità Giudiziaria;
- non promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio a 3-i;
- non attuare o istigare altri affinché pongano in essere pratiche corruttive di ogni genere;
- si può aderire a richieste di contributi o riservare atti di liberalità, limitatamente a proposte provenienti da associazioni non profit, enti o istituzioni, per promuovere iniziative di valore

benefico, culturale, sociale e assistenziale, approvate dal Vertice aziendale, nel rispetto dei limiti di *budget*.

2.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

2.2.1 APPROVVIGIONAMENTO DI BENI, LAVORI E SERVIZI

La regolamentazione dell'attività prevede:

- regole di comportamento trasparenti, imparziali, oggettive in ogni fase del processo di approvvigionamento volte ad assicurare la migliore configurazione possibile di costo, qualità e tempo;
- divieto di negoziare condizioni contrattuali occulte, che non risultino da idonea documentazione conservata unitamente a quella relativa all'acquisto;
- l'obbligo delle persone che operano nel processo di *procurement* di assicurare la riservatezza richiesta dalle circostanze per ciascuna notizia/informazione appresa in ragione della propria funzione lavorativa;
- la rotazione dei fornitori nelle forniture cicliche con offerta omogenea e diversa;
- una verifica dell'assenza di rapporti con fornitori che possono avere conflitti di interessi con dipendenti 3-i; in caso di esistenza di relazioni privilegiate[1]/conflitto di interesse tra il rappresentante di 3-i e la terza parte, l'obbligo di segnalarle;
- la verifica che le richieste di approvvigionamento arrivino da soggetti autorizzati;
- la formalizzazione e l'autorizzazione da parte di un adeguato livello gerarchico della scelta della modalità di approvvigionamento;
- la segregazione nelle principali attività;
- la formalizzazione dell'iter, relativo alle attività di approvvigionamento, a partire dalla definizione dell'esigenza fino all'autorizzazione e l'emissione di una richiesta di acquisto;
- il divieto di frammentazione delle richieste di acquisto;
- la sussistenza della coincidenza tra la richiesta di acquisto e l'ordine di acquisto;
- le modalità per il ricevimento dei beni e la dichiarazione di accettazione del bene/servizio acquistato;
- la formalizzazione del processo di *budgeting*, anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;

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

- le modalità e i contenuti dell'informazione che devono essere forniti ai fornitori riguardo l'insieme delle norme e prescrizioni che un'impresa appaltatrice/aggiudicataria di un ordine deve conoscere;
- clausole contrattuali standard, riguardanti i costi della sicurezza e le norme vigenti in materia che i fornitori devono dichiarare di conoscere;
- l'inserimento di specifiche clausole nei contratti con cui i terzi:
  - si obbligano a non tenere alcun comportamento, non realizzare alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. n. 231/2001;
  - dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Modello 231 adottato dalla società nonché clausole risolutive espresse che attribuiscano alla società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;
- specifiche clausole anticorruzione quali:
  - la dichiarazione del fornitore che non vi è stata mediazione o altra opera di terzi per la conclusione del contratto e di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;
  - l'obbligo del fornitore a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;
  - indicazione dei soggetti obbligati per i quali il fornitore si assume la garanzia del rispetto delle leggi applicabili, e in particolare delle Leggi anticorruzione;
  - l'applicazione di sanzioni nel caso di violazione da parte del fornitore degli obblighi, dichiarazioni e garanzie come sopra riportate, o in caso di violazione delle Leggi anticorruzione;
- idonei sistemi di monitoraggio e formalizzazione di report da sottoporre ad adeguato livello gerarchico per il monitoraggio della gestione degli ordini;
- la formazione specifica in materia di acquisizione beni, servizi e lavori per i dipendenti coinvolti nelle diverse fasi del processo di approvvigionamento;
- che l'archiviazione della documentazione relativa ad ogni attività di acquisto sia caratterizzata da completezza;

- il divieto di intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone[2] indicate nelle Liste di Riferimento[3] o facenti parte di organizzazioni presenti nelle stesse.
- nei casi di approvvigionamenti effettuati in urgenza, la definizione delle condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga;
- regole per la qualifica dei fornitori e controlli e responsabilità funzionali a garantire che la movimentazione dell'Albo Fornitori sia effettuata in presenza della documentazione prevista (es. nome cliente; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione)[4].

2.2.2 CONFERIMENTO DI CONTRATTI DI CONSULENZA O PRESTAZIONI PROFESSIONALI

La regolamentazione dell'attività prevede:

- il rispetto del principio di segregazione delle attività in fase di affidamento dell'incarico;
- la formalizzazione del processo di *budgeting* anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;
- le modalità per la gestione della individuazione, selezione e attribuzione dell'incarico con la definizione di criteri oggettivi, trasparenti e documentabili di assegnazione dell'incarico;
- che l'affidamento a soggetti appartenenti alla PA o loro familiari avvenga previa autorizzazione dell'Amministrazione di appartenenza;
- divieto di affidamento a soggetti appartenenti alla PA o loro familiari di incarichi quando la società abbia avanzato all'Amministrazione di appartenenza domanda per il rilascio di autorizzazioni, licenze, concessioni, o ovvero di altri atti amministrativi rilevanti ai fini della conduzione, della gestione, della programmazione e dello sviluppo della società;
- l'esistenza di un elenco di consulenti legali e tecnici, con l'evidenza degli ambiti di eccellenza per ciascun soggetto;

[2] Si intendono persone fisiche, persone giuridiche e persone fisiche appartenenti a organizzazioni individuate nelle Liste di Riferimento.

[3] Si tratta delle liste curate da ONU, UE e OFAC e rese disponibili sul sito web dell'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia ex art. 6 c. 1 del D.Lgs. 231/2007.

[4] Tale standard di controllo è previsto al fine di garantire una piena e adeguata copertura del rischio, sebbene in 3-i non sia presente un Albo Fornitori, in quanto le acquisizioni di beni, lavori e servizi sono svolte tramite una stazione appaltante esterna.

- che il ricorso alla negoziazione diretta con un unico operatore economico sia adeguatamente motivato e documentato, nonché sottoposto a idonei sistemi di controllo e sistemi autorizzativi;
- il rispetto delle previsioni normative in tema di proroghe e rinnovi;
- la verifica dell'esistenza di requisiti di onorabilità/professionalità dei consulenti;
- la formalizzazione delle motivazioni della consulenza e delle motivazioni della scelta del consulente;
- la tracciabilità e l'archiviazione di documenti giustificativi degli incarichi conferiti;
- la formale valutazione di congruità, prima di procedere al pagamento del corrispettivo, sulla base di quanto previsto contrattualmente;
- il divieto di intrattenere rapporti, negoziare e/o stipulare contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse. Si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»;
- l'inserimento di specifiche clausole nei contratti con cui i terzi:
  - si obbligano a non tenere alcun comportamento, non attuare alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. 231/2001;
  - dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Modello adottato dalla 3-i nonché clausole risolutive espresse che attribuiscano alla società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;
  - garantiscano il processo di tracciabilità delle attività che svolgono per conto della società tramite apposita documentazione e relativa archiviazione;
- specifiche clausole anticorruzione quali:
  - la dichiarazione del fornitore che non vi è stata mediazione o altra opera di terzi per la conclusione del contratto e di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;
  - l'obbligo del fornitore a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;
  - indicazione dei soggetti obbligati per i quali il consulente si assume la garanzia del rispetto delle leggi applicabili, e in particolare delle Leggi anticorruzione;
  - l'applicazione di sanzioni nel caso di violazione da parte del consulente degli obblighi, dichiarazioni e garanzie come sopra riportate, o in caso di violazione delle Leggi anticorruzione;

- una verifica dell'assenza di rapporti con consulenti che possono avere conflitti di interesse con dipendenti 3-i; in caso di esistenza di relazioni privilegiate[5]/conflitto di interesse tra il rappresentante di 3-i e la terza parte, l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto;
- clausole contrattuali «*standard*», riguardanti i costi della sicurezza e le norme vigenti in materia di lavoro;
- le modalità per il ricevimento e la dichiarazione di accettazione del bene/servizio acquistato;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga.

2.2.3 TRANSAZIONI FINANZIARIE (INCASSI E PAGAMENTI)

La regolamentazione dell'attività prevede:

- con riferimento ai pagamenti:
  - l'attestazione dell'esecuzione della prestazione;
  - la registrazione delle fatture ricevute;
  - l'iter per la predisposizione e l'autorizzazione della proposta di pagamento;
  - le modalità per l'effettuazione dei pagamenti;
  - la formalizzazione dell'attività di riconciliazione dei conti correnti bancari;
- con riferimento agli incassi, la tracciabilità della registrazione e contabilizzazione;
- il divieto di utilizzo del contante o altro strumento finanziario al portatore, 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;
- il divieto di 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; si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»;
- il divieto di accettare ed eseguire ordini di pagamento provenienti da soggetti non identificabili, e dei quali non sia tracciabile il pagamento (importo, nome/denominazione, indirizzo e numero

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

di conto corrente) o qualora non sia assicurata, la piena corrispondenza tra il nome del fornitore/cliente e l'intestazione del conto su cui far pervenire/da cui accettare il pagamento;

- che i pagamenti al beneficiario devono essere effettuati esclusivamente sul conto intestato allo stesso; non è consentito effettuare pagamenti su conti cifrati o in contanti, o a un soggetto diverso dal beneficiario né in un Paese diverso da quello del beneficiario o da quello dove la prestazione è stata eseguita;
- previsione di cd. «specimen» di firma in relazione ai livelli autorizzativi definiti per le esecuzioni di transazioni finanziarie;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»).

2.2.4 GESTIONE DEI RIMBORSI SPESE

La regolamentazione dell'attività prevede:

- le modalità operative per lo svolgimento delle attività nonché le modalità di archiviazione della documentazione rilevante;
- l'iter autorizzativo delle suddette spese e la segregazione dei soggetti deputati all'autorizzazione e al controllo di tali spese;
- la tipologia delle spese sostenibili e i limiti massimi delle spese;
- il controllo di merito, la completezza e accuratezza dei giustificativi di supporto dei rimborsi spese, da parte della struttura aziendale preposta.

2.2.5 GESTIONE DELLE SPESE DI RAPPRESENTANZA E DEI BENI DI RAPPRESENTANZA

La regolamentazione dell'attività prevede:

- le modalità operative per lo svolgimento delle attività nonché le modalità di archiviazione della documentazione rilevante;
- l'esistenza di un *budget* per le spese di rappresentanza e per i beni di rappresentanza;
- ruoli, responsabilità e modalità operative per l'approvazione di spese di rappresentanza e dei beni di rappresentanza *extra budget*;
- l'iter autorizzativo delle suddette spese e la segregazione dei soggetti deputati all'autorizzazione e al controllo di tali spese;
- la tipologia delle spese sostenibili e i limiti massimi delle spese;
- il controllo di merito, la completezza e accuratezza dei giustificativi di supporto delle spese di rappresentanza;
- la necessaria documentazione che consenta di risalire all'identità dei beneficiari delle spese di rappresentanza/beni di rappresentanza;
- il divieto di intrattenere rapporti, negoziare e/o stipulare contratti o atti con persone indicati nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse (si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»);
- con riferimento alla gestione dei beni di rappresentanza (omaggi), diffusione di regole per la:

- identificazione dei soggetti aziendali titolati a rilasciare omaggi (richiedente) e provvedere alla fornitura (acquirente);
- definizione delle tipologie di spese ammesse e dei relativi criteri e limiti;
- sistemi di tracciabilità degli omaggi e della società/persona che ha effettuato tale offerta o fornito tale omaggio ed eventuali soglie di valore;

- con riferimento alle spese di rappresentanza, definizione dei criteri e delle modalità per il loro sostenimento, in particolare:
  - tipologie di spese che possono essere erogate a titolo di rappresentanza;
  - soggetti aziendali abilitati a sostenere tali spese;
  - livelli di autorizzazione per il sostenimento e relativo rimborso delle spese effettuate.

2.2.6 EROGAZIONI LIBERALI

La regolamentazione dell'attività prevede:

- ruoli, responsabilità e modalità operative per la fase di richiesta, valutazione e approvazione dei contributi;
- l'esistenza di un *budget* approvato e monitorato nel tempo con l'individuazione di un soggetto responsabile di verificare il rispetto del margine di spesa stabilito nel *budget*;
- ruoli, responsabilità e modalità operative per l'approvazione di spese extra *budget*;
- il rispetto del criterio dell'alternanza nella selezione degli enti/associazioni/ fondazioni beneficiari del contributo;
- una descrizione circa la natura e le finalità del contributo;
- regole e responsabilità per la tracciabilità delle diverse fasi del processo e l'archiviazione della documentazione;
- il divieto di intrattenere rapporti, negoziare o stipulare contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse (si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»);
- con riferimento alle liberalità, la diffusione di regole per:
  - definizione e approvazione di un piano annuale dei progetti di liberalità e iniziativa *no profit* e relativa previsione di impegno economico (*budget*);
  - definizione di modalità e i criteri per erogare una liberalità e/o iniziativa non profit;
  - elaborazione/acquisizione di un resoconto sull'utilizzo delle donazioni/erogazioni effettuate e/o sull'esito della gestione delle iniziative *no profit.*

2.2.7 SELEZIONE, ASSUNZIONE E POLITICHE DI INCENTIVAZIONE DEL PERSONALE

La regolamentazione dell'attività prevede:

- criteri di selezione dei candidati oggettivi e trasparenti;
- la tracciabilità delle fonti di reperimento dei curricula;

- le modalità di formalizzazione dei giudizi e le modalità di approvazione dei candidati ritenuti idonei al termine dell'iter di selezione con la produzione della relativa evidenza;
- sistema premiante che includa obiettivi predeterminati, misurabili ma non eccessivamente sfidanti sì da indurre comportamenti non in linea con le previsioni del Modello;
- l'esistenza di un *budget* annuale per l'assunzione di personale che sia approvato e monitorato nel tempo;
- lo svolgimento di verifiche pre-assuntive finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che espongano la società al rischio di commissione di Reati presupposto in tema di responsabilità amministrativa d'impresa;
- 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;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere specifiche clausole con le quali i terzi:
  - si obbligano a non tenere alcun comportamento, non porre in essere alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. 231/2001;
  - dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Modello 231 nonché clausole risolutive espresse che attribuiscano alla società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;
  - garantiscano il processo di tracciabilità delle attività che svolgono per conto della società tramite apposita documentazione e relativa archiviazione;
- il divieto di assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse. (si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»);
- con riferimento alla gestione del rapporto di lavoro, il rispetto:
  - dei contratti collettivi nazionali per quanto attiene la retribuzione;
  - della normativa relativa all'orario di lavoro e altre indennità orarie, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria ed alle ferie;
  - delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
  - delle condizioni lavorative in termini non degradanti;
- con riferimento alla formulazione dell'offerta e assunzione:
  - la scelta del candidato coerentemente alla valutazione di idoneità;
  - l'applicazione (almeno) del trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili;
  - la verifica dell'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti in sede di sottoscrizione della lettera di assunzione.

2.2.8 NEGOZIAZIONE / STIPULA / ESECUZIONE DI CONTRATTI (INCLUSA LA FASE DI FATTURAZIONE)

La regolamentazione dell'attività prevede:

- la persona deputata a rappresentare la società nei confronti della controparte, cui conferire apposita delega e procura;
- l'elaborazione della bozza contrattuale, 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;
- le modalità di predisposizione, verifica e approvazione della documentazione da trasmettere alla controparte in relazione all'esecuzione della convenzione;
- la separazione delle attività di predisposizione dell'offerta e di presentazione dell'offerta, prevedendo specifiche forme di verifica della congruità dell'offerta, graduate in relazione alla tipologia e dimensione dell'attività contrattuale;
- in sede di definizione dell'offerta una verifica diretta a evitare il rischio di produzione alla controparte di documenti incompleti o inesatti che attestino, contrariamente al vero, l'esistenza delle condizioni o dei requisiti essenziali per l'aggiudicazione dell'incarico;
- la trasmissione di dati e informazioni attraverso un sistema che consenta di tracciare i singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- la verifica dello svolgimento delle attività in modo conforme a quanto previsto dal contratto/convenzione di concessione stipulata;
- le modalità di gestione delle fasi di consuntivazione dei beni/servizi a rimborso e della registrazione delle fatture dei beni/servizi acquistati;
- la formalizzazione del processo di *budgeting*, anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;
- la segregazione delle attività di negoziazione con i clienti delle varianti contrattuali, di ricalcolo/adeguamento del prezzo, e delle relative verifiche sull'importo da fatturare al cliente.

2.2.9 GESTIONE DEI CONTENZIOSI GIUDIZIALI E STRAGIUDIZIALI

La regolamentazione dell'attività prevede:

- la separazione delle attività tra la ricezione e la promozione delle contestazioni, della verifica dell'effettività dell'oggetto del contendere, della gestione del contenzioso in fase stragiudiziale e della gestione del contenzioso in fase giudiziale;
- reporting periodico sullo stato delle vertenze e sulle possibilità e sui termini di definizione stragiudiziale o di conciliazione giudiziale delle stesse;
- che la contestazione sia basata su parametri oggettivi e che l'eventuale transazione e/o conciliazione venga condotta dalla persona titolare di un'apposita procura e delega *ad litem*, che contempli il potere di conciliare o transigere la controversia;
- l'indicazione dei criteri di selezione di professionisti esterni;
- l'attribuzione dell'attività di supervisione del contenzioso e l'approvazione delle fatture emesse dal consulente;

- modalità di tracciabilità del processo interno;
- che i rapporti con l'Autorità giudiziaria e con la Pubblica Amministrazione nell'ambito del contenzioso giudiziale e stragiudiziale devono essere improntati ai principi di correttezza, trasparenza e tracciabilità, anche quando gestiti per il tramite di un legale esterno;
- che il processo deve essere gestito in modo da evitare che si verifichino fenomeni di induzione a non rendere dichiarazioni ovvero a renderle mendaci all'Autorità Giudiziaria.

2.2.10 GESTIONE DEI RAPPORTI CON SOGGETTI PUBBLICI

La regolamentazione per la gestione dei rapporti con soggetti pubblici ai fini dell'ottenimento di provvedimenti amministrativi (quali autorizzazioni, licenze e permessi) necessari per l'esercizio delle attività tipiche aziendali prevede:

- la separazione delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda, di presentazione della domanda e di gestione della concessione e/o dell'autorizzazione, prevedendo specifici sistemi di controllo al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo;
- specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la concessione e/o autorizzazione;
- l'individuazione della persona deputata a rappresentare la società nei confronti della PA concedente, cui conferire apposita delega e procura;
- la definizione di ruoli e compiti sulle fasi di ottenimento e gestione delle concessioni e/o autorizzazioni, con particolare riguardo ai presupposti di fatto e di diritto per la presentazione della relativa richiesta.

2.2.11 ACQUISIZIONE E/O GESTIONE DI CONTRIBUTI, SOVVENZIONI, FINANZIAMENTI, ASSICURAZIONI O GARANZIE CONCESSE DA SOGGETTI PUBBLICI

La regolamentazione dell'attività prevede:

- la separazione delle attività di monitoraggio delle opportunità di accesso a contributi e/o finanziamenti erogati dallo Stato o dall'Unione Europea, di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda, di presentazione della domanda e di gestione del contributo e/o finanziamento erogato, prevedendo specifici strumenti di controllo al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo;
- specifiche verifiche della veridicità e correttezza dei documenti la cui produzione è necessaria per accedere alla contribuzione e/o al finanziamento;
- l'individuazione della persona deputata a rappresentare la società nei confronti della PA erogante, cui conferire apposita delega e procura;
- la definizione di ruoli e compiti connessi al controllo dell'esatta corrispondenza tra la finalità concreta di utilizzo del contributo e/o del finanziamento erogato e il fine per il quale è stato ottenuto.

2.2.12 ATTIVITÀ CHE PREVEDONO L'INSTALLAZIONE, MANUTENZIONE, AGGIORNAMENTO O GESTIONE DI SOFTWARE PER TRASMISSIONE DI DATI E COMUNICAZIONI

La regolamentazione dell'attività prevede:

- adeguate misure di sicurezza per il trattamento informatico dei dati;

  con riferimento all'organizzazione della sicurezza per gli utenti esterni, i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. Gli utenti esterni, se reputato necessario, devono essere adeguatamente istruiti sulle modalità di utilizzo dei sistemi informatici, attraverso:

  - specifiche istruzioni fornite che definiscano le regole di loro gestione soprattutto in caso di accessi da remoto;
  - specifiche attività di formazione per garantire che il personale sia informato sulle correnti minacce *cyber* soprattutto in caso di accesso ai sistemi aziendali da remoto;

- con riferimento alla sicurezza fisica e ambientale, l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

3. B – AREA A RISCHIO NELL'AMBITO DELLA GESTIONE DEI SISTEMI INFORMATICI

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art. 24 bis del D.Lgs. 231/2001 (delitti informatici e trattamento illecito dei dati).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della gestione del sistema informatico è fatto espresso obbligo ai Destinatari di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Gestione dei sistemi informatici	Documenti informatici (art. 491-bis c.p.	Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio
	Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	Gestione dei profili utente e del processo di autenticazione
	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art 615-quater c.p.)	Gestione e protezione della postazione di lavoro
	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies.)	Gestione degli accessi da e verso l'esterno.
	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)	Gestione e protezione delle reti. Gestione di output di sistema e di dispositivi di memorizzazione (es. USB, CD)
	Danneggiamento di sistemi informatici o telematici di pubblica utilità (art.635 quinquies)	Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.).

Area a rischio	Reati associabili	Attività sensibili
	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640 quinquies)	Produzione e/o vendita di apparecchiature, dispositivi o programmi informatici e servizi di installazione e manutenzione di hardware, software, reti
	Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (Art. 1, comma 11 Decreto legge 21 settembre 2019 n.105)	Raccolta e trasmissione di comunicazioni/informative/dati agli Organi Preposti in materia di sicurezza nazionale cibernetica

3.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI NELLA GESTIONE DEI SISTEMI INFORMATICI

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i Destinatari, in relazione ai Delitti informatici, devono attenersi alle seguenti regole di comportamento e principi generali:

- assicurare che le misure di sicurezza informatica adottate siano costantemente aggiornate in relazione all'evoluzione della tecnologia;
- eseguire specifiche attività di valutazione del rischio al fine di rilevare e valutare potenziali vulnerabilità nei sistemi informatici;
- eseguire periodici audit indipendenti al fine di valutare e monitorare costantemente l'adeguatezza del sistema di controllo interno dei sistemi informatici;
- eseguire un'analisi dei rischi di sicurezza informatica e dei possibili controlli da adottare per ogni progetto di sviluppo o modifica dei sistemi informatici;
- monitorare i log dei sistemi informatici (l'accesso ai sistemi informatici degli utenti e amministratori deve essere coerente con le mansioni aziendali svolte);
- limitare l'accesso fisico ai luoghi in cui sono collocati le apparecchiature informatiche e i dispositivi di rete.

Ai Destinatari del Modello è, inoltre, fatto espresso divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
- 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;
- 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;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

- 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;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

- segnalare il furto, il danneggiamento o lo smarrimento degli strumenti informatici. Entro 24 ore dal fatto, il soggetto interessato dovrà far pervenire alla società l'originale della denuncia all'Autorità di Pubblica Sicurezza;
- evitare di introdurre e/o conservare all'interno della società 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;
- evitare di trasferire all'esterno della società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della società stessa se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;
- evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- segnalare senza ritardo alle aree competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della società solo prodotti ufficialmente acquisiti dall'azienda stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici;

- porre in essere comportamenti non in contrasto con leggi e regolamenti in materia di protezione e sicurezza delle banche dati e dei sistemi ospitanti (con particolare riferimento a quanto previsto dal Codice in materia di protezione dei dati personali);
- porre in essere comportamenti non in contrasto con leggi e regolamenti in materia di servizi di certificazione di firma elettronica.

3.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

3.2.1 GESTIONE DEI SISTEMI INFORMATICI

La regolamentazione dell'attività prevede:

- con riferimento all'organizzazione della sicurezza per gli utenti interni, la definizione dei ruoli e della responsabilità nella gestione delle modalità di accesso di utenti interni alla società e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, ivi incluso la definizione delle responsabilità e delle modalità operative degli utenti a cui è attribuito il ruolo di amministratore di sistema per l'utilizzo dei sistemi informatici;
- con riferimento all'organizzazione della sicurezza per gli utenti esterni, la definizione dei ruoli e delle responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. La regolamentazione prevede specifiche misure volte a prevenire gli accessi non autorizzati. Gli utenti esterni, se reputato necessario, devono essere adeguatamente istruiti sulle modalità di utilizzo dei sistemi informatici, attraverso:
  - specifiche istruzioni fornite che definiscano le regole di loro gestione soprattutto in caso di accessi da remoto;
  - specifiche attività di formazione per garantire che il personale sia informato sulle correnti minacce *cyber* soprattutto in caso di accesso ai sistemi aziendali da remoto;
- con riferimento alla classificazione e controllo dei beni, la definizione dei ruoli e delle responsabilità per l'identificazione e la classificazione degli *asset* aziendali (ivi inclusi dati e informazioni). Le regole per l'utilizzo accettabile delle informazioni e degli *asset* associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate soprattutto per l'accesso degli *asset* da remoto;
- con riferimento alla sicurezza fisica e ambientale, l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;
- con riferimento alla gestione delle comunicazioni e dell'operatività per:
  - il corretto e sicuro funzionamento degli elaboratori di informazioni;
  - la protezione da software pericoloso;
  - il *backup* di informazioni e software;

- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
- gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
- il controllo sui cambiamenti agli elaboratori e ai sistemi;
- la gestione di dispositivi rimovibili;
- adeguate misure di sicurezza da adottare per i dispositivi che accedono da remoto ai sistemi della società;
- l'adozione di controlli atti ad impedire l'utilizzo di software non consentiti;

- con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni:
  - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
  - delle modalità operative per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
  - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
  - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
  - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
  - la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
  - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
  - la custodia dei dispostivi di memorizzazione;
  - adeguate misure di sicurezza da adottare per l'autenticazione dei dispositivi che accedono da remoto ai sistemi dell'organizzazione (es. autenticazione a due fattori);
  - prevedere dei processi di review delle modalità di gestione degli accessi logici;
- con riferimento alla gestione degli incidenti e dei problemi di sicurezza informatica, adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, ed in particolare:
  - appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;

- l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della *root cause*;
- la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
- l'analisi di *report* e *trend* sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
- appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
- l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
- l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
- la manutenzione della base dati contenente informazioni su errori noti non ancora risolti, i rispettivi *workaround* e le soluzioni definitive, identificate o implementate;
- la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa;
- adeguati piani di *business resilience* e di risposta agli incidenti;
- prevedere dei processi di *review* delle modalità di gestione degli incidenti;

- i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica;
- con riferimento alla crittografia, l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;
- con riferimento alla sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi:
  - l'identificazione dei rischi connessi all'introduzione delle nuove tecnologie o nuovi strumenti software; l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
  - la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
  - la confidenzialità, autenticità e integrità delle informazioni;
  - la sicurezza nel processo di sviluppo dei sistemi informativi;
  - una *review* ed un aggiornamento periodico delle metodologie di gestione del rischio al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

4. C – AREA A RISCHIO NELL'AMBITO DELLA GESTIONE SOCIETARIA

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art. 25 ter del D.Lgs. 231/2001 (Reati societari).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della gestione societaria è fatto espresso obbligo ai Destinatari di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Gestione della contabilità e redazione del bilancio	False comunicazioni sociali (artt. 2621 e 2622 c.c.) e Falsità nelle relazioni e nelle comunicazioni dei responsabili della revisione legale (art. 27 del D.Lgs. 27 gennaio 2010 n. 39)[6] Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.) Formazione fittizia del capitale (art. 2632 c.c.)	Gestione/custodia della contabilità generale ed effettuazione delle chiusure contabili Redazione del bilancio di esercizio
Gestione dei rapporti con il Socio, la società di revisione, il Collegio sindacale	Impedito controllo (art. 2625 comma 2 c.c.) Art.29 Impedito controllo (art.29 del D.Lgs. 27 gennaio 2010 n. 39)[7]	Gestione dei rapporti con il Socio e con la società di revisione[8] Gestione dei rapporti con il Collegio sindacale
Rapporti con le Autorità di Vigilanza e altri Organi di controllo	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c. c.)	Gestione dei rapporti con il Magistrato della Corte dei conti[9]
Operazioni societarie che possono incidere sul capitale	Operazioni in pregiudizio dei creditori (art. 2629 cc) Formazione fittizia del capitale (art. 2632 c. c.)	Gestione delle operazioni societarie straordinarie che possono incidere sul capitale
Predisposizione e divulgazione verso l'esterno di dati e notizie relativi alla società	False comunicazioni sociali (artt. 2621 e 2622 c.c.) e Falsità nelle relazioni e nelle comunicazioni dei responsabili della revisione legale (art. 27 del D.Lgs. 27 gennaio 2010 n. 39)[10]	Predisposizione di dati e notizie relativi alla società Divulgazione verso l'esterno di dati e notizie relativi alla società

4.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI SOCIETARI

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i Destinatari, in relazione ai Reati societari, devono attenersi alle seguenti regole di comportamento e principi generali:

- tenere un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e dei regolamenti nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, con lo scopo di fornire un'informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della società; a tal fine, è fatto espresso divieto di:

[6] L'art. 37, commi 34 e 35, D.Lgs. 27 gennaio 2010 n. 39, che attua la direttiva 2006/43/CE relativa alla revisione legale dei conti, ha abrogato l'art. 2624 c.c. non effettuando al contempo il necessario coordinamento con l'art. 25 ter del D.Lgs. 231/2001. Stando il principio di tassatività vigente nel diritto penale la fattispecie ex art.27 del D.Lgs. 39/2010 non dovrebbe quindi essere annoverata nel catalogo dei reati presupposto della responsabilità amministrativa dell'ente. In via prudenziale si ritiene di tenerne comunque conto nell'elaborazione del Modello.

[7] Si precisa che l'art. 37, commi 34 e 35, D.Lgs. 27 gennaio 2010 n. 39, che attua la direttiva 2006/43/CE relativa alla revisione legale dei conti, nel modificare l'art 2625 c.c., non ha effettuato il coordinamento con l'art 25 ter del D.Lgs. 231/2001. L'art. 25 ter del D.Lgs. 231/2001 richiama l'art 2625 c.c., che nella nuova versione non comprende più l'impedito controllo dei revisori, il quale viene spostato nel D.Lgs. 39/2010, all'art 29, il quale non è richiamato dall'art 25 ter e prevede due nuove fattispecie (sotto forma di illecito amministrativo e penale) di impedito controllo relativamente alla medesima attività di revisione. Stando il principio di tassatività vigente nel diritto penale, la fattispecie prevista dall'art.29 del D.Lgs. 39/2010 non dovrebbe essere annoverata nel catalogo dei reati presupposto della responsabilità amministrativa dell'ente; peraltro, in via prudenziale si ritiene di tenerne comunque conto nell'elaborazione del Modello.

[8] Si veda quanto riportato nella nota precedente

[9] Pur non essendovi evidenze dell'inquadramento del Magistrato della Corte dei conti come autorità pubblica di vigilanza ai sensi dell'art. 2638, commi 1 e 2 c.c. si ritiene in via prudenziale considerare l'attività come sensibile anche nel presente documento.

[10] Si veda quanto riportato nella nota 6.

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della società;
- omettere di comunicare dati ed informazioni richiesti dalla normativa in vigore riguardo alla situazione economica, patrimoniale e finanziaria della società;

- attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione dei bilanci, nel piano dei conti di Contabilità Generale, e in particolare, in relazione ai flussi informativi che determinano il valore di poste di bilancio di carattere valutativo;
- cooperare con il Collegio sindacale, nonché con gli altri organi di controllo, ottemperando tempestivamente a ogni legittima richiesta proveniente da tali organi ed evitando comportamenti omissivi e ostruzionistici o comunque ostacolo allo svolgimento delle attività di controllo;
- osservare scrupolosamente tutte le norme che tutelano l'integrità e l'effettività del capitale sociale; a tal fine, è fatto divieto di:
  - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
  - ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
  - effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
  - procedere, con qualsiasi modalità, a formazione o aumento fittizi del capitale sociale;
- effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità pubbliche di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate ovvero alla corretta ed informata formazione della volontà degli organi sociali; in ordine a tale punto è fatto divieto di:
  - esporre, in tali comunicazioni e nella documentazione trasmessa, fatti non rispondenti al vero, oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della società;
  - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle autorità pubbliche di vigilanza, anche in sede di ispezione.

4.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

4.2.1 GESTIONE DELLA CONTABILITÀ E REDAZIONE DEL BILANCIO

La regolamentazione dell'attività prevede:

- la definizione delle principali fasi nelle quali si articola l'attività in oggetto, quali:
  - la gestione della contabilità generale;

- la valutazione e stima delle poste di bilancio;
- la redazione del bilancio civilistico;

- la formalizzazione e la diffusione, al personale coinvolto in attività di predisposizione del bilancio, di norme che definiscano con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio civilistico e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente integrate/aggiornate dalle indicazioni fornite dall'ufficio competente sulla base delle novità in termini di normativa civilistica e diffuse ai destinatari sopra indicati;
- la formalizzazione di istruzioni rivolte alle aree con cui si stabilisca quali dati e notizie debbano essere forniti alla Direzione competente per le attività di «amministrazione e controllo» in relazione alle chiusure annuali, con quali modalità e la relativa tempistica;
- i compiti e le responsabilità dei soggetti coinvolti nel processo di formazione del bilancio e un sistema di controllo che garantisca la correttezza e la veridicità delle informazioni e dei dati forniti e la certezza della provenienza degli stessi;
- l'utilizzo di un sistema (anche informatico) che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- che il sistema utilizzato per la gestione della contabilità debba essere strutturato in modo che le eventuali modifiche ai dati contabili siano effettuate solo dagli utenti autorizzati mediante profilatura a sistema;
- che sia fornita adeguata giustificazione, documentazione e archiviazione di eventuali modifiche apportate al Progetto di bilancio;
- la tempestiva messa a disposizione del Progetto di bilancio a tutti i componenti del Consiglio di Amministrazione, con un congruo anticipo rispetto alla riunione del Consiglio per l'approvazione dello stesso, nonché del giudizio sul bilancio - o attestazione similare, chiara e analitica - da parte della società di revisione;
- l'attribuzione di ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio e degli altri documenti contabili societari dalla loro formazione al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;
- meccanismi idonei ad assicurare che eventuali comunicazioni sul bilancio vengano redatte, al fine di assicurare la correttezza del risultato e la condivisione dello stesso. Tali meccanismi comprendono idonee scadenze, la definizione dei soggetti interessati, gli argomenti da trattare, i flussi informativi;
- trascrizione, pubblicazione e archiviazione dei verbali di assemblea.

4.2.2 GESTIONE DEI RAPPORTI CON IL SOCIO, LA SOCIETÀ DI REVISIONE, IL COLLEGIO SINDACALE

La regolamentazione dell'attività prevede:

- la formalizzazione di direttive che sanciscono l'obbligo alla massima collaborazione e trasparenza nei rapporti con la società di revisione, il Collegio sindacale e con gli azionisti;

- l'individuazione dei responsabili delle attività di ricezione, consolidamento e trasmissione dei dati, delle informazioni e dei documenti richiesti;
- specifici sistemi di controllo che garantiscano la provenienza e la verifica della veridicità e della completezza dei dati, anche mediante il confronto con i dati e le informazioni contenute in prospetti e/o in documenti e/o atti già comunicati;
- l'obbligo di indire specifiche riunioni di condivisione dei dati e/o delle informazioni trasmesse, al fine di garantire la corretta informazione da parte dei soggetti che esercitano detto controllo, e l'obbligo di verbalizzazione delle relative decisioni e azioni conseguenti;
- che venga garantita la completezza, l'inerenza e la correttezza delle informazioni dei documenti forniti alla società di revisione, al Collegio sindacale e che si rendano disponibili agli stessi le informazioni e/o i documenti richiesti dagli stessi e/o necessari per lo svolgimento delle attività di controllo loro deputate garantendo il rispetto della normativa di riferimento;
- l'obbligo di trasmissione alla società di revisione legale dei conti e al Collegio sindacale – con congruo anticipo – di tutti i documenti relativi agli argomenti posti all'ordine del giorno sui quali essi debbano esprimere un parere ai sensi di legge;
- che l'Organismo di Vigilanza acquisisca il Progetto di bilancio, prima della riunione del Consiglio di Amministrazione indetta per l'approvazione dello stesso.

4.2.3 RAPPORTI CON LE AUTORITÀ DI VIGILANZA E ALTRI ORGANI DI CONTROLLO

La regolamentazione dell'attività prevede:

- la formalizzazione di direttive che sanciscono l'obbligo alla massima collaborazione e trasparenza nei rapporti con le Autorità di Vigilanza e con gli altri organi di controllo;
- l'identificazione di un soggetto responsabile per la gestione dei rapporti con le predette autorità e altri organi di controllo, appositamente delegato dai vertici aziendali;
- l'individuazione dei responsabili delle attività di ricezione, consolidamento e trasmissione, validazione e riesame dei dati, delle informazioni e dei documenti richiesti dalle predette autorità e altri organi di controllo;
- che sia garantita l'archiviazione e conservazione dei predetti dati, delle informazioni e dei documenti trasmessi alle Autorità di Vigilanza e agli altri organi di controllo.

4.2.4 OPERAZIONI SOCIETARIE CHE POSSONO INCIDERE SUL CAPITALE

La regolamentazione dell'attività prevede:

- che tutte le operazioni sui conferimenti, sugli utili e sulle riserve, le operazioni sul capitale sociale, nonché l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni debbano essere effettuate nel rispetto delle norme di legge applicabili;
- la formalizzazione di ruoli, responsabilità e modalità di predisposizione di documenti alla base di delibere del Consiglio di Amministrazione su operazioni che possono incidere sul capitale;
- regole di gestione delle operazioni di valutazione, autorizzazione e gestione delle operazioni sul capitale e l'archiviazione degli atti di delibera e relativi documenti a supporto predisposti;
- che, qualora tali operazioni richiedessero il coinvolgimento di dipendenti della società, venga previsto il tracciamento e il controllo delle specifiche attività svolte.

4.2.5 PREDISPOSIZIONE E DIVULGAZIONE VERSO L'ESTERNO DI DATI E NOTIZIE RELATIVI ALLA SOCIETÀ

La regolamentazione dell'attività prevede:

- l'obbligo di mantenere riservate le informazioni acquisite nello svolgimento dei compiti aziendali e di utilizzare i documenti e le informazioni a carattere riservato esclusivamente nell'espletamento delle aree di rispettiva competenza;
- la conservazione e l'archiviazione della documentazione riservata, acquisita nello svolgimento delle mansioni, in luogo tale da consentire l'accesso esclusivamente alle persone autorizzate;
- la previsione di specifiche cautele contrattuali, volte a regolare il trattamento e l'accesso a Informazioni riservate da parte di consulenti attraverso la previsione di specifiche clausole di riservatezza e di rispetto del Modello 231.

5. D – AREA A RISCHIO NELL'AMBITO DEI DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art. 25 quinquies del D.Lgs. 231/2001 (delitti contro la personalità individuale).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito dei delitti contro la personalità individuale, è fatto espresso obbligo ai Destinatari di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Approvvigionamento di beni, lavori e servizi	Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)	Processo di Approvvigionamento Gestione Contrattuale
Conferimento di contratti di consulenza o prestazioni professionali	Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)	Processo di Approvvigionamento Gestione Contrattuale
Selezione, assunzione e politiche di incentivazione del personale	Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)	Selezione e assunzione del personale esterno

5.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI CONTRO LA PERSONALITÀ INDIVIDUALE

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, per i Destinatari è previsto l'espresso divieto di commettere delitti contro la personalità individuale, quali ad esempio, la riduzione in schiavitù o in condizioni analoghe di una persona ovvero lo sfruttamento della stessa in considerazione del suo stato di bisogno.

5.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

5.2.1 APPROVVIGIONAMENTO DI BENI, LAVORI E SERVIZI

La regolamentazione dell'attività prevede:

- clausole contrattuali «*standard*», riguardanti i costi della sicurezza e le norme vigenti in materia di lavoro - di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza, che i fornitori devono dichiarare di conoscere e che si obblighino a rispettare.

5.2.2 CONFERIMENTO DI CONTRATTI DI CONSULENZA O PRESTAZIONI PROFESSIONALI

La regolamentazione dell'attività prevede:

- clausole contrattuali «*standard*», riguardanti i costi della sicurezza e le norme vigenti in materia di lavoro - di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza, che i fornitori devono dichiarare di conoscere e che si obblighino a rispettare.

5.2.3 SELEZIONE, ASSUNZIONE E POLITICHE DI INCENTIVAZIONE DEL PERSONALE

La regolamentazione dell'attività prevede:

- con riferimento alla formulazione dell'offerta e assunzione:
  - di procedere alla scelta coerentemente alla valutazione di idoneità;
  - l'applicazione (almeno) del trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili;
  - la verifica dell'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti in sede di sottoscrizione della lettera di assunzione;
- con riferimento alla gestione del rapporto di lavoro, il rispetto:
  - dei contratti collettivi nazionali ed aziendali per quanto attiene la retribuzione;
  - della normativa relativa all'orario di lavoro e altre indennità orarie, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria ed alle ferie;
  - delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
  - delle condizioni lavorative in termini non degradanti.

6. E – AREA A RISCHIO NELL'AMBITO DELLA GESTIONE DELLA SICUREZZA E SALUTE SUI LUOGHI DI LAVORO

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).

Quanto ai criteri oggettivi di imputazione della responsabilità all'ente, occorre fare riferimento all'art. 5 del D.Lgs. 231/2001, 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.

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:

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

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto di quanto previsto nell'ambito del lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge.

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

- prevedere 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 strutture 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 anche 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.

La condotta illecita per 3-i potrebbe dunque configurarsi nel caso di Reati di omicidio colposo e lesioni personali colpose gravi o gravissime causati da una mancata predisposizione dei presidi di sicurezza e salute sui luoghi di lavoro previsti dalla legge e con un vantaggio per la società che potrebbe derivare dal conseguente risparmio ottenuto in termini di costi o di tempi.

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art.25 septies del D.Lgs. 231/2001.

Area a rischio	Reati associabili	Attività sensibili
Pianificazione	Omicidio colposo (art. 589 c.p.) Lesioni personali colpose (art. 590 c.p.)	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.
Attuazione e funzionamento		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: 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.
Controllo e azioni correttive		Attività di controllo e azioni correttive volte a definire: Misura e monitoraggio delle prestazioni; Registrazione e monitoraggio degli infortuni, incidenti, non conformità, azioni correttive e preventive; Modalità di gestione delle registrazioni; Modalità di esecuzione audit periodici

Riesame della direzione		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.

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della gestione della sicurezza e salute sui luoghi di lavoro è fatto espresso obbligo ai Destinatari di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

6.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI IN MATERIA DI SICUREZZA E SALUTE SUI LUOGHI DI LAVORO

La prevenzione degli infortuni e la tutela della sicurezza e della salute sul luogo di lavoro rappresenta un'esigenza di fondamentale rilievo a protezione delle proprie risorse umane e dei terzi.

In tale contesto, 3-i si impegna altresì a prevenire e reprimere comportamenti e pratiche che possano avere come effetto la mortificazione del dipendente nelle sue capacità e aspettative professionali, ovvero che ne determinino l'emarginazione nell'ambiente di lavoro, il discredito o la lesione della sua immagine.

In particolare, i principi e i criteri fondamentali in base al quale vengono assunte le decisioni, in materia di salute e sicurezza, sono:

- evitare i rischi;
- valutare i rischi che non possono essere evitati;
- combattere i rischi alla fonte;
- adeguare il lavoro all'uomo, in particolare per quanto concerne la concezione dei posti di lavoro e la scelta delle attrezzature di lavoro e dei metodi di lavoro e di produzione, in particolare per attenuare il lavoro monotono e il lavoro ripetitivo e per ridurre gli effetti di questi lavori sulla salute;
- tener conto del grado di evoluzione della tecnica;
- sostituire ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- programmare la prevenzione, mirando a un complesso coerente che integri nella medesima tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali l'influenza dei fattori dell'ambiente di lavoro;
- dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale;
- impartire adeguate istruzioni ai lavoratori.

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i Destinatari, in relazione ai delitti di omicidio colposo e lesione personali gravi o gravissime, devono attenersi alle seguenti regole di comportamento e principi generali:

- divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di Reato rientranti tra quelle sopra considerate (art. 25-septies del D.Lgs. 231/2001);
- divieto di tenere comportamenti in violazione delle procedure interne di 3-i.

6.2 MODELLO ORGANIZZATIVO E DI GESTIONE DELLA SICUREZZA

3-1 attua ed osserva le disposizioni contenute nel Decreto Legislativo n. 81/2008, mediante l'azione di un modello organizzativo e di gestione della sicurezza conforme alle «Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL)», proposte dall'art. 30 del menzionato decreto del 2008. Gli elementi di tale modello sono i seguenti:

Sistema organizzativo

Il Datore di Lavoro è dotato di poteri illimitati di spesa e dei necessari e autonomi poteri decisionali, organizzativi e gestionali al fine di garantire il rispetto della normativa vigente in materia di salute e sicurezza nei luoghi di lavoro.

Il *Datore di lavoro* ha, inoltre, la responsabilità di:

- rappresentare la Società per l'attuazione delle politiche direzionali e presidiare il rapporto con i soggetti istituzionali;
- in esecuzione degli obblighi informativi di cui all'art. 6 del D.lgs. 231/2001, ferme restando le comunicazioni ad evento, inviare all'Organismo di Vigilanza una relazione periodica avente ad oggetto l'attività svolta, per quanto di competenza, in attuazione dell'art. 30 del Dlgs. 81/2008 e s.m.i. e con riguardo all'art. 25 septies del D.Lgs. 231/2001 e s.m.i..

Responsabile Servizio Prevenzione e Protezione (RSPP)

Il Datore di lavoro deve nominare il Responsabile Servizio Prevenzione e Protezione (RSPP) con il compito di:

- supportarlo nella valutazione dei rischi connessi alle attività;
- individuare il programma delle misure ritenute opportune;
- promuovere il miglioramento delle condizioni di lavoro.

L'RSPP si avvale di uno o più ASPP.

Dirigenti e Preposti

Il Datore di lavoro è tenuto a prevedere alla concreta individuazione dei Dirigenti e dei Preposti ai fini della salute e sicurezza nei luoghi di lavoro, in base ai seguenti criteri.

I soggetti nominati Dirigenti ai fini della salute e sicurezza nei luoghi di lavoro, nell'ambito del relativo ruolo definito dall'art. 2, lett. d) del D.Lgs. 81/2008 sopra richiamato, nei limiti delle attribuzioni e competenze ad essi conferite nell'ambito dell'organizzazione aziendale, hanno gli obblighi definiti nell'articolo 18 del Decreto medesimo.

I soggetti nominati Preposti ai fini della salute e sicurezza nei luoghi di lavoro, nell'ambito del relativo ruolo definito dall'art. 2, lett. e) del D.Lgs. 81/2008 sopra richiamato, secondo le loro attribuzioni e competenze, adempiono ai seguenti obblighi, indicati nell'art. 19 del Decreto medesimo.

Sistema autorizzativo

Il Datore di Lavoro è dotato di illimitati poteri di spesa e dei necessari poteri in materia di gestione e organizzazione, per l'adempimento di tutti gli obblighi che su di esso gravano in materia di salute e sicurezza sul lavoro, con facoltà di delegare in tutto o in parte tali poteri fatta eccezione per gli obblighi non delegabili ai sensi dell'art. 17 comma 1 (i. la valutazione di tutti i rischi con la

conseguente elaborazione del documento previsto dall'art.28 del D.Lgs. n.81/08; ii. La designazione del responsabile del Servizio di Prevenzione e Protezione dai rischi) e fatto salvo l'obbligo di vigilanza di cui all'art. 16, comma 3 del Decreto medesimo.

Il Datore di Lavoro della Società opera con la più ampia autonomia e senza limiti di importo per qualsivoglia impegno verso chicchessia ai fini di garantire la salute, la sicurezza, l'igiene del lavoro e l'incolumità dei terzi.

6.3 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

6.3.1 PIANIFICAZIONE

L'attività di pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro è volta a:

- fissare gli obiettivi coerenti con la politica aziendale;
- stabilire i processi necessari al raggiungimento degli obiettivi;
- definire e assegnare risorse.

Per tale attività la regolamentazione prevede:

- Politica e obiettivi: l'esistenza di un documento formalizzato di Politica che definisce gli indirizzi e gli obiettivi generali in tema di salute e sicurezza che l'azienda stabilisce di raggiungere:
  - formalmente approvato dall'Alta direzione;
  - contenente l'impegno a essere conforme con le vigenti leggi in materia di salute e sicurezza applicabili e con gli altri requisiti sottoscritti;
  - contenente l'impegno alla prevenzione degli infortuni e delle malattie professionali e al miglioramento continuo della gestione e delle prestazioni del sistema salute e sicurezza;
  - adeguatamente diffuso ai dipendenti e alle parti interessate;
  - periodicamente riesaminato per assicurare che gli obiettivi in esso indicati siano appropriati e adeguati rispetto ai rischi presenti nell'organizzazione (ad es. ai nuovi regolamenti e leggi).
- Piani annuali e pluriennali: l'esistenza di un Piano degli Investimenti in materia di salute e sicurezza sul lavoro, approvato dagli organi societari delegati:
  - contenente una chiara individuazione delle scadenze, responsabilità e disponibilità delle risorse necessarie per l'attuazione (finanziarie, umane, logistiche, di equipaggiamento);
  - adeguatamente comunicato all'organizzazione in modo che il personale ne abbia una sufficiente comprensione.
- Definizione delle modalità e dei criteri da adottarsi per:
  - l'aggiornamento riguardo la legislazione rilevante e le altre prescrizioni applicabili in tema di salute e sicurezza;

- l'individuazione delle aree aziendali di applicabilità di tali prescrizioni e le modalità di diffusione delle stesse.

6.3.2 ATTUAZIONE E FUNZIONAMENTO

L'attività di Attuazione e Funzionamento è 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;
- modalità di controllo operativo;
- gestione delle emergenze.

Per tale attività la regolamentazione interna dovrà prevedere:

- **Organizzazione e Responsabilità – Datore Di Lavoro**: l'adozione di disposizioni organizzative per l'individuazione della figura datoriale che tengano conto della struttura organizzativa della Società e del settore di attività produttiva.
- **Organizzazione e Responsabilità RSPP/ASPP/RGE:** l'esistenza di disposizioni organizzative che, con riferimento alle figure del Responsabile del Servizio di Prevenzione e Protezione (RSPP), degli Addetti al Servizio di Prevenzione e Protezione (ASPP), del Responsabile della gestione delle emergenze e di prevenzione incendi (RGE), previsti ai sensi della normativa vigente:
  - prevedano una formale designazione di tali figure;
  - definiscano, in considerazione dell'ambito di attività, i requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tali figure (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, titoli specifici, specifiche competenze);
  - prevedano la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  - prevedano la tracciabilità della formale accettazione dell'incarico con riferimento alla figura del RSPP.
- **Organizzazione e Responsabilità – Medico Competente:** l'adozione di disposizioni organizzative che con riferimento al Medico Competente previsto ai sensi della normativa vigente:
  - prevedano la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
  - definiscano la documentazione sanitaria e di rischio da predisporre secondo la normativa vigente (es. Cartella Sanitaria);
  - prevedano la tracciabilità della formale accettazione da parte del Medico Competente.
- **Organizzazione e Responsabilità - Sicurezza nei cantieri temporanei o mobili:** l'adozione di norme interne che:
  - disciplinino le modalità di individuazione ed assegnazione dell'incarico di Coordinatore in materia di salute e sicurezza per la progettazione dell'opera e di Coordinatore in materia di

sicurezza e di salute durante la realizzazione dell'opera, tenendo conto dei requisiti professionali previsti dalle norme di legge;

- prevedano la tracciabilità della valutazione dei requisiti e dell'accettazione dell'incarico da parte dei Coordinatori.

- **Sistema di deleghe di funzioni:** l'adozione di un sistema di deleghe definite secondo i seguenti principi:
  - effettività relativamente alla sussistenza di autonomia decisionale e finanziaria del delegato;
  - idoneità tecnico professionale ed esperienza del delegato;
  - vigilanza sull'attività del delegato, non acquiescenza, non ingerenza;
  - certezza, specificità e consapevolezza.

  Al fine di rispettare i suddetti principi, il sistema di deleghe adottato deve prevedere:
  - la verifica della tracciabilità e della permanenza delle deleghe;
  - la possibilità per il delegato di sub-delegare funzioni in materia di salute e sicurezza;
  - la tracciabilità dei criteri in base ai quali viene determinata la coerenza tra funzioni delegate e poteri decisionali e di spesa assegnati;
  - la modalità di controllo circa la permanenza in capo al delegato dei requisiti tecnico-professionali, un piano periodico di aggiornamento e sviluppo tecnico professionale del delegato;
  - un flusso informativo formalizzato continuo/ periodico tra delegante e delegato e un'attività di vigilanza formalizzata;
  - l'identificazione dell'ambito di operatività della delega;
  - la tracciabilità dell'accettazione espressa della delega da parte dei delegati/subdelegati.

- **Individuazione e valutazione dei rischi – Ruoli e responsabilità:** l'adozione di norme interne che identifichino ruoli, responsabilità e modalità per lo svolgimento, approvazione ed aggiornamento della valutazione di tutti i rischi presenti nell'ambito di 3-i. In particolare, le procedure dovranno:
  - identificare i ruoli, autorità, requisiti di competenza e necessità di addestramento del personale responsabile per condurre l'identificazione dei pericoli, l'identificazione del rischio ed il controllo del rischio;
  - identificare le responsabilità per la verifica, l'approvazione e l'aggiornamento dei contenuti del Documento di Valutazione dei Rischi (DVR);
  - identificare modalità e criteri per la revisione in tempi o periodi determinati dei processi di identificazione dei pericoli e valutazione del rischio;
  - prevedere, laddove necessario, la tracciabilità dell'avvenuto coinvolgimento del Medico Competente nel processo di identificazione dei pericoli e valutazione dei rischi;
  - prevedere 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;

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

- **Presenza del Documento di Valutazione dei Rischi (DVR):** l'adozione del Documento di relazione sulla Valutazione dei Rischi redatto secondo le disposizioni vigenti contenente almeno:
  - il procedimento di valutazione, con la specifica dei criteri adottati;
  - l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione;
  - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.
- **Controllo operativo – Affidamento compiti e mansioni:** l'adozione di norme interne che individuino i criteri e le modalità definite per l'affidamento delle mansioni ai lavoratori da parte del Datore di Lavoro. In particolare, tali norme interne prevedono:
  - i criteri di affidamento delle mansioni ai lavoratori in base alle capacità e alle condizioni degli stessi in rapporto alla loro salute e alla sicurezza, e a quanto emerso dai risultati degli accertamenti sanitari eseguiti;
  - le misure organizzative per la partecipazione del Medico Competente e del RSPP nella definizione di ruoli e responsabilità dei lavoratori;
  - la tracciabilità delle attività di valutazione svolte a tale scopo.
- **Controllo operativo – Dispositivi di protezione individuale (DPI) - laddove applicabili:** l'adozione di norme interne per la gestione, distribuzione e il mantenimento in efficienza dei Dispositivi di Protezione Individuali. In particolare, tali norme interne prevedono:
  - le modalità per la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buon stato di conservazione ed efficienza dei DPI;
  - la tracciabilità delle attività di consegna e verifica funzionalità dei DPI (es. *check list* mirate quali elenchi dei dispositivi di protezione individuale da consegnare, condivisi con il RSPP).
- **Gestione delle emergenze:** l'adozione di norme interne per la gestione delle emergenze atta a mitigare gli effetti sulla salute della popolazione e sull'ambiente esterno. In particolare, tali norme interne prevedono:
  - l'individuazione delle misure per il controllo di situazioni di rischio in caso di emergenza;
  - l'indicazione sulle modalità di abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
  - 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;

- l'individuazione dei provvedimenti per evitare rischi per la salute della popolazione o deterioramento dell'ambiente esterno;
- l'indicazione sulle modalità e sulla tempistica/frequenza di svolgimento delle prove di emergenza.

- **Gestione del rischio incendio:** l'esistenza di norme interne che definiscano le misure necessarie per la prevenzione incendi. In particolare, tali norme interne contengono:
  - il monitoraggio delle attività da svolgersi al fine della richiesta di rilascio e rinnovo del Certificato Prevenzione Incendi;
  - le indicazioni sulle modalità di informazione ai lavoratori sulle norme di comportamento da attuarsi in caso di incendio;
  - le indicazioni sulle modalità di tenuta ed aggiornamento del registro incendio.
- **Consultazione e comunicazione:** l'adozione di un calendario che preveda riunioni periodiche di tutte le figure competenti per la verifica della situazione nella gestione delle tematiche riguardanti salute e sicurezza e di una adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.
- **Diffusione delle informazioni:** l'adozione di norme interne che disciplinino la diffusione delle informazioni relative alla salute e sicurezza, tale da garantire a tutti i livelli aziendali conoscenze utili all'identificazione, riduzione e gestione dei rischi in ambiente di lavoro. In particolare, tali norme interne disciplinano:
  - l'informativa periodica del Datore di Lavoro verso i lavoratori;
  - l'informativa al Medico Competente, laddove necessario, relativamente ai processi e rischi connessi all'attività produttiva.
- **Formazione, sensibilizzazione e competenze**: l'adozione di norme interne che regolamentino il processo di formazione. In particolare, tali norme interne definiscono:
  - le modalità di erogazione della formazione di ciascun lavoratore su: rischi dell'impresa, misure di prevenzione e protezione, rischi specifici e norme di sicurezza, caratteristiche delle sostanze pericolose (schede di sicurezza e norme di buona pratica operativa), procedure di emergenza, nominativi e ruoli del RSPP e del medico competente, laddove applicabile, istruzioni d'uso delle attrezzature di lavoro e dei dispositivi di protezione individuale;
  - i criteri di erogazione della formazione di ciascun lavoratore (es. all'assunzione, trasferimento o cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze pericolose);
  - con riferimento ai soggetti coinvolti nella gestione delle tematiche della salute e della sicurezza, l'identificazione dell'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa (Rappresentanti dei Lavoratori per la Sicurezza, Addetti al Servizio di Prevenzione e Protezione, Squadre di Emergenza e Pronto Soccorso);
  - 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).

- **Rapporti con fornitori e contrattisti – informazione e coordinamento:** l'esistenza di norme interne che definiscano:
  - le modalità e i contenuti dell'informazione che deve essere fornita alle imprese esterne riguardo l'insieme delle norme e prescrizioni che un'impresa appaltatrice aggiudicataria di un ordine deve conoscere ed impegnarsi a rispettare e a far rispettare ai propri dipendenti;
  - i ruoli, le responsabilità e le 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.
- **Rapporti con fornitori e contrattisti – qualifica:** l'adozione di norme interne che definiscano modalità di qualifica dei fornitori. In particolare, tali norme interne devono tener conto:
  - dei risultati della verifica dei requisiti tecnico-professionali degli appaltatori;
  - della rispondenza di quanto eventualmente fornito con le specifiche di acquisto e le migliori tecnologie disponibili in tema di tutela della salute e della sicurezza.
- **Rapporti con fornitori e contrattisti – clausole contrattuali:** l'esistenza di clausole contrattuali standard riguardanti i costi della sicurezza nei contratti di somministrazione, di appalto e di subappalto.
- **Gestione degli *asset*:** l'esistenza di norme interne che disciplinano le attività di manutenzione/ispezione degli asset aziendali affinché ne sia sempre garantita l'integrità ed adeguatezza. In particolare, tali norme prevedono:
  - le verifiche periodiche di adeguatezza e integrità degli *asset* e di conformità ai requisiti normativi applicabili;
  - la pianificazione, effettuazione e verifica delle attività di ispezione e manutenzione tramite personale qualificato e idoneo.

6.3.3 CONTROLLO AZIONI CORRETTIVE

L'attività di controllo e azioni correttive è volta a definire:

- la misura e il monitoraggio delle prestazioni;
- la registrazione e il monitoraggio degli infortuni, incidenti, non conformità, azioni correttive e preventive;
- le modalità di gestione delle registrazioni;
- modalità di esecuzione audit periodici.
- **Misura e il monitoraggio delle prestazioni – infortuni:** l'adozione di norme interne che indichino:
  - ruoli, responsabilità e modalità di segnalazione, rilevazione, investigazione interna degli infortuni;
  - ruoli, responsabilità e modalità di segnalazione, tracciabilità ed investigazione degli incidenti occorsi e dei «mancati incidenti»;
  - modalità di comunicazione degli infortuni/incidenti occorsi dai responsabili operativi al Datore di Lavoro competente e al responsabile del servizio di prevenzione e protezione.

- **Misura e monitoraggio delle prestazioni – altri dati (diversi da infortuni e incidenti**): l'adozione norme interne che definiscano ruoli, responsabilità e modalità di registrazione e monitoraggio (anche attraverso l'uso di indicatori) per i dati riguardanti:
  - la sorveglianza sanitaria;
  - la sicurezza degli impianti (apparecchi di sollevamento e ascensori, impianti elettrici, attrezzature a pressione, serbatoi interrati, apparecchiature laser, macchine);
  - le sostanze ed i preparati pericolosi utilizzati in azienda (schede di sicurezza).
- **Misura e monitoraggio delle prestazioni – cause/controversie:** l'esistenza di norme interne che definiscano ruoli, responsabilità e modalità di monitoraggio delle controversie/contenzioso pendenti relativi agli infortuni occorsi sui luoghi di lavoro al fine di identificare le aree a maggior rischio infortuni.
- **Attività di verifica periodica:** l'esistenza di norme interne che disciplinino ruoli, responsabilità e modalità operative riguardo le attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza. In particolare, al fine di definire:
  - la tempistica per la programmazione delle attività;
  - le competenze necessarie per il personale coinvolto nelle attività di audit nel rispetto del principio dell'indipendenza dell'auditor rispetto all'attività che deve essere verificata;
  - le modalità di individuazione e l'applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di gestione della salute e sicurezza in azienda o dalla normativa e prescrizioni applicabili;
  - le modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
  - le modalità di comunicazione dei risultati dell'audit al Vertice aziendale.
- **Reporting:** l'adozione di norme interne che disciplinino ruoli, responsabilità e modalità operative delle attività di reporting verso il Vertice. Tale report deve garantire la tracciabilità e la disponibilità dei dati relativi alle attività inerenti al sistema di gestione della sicurezza e in particolare l'invio periodico delle informazioni inerenti a:
  - scostamenti tra i risultati ottenuti e gli obiettivi programmati;
  - risultati degli audit;
  - risultati del monitoraggio della performance del sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (infortuni, altri dati);
  - spese sostenute e risultati di miglioramento raggiunti in relazione alle suddette spese.

6.3.4 RIESAME DELLA DIREZIONE

L'attività di riesame periodico della Direzione Aziendale è volta a 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.

La regolamentazione dell'attività prevede:

- **Conduzione del processo di riesame:** l'adozione di norme interne che definiscano ruoli, responsabilità e modalità di conduzione del processo di riesame effettuato dalla Direzione

Aziendale in relazione all'efficacia e all'efficienza del sistema di gestione della salute e sicurezza. Tale procedura prevede lo svolgimento delle seguenti attività:

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

7. F – AREA A RISCHIO NELL'AMBITO DEL REATO DI AUTORICICLAGGIO

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione del Reato di autoriciclaggio di cui all'art. 25-octies del D.Lgs.231/2001.

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della prevenzione del Reato di autoriciclaggio, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

AREA A RISCHIO	REATI ASSOCIABILI	ATTIVITÀ SENSIBILI
Gestione delle politiche fiscali e predisposizione delle dichiarazioni dei redditi e gestione degli adempimenti contributivi	Autoriciclaggio (art.648 ter.1 c.p.)	Gestione degli adempimenti fiscali e contributivi
Gestione della fatturazione passiva	Autoriciclaggio (art.648 ter.1 c.p.)	Registrazione delle fatture passive e delle note di credito
Gestione della contabilità e redazione del bilancio	Autoriciclaggio (art.648 ter.1 c.p.)	Gestione/custodia della contabilità generale ed effettuazione delle chiusure contabili Redazione del bilancio di esercizio
Gestione delle poste valutative	Autoriciclaggio (art.648 ter.1 c.p).	Definizione delle poste valutative

7.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEL REATO DI AUTORICICLAGGIO

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i destinatari, in relazione *al reato di autoriciclaggio*, devono attenersi, oltre alle regole di comportamento e principi generali già rilevati nell'ambito dei reati nei rapporti con la pubblica amministrazione e con soggetti privati nonché ai reati societari, a quanto di seguito previsto:

- obbligo di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, in tutte le attività finalizzate all'emissione delle fatture ed alla relativa registrazione, alla tenuta della contabilità, alla registrazione della relativa movimentazione ed alla predisposizione dei bilanci;
- assicurare che tutto il processo di gestione della contabilità aziendale sia condotto in maniera trasparente e documentabile.

nello specifico è fatto assoluto divieto di erogare prestazioni non necessarie, fatturare prestazioni non effettivamente erogate, duplicare la fatturazione per una medesima prestazione, omettere l'emissione di note di credito qualora siano state fatturate, anche per errore, prestazioni in tutto o in parte inesistenti o non finanziabili.

7.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

7.2.1 GESTIONE DELLE POLITICHE FISCALI E PREDISPOSIZIONE DELLE DICHIARAZIONI DEI REDDITI E GESTIONE DEGLI ADEMPIMENTI CONTRIBUTIVI

La regolamentazione dell'attività prevede:

- ruoli, responsabilità e modalità operative per:
  - la corretta determinazione delle imposte e dei contributi;
  - assicurare che le attività attinenti al processo fiscale e contributivo, incluse le modalità operative per la fruizione di servizi prestati da professionisti esterni, siano svolte con diligenza, professionalità, trasparenza, correttezza e nel rispetto di tutte le leggi applicabili e in coerenza con il presente Modello;
  - la tenuta di registri contabili con gli stessi criteri di ordine, sistematicità e tempestività di quelli amministrativi;
- il rispetto del principio di segregazione delle attività;
- un sistema di controlli sulle attività propedeutiche all'elaborazione delle dichiarazioni fiscali che includa l'effettuazione di verifiche complementari da parte di soggetti interni ed esterni indipendenti;
- un sistema di controlli sulle attività propedeutiche all'elaborazione dei contributi previdenziali che includa l'effettuazione di verifiche complementari da parte di soggetti interni indipendenti;
- la tracciabilità delle attività e dei documenti inerenti al processo, assicurandone l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli eseguiti che supportano le attività e la conservazione della documentazione inerente, nel rispetto dei termini di legge;
- l'utilizzo di un sistema per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- indagini e verifiche su eventuali variazioni in termini di determinazione delle imposte intercorse rispetto al periodo precedente;

- verifica della corrispondenza tra gli importi contabilizzati e gli importi determinati mediante la documentazione di calcolo delle stesse;
- preliminarmente alla trasmissione telematica della dichiarazione IVA, effettuazione di un'analisi di corrispondenza tra quanto inviato con comunicazione dati IVA e quanto deve essere inserito nella dichiarazione.

7.2.2 GESTIONE DELLA FATTURAZIONE PASSIVA

Con riferimento alla gestione della fatturazione passiva la regolamentazione dell'attività prevede:

- ruoli, responsabilità e modalità operative per:
  - l'esecuzione e la verifica di tutte le fasi di lavorazione delle fatture;
  - la verifica di completezza, correttezza e conformità delle fatture a quanto previsto dalla normativa;
  - le verifiche di coerenza tra i dati della fattura, i documenti di ciclo passivo presenti a sistema e i documenti autorizzativi per il pagamento;
- il rispetto del principio di segregazione;
- la formalizzazione del processo di budgeting, anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;
- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»);
- la gestione delle attività relative alla fatturazione passiva e ai relativi pagamenti attraverso il supporto di adeguati sistemi informativi gestionali che:
  - garantiscano la registrazione di tutte le fasi del processo che comportano la generazione di un costo;
  - consentano la verifica della corretta imputazione della fattura al conto di destinazione.

7.2.3 GESTIONE DELLA CONTABILITÀ E REDAZIONE DEL BILANCIO

Con riferimento alla Gestione della contabilità e redazione del bilancio si rinvia a quanto riportato nel presente documento nell'ambito della gestione della contabilità e redazione del bilancio.

Inoltre la regolamentazione dell'attività prevede:

- che i processi amministrativo-contabili debbano essere definiti e regolamentati nell'ambito di un modello di Governo e Controllo che garantisca la definizione dei ruoli, degli strumenti e delle modalità operative relative a tali processi e che preveda verifiche periodiche sull'attendibilità dei controlli previsti sulle principali fasi dei processi;
- che debbano essere definiti i compiti e le responsabilità nel processo di tenuta della contabilità e nella formazione del bilancio e un sistema di controllo che garantisca la correttezza e la veridicità delle informazioni e dei dati forniti e la certezza della provenienza degli stessi.

7.2.4 GESTIONE DELLE POSTE VALUTATIVE

La regolamentazione dell'attività prevede:

- le modalità operative per lo svolgimento delle attività nonché modalità di archiviazione della documentazione rilevante;
- il rispetto del principio di segregazione;
- l'utilizzo di un sistema per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- verifica, in sede di determinazione delle poste valutative, della corretta applicazione dei criteri utilizzati per la loro determinazione;
- che i fondi registrati in bilancio debbano essere:
  - basati su eventi segnalati alla struttura che si occupa di registrare le poste in contabilità, dalle strutture competenti mediante comunicazioni formali;
  - valutati, valorizzati e movimentati sulla base di criteri chiari, trasparenti e applicati con continuità, anche con l'eventuale supporto di professionisti esterni;
  - formalizzati in note informative, tracciate e archiviate, che esplicitino le analisi effettuate;
  - approvati da adeguati livelli di Management.

8. G – AREA A RISCHIO NELL'AMBITO DELLA CRIMINALITÀ ORGANIZZATA

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art. 24 ter del D.Lgs. 231/2001 (delitti di criminalità organizzata).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della prevenzione dei Reati nell'ambito della criminalità organizzata, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Approvvigionamento di beni, lavori e servizi	Associazione per delinquere (art. 416 c.p.) Tutti i delitti se commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p., per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91). Favoreggiamento personale (art. 378 c.p.)	Pianificazione e programmazione degli approvvigionamenti Processo di approvvigionamento
Conferimento di contratti di consulenza o prestazioni professionali	Associazione per delinquere (art. 416 c.p.) Tutti i delitti se commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p., per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91). Favoreggiamento personale (art. 378 c.p.)	Pianificazione e programmazione degli approvvigionamenti Processo di approvvigionamento
Transazioni finanziarie (incassi e pagamenti)	Associazione per delinquere (art. 416 c.p.) Tutti i delitti se commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p., per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91). Favoreggiamento personale (art. 378 c.p.)	Gestione degli incassi Gestione dei pagamenti

8.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI NELL'AMBITO DELLA CRIMINALITÀ ORGANIZZATA

Nell'ambito delle attività operative, i Destinatari, nell'ambito dei Reati relativi alla criminalità organizzata, devono attenersi alle seguenti regole di comportamento e principi generali:

- effettuazione di verifiche preliminari sulla effettiva titolarità del rapporto contrattuale in capo alla terza parte contraente;
- siano individuati degli indicatori di anomalia che consentano di rilevare eventuali transazioni a «rischio» o «sospette» sulla base dei seguenti elementi:
  - profilo soggettivo della controparte (es. esistenza di precedenti penali; ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose riferibili a Reati previsti dal Decreto);
  - comportamento della controparte (es. mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli);
  - dislocazione territoriale della controparte;
  - profilo economico-patrimoniale dell'operazione (es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica);
  - caratteristiche e finalità dell'operazione (es. modifiche delle condizioni contrattuali standard, finalità dell'operazione).
  - ciascuna operazione con terze parti sia soggetta al preventivo screening della controparte, volto a identificarne l'idoneità tecnica e soggettiva alle attività per le quali il rapporto contrattuale si va instaurando;
  - ciascuna operazione con parti terze avvenga sulla base di documentazione autorizzata da soggetti dotati di idonei poteri;
  - sia formalizzato il contratto che disciplini le modalità e i principi con i quali sono gestiti i rapporti con le parti terze, nonché le attività svolte per conto della controparte;
  - la documentazione riguardante ogni singola operazione sia archiviata allo scopo di garantire la completa tracciabilità documentale della stessa.

8.1.1 APPROVVIGIONAMENTO DI BENI, LAVORI E SERVIZI

La regolamentazione dell'attività prevede:

- divieto di negoziare condizioni contrattuali occulte, che non risultino da idonea documentazione conservata unitamente a quella relativa all'acquisto;
- la rotazione dei fornitori nelle forniture cicliche con offerta omogenea e diversa;

- una verifica dell'assenza di rapporti con fornitori che possono avere conflitti di interessi con dipendenti 3-i; in caso di esistenza di relazioni privilegiate[11]/conflitto di interesse tra il rappresentante di 3-i e la terza parte, l'obbligo di segnalarle;
- la verifica che le richieste di approvvigionamento arrivino da soggetti autorizzati;
- la formalizzazione e l'autorizzazione da parte di un adeguato livello gerarchico della scelta della modalità di approvvigionamento;
- la segregazione nelle principali attività;
- la formalizzazione dell'iter, relativo alle attività di approvvigionamento, a partire dalla definizione dell'esigenza fino all'autorizzazione e l'emissione di una richiesta di acquisto;
- la sussistenza della coincidenza tra la richiesta di acquisto e l'ordine di acquisto;
- le modalità per il ricevimento dei beni e la dichiarazione di accettazione del bene/servizio acquistato;
- la formalizzazione del processo di budgeting, anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;
- le modalità e i contenuti dell'informazione che devono essere forniti ai fornitori riguardo l'insieme delle norme e prescrizioni che un'impresa appaltatrice/aggiudicataria di un ordine deve conoscere;
- clausole contrattuali standard, riguardanti i costi della sicurezza e le norme vigenti in materia che i fornitori devono dichiarare di conoscere;
- l'inserimento di specifiche clausole nei contratti con cui i terzi:
  - si obbligano a non tenere alcun comportamento, non porre in essere alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. n. 231/2001;
  - dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Modello 231 adottato dalla società nonché clausole risolutive espresse che attribuiscano alla società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;
- idonei sistemi di monitoraggio e formalizzazione di report da sottoporre ad adeguato livello gerarchico per il monitoraggio della gestione degli ordini;
- la formazione specifica in materia di acquisizione beni, servizi e lavori per i dipendenti coinvolti nelle diverse fasi del processo di approvvigionamento;
- che l'archiviazione della documentazione relativa ad ogni attività di acquisto sia caratterizzata da completezza;

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

- il divieto di intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone[12] indicate nelle Liste di Riferimento[13] o facenti parte di organizzazioni presenti nelle stesse.
- nei casi di approvvigionamenti effettuati in urgenza, la definizione delle condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga;
- regole per la qualifica dei fornitori e controlli e responsabilità funzionali a garantire che la movimentazione dell'Albo Fornitori sia effettuata in presenza della documentazione prevista (es. nome cliente; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione)[14].

8.1.2 CONFERIMENTO DI CONTRATTI DI CONSULENZA O PRESTAZIONI PROFESSIONALI

La regolamentazione dell'attività prevede:

- il rispetto del principio di segregazione delle attività in fase di affidamento dell'incarico;
- la formalizzazione del processo di *budgeting* anche con riferimento alla gestione degli *extrabudget*, al fine di consentire la pianificazione e il monitoraggio dei costi e ricavi;
- le modalità per la gestione della individuazione, selezione e attribuzione dell'incarico con la definizione di criteri oggettivi, trasparenti e documentabili di assegnazione dell'incarico;
- l'esistenza di un elenco di consulenti legali e tecnici, con l'evidenza degli ambiti di eccellenza per ciascun soggetto;
- che il ricorso alla negoziazione diretta con un unico operatore economico sia adeguatamente motivato e documentato, nonché sottoposto a idonei sistemi di controllo e sistemi autorizzativi;
- il rispetto delle previsioni normative in tema di proroghe e rinnovi;
- la verifica dell'esistenza di requisiti di onorabilità/professionalità dei consulenti;

[12] Si intendono persone fisiche, persone giuridiche e persone fisiche appartenenti a organizzazioni individuate nelle Liste di Riferimento.

[13] Si tratta delle liste curate da ONU, UE e OFAC e rese disponibili sul sito web dell'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia ex art. 6 c. 1 del D.Lgs. 231/2007

[14] Tale standard di controllo è previsto al fine di garantire una piena e adeguata copertura del rischio, sebbene in 3-i non sia presente un Albo Fornitori, in quanto le acquisizioni di beni, lavori e servizi sono svolte tramite una stazione appaltante esterna.

- la formalizzazione delle motivazioni della consulenza e delle motivazioni della scelta del consulente;
- la tracciabilità e l'archiviazione di documenti giustificativi degli incarichi conferiti;
- la formale valutazione di congruità, prima di procedere al pagamento del corrispettivo, sulla base di quanto previsto contrattualmente;
- il divieto di intrattenere rapporti, negoziare e/o stipulare contratti o atti con persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse. Si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»;
- l'inserimento di specifiche clausole nei contratti con cui i terzi:
  - si obbligano a non tenere alcun comportamento, non attuare alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. 231/2001;
  - dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Modello adottato dalla 3-i nonché clausole risolutive espresse che attribuiscano alla società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;
  - garantiscano il processo di tracciabilità delle attività che svolgono per conto della società tramite apposita documentazione e relativa archiviazione;
- una verifica dell'assenza di rapporti con consulenti che possono avere conflitti di interesse con dipendenti 3-i; in caso di esistenza di relazioni privilegiate[15]/conflitto di interesse tra il rappresentante di 3-i e la terza parte, l'obbligo di segnalarle, di astenersi dalla negoziazione/gestione del contratto;
- clausole contrattuali «*standard*», riguardanti i costi della sicurezza e le norme vigenti in materia di lavoro;
- le modalità per il ricevimento e la dichiarazione di accettazione del bene/servizio acquistato;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga.

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

8.1.3 TRANSAZIONI FINANZIARIE (INCASSI E PAGAMENTI)

La regolamentazione dell'attività prevede, con riferimento ai pagamenti:

- l'attestazione dell'esecuzione della prestazione;
- la registrazione delle fatture ricevute;
- l'iter per la predisposizione e l'autorizzazione della proposta di pagamento;
- le modalità per l'effettuazione dei pagamenti;
- la formalizzazione dell'attività di riconciliazione dei conti correnti bancari;

- con riferimento agli incassi, le modalità per la registrazione e la contabilizzazione degli incassi;
- il divieto di utilizzo del contante o altro strumento finanziario al portatore, 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;
- il divieto di 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; si veda quanto riportato nella sezione «*Approvvigionamento di beni, lavori e servizi*»;
- il divieto di accettare ed eseguire ordini di pagamento provenienti da soggetti non identificabili, e dei quali non sia tracciabile il pagamento (importo, nome/denominazione, indirizzo e numero di conto corrente) o qualora non sia assicurata, la piena corrispondenza tra il nome del fornitore/cliente e l'intestazione del conto su cui far pervenire/da cui accettare il pagamento;
- che i pagamenti al beneficiario devono essere effettuati esclusivamente sul conto intestato allo stesso; non è consentito effettuare pagamenti su conti cifrati o in contanti, o a un soggetto diverso dal beneficiario né in un Paese diverso da quello del beneficiario o da quello dove la prestazione è stata eseguita;
- previsione di cd. «specimen» di firma in relazione ai livelli autorizzativi definiti per le esecuzioni di transazioni finanziarie;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»);

9. H – AREA A RISCHIO NELL'AMBITO DELLA GESTIONE DI SOFTWARE ED ALTRO MATERIALE PROTETTO DA DIRITTO D'AUTORE

Nell'ambito dell'operatività aziendale la violazione dei diritti d'autore potrebbe configurarsi nell'utilizzo di opere di ingegno senza averne l'autorizzazione, in relazione ad attività quali, ad esempio, la gestione delle licenze software, la gestione dei sistemi informativi, lo sviluppo *software* per i clienti, la gestione della comunicazione esterna mediante utilizzo di materiale soggetto a *copyright*, l'utilizzo di banche dati.

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art.25 novies del D.Lgs.231/2001 (delitti in materia di violazione del diritto d'autore).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della gestione delle licenze *software* o di altro materiale protetto dalle norme sulla proprietà intellettuale, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Gestione delle licenze SW	Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 bis l. 633/1941)	Gestione del processo di acquisto delle licenze software Inventariazione e verifica delle licenze in uso
Gestione dei sistemi informativi		Gestione di server/reti telematiche per la condivisione di opere dell'ingegno o parti di esse
Sviluppo software *per i clienti*		Sviluppo software Manutenzione evolutiva del software
Utilizzo di Banche dati	Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis l. 633/1941 comma 2)	Estrazione, reimpiego, riproduzione e distribuzione del contenuto di banche dati
Gestione della comunicazione esterna mediante utilizzo di materiale soggetto a copyright	Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, l. 633/1941 comma 1 lett. a) bis) e comma 3) (art.171 ter, l.633/1941, comma 1)	Utilizzo di immagini per la vendita di prodotti-servizi

9.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI NELLA PREVENZIONE DEI DELITTI COMMESSI IN VIOLAZIONE DELLE NORME CHE TUTELANO LA PROPRIETÀ INTELLETTUALE

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i Destinatari, in relazione ai *delitti commessi in violazione dei diritti d'autore,* devono attenersi alle seguenti regole di comportamento e principi generali:

- 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;
- l'obbligo di rispettare 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;
- a meccanismi autorizzativi per l'utilizzo, la riproduzione, l'elaborazione, la duplicazione e la distribuzione di Opere o di parti delle stesse;

- l'adozione di strumenti di protezione (es. diritti di accesso) relativi alla conservazione e all'archiviazione di Opere assicurandone l'inventariazione.

9.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

9.2.1 GESTIONE DELLE LICENZE SOFTWARE

La regolamentazione dell'attività prevede:

- la tracciabilità delle fasi principali di acquisto, definizione, verifica, dismissione delle licenze software in uso presso l'azienda;
- l'installazione delle licenze software e la definizione, da parte del responsabile del contratto, di un piano di dettaglio dell'attività di installazione che viene effettuata sulla base dell'ambiente sul quale deve essere reso disponibile il software; la definizione dell'inventario degli *asset* aziendali (incluse le basi dati in essi contenute) utilizzati ai fini dell'operatività del sistema informatico e telematico e l'adozione di politiche di conformità legale (*copyright*), ove applicabili;
- la verifica - in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento - della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo;
- nell'ambito dell'acquisizione di prodotti/opere tutelati da diritti di proprietà industriale/intellettuale la definizione, qualora applicabile, di clausole contrattuali contenenti l'impegno/attestazione (a seconda dei casi) della controparte:
  - di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni, modelli od opere tutelate dal diritto d'autore oggetto di cessione ovvero di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
  - che i diritti di utilizzo e/o di sfruttamento delle privative industriali e/o intellettuali, oggetto di cessione o di concessione in uso, non violano alcun diritto di proprietà industriale/intellettuale in capo a terzi;
  - a manlevare e tenere indenne la 3-i da qualsivoglia danno o pregiudizio dovesse derivarle per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

9.2.2 GESTIONE DEI SISTEMI INFORMATIVI (GESTIONE DI SERVER/RETI TELEMATICHE PER LA PUBBLICAZIONE DI OPERE DELL'INGEGNO O PARTI DI ESSE)

La regolamentazione dell'attività prevede:

- 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;

- con riferimento alla gestione delle comunicazioni e dell'operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni:
  - la protezione da software pericoloso;
  - il backup di informazioni e software;
  - la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
  - gli strumenti per effettuare la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
  - una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
  - il controllo sui cambiamenti agli elaboratori e ai sistemi;
  - la gestione di dispositivi rimovibili;
  - adeguate misure di sicurezza da adottare per i dispositivi che accedono da remoto ai sistemi dell'organizzazione;
  - l'adozione di controlli atti ad impedire l'utilizzo di software non consentiti;
  - attività di *assessment* o *performance test* per verificare la *capacity* della rete e delle connessioni remote;
- con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni:
  - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
  - le modalità operative di registrazione/cancellazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
  - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
  - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
  - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
  - la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
  - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
  - adeguato monitoraggio del traffico e degli accessi da remoto;

- adeguate misure di sicurezza da adottare per l'autenticazione dei dispositivi che accedono da remoto ai sistemi dell'organizzazione (es. autenticazione a due fattori);
- prevedere dei processi di *review* delle modalità di gestione degli accessi logici;

- la definizione di un inventario degli *asset* aziendali (incluse le basi dati in essi contenute) utilizzati ai fini dell'operatività del sistema informatico e telematico e l'adozione di politiche di conformità legale (*copyright*), ove applicabili;
- la verifica - in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento - della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo.

9.2.3 SVILUPPO SOFTWARE PER I CLIENTI

La regolamentazione dell'attività prevede:

- la gestione dello sviluppo *software* per i clienti con l'indicazione:
  - delle modalità di definizione dei requisiti;
  - delle modalità di gestione del processo di sviluppo;
  - la verifica formale che non sia utilizzato *software* già brevettato o licenziato da altri soggetti. In particolare, sono formalizzate le responsabilità, gli input e gli output, gli indicatori per il controllo e le varie fasi/attività proprie del processo, evidenziando le peculiarità connesse con i diversi approcci metodologici previsti;
- la tracciabilità delle fasi principali di definizione dei requisiti e delle fasi di sviluppo, test e installazione di quanto sviluppato;
- l'installazione di programmi informatici protetti e la definizione, da parte del responsabile del contratto, di un piano di dettaglio dell'attività di installazione che viene effettuata sulla base dell'ambiente sul quale deve essere reso disponibile il software.

9.2.4 UTILIZZO DI BANCHE DATI (ESTRAZIONE, REIMPIEGO, RIPRODUZIONE E DISTRIBUZIONE)

La regolamentazione dell'attività prevede:

- la gestione delle banche dati con l'indicazione:
  - delle modalità di acquisizione di banche dati;
  - delle modalità di impiego, riproduzione e distribuzione delle banche dati;
  - delle modalità di monitoraggio delle banche dati al fine di prevenirne la duplicazione anche attraverso un sistema che consente, in caso di tentata duplicazione, la segnalazione e l'individuazione dell'utente che ha tentato di eseguire l'attività e il momento del tentativo;
- la separazione dei compiti fra chi esprime il fabbisogno, chi ne analizza le esigenze e la struttura che gestisce il processo di approvvigionamento delle banche dati;
- nell'ambito dell'acquisizione di prodotti/opere tutelati da diritti di proprietà industriale/intellettuale la definizione, qualora applicabile, di clausole contrattuali contenenti l'impegno/attestazione (a seconda dei casi) della controparte:

- di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni, modelli od opere tutelate dal diritto d'autore oggetto di cessione ovvero di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
- che i diritti di utilizzo e/o di sfruttamento delle privative industriali e/o intellettuali, oggetto di cessione o di concessione in uso, non violano alcun diritto di proprietà industriale/intellettuale in capo a terzi;
- a manlevare e tenere indenne la 3-i da qualsivoglia danno o pregiudizio dovesse derivarle per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione;

- la tracciabilità delle attività di acquisto, di estrazione e di distribuzione del contenuto di una banca dati;
- la definizione di un inventario degli *asset* aziendali (incluse le basi dati in essi contenute) utilizzati ai fini dell'operatività del sistema informatico e telematico e l'adozione di politiche di conformità legale (*copyright*), ove applicabili;
- la verifica - in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento - della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo.

9.2.5 GESTIONE DELLA COMUNICAZIONE ESTERNA MEDIANTE UTILIZZO DI MATERIALE SOGGETTO A COPYRIGHT

La regolamentazione dell'attività prevede:

- le modalità di pubblicazione e aggiornamento dei contenuti del sito internet aziendale e le relative responsabilità;
- il rispetto della normativa di riferimento per il pagamento dei diritti di copyright;
- l'individuazione dei responsabili delle attività di ideazione e la realizzazione di filmati/spot istituzionali e/o informativi e di redazione/revisione e progettazione grafica di materiali promo-informativi;
- la formalizzazione di direttive che sanciscono l'obbligo del rispetto delle norme di utilizzo, distribuzione e riproduzione dei dati;
- che sia garantita l'archiviazione e conservazione dei dati, delle informazioni e del materiale utilizzato;
- nell'ambito dell'acquisizione di prodotti/opere tutelati da diritti di proprietà industriale/intellettuale, la definizione, qualora applicabile, di clausole contrattuali contenenti l'impegno/attestazione (a seconda dei casi) della controparte:
  - di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni, modelli od opere tutelate dal diritto d'autore oggetto di cessione ovvero di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
  - che i diritti di utilizzo e/o di sfruttamento delle privative industriali e/o intellettuali, oggetto di cessione o di concessione in uso, non violano alcun diritto di proprietà industriale/intellettuale in capo a terzi;

- a manlevare e tenere indenne 3-i da qualsivoglia danno o pregiudizio dovesse derivarle per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione;

- la verifica – in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento – della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo.

10. I – AREA A RISCHIO NELL'AMBITO DEI REATI AMBIENTALI

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo, l'individuazione delle cosiddette «aree a rischio», ossia di quelle aree della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei Reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di cui all'art.25 undecies del D.Lgs.231/2001 (Reati ambientali).

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della gestione della tutela ambientale, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Gestione dei rifiuti prodotti	Attività di gestione di rifiuti non autorizzata (Art. 256 del D. Lgs.152/2006) Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (Art. 258 del D.Lgs. 152/2006) (Art. 256 del D. Lgs.152/2006) Traffico illecito di rifiuti (Art. 259 del D. Lgs.152/2006) Attività organizzate per il traffico illecito di rifiuti (art.452-quaterdecies c.p.) Inquinamento ambientale (art. 452 bis c.p.) Disastro ambientale (art.452 quater c.p.) Delitti colposi contro l'ambiente (art. 452 quinquies c.p.) Circostanze aggravanti (art.452 octies c.p.)	Attività di raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, realizzazione e gestione di impianti di smaltimento o di recupero di rifiuti

10.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI AMBIENTALI

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, i Destinatari, in relazione ai *Reati ambientali*, devono attenersi, oltre alle regole di comportamento e principi generali già rilevati nell'ambito dei Reati nei rapporti con la Pubblica Amministrazione e con soggetti privati, a quanto di seguito previsto:

- ogni azione che possa avere impatto ambientale deve tendere alla riduzione al minimo dei danni reali o potenziali causabili all'ambiente;

- devono essere adottate delle misure dirette alla prevenzione della produzione e alla riduzione della nocività dei rifiuti;

- la produzione di rifiuti può essere ridotta alla fonte, privilegiando l'approvvigionamento di beni di consumo che producano la minor quantità di rifiuti al termine della vita utile;
- i rifiuti prodotti possono essere riutilizzati e riciclati, procrastinando il più possibile nel tempo la loro trasformazione in rifiuto e diminuendo la quantità complessiva del rifiuto prodotto;
- il deposito temporaneo e il successivo conferimento dei rifiuti devono essere effettuati in condizioni di sicurezza e nel rispetto della normativa vigente;
- devono essere prese tutte le precauzioni necessarie a limitare al minimo l'inquinamento dell'aria e a contenere comunque le emissioni al di sotto dei limiti fissati dalla legge;
- devono essere adottate specifiche procedure per prevenire le emergenze ambientali e per essere pronti a limitare i danni qualora le stesse dovessero verificarsi.

10.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

10.2.1 GESTIONE DEI RIFIUTI PRODOTTI

La regolamentazione dell'attività prevede:

- con riferimento alla gestione dei rifiuti prodotti:
  - il rispetto degli adempimenti previsti dalla normativa o dagli atti autorizzativi in relazione ai rifiuti prodotti;
  - la gestione della raccolta e del deposito temporaneo dei rifiuti nel luogo di produzione al fine di garantire: il rispetto dei requisiti per il deposito temporaneo e del divieto di miscelazione dei rifiuti pericolosi con i rifiuti non pericolosi e di rifiuti pericolosi che abbiano caratteristiche di pericolosità differenti;
  - la verifica iniziale e periodica del possesso delle iscrizioni/comunicazioni/ autorizzazioni previste dalla normativa per la gestione dei rifiuti da parte dei soggetti terzi a cui vengono conferiti i rifiuti prodotti (inclusa la verifica delle targhe dei mezzi);
  - la predisposizione e archiviazione della documentazione amministrativa relativa alla gestione dei rifiuti;
  - la tracciabilità di tutte le attività relative alla gestione dei rifiuti;
- con riferimento alla selezione e affidamento a terzi (per i soli casi in cui tale attività è di competenza 3-i):
  - l'identificazione delle tipologie di fornitori;
  - la qualifica iniziale e riqualifica periodica dei fornitori per la verifica del rispetto di requisiti normativi ad essi applicabili e delle loro prestazioni ambientali (es. verifica autorizzazioni per svolgimento attività di trasporto, intermediazione, recupero o smaltimento rifiuti, accreditamento dei laboratori, idoneità tecnica delle società di consulenza, disponibilità di mezzi da parte delle società di manutenzione);

- la definizione di specifiche tecniche e clausole contrattuali riguardanti le questioni relative al rispetto delle norme in materia di tutela ambientale applicabili e all'attribuzione di responsabilità in materia ambientale (es. responsabilità in materia di gestione dei rifiuti e definizione del ruolo di produttore, obblighi in caso di eventi contaminanti, obbligo di informativa alla Committente, titolarità di eventuali autorizzazioni necessarie allo svolgimento dell'attività affidata);
- la tracciabilità di tutte le attività relative al processo di selezione e affidamento a terzi di attività rilevanti;

- con riferimento al monitoraggio delle prestazioni dei fornitori:
  - il monitoraggio sull'operatività dei fornitori;
  - la verifica della permanenza della validità di requisiti specifici necessari per lo svolgimento delle attività (es. accreditamenti, certificazioni, autorizzazioni);
  - la tracciabilità di tutte le attività relative al processo di monitoraggio delle prestazioni dei fornitori.

11. L – AREA A RISCHIO NELL'AMBITO DEI REATI DI RAZZISMO E XENOFOBIA

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione dei Reati di razzismo e xenofobia di cui all'art. 25-terdecies del D.Lgs.231/2001.

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della prevenzione dei Reati di razzismo e xenofobia, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Eventi e sponsorizzazioni	Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 604 bis c.p.)	Gestione del logo aziendale Gestione della comunicazione

11.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI DI RAZZISMO E XENOFOBIA

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, per i Destinatari è previsto l'espresso divieto di commettere o adottare una condotta che accetti consapevolmente il rischio che possano essere commessi delitti di razzismo e xenofobia quali:

- fare propaganda di qualsiasi idea fondata sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;
- istigare a commettere o commettere violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi;
- partecipare a organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, o prestare assistenza alla loro attività;

- promuovere o dirigere tali organizzazioni, associazioni, movimenti o gruppi;
- diffondere tramite piattaforme digitali (es. *social network*) contenuti che promuovano ovvero incitino alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, nonché neghino o minimizzino l'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

11.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

11.2.1 EVENTI E SPONSORIZZAZIONI

La regolamentazione dell'attività prevede:

- l'esecuzione di verifiche preventive sul promotore e\o sulle iniziative oggetto di sponsorizzazione al fine di verificare che gli stessi non siano contrari ai principi etici (es. incitamento alla discriminazione per motivi razziali);
- la verifica preliminare dei contenuti da utilizzare per eventi, da pubblicare su *social network*, sito internet istituzionale o su altre piattaforme della società al fine di prevenire l'insorgere di situazioni pregiudizievoli per la società;
- con riferimento alla gestione di eventi:
  - l'esistenza di un *budget* per l'organizzazione degli eventi, approvato e monitorato;
  - definizione, aggiornamento periodico e approvazione, da parte di soggetti di adeguato livello gerarchico, di un piano degli eventi;
  - definizione, formalizzazione e comunicazione dei criteri per l'individuazione degli eventi.

12. M – AREA A RISCHIO NELL'AMBITO DELLA GESTIONE DEGLI ADEMPIMENTI TRIBUTARI

Le analisi svolte hanno permesso di individuare le attività della società rappresentate nella successiva tabella, con riferimento al rischio di commissione di Reati tributari di cui all'art. 25 - quinquiesdecies del D.Lgs.231/2001.

In via preventiva e al fine di garantire l'irreprensibilità della condotta dei Destinatari, nell'ambito della prevenzione dei Reati tributari, è fatto espresso obbligo di prendere debita cognizione e seguire le procedure interne a prevenzione dei rischi/Reato.

Area a rischio	Reati associabili	Attività sensibili
Approvvigionamento di beni, lavori e servizi	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000) Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000) Occultamento o distruzione documenti contabili (art. 10 D.Lgs. 74/2000)	Processo di Approvvigionamento Gestione Contrattuale Gestione anagrafica fornitori

Area a rischio	Reati associabili	Attività sensibili
Conferimento di contratti di consulenza o prestazioni professionali	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D. Lgs. 74/2000) Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs 74/2000)	Processo di Approvvigionamento Gestione Contrattuale
Erogazioni liberali	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D. Lgs. 74/2000)	Erogazioni liberali
Gestione dei rimborsi spese	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D.Lgs. 74/2000) Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)	Rimborsi spese
Gestione della fatturazione passiva	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D. Lgs. 74/2000) Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)	Registrazione delle fatture passive e delle note di credito
Gestione della fatturazione attiva	Emissione di fatture o altri documenti per operazioni inesistenti (art 8 D. Lgs. 74/2000)	Emissione e registrazione delle fatture attive / note di debito
Transazioni finanziarie (incassi e pagamenti)	Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000) Sottrazione fraudolenta al pagamento delle imposte (art 11 - D.lgs. 74/2000)	Gestione degli incassi Gestione dei pagamenti
Gestione della contabilità e redazione del bilancio	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D. Lgs. 74/2000)	Gestione della contabilità e redazione del bilancio
Gestione delle poste valutative	Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)	Definizione delle poste valutative
Gestione delle politiche fiscali e predisposizione delle dichiarazioni dei redditi e gestione degli adempimenti contributivi	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2 D. Lgs. 74/2000) Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)	Gestione degli adempimenti fiscali e contributivi
Operazioni societarie che possono incidere sul capitale	Sottrazione fraudolenta al pagamento delle imposte (art 11 - D.lgs. 74/2000)	Gestione delle operazioni societarie straordinarie che possono incidere sul capitale

12.1 REGOLE DI COMPORTAMENTO E PRINCIPI GENERALI APPLICABILI PER LA PREVENZIONE DEI REATI TRIBUTARI

Nelle attività lavorative e nell'espletamento di tutte le relative operazioni, per i Destinatari è previsto l'espresso divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione nella contabilità separata di dati falsi, lacunosi o, comunque, non rispondenti alla realtà;

- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società, anche ai fini della contabilità separata;
- restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- adottare comportamenti a rischio aventi per oggetto o per scopo di non adempiere agli obblighi fiscali previsti dalle normative applicabili.

12.2 STANDARD DI CONTROLLO SPECIFICI

Fermo restando quanto definito dalle procedure che verranno definite ed adottate da 3-i, qui di seguito si riporta l'elenco degli standard di controllo specifici ai fini della gestione dell'area a rischio identificata.

12.2.1 APPROVVIGIONAMENTO DI BENI, LAVORI E SERVIZI

La regolamentazione dell'attività prevede:

- regole per la qualifica dei fornitori e controlli e responsabilità funzionali a garantire che la movimentazione dell'Albo Fornitori sia effettuata in presenza della documentazione prevista (es. nome cliente; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione)[16];
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga;
- che il ricorso alla negoziazione diretta con un unico operatore economico sia adeguatamente motivato e documentato, nonché sottoposto a idonei sistemi di controllo e sistemi autorizzativi;
- nei casi di approvvigionamenti effettuati in urgenza, la definizione delle condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- le modalità per il ricevimento e la dichiarazione di accettazione del bene/servizio acquistato; eventuali disallineamenti devono essere opportunamente gestiti al fine di garantire la correttezza degli importi registrati (anche mediante stanziamenti a note di credito da ricevere) e successivamente fatturati/pagati. Nel caso di prestazioni professionali e consulenze, deve essere effettuata una formale valutazione di congruità, prima di procedere al pagamento del corrispettivo, sulla base di quanto previsto contrattualmente, dal soggetto che ha usufruito della

[16] Tale standard di controllo è previsto al fine di garantire una piena e adeguata copertura del rischio, sebbene in 3-i non sia presente un Albo Fornitori, in quanto le acquisizioni di beni, lavori e servizi sono svolte tramite una stazione appaltante esterna.

consulenza/prestazione professionale con riferimento alle prestazioni ricevute che devono essere adeguatamente documentate;

- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati.

12.2.2 CONFERIMENTO DI CONTRATTI DI CONSULENZA O PRESTAZIONI PROFESSIONALI

La regolamentazione dell'attività prevede:

- regole per la qualifica dei fornitori e controlli e responsabilità funzionali a garantire che la movimentazione dell'Albo Fornitori sia effettuata in presenza della documentazione prevista;
- una verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità non abbiano sede o residenza in «paradisi fiscali» così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE). Adozione di modalità di escalation autorizzativa in caso di deroga;
- che il ricorso alla negoziazione diretta con un unico operatore economico sia adeguatamente motivato e documentato, nonché sottoposto a idonei sistemi di controllo e sistemi autorizzativi;
- nei casi di approvvigionamenti effettuati in urgenza, la definizione delle condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura;
- utilizzo di format contrattuali che prevedono, tra l'altro, il divieto per i fornitori di beni e servizi/consulenti a cui è stato attribuito l'incarico, di conferire procura all'incasso nonché - ai fini della liquidazione/pagamento delle fatture - l'applicazione del principio di domiciliazione bancaria esclusivamente nel Paese di residenza/sede legale del fornitore di beni e servizi, a seconda che sia persona fisica o giuridica, salvo specifica richiesta da parte del fornitore stesso di domiciliazione bancaria in altro Paese;
- le modalità per il ricevimento e la dichiarazione di accettazione del bene/servizio acquistato; eventuali disallineamenti devono essere opportunamente gestiti al fine di garantire la correttezza degli importi registrati (anche mediante stanziamenti a note di credito da ricevere) e successivamente fatturati/pagati. Nel caso di prestazioni professionali e consulenze, deve essere effettuata una formale valutazione di congruità, prima di procedere al pagamento del corrispettivo, sulla base di quanto previsto contrattualmente, dal soggetto che ha usufruito della consulenza/prestazione professionale con riferimento alle prestazioni ricevute che devono essere adeguatamente documentate;
- le modalità per la gestione della individuazione, selezione e attribuzione dell'incarico a consulenti e collaboratori che svolgono prestazioni professionali a favore della società con la definizione di criteri oggettivi, trasparenti e documentabili di assegnazione dell'incarico e laddove possibile la comparazione tra diversi offerenti;
- la formalizzazione delle motivazioni della consulenza e delle motivazioni della scelta del consulente.

12.2.3 EROGAZIONI LIBERALI

La regolamentazione dell'attività prevede:

- che la concessione di contributi e/o la devoluzione a titolo gratuito di Hardware e Software dismessi deve essere effettuata solo in favore di enti/associazioni/ fondazioni i cui requisiti sono predeterminati e che svolgono la loro attività in settori predefiniti;
- con riferimento alle liberalità, previsione e diffusione di regole per:
  - definizione e approvazione di un piano annuale dei progetti di liberalità e iniziativa non profit e relativa previsione di impegno economico (*budget*);
  - definizione di modalità e i criteri per erogare una liberalità e/o iniziativa non profit;
  - elaborazione/acquisizione di un resoconto sull'utilizzo delle donazioni/erogazioni effettuate e/o sull'esito della gestione delle iniziative non profit.

12.2.4 GESTIONE DEI RIMBORSI SPESE

La regolamentazione dell'attività prevede:

- il controllo di merito, la completezza e accuratezza dei giustificativi a supporto dei rimborsi spese, da parte della struttura aziendale preposta;
- la tipologia delle spese sostenibili e i limiti massimi delle spese.

12.2.5 GESTIONE DELLA FATTURAZIONE PASSIVA

La regolamentazione dell'attività prevede:

- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»);
- la gestione delle attività relative alla fatturazione passiva e ai relativi pagamenti attraverso il supporto di adeguati sistemi informativi gestionali che:
  - garantiscano la registrazione di tutte le fasi del processo che comportano la generazione di un costo;
  - consentano la verifica della corretta imputazione della fattura al conto di destinazione.

12.2.6 GESTIONE DELLA FATTURAZIONE ATTIVA

La regolamentazione dell'attività prevede:

- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»);
- la definizione, formalizzazione e diffusione di criteri, limiti e modalità predefiniti funzionali alla registrazione/emissione delle note di credito/debito;

- che non è consentita l'emissione di fatture attive:
  - in assenza della documentazione attestante l'avvenuta erogazione del servizio /bene;
  - in assenza di corrispondenza di quanto fatturare rispetto a quanto previsto contrattualmente;
  - in presenza di una duplice registrazione di documenti contabili emessi dal medesimo fornitore/cliente nello stesso esercizio;
- che è garantita nell'ambito dell'emissione delle fatture attive:
  - la corretta indicazione del fornitore, del numero e della data fattura;
  - che sia riportata la corretta descrizione dell'IVA applicata/applicabile;
  - la correttezza del conteggio inerente all'applicazione della ritenuta d'acconto;
  - che i dati inerenti alle fatture attive siano accuratamente trasferiti nel libro giornale, nel partitario clienti e nel registro IVA vendite.

12.2.7 TRANSAZIONI FINANZIARIE (INCASSI E PAGAMENTI)

La regolamentazione dell'attività prevede:

- le modalità per il ricevimento e la dichiarazione di accettazione del bene/servizio acquistato; eventuali disallineamenti devono essere opportunamente gestiti al fine di garantire la correttezza degli importi registrati (anche mediante stanziamenti a note di credito da ricevere) e successivamente fatturati/pagati. Nel caso di prestazioni professionali e consulenze, deve essere effettuata una formale valutazione di congruità, prima di procedere al pagamento del corrispettivo, sulla base di quanto previsto contrattualmente, dal soggetto che ha usufruito della consulenza/prestazione professionale con riferimento alle prestazioni ricevute che devono essere adeguatamente documentate;
- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- una verifica della completezza e accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi e lavori ricevuti/prestati/collaudati (cd. «*three way match*»);
- le modalità per la registrazione e la contabilizzazione degli incassi;
- alimentazione di un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi residenti nei sistemi informativi;
- previsione di cd. «*specimen*» di firma in relazione ai livelli autorizzativi definiti per le esecuzioni di transazioni finanziarie;
- che gli Ordini di Acquisto e/o i Contratti prevedano una chiara descrizione del bene, servizio o prestazione professionale oggetto del contratto e delle modalità di certificazione dell'avvenuta prestazione;
- con riferimento ai pagamenti:
  - l'attestazione dell'esecuzione della prestazione;

- i controlli e le modalità di registrazione delle fatture ricevute;
- l'iter per la predisposizione e l'autorizzazione della proposta di pagamento;
- le modalità per l'effettuazione dei pagamenti;
- la formalizzazione dell'attività di riconciliazione dei conti correnti bancari per causale di uscita; le eventuali poste in riconciliazione sono giustificate e tracciate con la documentazione di supporto;

- i pagamenti al beneficiario devono essere effettuati esclusivamente sul conto intestato allo stesso; non è consentito effettuare pagamenti su conti cifrati o in contanti, o a un soggetto diverso dal beneficiario né in un Paese diverso da quello del beneficiario o da quello dove la prestazione è stata eseguita;

12.2.8 GESTIONE DELLA CONTABILITÀ E REDAZIONE DEL BILANCIO

La regolamentazione dell'attività prevede:

- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- con riferimento alla contabilizzazione di *asset* alienati/ceduti/radiati:
  - definizione e diffusione di regole formalizzate che prevedano il coinvolgimento degli opportuni livelli di Management e di procuratori abilitati;
  - definizione preventiva dei driver funzionali alla determinazione del valore contabile residuo dell'*asset*;
- la formalizzazione e la diffusione, al personale coinvolto in attività di predisposizione del bilancio, di norme che definiscano con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio civilistico e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente integrate/aggiornate dalle indicazioni fornite dall'ufficio competente sulla base delle novità in termini di normativa civilistica e diffuse ai destinatari sopra indicati;
- la formalizzazione di istruzioni con cui si stabilisca quali dati e notizie debbano essere forniti per le attività di «amministrazione e controllo» in relazione alle chiusure annuali, con quali modalità e la relativa tempistica;
- che il sistema utilizzato per la gestione della contabilità debba essere strutturato in modo che le eventuali modifiche ai dati contabili siano effettuate solo dagli utenti autorizzati mediante profilatura a sistema, nei tempi consentiti e venga mantenuta traccia delle modifiche effettuate. A valle della chiusura del periodo contabile a sistema le modifiche devono essere consentite solo ai «superutenti» opportunamente autorizzati;
- trascrizione, pubblicazione e archiviazione dei verbali di assemblea.

12.2.9 GESTIONE DELLE POSTE VALUTATIVE

La regolamentazione dell'attività prevede:

- l'utilizzo di un sistema (anche informatico) per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- che i fondi registrati in bilancio debbano essere:
  - basati su eventi segnalati alla struttura che si occupa di registrare le poste in contabilità, dalle strutture competenti mediante comunicazioni formali;
  - valutati, valorizzati e movimentati sulla base di criteri chiari, trasparenti e applicati con continuità, anche con l'eventuale supporto di professionisti esterni;
  - formalizzati in note informative, tracciate e archiviate, che esplicitino le analisi effettuate;
  - approvati da adeguati livelli di Management;
- verifica, in sede di determinazione delle poste valutative, della corretta applicazione dei criteri utilizzati per loro determinazione.

12.2.10 GESTIONE DELLE POLITICHE FISCALI E PREDISPOSIZIONE DELLE DICHIARAZIONI DEI REDDITI E GESTIONE DEGLI ADEMPIMENTI CONTRIBUTIVI

La regolamentazione dell'attività prevede:

- l'utilizzo di un sistema per la trasmissione di dati e informazioni per la gestione degli accessi, che consenta la tracciatura dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e la rilevazione degli accessi non autorizzati;
- un sistema di controlli sulle attività propedeutiche all'elaborazione delle dichiarazioni fiscali che includa l'effettuazione di verifiche complementari da parte di soggetti interni ed esterni indipendenti;
- indagini e verifiche su eventuali variazioni in termini di determinazione delle imposte intercorse rispetto al periodo precedente;
- verifica della corrispondenza tra gli importi contabilizzati e gli importi determinati mediante la documentazione di calcolo delle stesse;
- preliminarmente alla trasmissione telematica della dichiarazione IVA, effettuazione di un'analisi di corrispondenza tra quanto inviato con comunicazione dati IVA e quanto deve essere inserito nella dichiarazione.

12.2.11 OPERAZIONI SOCIETARIE CHE POSSONO INCIDERE SUL CAPITALE

La regolamentazione dell'attività prevede:

- che tutte le operazioni sui conferimenti, sugli utili e sulle riserve, le operazioni sul capitale sociale, nonché l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni debbano essere effettuate nel rispetto delle norme di legge applicabili;
- la formalizzazione di ruoli, responsabilità e modalità di predisposizione di documenti alla base di delibere del Consiglio di Amministrazione su operazioni che possono incidere sul capitale;
- regole di gestione delle operazioni di valutazione, autorizzazione e gestione delle operazioni sul capitale e l'archiviazione degli atti di delibera e relativi documenti a supporto predisposti;

- che, qualora tali operazioni richiedessero il coinvolgimento dei responsabili delle unzioni organizzative della società (ad es. stime, perizie, proposte, valutazioni programmi, etc.), dovrà essere previsto il tracciamento e il controllo delle specifiche attività svolte;
- un parere obbligatorio da parte del responsabile della Direzione competente per le attività di «amministrazione e controllo» e del Responsabile Legale sulle operazioni sul capitale sociale;
- nel caso di operazioni straordinarie, la società ha definito un processo di valutazione dell'identità della controparte con cui viene effettuata l'operazione, al fine di identificare eventuali portatori interni di interesse all'operazione e/o legami con soci/amministratori;
- nel caso di operazioni straordinarie la società predispone uno studio di fattibilità preliminare che tenga in considerazione:
  - i dati e i requisiti di base dell'operazione;
  - gli aspetti e i potenziali impatti da considerare;
  - i riflessi fiscali dell'operazione e l'eventuale necessità di pareri indipendenti (*legal opinion*, *fiscal opinion*, ecc.).

12.2.12 GESTIONE DELLE SPESE DI RAPPRESENTANZA E DEI BENI DI RAPPRESENTANZA

La regolamentazione dell'attività prevede:

- l'esistenza di un *budget* per le spese di rappresentanza e per i beni di rappresentanza approvato e monitorato nel tempo con l'individuazione di un soggetto responsabile di verificare il rispetto del margine di spesa stabilito nel budget;
- con riferimento alle spese di rappresentanza, definizione dei criteri e delle modalità per il loro sostenimento, in particolare:
  - tipologie di spese che possono essere erogate a titolo di rappresentanza;
  - soggetti aziendali abilitati a sostenere tali spese;
  - livelli di autorizzazione per il sostenimento e relativo rimborso delle spese effettuate;
- istituzione e conservazione, presso il soggetto aziendale abilitato, di un registro delle spese di rappresentanza;
- con riferimento alla gestione dei beni di rappresentanza (omaggi), diffusione di regole per la:
  - identificazione dei soggetti aziendali titolati a rilasciare omaggi (richiedente) e provvedere alla fornitura (acquirente);
  - definizione delle tipologie di spese ammesse e dei relativi criteri e limiti;
  - sistemi di tracciabilità degli omaggi e della società/persona che ha effettuato tale offerta o fornito tale omaggio ed eventuali soglie di valore.