MODELLO DI ORGANIZZAZIONE E GESTIONE
AI SENSI DEL
DECRETO LEGISLATIVO 231/2001

PARTE GENERALE

INDICE

1. PREMESSA

1.1 SCOPO DEL DOCUMENTO

La presente **Parte Generale** del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001 ("**Modello**" o "**MOG 231**") ha lo scopo di:

- illustrare il quadro normativo di riferimento e la logica complessiva della responsabilità amministrativa degli enti;
- definire i principi generali, l'impostazione metodologica e l'architettura del sistema di prevenzione;
- descrivere le regole trasversali relative a governance, attribuzione poteri, OdV, sistema disciplinare, formazione e comunicazione, whistleblowing, gestione terze parti, aggiornamento e miglioramento continuo;
- fungere da base comune per la Parte Speciale e per gli allegati operativi (procedure, policy, modulistica e registrazioni).

1.2 CAMPO DI APPLICAZIONE

Il Modello si applica:

- a tutte le attività svolte da LINGOTTO S.r.l. e a tutti i processi aziendali, inclusi quelli "strumentali" (amministrazione e finanza, IT/privacy, gestione terze parti, ecc.);
- ai destinatari indicati al successivo paragrafo 1.3, nei limiti di competenza e per quanto connesso alle attività svolte "per", "nell'interesse di" o "con" la Società.

1.3 DESTINATARI

Sono destinatari del Modello:

- amministratori, soggetti apicali e titolari di poteri di rappresentanza, amministrazione o direzione;
- dipendenti e collaboratori (a qualunque titolo);

- terze parti (fornitori, consulenti, trasportatori, partner, clienti), nella misura in cui operino con/per la Società, con vincoli contrattuali e regole di condotta.

Tutti i destinatari sono tenuti:

- a conoscere e rispettare le prescrizioni applicabili;
- a collaborare con l'OdV (riscontri, documenti, informazioni);
- a segnalare violazioni o anomalie tramite i canali previsti.

1.4 Finalità del Modello ex D.Lgs. 231/2001

LINGOTTO S.r.l. adotta il Modello al fine di:

- prevenire, per quanto ragionevolmente possibile, la commissione di reati-presupposto nell'interesse o vantaggio della Società;
- strutturare un sistema di controllo interno coerente con la realtà organizzativa e le attività svolte;
- promuovere cultura di legalità, correttezza, trasparenza, tracciabilità e responsabilizzazione.

1.5 Struttura del Modello

Il Modello è composto da:

- **Parte Generale** (presente documento): principi, regole e presidi trasversali;
- **Parte Speciale**: descrizione delle attività sensibili, dei protocolli e dei controlli specifici, con le relative evidenze e flussi;
- **Allegati**: organigrammi, deleghe/procure, procedure e policy, modulistica e registrazioni, regolamento OdV, matrice flussi, action plan e ogni documento operativo richiamato.

1.6 Principi generali del sistema di controllo interno

In coerenza con l'impostazione manualistica, il sistema di prevenzione si fonda su:

1. **separazione dei ruoli** (chi autorizza ≠ chi esegue ≠ chi controlla ≠ chi registra);
2. **tracciabilità** delle attività e delle decisioni (documenti e registrazioni che consentono la ricostruzione ex post);

3. **oggettivazione** dei processi decisionali tramite criteri, regole e controlli predefiniti.

1.7 Approccio per processi e logica PDCA (Plan–Do–Check–Act)

Il Modello è concepito come sistema dinamico di prevenzione, gestito secondo ciclo **PDCA**:

- **PLAN**: mappatura processi, individuazione attività sensibili, definizione protocolli e controlli;
- **DO**: attuazione del sistema (procedure, deleghe/procure, formazione, comunicazione);
- **CHECK**: verifiche, audit e controlli (con ruolo centrale dell'OdV);
- **ACT**: aggiornamento e miglioramento continuo (azioni correttive/preventive, revisioni, riesami).

1.8 Integrazione con policy, procedure e sistemi di gestione

Il Modello 231:

- valorizza e coordina le procedure e policy già esistenti (amministrativo-contabile, riconciliazioni, sicurezza, segnalazioni, privacy/GDPR, regole omaggi, politica aziendale);
- garantisce coerenza tra presidi operativi e requisiti 231 (mappatura, protocolli, controlli finanziari, flussi all'OdV, sistema disciplinare, formazione, aggiornamento);
- favorisce un quadro unitario di compliance e controllo, verificabile tramite evidenze.

1.9 Principio di tolleranza zero e divieti fondamentali

È vietato:

- porre in essere o agevolare condotte illecite o tentare di eludere i controlli del Modello;
- alterare, falsificare, occultare o distruggere documenti, registrazioni o evidenze;
- ostacolare le attività dell'OdV o omettere informazioni dovute;
- adottare ritorsioni o condotte discriminatorie verso chi segnala in buona fede.

1.10 DEFINIZIONI, ACRONIMI E TERMINI ESSENZIALI

1.10.1 Definizioni generali

- Azione correttiva (AC): intervento per eliminare la causa di una non conformità rilevata o di altra situazione indesiderabile e prevenire il ripetersi dell'evento.
- Azione preventiva (AP): intervento per eliminare la causa di una possibile non conformità o rischio e prevenirne l'insorgenza.
- Attività sensibili: attività/aree/processi nel cui ambito possono essere commessi reati-presupposto; saranno individuate e dettagliate nella Parte Speciale.
- Audit/Verifica: attività di controllo (documentale e/o in campo) volta a valutare l'effettiva applicazione del Modello e la conformità a procedure/protocolli.
- Beneficiario effettivo (BE): persona fisica che possiede o controlla un'entità ovvero ne risulta titolare effettivo (definizione di matrice AML; rilevante in due diligence).
- Codice Etico / Codice di comportamento: documento che stabilisce principi e regole di condotta; può essere integrato nella politica aziendale o in specifiche policy.
- Compliance: insieme di attività finalizzate ad assicurare conformità a norme, regolamenti, standard e procedure interne.
- Controlli di linea (1° livello): controlli svolti all'interno del processo da chi lo esegue/gestisce, secondo responsabilità assegnate.
- Controlli di secondo livello (2° livello): controlli svolti da funzione diversa da chi esegue (es. verifica incrociata, riconciliazioni, riesami).
- Controlli di terzo livello (3° livello): controlli indipendenti (es. OdV, revisore, audit esterni).
- Deleghe: attribuzioni formali di funzioni e poteri (anche con autonomia di spesa), conferite per iscritto a soggetti competenti.
- Evidenze/Registrazioni: documenti o registri che dimostrano l'esecuzione di un'attività o di un controllo (audit trail).
- Flussi informativi: comunicazioni periodiche e straordinarie verso OdV/Organo amministrativo su fatti rilevanti per il Modello.

- **Gap analysis (AS IS / TO BE)**: confronto tra presidi esistenti ("AS IS") e requisiti/assetto atteso ("TO BE") per definire azioni di miglioramento.
- **Gestione documentale**: sistema di versioning, distribuzione controllata, archiviazione e conservazione dei documenti del Modello.
- **Illecito amministrativo dipendente da reato**: illecito dell'ente ai sensi del D.Lgs. 231/2001, fondato sulla commissione di un reato-presupposto.
- **Interesse/Vantaggio**: criterio di imputazione ex art. 5 D.Lgs. 231/2001; l'ente risponde se il reato è commesso nel suo interesse o vantaggio.
- **Matrice flussi**: tabella che definisce fonte, contenuto, frequenza, destinatario, evidenza e modalità di trasmissione dei flussi verso l'OdV.
- **Mappa processi**: rappresentazione dei processi aziendali (core e strumentali), base per individuare attività sensibili.
- **Modello / MOG 231**: sistema organizzativo, gestionale e di controllo adottato ai sensi degli artt. 6 e 7 D.Lgs. 231/2001.
- **Non Conformità (NC)**: mancato rispetto di un requisito del Modello (normativo o interno), di una procedura o di un protocollo.
- **Organo amministrativo**: organo titolare della gestione e rappresentanza dell'ente (amministratore unico, CdA, amministratori disgiunti, ecc.).
- **Organismo di Vigilanza (OdV)**: organismo dotato di autonomi poteri di iniziativa e controllo, incaricato di vigilare sul Modello e curarne l'aggiornamento.
- **Parte Generale**: sezione del Modello con principi generali, governance, OdV, disciplinare, formazione, whistleblowing, terze parti, aggiornamento.
- **Parte Speciale**: sezione del Modello dedicata alle attività sensibili e ai protocolli specifici per prevenire i reati rilevanti.
- **PDCA**: ciclo Plan–Do–Check–Act per la gestione e il miglioramento continuo del sistema di prevenzione.

- **Policy**: documento interno che definisce principi e regole operative su uno specifico ambito (es. omaggi, privacy, sicurezza, terze parti).
- **Presidio/Controllo**: misura organizzativa, procedurale o tecnica che riduce il rischio di reato (preventiva o detective).
- **Procedura**: insieme formalizzato di regole operative, responsabilità e controlli che disciplinano un processo.
- **Procura**: atto con cui si conferisce il potere di rappresentanza verso terzi (con limiti e condizioni).
- **Protocollo 231**: regola/insieme di controlli specifici che presidiano un'attività sensibile ai fini 231.
- **Reato-presupposto**: fattispecie di reato che può determinare la responsabilità dell'ente se commessa nel suo interesse/vantaggio.
- **Riesame della Direzione**: valutazione periodica dell'adeguatezza/efficacia del sistema e definizione di miglioramenti (logica PDCA).
- **Risk assessment 231**: attività di identificazione e valutazione dei rischi-reato, base per protocolli e controlli.
- **Segnalazione**: comunicazione di violazioni o sospetti di violazione del Modello, norme o procedure.
- **Sistema disciplinare**: insieme di misure e sanzioni per violazioni del Modello (requisito essenziale ex artt. 6–7 D.Lgs. 231/2001).
- **Soggetti apicali / sottoposti**: categorie ex art. 5 D.Lgs. 231/2001 (apicali: rappresentanza/gestione/direzione; sottoposti: diretti/vigilati).
- **Terze parti**: soggetti esterni che operano con/per la Società (fornitori, consulenti, trasportatori, partner, clienti).
- **Whistleblowing**: sistema di segnalazione e tutela del segnalante disciplinato dal D.Lgs. 24/2023 e integrato nel Modello.

1.10.2 Acronimi normativi e di sistema (principali)

- 231 / D.Lgs. 231/2001: Decreto legislativo 8 giugno 2001, n. 231.
- AML/CFT: Anti-Money Laundering / Counter Financing of Terrorism (antiriciclaggio e contrasto finanziamento del terrorismo).
- CCNL: Contratto Collettivo Nazionale di Lavoro.
- CdA: Consiglio di Amministrazione (ove applicabile).
- CoC: Chain of Custody (catena di custodia; standard di tracciabilità).
- COP: Code of Practices (standard RJC).
- DPI: Dispositivi di Protezione Individuale.
- DPO: Data Protection Officer (Responsabile della Protezione dei Dati), ove nominato.
- DVR: Documento di Valutazione dei Rischi (D.Lgs. 81/2008).
- GDPR: Regolamento (UE) 2016/679.
- ISO: International Organization for Standardization (standard ISO 9001/14001/45001, ecc.).
- IT: Information Technology.
- KPI: Key Performance Indicator (indicatore chiave di prestazione/monitoraggio).
- NC: Non Conformità.
- OAM: Organismo Agenti e Mediatori (rilevante per registri di settore ove applicabile).
- OdV: Organismo di Vigilanza.
- PA: Pubblica Amministrazione.
- PEC: Posta Elettronica Certificata.
- RJC: Responsible Jewellery Council.
- SA8000: standard su responsabilità sociale.
- SG: Sistema di Gestione.
- SGRA / SG231: Sistema di Gestione per la Responsabilità Amministrativa (modello “manuale”).
- SSL: Salute e Sicurezza sul Lavoro.
- Titolare (privacy): soggetto che determina finalità e mezzi del trattamento (GDPR).
- Responsabile (privacy): soggetto che tratta dati per conto del titolare (GDPR).

- AUA: Autorizzazione Unica Ambientale.
- CER/EER: Codici Europei dei Rifiuti / Elenco Europeo dei Rifiuti.
- DDT: Documento di Trasporto.
- INPS: Istituto Nazionale della Previdenza Sociale.
- INAIL: Istituto Nazionale Assicurazione Infortuni sul Lavoro.
- PS / TULPS: Pubblica Sicurezza / Testo Unico delle Leggi di Pubblica Sicurezza.
- Albo Gestori Ambientali: Albo Nazionale Gestori Ambientali.

1.11 GESTIONE DOCUMENTALE (VERSIONI, REVISIONI, DISTRIBUZIONE CONTROLLATA)

La Società assicura:

- controllo delle revisioni (storia revisioni, data, motivazione aggiornamento);
- distribuzione controllata ai destinatari interni e accessibilità per le terze parti limitatamente alle sezioni pertinenti;
- archiviazione ordinata (cartacea e/o digitale), con conservazione delle evidenze e tracciabilità delle modifiche (versioning);
- coerenza tra Modello, procedure, policy e registrazioni (allineamento documentale e aggiornamento coordinato).

2. IL QUADRO NORMATIVO (D.lgs. 231/2001)

2.1 OGGETTO, AMBITO SOGGETTIVO E NATURA DELL'ILLECITO (ARTT. 1–2)

Il D.lgs. 8 giugno 2001 n. 231 disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.

L'ambito soggettivo comprende, in via generale, enti forniti di personalità giuridica e società/associazioni anche prive di personalità giuridica, con le esclusioni previste dalla norma (Stato, enti pubblici territoriali, enti pubblici non economici e altri soggetti pubblici indicati dalla disposizione).

La responsabilità prevista dal decreto è qualificata come amministrativa, ma ha un impianto para-penalistico: presuppone un reato-presupposto commesso da una persona fisica, è accertata con regole processuali speciali e comporta un sistema sanzionatorio che include misure interdittive, confisca e pubblicazione della sentenza (cfr. *infra*).

Principio di autonomia: la responsabilità dell'ente è autonoma rispetto a quella della persona fisica (art. 2), nel senso che segue una propria disciplina e presupposti (pur dipendendo da un reato-presupposto).

2.2 CRITERI OGGETTIVI DI IMPUTAZIONE: "CHI" E "PERCHÉ" L'ENTE RISPONDE (ART. 5)

Il fulcro del sistema risiede nell'art. 5, che lega l'illecito dell'ente a reati commessi:

- da **soggetti in posizione apicale** (rappresentanza, amministrazione o direzione dell'ente o di sua unità organizzativa autonoma; ovvero soggetti che esercitano di fatto gestione e controllo);
- da **soggetti sottoposti** alla direzione o vigilanza degli apicali;
- **nell'interesse o a vantaggio** dell'ente.

Il criterio "**interesse/vantaggio**" è un requisito decisivo: esclude, in linea generale, l'imputazione quando il soggetto abbia agito **nell'interesse esclusivo proprio o di terzi** (art. 5).

In prospettiva "manuale", questo significa che il Modello deve presidiare non solo l'atto finale (il reato), ma le **condizioni organizzative** che potrebbero rendere quel reato "funzionale" a un

interesse o a una utilità per l'ente (riduzione costi, accelerazione pratiche, schermatura flussi, vantaggi competitivi, ecc.).

2.3 Reati commessi all'estero (art. 4)

Il decreto disciplina espressamente l'ipotesi di **reati commessi all'estero** (art. 4), prevedendo la possibilità di responsabilità dell'ente italiano al ricorrere delle condizioni ivi indicate e in coordinamento con i relativi criteri di punibilità previsti dal codice penale. Questa previsione è "di sistema": anche quando l'ente opera prevalentemente in Italia, il Modello deve essere concepito in modo da reggere l'eventuale dimensione transnazionale di alcune condotte (soggetti, flussi, controparti, ecc.).

2.4 Principio di "autonomia" del binomio ente/persona fisica e casi particolari (art. 8)

Il decreto prevede regole che rafforzano l'autonomia dell'illecito dell'ente rispetto alle vicende della persona fisica (art. 8), stabilendo che la responsabilità dell'ente può sussistere anche in situazioni in cui l'autore non sia identificato o non sia imputabile, secondo i limiti della norma.

Sul piano "manuale", ciò impone un'impostazione del Modello centrata su **processi, controlli ed evidenze**, non su "colpe individuali".

2.5 Il "catalogo" dei reati-presupposto: logica e gestione (Capo I, Sez. III; artt. 24 ss.)

Il decreto dedica una parte specifica alla responsabilità dell'ente per determinate fattispecie, mediante un catalogo progressivamente ampliato (artt. 24 e seguenti, con articoli "bis", "ter", ecc.).

In Parte Generale è essenziale fissare la regola metodologica:

- la Parte Generale descrive **il quadro**, il **metodo**, i **requisiti esimenti** e il sistema di governo/controllo;
- la Parte Speciale (successiva) seleziona, tra i reati, quelli **astrattamente applicabili** ai processi aziendali e costruisce i relativi protocolli.

2.6 L'EFFICACIA ESIMENTE ED I REQUISITI DEL MODELLO (ARTT. 6–7)

2.6.1 Art. 6: reati commessi da apicali e condizioni di esonero

L'art. 6 è centrale: disciplina l'ipotesi in cui il reato sia commesso da un **apicale** e individua le condizioni in presenza delle quali l'ente può essere esonerato da responsabilità. In sintesi, **l'ente non deve limitarsi solo ad avere regole**, ma deve dimostrare di avere adottato e attuato un sistema idoneo e presidiato da un organismo di vigilanza efficace.

Le condizioni tipiche richiedono, tra l'altro:

- adozione, prima del fatto, di un **Modello idoneo** a prevenire reati della specie;
- istituzione di un **Organismo di Vigilanza** con autonomi poteri di iniziativa e controllo;
- commissione del reato mediante **elusione fraudolenta** del Modello;
- assenza di omessa o insufficiente vigilanza dell'OdV.

Contenuti "minimi" del Modello (art. 6, comma 2)

Il comma 2 dell'art. 6 specifica, in termini di "requisiti strutturali", cosa deve fare un Modello per essere adeguato:

- **individuare le attività** nel cui ambito possono essere commessi reati;
- prevedere **protocolli** idonei a programmare formazione e attuazione delle decisioni dell'ente;
- individuare modalità di **gestione delle risorse finanziarie** idonee a impedire la commissione dei reati;
- imporre **obblighi di informazione** verso l'OdV;
- introdurre un **sistema disciplinare** idoneo a sanzionare il mancato rispetto delle misure.

Linee guida (art. 6, comma 3)

Il comma 3 riconosce invece il ruolo dei **codici di comportamento/linee guida** elaborati dalle associazioni rappresentative (logica di standardizzazione "soft law") quali riferimenti per costruire modelli coerenti con la disciplina.

2.6.2 Art. 7: reati commessi da sottoposti e "efficace attuazione"

L'art. 7 disciplina l'ipotesi di reati commessi da soggetti **sottoposti** alla direzione o vigilanza degli apicali e fonda la responsabilità dell'ente sul difetto di **direzione e vigilanza**.

La norma valorizza il concetto di **efficace attuazione** del Modello: il comma 4 indica componenti tipiche dell'efficace attuazione:

- verifiche periodiche ed eventuale modifica del Modello quando emergano violazioni significative o mutamenti organizzativi;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure.

La **regola pratica (Parte Generale)** si può così sintetizzare come segue.

L'efficacia si dimostra tramite evidenze: i) procedure applicate, ii) audit svolti, iii) non conformità gestite, iv) formazione, v) sanzioni quando necessario, vi) flussi all'OdV, vii) aggiornamenti e versioning.

2.7 IL SISTEMA SANZIONATORIO (CAPO I, SEZ. II; ARTT. 9–23)

2.7.1 Tipi di sanzioni (artt. 9, 18, 19)

Il decreto prevede all'art. 9 che:

1. le **sanzioni** per gli illeciti amministrativi dipendenti da reato sono (comma 1):
   a) la sanzione pecuniaria;
   b) le sanzioni interdittive;
   c) la confisca;
   d) la pubblicazione della sentenza.
2. le sanzioni **interdittive** sono (comma 2) :
   a) l'interdizione dall'esercizio dell'attività;
   b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
   c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
   d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
   e) il divieto di pubblicizzare beni o servizi.

La loro durata è definita dal decreto e la loro applicazione è governata da criteri specifici (infra, artt. 13–16).

Oltre alle predette sanzioni, l'art. 19 disciplina altresì la **confisca** del prezzo o profitto del reato (o di somme/beni di valore equivalente nei limiti previsti).

Nei confronti dell'ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede.

Quando non è possibile eseguire la confisca, oppure la stessa abbia ad oggetto stabilimenti industriali o parti di essi che siano stati dichiarati di interesse strategico nazionale, il provvedimento può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

2.7.2 Sanzione pecuniaria: criterio "per quote" e commisurazione (artt. 10–12)

Il decreto costruisce la sanzione pecuniaria con il sistema "**per quote**".

L'art. 10 disciplina l'applicazione della sanzione pecuniaria e la logica di quantificazione. L'art. 11 indica i criteri di commisurazione (gravità del fatto, grado di responsabilità dell'ente, attività svolta per eliminare/attenuare conseguenze e per prevenire ulteriori illeciti, ecc.).

L'art. 12 prevede casi di riduzione della sanzione pecuniaria in presenza di specifiche condizioni (logica "premiale" /attenuativa).

2.7.3 Presupposti, scelta e casi particolari delle interdittive (artt. 13–17)

Il decreto disciplina in modo articolato le interdittive:

- art. 13: condizioni per l'applicazione delle interdittive;
- art. 14: criteri di scelta (mirate alla specifica attività cui si riferisce l'illecito);
- art. 15: commissario giudiziale in luogo dell'interdizione che interrompe l'attività (prosecuzione dell'attività tramite commissario, con compiti e poteri indicati dal giudice);
- art. 16: interdizione definitiva in casi particolarmente gravi e reiterati (nei limiti della norma);
- art. 17: riparazione delle conseguenze del reato (logica riparatoria rilevante ai fini delle interdittive).

2.7.4 Prescrizione (art. 22)

L'art. 22 disciplina la **prescrizione** dell'illecito amministrativo dipendente da reato e i relativi effetti (decorrenza, interruzioni/sospensioni nei limiti previsti).

Le sanzioni amministrative si prescrivono nel termine di cinque anni dalla data di consumazione del reato. Per effetto della interruzione inizia un nuovo periodo di prescrizione.

Interrompono la prescrizione la richiesta di applicazione di misure cautelari interdittive e la contestazione dell'illecito amministrativo a norma dell'articolo 59. Se l'interruzione è avvenuta mediante la contestazione dell'illecito amministrativo dipendente da reato, la prescrizione non corre fino al momento in cui passa in giudicato la sentenza che definisce il giudizio.

2.7.5 Delitti tentati (art. 26)

Il decreto disciplina anche l'ipotesi di **delitti tentati** (art. 26), prevedendo la riduzione delle sanzioni nei termini indicati e la disciplina delle interdittive correlata.

Le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà in relazione alla commissione, nelle forme del tentativo, dei delitti indicati nel presente capo del decreto.

L'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

2.8 Responsabilità patrimoniale e vicende modificative (Capo II; artt. 27–33)

2.8.1 Responsabilità patrimoniale (art. 27)

Il decreto prevede la responsabilità patrimoniale dell'ente per le sanzioni pecuniarie e disciplina la regola generale di imputazione e garanzia patrimoniale (art. 27).

Dell'obbligazione per il pagamento della sanzione pecuniaria risponde soltanto l'ente con il suo patrimonio o con il fondo comune. I crediti dello Stato derivanti degli illeciti amministrativi dell'ente relativi a reati hanno privilegio secondo le disposizioni del codice di procedura penale sui crediti dipendenti da reato. A tale fine, la sanzione pecuniaria si intende equiparata alla pena pecuniaria.

2.8.2 Trasformazione, fusione, scissione, cessione (artt. 28–33)

La disciplina delle vicende modificative è un pilastro "da Parte Generale" perché assicura continuità di responsabilità e regole di riparto:

- art. 28: trasformazione;
- art. 29: fusione;
- art. 30: scissione;
- art. 31–33: criteri e regole su ripartizione/solidarietà e limiti in caso di scissione e cessione (nei termini della disciplina).

2.9 PROCEDIMENTO DI ACCERTAMENTO E MISURE CAUTELARI (CAPO III; ARTT. 34 SS.)

2.9.1 Disposizioni generali sul procedimento (art. 34-35)

Il decreto disciplina il procedimento di accertamento e applicazione delle sanzioni amministrative, prevedendo un raccordo con le regole del processo penale e disposizioni specifiche: "Per il procedimento relativo agli illeciti amministrativi dipendenti da reato, si osservano le norme di questo capo nonché, in quanto compatibili, le disposizioni del codice di procedura penale e del decreto legislativo 28 luglio 1989, n. 271. (art. 34 e seguenti" (art. 34).

All'ente si applicano le disposizioni processuali relative all'imputato, in quanto compatibili (art. 35).

2.9.2 Attribuzioni del giudice penale e regole processuali (art. 36 e segg.)

La competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono.

Per il procedimento di accertamento dell'illecito amministrativo dell'ente si osservano le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende.

Non si procede all'accertamento dell'illecito amministrativo dell'ente quando l'azione penale non può essere iniziata o proseguita nei confronti dell'autore del reato per la mancanza di una condizione di procedibilità (art.37).

L'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo; l'ente che intende partecipare al procedimento si costituisce depositando nella cancelleria dell'autorità giudiziaria procedente una dichiarazione contenente a pena di inammissibilità:

a) la denominazione dell'ente e le generalità del suo legale rappresentante;

b) il nome ed il cognome del difensore e l'indicazione della procura;

c) la sottoscrizione del difensore;

d) la dichiarazione o l'elezione di domicilio.

La procura, conferita nelle forme previste dall'articolo 100, comma 1, del codice di procedura penale, è depositata nella segreteria del pubblico ministero o nella cancelleria del giudice ovvero è presentata in udienza unitamente alla dichiarazione di cui al comma 2.

Quando non compare il legale rappresentante, l'ente costituito é rappresentato dal difensore (art. 39).

L'ente che non ha nominato un difensore di fiducia o ne è rimasto privo è assistito da un *difensore di ufficio* (art. 40).

L'ente che non si costituisce è dichiarato *contumace* (art. 41).

Nel caso di *trasformazione, di fusione o di scissione* dell'ente originariamente responsabile, il procedimento prosegue nei confronti degli enti risultanti da tali vicende modificative o beneficiari della scissione, che partecipano al processo, nello stato in cui lo stesso si trova, depositando la dichiarazione di cui all'articolo 39, comma 2 (art. 42).

Quanto alle *notifiche* nel processo penale nei confronti dell'ente: per la prima notificazione si osservano le disposizioni dell'art. 154 c. III c.p.p. Sono comunque valide le notificazioni eseguite mediante consegna al legale rappresentante, anche se imputato del reato da cui dipende l'illecito amministrativo. Se l'ente ha dichiarato o eletto domicilio nella dichiarazione di cui all'articolo 39 o in altro atto comunicato all'autorità giudiziaria, le notificazioni sono eseguite ai sensi dell'articolo 161 del codice di procedura penale. Se non è possibile eseguire le notificazioni nei modi previsti dai commi precedenti, l'autorità giudiziaria dispone nuove ricerche. Qualora le ricerche non diano esito positivo, il giudice, su richiesta del pubblico ministero, sospende il procedimento (art. 43).

2.9.3 Misure cautelari interdittive (art. 45 e segg.)

Una parte essenziale del quadro normativo, spesso sottovalutata, riguarda le **misure cautelari**: l'art. 45 prevede l'applicazione (su richiesta del PM) di una misura cautelare interdittiva quando

sussistono gravi indizi di responsabilità dell'ente e un concreto pericolo di reiterazione di illeciti della stessa indole.

La norma consente, in alternativa, la nomina di un **commissario giudiziale** (richiamo all'art. 15) per un periodo pari alla durata della misura che sarebbe stata applicata.

Nel disporre le misure cautelari, il giudice tiene conto della specifica idoneità di ciascuna in relazione alla natura e al grado delle esigenze cautelari da soddisfare nel caso concreto.

Ogni misura cautelare deve essere proporzionata all'entità del fatto e alla sanzione che si ritiene possa essere applicata all'ente.

L'interdizione dall'esercizio dell'attività può essere disposta in via cautelare soltanto quando ogni altra misura risulti inadeguata.

Le misure cautelari non possono essere applicate congiuntamente.

2.9.4 Sequestro preventivo e confisca (art. 53 in relazione all'art. 19)

L'art. 53 prevede il **sequestro preventivo** delle cose di cui è consentita la confisca ai sensi dell'art. 19, richiamando la disciplina del codice di procedura penale per quanto applicabile.

2.9.5 Sequestro conservativo (art. 54)

Se vi è fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento e di ogni altra somma dovuta all'erario dello Stato, il pubblico ministero, in ogni stato e grado del processo di merito, chiede il sequestro conservativo dei beni mobili e immobili dell'ente o delle somme o cose allo stesso dovute. Si osservano le disposizioni di cui agli articoli 316, comma 4, 317, 318, 319 e 320 del codice di procedura penale, in quanto applicabili.

2.10 CHIARIMENTI "OPERATIVI": IDONEITÀ VS EFFICACIA E LOGICA DELLE EVIDENZE

Una delle finalità della Parte Generale del Modello Organizzativo di Gestione è quella di rendere chiaro che:

- ✓ il decreto NON premia la presenza di un mero documento, ma la **tenuta effettiva** del sistema (Modello + OdV + procedure + flussi + controlli + aggiornamento);

- ✓ l'idoneità si misura sulla capacità di prevenire reati "della specie" e sulla dimostrabilità dell'attuazione (registrazioni, audit, sanzioni disciplinari, riesami e aggiornamenti);
- ✓ le sanzioni interdittive e le misure cautelari (art. 45) rendono il sistema 231 un presidio di **continuità operativa** e non solo un adempimento.

2.10.1 Requisiti di "idoneità" del Modello: concetti operativi e standard di efficacia (artt. 6–7 D.lgs. 231/2001)

A) IDONEITÀ DEL MODELLO E "MOMENTO" DELLA VALUTAZIONE (ART. 6, CO. 1 E CO. 2)

Il Decreto Legislativo collega l'esimente sia all'adozione che **all'efficace attuazione** di modelli "**idonei a prevenire reati della specie** di quello verificatosi" (art. 6, co. 1, lett. a). In prospettiva manualistica, l'**idoneità** va intesa come **idoneità preventiva** (valutazione "ex ante"): il Modello deve essere progettato e strutturato in modo tale che, se correttamente attuato, sia ragionevolmente capace di ridurre/impedire il rischio di commissione dei reati nel perimetro aziendale.

Il legislatore, al fine di concretizzare il concetto di idoneità, elenca i **contenuti strutturali minimi** del Modello (art. 6, co. 2), imponendo che esso:

- individui le attività nel cui ambito possono essere commessi reati;
- preveda protocolli idonei a programmare la formazione e attuazione delle decisioni dell'ente;
- individui modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- preveda obblighi di informazione verso l'Organismo di Vigilanza;
- introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure.

Conseguenza operativa ("manuale"): l'idoneità non coincide con la mera esistenza di documenti, ma con la **coerenza** tra i) mappa attività/decisioni sensibili, *ii)* protocolli e responsabilità, *iii)* controlli su finanza e tracciabilità, *iv)* flussi verso OdV, *v)* disciplina e deterrenza.

B) "EFFICACE ATTUAZIONE": EVIDENZE, TRACCIABILITÀ E CONTINUITÀ (ART. 7, CO. 4)

L'art. 7 disciplina l'ipotesi di reato commesso da sottoposti e lega la responsabilità dell'ente a carenze di direzione/vigilanza; soprattutto, definisce i contenuti dell'**efficace attuazione** del Modello (art. 7, co. 4), richiedendo:

- verifiche periodiche e modifica del Modello quando siano scoperte violazioni significative o intervengano mutamenti nell'organizzazione o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure.

Conseguenza operativa ("manuale"): l'efficacia si dimostra tramite **evidenze** che documentino l'attuazione reale e continuativa del sistema, tra cui (senza esaurire):

- diffusione controllata del Modello e delle procedure;
- formazione effettuata e registrata;
- controlli di linea e di secondo livello realmente svolti e tracciati;
- flussi informativi all'OdV e verbalizzazioni;
- gestione delle non conformità/azioni correttive e aggiornamenti (versioning);
- applicazione del sistema disciplinare in caso di violazioni (senza automatismi, ma con effettività e proporzionalità).

C) RUOLO DELL'ODV COME REQUISITO DI SISTEMA E "PROVA" DI EFFETTIVITÀ (ART. 6, CO. 1, LETT. B E D)

Per i reati commessi da apicali, l'esimente richiede (tra l'altro) che:

- il compito di vigilare sul funzionamento e l'osservanza del Modello e curarne l'aggiornamento sia affidato a un organismo dotato di autonomi poteri di iniziativa e controllo;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Conseguenza operativa ("manuale"): l'OdV non è un "accessorio", ma un presupposto strutturale di validità del sistema. In termini di evidenze, la presenza di: (i) piano verifiche, (ii) audit e follow-up, (iii) gestione flussi e segnalazioni, (iv) reporting agli organi societari, è uno degli indicatori più forti di effettiva attuazione del Modello.

D) "ELUSIONE FRAUDOLENTA DEL MODELLO" E SOGLIA DI PRESIDIO (ART. 6, CO. 1, LETT. C)

Il decreto richiede, tra le condizioni esimenti per i reati commessi dagli apicali, che il reato sia stato commesso **eludendo fraudolentemente** il Modello adottato (art. 6, co. 1, lett. c). In logica manualistica, ciò implica che il Modello deve essere costruito con presìdi tali da rendere la commissione del reato **non "fisiologica"**, ma possibile solo attraverso un aggiramento deliberato e occulto dei controlli (alterazioni, falsificazioni, collusioni, bypass dei poteri, manipolazioni delle evidenze).

Nota metodologica: l'utillizzo di questa logica rafforza la necessità di (i) segregazione, (ii) controlli indipendenti, (iii) tracciabilità delle operazioni e delle autorizzazioni, (iv) archiviazione e immodificabilità/ricostruibilità delle registrazioni.

E) LINEE GUIDA E "STANDARD DI BUONA ORGANIZZAZIONE" (ART. 6, CO. 3)

L'art. 6, co. 3 prevede che i Modelli possano essere adottati sulla base di **codici di comportamento** elaborati dalle associazioni rappresentative e comunicati al Ministero della Giustizia.

Ciò fonda, sul piano sistematico, il ricorso a standard e best practice nella progettazione del Modello (impostazione per processi, sistema disciplinare, OdV, flussi, controlli finanziari), ferma la necessaria personalizzazione "su misura" dell'organizzazione e dei rischi effettivi.

F) COORDINAMENTO CON LA DISCIPLINA DELLE SEGNALAZIONI (EVOLUZIONE NORMATIVA)

Il quadro 231 deve oggi essere letto in coordinamento con la disciplina whistleblowing, che ha inciso anche sul sistema delle segnalazioni e tutele in ambito enti privati e, in via sistemica, sull'architettura di compliance aziendale.

2.11 MAPPA DEL D.LGS. 231/2001: INDICE RAGIONATO E COLLOCAZIONE DEI REQUISITI DEL MODELLO

Questa sezione ha lo scopo di rendere immediatamente intelleggibile **dove** il Decreto colloca i presupposti della responsabilità, le sanzioni, il procedimento e i requisiti organizzativi, così da orientare la conoscenza della struttura del Modello.

CAPO I – RESPONSABILITÀ AMMINISTRATIVA DELL'ENTE

Sezione I – Principi generali e criteri di attribuzione (artt. 1 – 8)

Contiene l'ossatura concettuale del sistema: ambito soggettivo, natura dell'illecito, criteri di imputazione (art. 5), reati all'estero (art. 4), e soprattutto i criteri di esonero collegati alla struttura organizzativa (artt. 6–7).

Sezione II – Sanzioni in generale (artt. 9 – 23)

Disciplina l'apparato sanzionatorio (pecuniarie, interdittive, confisca, pubblicazione sentenza), criteri di commisurazione e istituti correlati (riduzioni, criteri di scelta delle interdittive, commissariamento in luogo dell'interdizione, prescrizione).

Sezione III – Responsabilità amministrativa per reati previsti dal codice penale (artt. 24 – 26)

Introduce il nucleo originario del catalogo reati (artt. 24–26), che nel tempo è stato ampliato mediante ulteriori articoli (24-bis, 24-ter, 25 e seguenti, ecc.). In Parte Generale è essenziale fissare la regola: catalogo in evoluzione → necessità di aggiornamento periodico del Modello.

CAPO II – RESPONSABILITÀ PATRIMONIALE E VICENDE MODIFICATIVE DELL'ENTE (ARTT. 27–33)

Il Capo II assicura continuità della responsabilità e disciplina le conseguenze di trasformazioni, fusioni, scissioni, cessione/trasferimento, con regole di riparto e limiti. È il fondamento normativo per prevedere, nel Modello, un "trigger" di aggiornamento in caso di operazioni straordinarie.

CAPO III – PROCEDIMENTO DI ACCERTAMENTO E DI APPLICAZIONE DELLE SANZIONI AMMINISTRATIVE (ARTT. 34–82)

È la parte "processuale" del Decreto: disciplina regole del procedimento, soggetti e competenze, prove, indagini, giudizio, impugnazioni ed esecuzione.

Il Capo III chiarisce che la responsabilità 231 è accertata in un contesto "para-penale", con forte rilevanza di documenti, tracciabilità, e difesa tecnica.

All'interno del Capo III, è particolarmente rilevante (anche per la Parte Generale) la **Sezione IV – Misure cautelari (artt. 45–54)** che prevede misure interdittive in via cautelare (art. 45) e disciplina criteri di scelta e istituti collegati. È la base normativa per affermare che il Modello è anche presidio di continuità operativa (riduce rischio interdittive cautelari, nei limiti della disciplina).

CAPO IV – DISPOSIZIONI DI ATTUAZIONE E DI COORDINAMENTO (ARTT. 83–85)

Contiene norme finali/di coordinamento, utili a chiudere l'impianto sistematico e a collocare le regole operative e di raccordo con altri istituti.

3. DESCRIZIONE DELLA SOCIETÀ E CONTESTO OPERATIVO

3.1 PROFILO SOCIETARIO (DATI ESSENZIALI)

La LINGOTTO S.r.l. è una società a responsabilità limitata con sede legale in Valenza (AL), Strada per Solero 6/B, iscritta al Registro delle Imprese di Alessandria - Asti con numero REA AL-150533 e P.IVA/C.F. 01278020068:

Il domicilio digitale/PEC è il seguente: lingottosrl@legalmail.it

La società è stata costituita il 17 giugno 1986 ed è operativa dal 21 novembre 1986. Il capitale sociale sottoscritto è pari a euro 120.000,00. L'assetto societario evidenzia 3 soci e 3 amministratori, con rappresentanza attribuita a più persone.

3.2 ATTIVITÀ ESERCITATA E CODICI ATTIVITÀ

La visura indica come attività esercitate in sede:

- il commercio all'ingrosso di oro puro e metalli preziosi;
- la raccolta e trasporto di rifiuti non pericolosi avviati a recupero/riciclaggio;
- la lavorazione metalli preziosi.

Codice ATECO prevalente: 46.82.2.

La società risulta abilitata allo svolgimento di attività di import-export.

3.3 CONTESTO AUTORIZZATIVO

Dalla visura camerale risultano le seguenti iscrizioni, autorizzazioni e licenze pertinenti per al contesto operativo:

- Registro Esercenti il Commercio (Provincia di Alessandria) n. 26519 (cat. ord.);
- Albo Nazionale Gestori Ambientali: iscrizione n. TO/001266 (Sezione di Torino); categoria 4 - raccolta e trasporto di rifiuti speciali non pericolosi, classe F;
- Licenze di Pubblica Sicurezza (Questura): n. 1572 del 26/05/2015 - tipo 027 oggetti preziosi (commercio); n. 1571 del 26/05/2015 - tipo 026 oggetti preziosi (fabbricazione) orafi.
- Autorizzazione Unica Ambientale (Provincia) n. 68 del 15/01/2014;

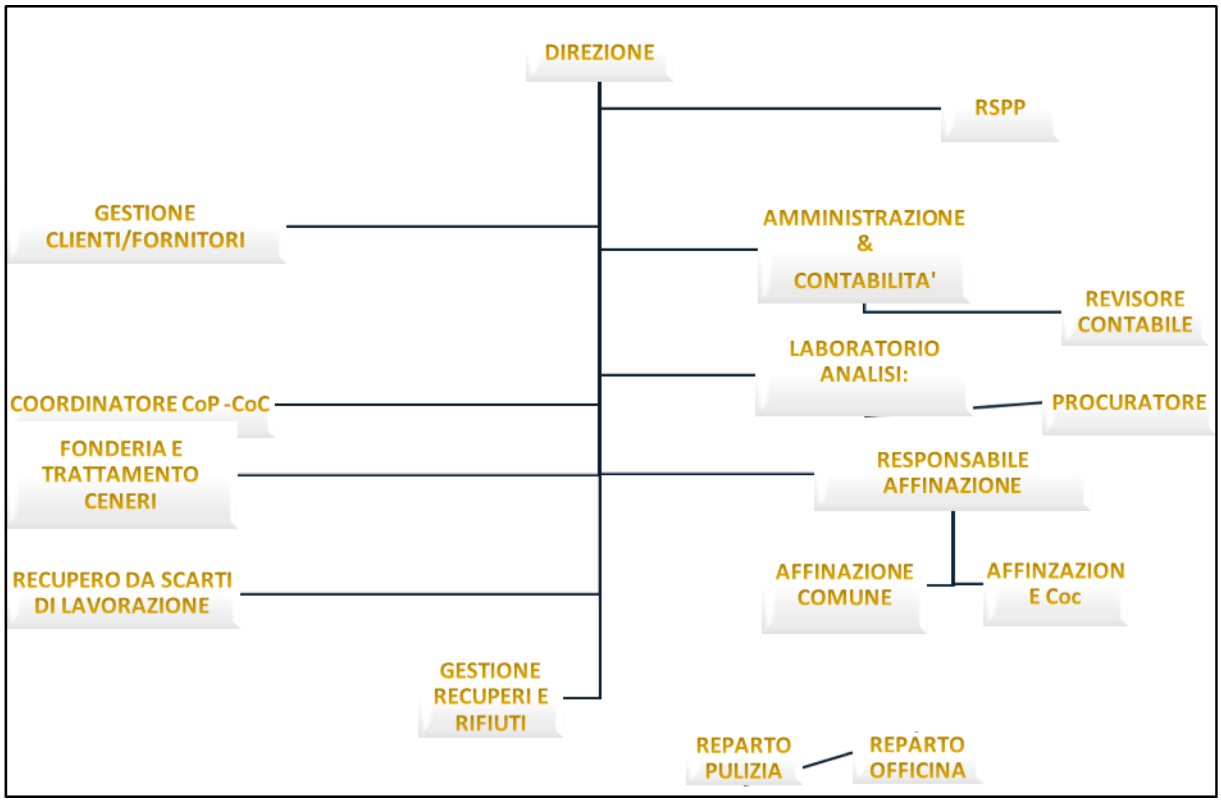
- Iscrizione nel registro degli operatori professionali in oro *ex* art. 1, comma 3-*bis* della legge n. 7 del 2000 - *data delibera* 09/05/2025 - *n° iscrizione* opo98

3.4 ASSETTO DIMENSIONALE E ORGANIZZATIVO

Gli addetti risultano in numero di 18 (dato INPS al 31/03/2025).

La dimensione dell'organizzazione impone un Modello proporzionato ma effettivo, con particolare attenzione alla chiara attribuzione di ruoli e poteri, alla segregazione dei compiti e alla tracciabilità delle operazioni in processi caratterizzati da elevato valore e specifica regolazione.

Di seguito l'organigramma aziendale:



3.5 PROCESSI AZIENDALI (MAPPA PROCESSI) E PUNTI DI ATTENZIONE 231

La mappa processi aziendale descrive i principali macro-processi operativi e di supporto; a titolo di sintesi, i processi "*core*" includono:

- Acquisto metalli (rottami auriferi/argentiferi da operatori), con controlli su documenti e tracciabilità;
- Magazzino (carichi/scarichi, giacenze, controlli);
- Vendita (DDT/fatture, consegne, tracciabilità);
- Lavorazioni conto terzi (coerenza merce/documenti/fatturazione; resa al cliente);
- Lavorazione interna: fusione → verga → saggiatura → affinazione chimica → recupero metalli puri e documentazione interna (DDT interno);
- Amministrazione: contabilità/fisco; pagamenti/incassi; archiviazione e tracciabilità flussi finanziari e movimenti di magazzino contabile.

Questa struttura costituisce la base per:

- identificazione attività sensibili (Parte Speciale);
- definizione protocolli di controllo (Protocolli);
- impostazione flussi verso OdV (Regolamento O.d.V.).

3.6 POLITICA AZIENDALE E STANDARD (INTEGRAZIONE CON MODELLO)

La Politica aziendale richiama, in sintesi:

- orientamento a soddisfazione cliente e miglioramento continuo;
- riferimenti a ISO 9001, ISO 14001, OHSAS/SSL, SA8000 e standard RJC (COP 2019 e Chain of Custody);
- impegni di due diligence verso i fornitori ed i clienti (verifica liceità provenienza; stop transazioni sospette e segnalazioni), oltre a indirizzi su supply chain e diritti umani.

Il Modello 231 si coordina con tali impegni, traducendoli in regole organizzative, procedure e controlli verificabili (registrazioni, audit, azioni correttive e riesami).

3.7 PRESIDI DI SICUREZZA FISICA E CATENA DI CUSTODIA

La procedura interna in materia di sicurezza descrive, tra l'altro:

- videosorveglianza esterna e controllo accessi;
- caveau protetto con vetri antiproiettile e presidi antirapina;

- polizze assicurative e identificazione del materiale all'ingresso e durante trasferimenti;
- trasporti con trasportatori incaricati e, per catena di custodia, contenitori sigillati con verifica del sigillo.

Tali presidi contribuiscono a ridurre rischi di appropriazione indebita, manomissione o dispersione di materiale, frodi sulla tracciabilità e, più in generale, condotte che possono riflettersi in profili di rischio-reato rilevanti ai fini del Modello 231 (con dettaglio nella Parte Speciale).

4. COSTRUZIONE DEL MODELLO / PROGETTO / GAP ANALYSIS / ACTION PLAN

4.1 PREMESSA

L'adozione del Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001 ("Modello" o "MOG 231") costituisce, per LINGOTTO S.r.l., uno strumento di **governance e controllo dell'agire imprenditoriale** e di **prevenzione** dei rischi-reato, integrato con i principi e le regole interne già adottate dall'azienda (policy, procedure, controlli, registrazioni).

Tale impostazione è coerente con l'approccio "manualistico" basato su un sistema "piramidale" (principi → controlli → procedure → modulistica/registrazioni) e sul ciclo *PDCA (PLAN–DO–CHECK–ACT)* quale metodo di implementazione e miglioramento continuo del sistema.

Nel caso di LINGOTTO S.r.l., l'esigenza di un assetto 231 strutturato si correla anche alle caratteristiche del contesto operativo (gestione/lavorazione di metalli preziosi; movimentazioni ad alto valore; processi di recupero/affinazione; tracciabilità tecnico-documentale; contesto autorizzativo/controlli), come risultante dalla mappatura dei processi e dalla documentazione interna di presidio (amministrativo-contabile, riconciliazioni, sicurezza, segnalazioni).

4.2 IL PROGETTO PER LA DEFINIZIONE DEL MODELLO 231 ("PROGETTO")

Al fine di rendere il proprio assetto organizzativo conforme ai requisiti del D.lgs. 231/2001 e coerente con le Linee Guida di riferimento, la Società avvia un insieme strutturato di attività (di seguito, il "**Progetto**") finalizzato alla **costruzione**, **formalizzazione** e **messa a regime** del Modello.

La metodologia del Progetto è definita in termini di: organizzazione, modalità operative, strutturazione per fasi, assegnazione responsabilità alle funzioni coinvolte e validazione degli output, così da garantire qualità, tracciabilità e autorevolezza dei risultati.

Assetto di governo del Progetto (schema standard):

- **Alta Direzione / Organo amministrativo**: definisce indirizzi e priorità, approva i documenti finali e l'Action Plan, assicura risorse. (Nel caso di LINGOTTO S.r.l.: amministrazione pluripersonale disgiuntiva come da organigramma/visura).

- **Team di Lavoro**: gruppo interfunzionale che supporta raccolta documentale, interviste, analisi processi/controlli, validazione delle schede di processo e delle proposte di miglioramento.
- **Key Officer / referenti di processo**: soggetti intervistati e responsabili di fornire evidenze operative e descrivere controlli in essere per i processi sensibili.
- **Supporto specialistico** (ove necessario): competenze legali/compliance, contabili, IT/privacy, ambiente/sicurezza, per completare analisi e protocolli.

Il Progetto è articolato in **quattro fasi**, secondo lo schema consolidato dei modelli di riferimento: (1) avvio e identificazione processi sensibili, (2) analisi processi/controlli, (3) gap analysis e action plan, (4) definizione del Modello.

4.3 FASE 1 – AVVIO DEL PROGETTO E INDIVIDUAZIONE DEI PROCESSI/ATTIVITÀ SENSIBILI

Obiettivo: presentazione del Progetto, raccolta e analisi della documentazione, e preliminare individuazione dei processi/attività nel cui ambito possono astrattamente essere commessi reati 231 (processi/attività "sensibili").

Attività tipiche (manuale operativo):

1. Kick-off con Alta Direzione e Team di Lavoro: definizione scopo, perimetro, output attesi, calendario e modalità di condivisione evidenze.
2. Raccolta documentale ("*document request list*"): organigrammi e assetto poteri; procedure e controlli; policy; registrazioni e report periodici; strumenti IT e sicurezza; gestione segnalazioni.
    - Esempi già disponibili per LINGOTTO srl: mappa processi; procedure amministrativo-contabili e di riconciliazione; procedure sicurezza; procedura segnalazioni; politica aziendale; documenti privacy/data protection.
3. Mappatura preliminare dei macro-processi e identificazione aree sensibili (core e strumentali), sulla base del contesto operativo e della struttura di controllo esistente (segregazione, autorizzazioni, tracciabilità, riconciliazioni).

Output di Fase 1 (deliverable):

- elenco processi/attività sensibili (prima matrice "processo → rischio astratto");

- piano interviste e lista key officer;
- indice preliminare Parte Speciale e schema protocolli.

4.4 FASE 2 – ANALISI DEI PROCESSI E DELLE ATTIVITÀ SENSIBILI (PROCESS ANALYSIS)

Obiettivo: analizzare in dettaglio processi/attività sensibili e **meccanismi di controllo in essere**, con attenzione ai controlli preventivi e agli elementi di compliance già presenti.

Metodologia:

- conduzione di **interviste strutturate** con key officer e personale indicato, per raccogliere informazioni su: processi elementari/attività svolte, soggetti interni/esterni coinvolti, ruoli/responsabilità, controlli esistenti; con successiva condivisione e validazione dei risultati.
- formalizzazione per ciascun processo sensibile di una **scheda processo** (o "process sheet") che descrive: fasi, input/output, documenti generati, autorizzazioni, controlli, segregazioni, anomalie/criticità.

Applicazione a LINGOTTO srl:

- processi core: acquisto, magazzino, vendita, lavorazioni conto terzi, lavorazione interna (fusione–saggiatura–affinazione), amministrazione.
- controlli finanziari/contabili: tracciabilità documentale, verifiche incrociate, riconciliazioni giornaliere/mensili, quadrature magazzino contabile vs fisico, riesame revisore.
- sicurezza fisica e catena di custodia: videosorveglianza, caveau, accessi, trasporti incaricati, sigilli e confronto sigilli in CoC.
- segnalazioni e tutele: canali, riservatezza, divieto di ritorsione, conservazione 5 anni.
- terze parti/supply chain: principi di due diligence e stop transazioni sospette in policy.

Output di Fase 2:

- "**Matrice identificazione aree a rischio**" (processi sensibili, ruoli, controlli, evidenze);
- raccolta evidenze (procedure, registrazioni, report, esempi documentali);
- elenco criticità/aree di rafforzamento emerse dalle interviste.

4.5 FASE 3 – GAP ANALYSIS ED ACTION PLAN

Obiettivo: individuare (i) i requisiti organizzativi caratterizzanti un Modello idoneo e (ii) le azioni di miglioramento del sistema esistente, tramite **analisi comparativa ("gap analysis")** tra assetto "*as is*" e assetto "*to be*" conforme alle previsioni del D.lgs. 231/2001.

4.5.1 Metodologia di gap analysis ("as is" vs "to be")

La gap analysis è condotta confrontando:

- AS IS: controlli e presìdi effettivamente esistenti (procedure, deleghe, controlli contabili, tracciabilità, flussi informativi, formazione, gestione segnalazioni, controlli terze parti);
- TO BE: requisiti di un sistema 231 "a tendere", ricavati dal D.lgs. 231/2001 e dalle linee guida, per ciascun processo/reato e per ciascun requisito trasversale (governance, OdV, flussi, disciplinare, ecc.).

In linea con l'approccio consolidato, la soglia di accettabilità del rischio è rappresentata da un sistema di controllo tale da **non poter essere eluso se non fraudolentemente**, ferma restando la necessità di adeguare i presidi alla concreta realtà aziendale.

4.5.2 Aree tipiche oggetto di gap analysis (checklist "manuale")

La gap analysis valuta, almeno:

- **Sistema di deleghe/procure e poteri** (chiarezza, limiti, spese, segregazione, evidenze autorizzative);
- **Sistema procedure e protocolli** (completezza, responsabilità, tracciabilità, punti di controllo, registrazioni);
- **Gestione risorse finanziarie** (tracciabilità, riconciliazioni, verifiche incrociate, quadrature);
- **OdV** (requisiti, poteri, flussi, reporting, archivi);
- **Whistleblowing/Segnalazioni** (canali, riservatezza, divieto ritorsione, tempi, coordinamento con OdV);
- **Terze parti** (due diligence, contratti, monitoraggi, catena di custodia);
- **IT/Privacy** (ruoli, misure, gestione accessi e incidenti) – coerentemente con la documentazione privacy.

4.5.3 Action Plan: struttura, priorità, responsabilità, evidenze

Sulla base dei gap, viene predisposto un **piano di attuazione (Action Plan)** volto a individuare requisiti organizzativi e azioni di miglioramento del sistema di controllo interno (processi e procedure), condiviso con Team di Lavoro e Alta Direzione.

Contenuti minimi dell'Action Plan:

- **Azione** (descrizione puntuale della misura: es. nuova procedura, revisione deleghe, introduzione controllo, formalizzazione flusso);
- **Ambito** (processo sensibile / requisito trasversale);
- **Motivazione** (gap e rischio coperto);
- **Owner** (responsabile attuazione) e **funzioni coinvolte**;
- **Priorità** (Alta/Media/Bassa) e **tempistica** (target date);
- **Evidenze richieste** (documenti/registrazioni che dimostrano implementazione);
- **Modalità di verifica** (audit OdV / controllo di linea / riesame direzione);
- **Stato** (aperto / in corso / chiuso) e data chiusura.

4.6 FASE 4 – DEFINIZIONE DEL MODELLO (PARTE GENERALE, PARTE SPECIALE, ALLEGATI)

Obiettivo: predisporre il Modello articolato in tutte le sue componenti (Parte Generale, Parti Speciali, allegati/procedure e regole di funzionamento) in conformità al D.Lgs. 231/2001 e alle indicazioni di riferimento, valorizzando i risultati delle fasi precedenti e le scelte di indirizzo dell'Alta Direzione.

Attività tipiche:

- redazione Parte Generale (governance, OdV, disciplinare, formazione, whistleblowing, terze parti, aggiornamento);
- redazione Parte Speciale per processo/reato (protocolli e controlli, flussi informativi, evidenze);
- definizione sistema documentale (procedure/modulistica/registrazioni) e raccordo con procedure esistenti, tra cui:
  - mappa processi;
  - procedure amministrativo-contabili e riconciliazioni;

- presidi sicurezza e catena di custodia;
- procedura segnalazioni;
- policy aziendale e principi di due diligence;
- predisposizione/aggiornamento del set "fondamentale" (organigrammi, deleghe, regolamento OdV, matrice flussi, action plan).

4.7 ADOZIONE, ATTUAZIONE E MESSA A REGIME DEL MODELLO (ROLL-OUT)

La costruzione del Modello comporta un'attività di assessment dell'assetto esistente per renderlo coerente con i principi di controllo introdotti dal D.lgs. 231/2001 e quindi idoneo a prevenire, con ragionevole certezza, i reati-presupposto.

In tale prospettiva, il Modello:

- si innesta nel sistema organizzativo e di controllo già adottato dalla Società (procedure, controlli, tracciabilità, riconciliazioni, sicurezza);
- viene diffuso ai destinatari e supportato da formazione e comunicazione;
- è monitorato mediante audit e gestione non conformità/azioni correttive secondo PDCA.

L'Action Plan costituisce lo strumento operativo di messa a regime: le azioni sono assegnate, tracciate, verificate e chiuse con evidenze; l'OdV (una volta nominato) verifica l'effettività delle misure e promuove l'aggiornamento del ciclo PDCA in caso di necessità.

5. SISTEMA DI GOVERNANCE, DELEGHE E PROCURE

5.1 Modello di governance e organi

L'organigramma societario MOG 231 e la visura descrivono:

- amministrazione con **più amministratori** (n. 3) e poteri disgiunti (come da indicazione in visura);
- presenza di **Revisore Unico**.
- presenza **Procuratore Speciale**

In ottica 231, la governance deve assicurare:

- chiarezza delle responsabilità;
- controlli "di vertice" sulle operazioni più esposte;
- tracciabilità dei processi decisionali e finanziari.

5.2 Assetto proprietario (cenni)

Le quote sociali risultano detenute da tre soci con percentuali indicate in visura e nell'organigramma societario.

5.3 Poteri degli amministratori (estratto visura) e implicazioni 231

La visura attribuisce poteri significativi in particolare su:

- operatività bancaria (apertura conti, disposizioni a debito, assegni, ecc.);
- gestione pratiche amministrative/previdenziali/lavoro e commerciali;
- gestione pratiche tutela ambiente e responsabilità laboratorio/reparto fusioni ai fini licenza PS;
- gestione pratiche tutela sanità.

Presidio chiave: in presenza di poteri ampi e disgiunti, il Modello deve rafforzare **segregazione** e **controlli incrociati**, soprattutto su flussi finanziari, acquisti/vendite di metalli, rapporti con autorità e gestione ambientale.

5.4 Principi per deleghe/procure e ordini di servizio (standard)

Lo standard richiede che responsabilità e poteri siano:

- chiari, formalizzati e comunicati;

- strutturati evitando sovrapposizioni e concentrazioni;
- deleghe e procure: atto scritto a data certa, conferite a soggetti competenti, con autonomia di spesa, accettazione scritta e aggiornamento tempestivo.

5.5 Sistema di procedure interne e tracciabilità (regola generale)

Le procedure interne devono:

- regolare modi e tempi dei processi;
- definire responsabilità nel rispetto della separazione ruoli;
- prevedere tracciabilità (chi autorizza, chi esegue, chi verifica, chi registra) e supporti documentali verificabili ex post.

Le procedure devono inoltre essere diffuse, archiviate ordinatamente e aggiornate; ed essere completate con controlli (riconciliazioni/quadrature) specie su flussi finanziari.

5.6 Gestione delle risorse finanziarie (principi e presidi già presenti)

5.6.1 Principio di tracciabilità finanziaria

Le procedure amministrativo-contabili stabiliscono che ogni operazione sia:

- supportata da documento (ordine, DDT, fattura, distinta bancaria, ecc.);
- registrata tempestivamente nel gestionale (entro 10 gg lavorativi);
- archiviata in modo ordinato, consentendo ricostruzione completa dell'operazione.

5.6.2 Presidi sull'area amministrativa

La procedura prevede un'area amministrativa con due risorse e controlli quali:

- verifica incrociata;
- riconciliazioni giornaliere e mensili;
- quadratura quotidiana magazzino contabile vs fisico;
- controlli trimestrali del revisore legale.

5.6.3 Procedura di riconciliazione bancaria e di cassa

È formalizzato un controllo giornaliero tra scritture e saldi home banking/cassa, con riconciliazione mensile e riesame trimestrale del revisore.

Valenza 231: questi controlli sono presidi "hard" contro rischi di distrazione fondi, falsi, frodi contabili/tributarie e opacità finanziaria.

5.7 TRACCIABILITÀ TECNICA DELLE LAVORAZIONI E DEI FLUSSI DI METALLO (CONTO LAVORAZIONE)

La procedura amministrativa prescrive, per il conto lavorazione, indicazioni obbligatorie in DDT/fattura (peso conferito, tipologia, peso post-lavorazione, titolo determinato, rese), garantendo tracciabilità tecnica e documentale.

Valenza 231: riduce spazi di manomissione documentale, frodi su quantità/qualità, contestazioni e rischi indiretti (es. ricettazione/impiego).

5.8 PRESIDI SU OMAGGI/OSPITALITÀ, SEGNALAZIONI E ANTI-RITORSIONE

Le "Regole Omaggi" richiamano obbligo di segnalazione alla Proprietà in caso di sospette violazioni e divieto di ritorsione verso chi segnala in buona fede.

Questi elementi devono essere integrati con:

- sistema disciplinare (cap. 7);
- whistleblowing (cap. 9);
- clausole con terze parti (cap. 10).

6. ORGANISMO DI VIGILANZA (ODV)

6.1 RUOLO DELL'ODV NEL SISTEMA 231 (ART. 6)

L'Organismo di Vigilanza ("OdV") è l'organo previsto dall'art. 6 del D.lgs. 231/2001 cui è affidato il compito di vigilare sul funzionamento, sull'osservanza e sull'adeguatezza del Modello di organizzazione, gestione e controllo (il "Modello"), nonché di curarne l'aggiornamento.

In tale prospettiva, l'OdV rappresenta una componente essenziale del sistema di controllo interno e svolge, in termini metodologici, la funzione di "CHECK" nel ciclo di miglioramento continuo (Plan–Do–Check–Act), verificando che le misure del Modello siano concretamente applicate e siano efficaci rispetto ai rischi da prevenire.

L'OdV non esercita funzioni gestorie, né si sostituisce alle responsabilità operative delle funzioni aziendali; opera, invece, quale presidio indipendente di controllo, con poteri di iniziativa e verifica, e con un canale di interlocuzione diretto con l'Organo amministrativo.

Rientrano tipicamente nelle attribuzioni dell'OdV, in via generale:

- predisporre (e aggiornare) un piano annuale di attività di vigilanza, definendo verifiche, priorità, metodologie e follow-up;
- verificare l'effettiva attuazione del Modello (protocolli/procedure, tracciabilità, controlli di linea e di secondo livello) e rilevare eventuali scostamenti o non conformità;
- esaminare i flussi informativi periodici e le informative straordinarie, valutandone la rilevanza ai fini del Modello e proponendo eventuali misure correttive;
- proporre aggiornamenti del Modello a fronte di evoluzioni normative, modifiche organizzative o esiti di audit/controlli;
- monitorare, per quanto di competenza, l'adeguatezza dei programmi di formazione e comunicazione sul Modello e la loro effettiva realizzazione (evidenze).

6.2 REQUISITI: AUTONOMIA, INDIPENDENZA, PROFESSIONALITÀ, CONTINUITÀ

In coerenza con le migliori prassi delle linee guida di settore e con la ratio dell'art. 6 D. Lgs. 231/2001, l'OdV deve possedere i seguenti requisiti:

- **autonomia**: capacità di operare senza condizionamenti, con poteri propri di iniziativa e controllo e con risorse adeguate (anche economiche) rispetto al piano di vigilanza;
- **indipendenza**: collocazione tale da garantire assenza di conflitti di interesse e di subordinazione funzionale alle aree controllate; reporting diretto all'Organo amministrativo;
- **professionalità:** competenze giuridiche e organizzative, nonché capacità di analisi dei processi e dei controlli, con possibilità di integrare competenze specialistiche (es. contabile, IT/privacy, salute e sicurezza, ambiente) mediante supporto esterno;
- **continuità d'azione**: effettiva operatività nel tempo, assicurata da programmazione delle attività, periodicità delle verifiche, tracciabilità delle risultanze e follow-up delle azioni correttive.

La composizione dell'OdV (monocratica o collegiale) è definita dall'Organo amministrativo in funzione della dimensione, complessità e struttura della Società.

In contesti organizzativi di dimensione contenuta, è frequente l'adozione di un OdV monocratico, ferma la possibilità di avvalersi di competenze specialistiche quando necessario.

Devono, inoltre, essere disciplinate (in sede di nomina/regolamento) le principali cause di incompatibilità e conflitto di interessi, nonché gli obblighi di riservatezza e correttezza nello svolgimento dell'incarico.

6.3 NOMINA, DURATA, DECADENZA E SOSTITUZIONE

L'OdV è nominato dall'Organo amministrativo con atto formale (delibera/lettera di incarico) che ne definisce almeno: composizione, durata dell'incarico, compenso, budget e poteri di spesa, canali di reporting, obblighi di riservatezza e cause di decadenza/revoca.

La durata dell'incarico deve essere tale da garantire stabilità e continuità (coerentemente con il ciclo di vigilanza e aggiornamento del Modello), prevedendo comunque la possibilità di rinnovo e la verifica periodica della permanenza dei requisiti.

Costituiscono, in via generale, cause di decadenza/revoca (da declinare nell'atto di nomina e nel regolamento): perdita dei requisiti di autonomia/indipendenza/professionalità, sopravvenienza di

conflitti di interesse non sanabili, violazione grave degli obblighi di riservatezza, grave inadempimento dell'incarico o impossibilità sopravvenuta a svolgerlo.

In caso di cessazione dall'incarico, l'Organo amministrativo procede senza ritardo alla sostituzione, assicurando la continuità delle attività e la conservazione dell'archivio OdV.

6.4 POTERI E BUDGET; ACCESSO ALLE INFORMAZIONI

Per assicurare effettività alla funzione di vigilanza, l'OdV deve disporre di poteri adeguati, proporzionati e concretamente esercitabili, tra cui:

- libero accesso alla documentazione rilevante ai fini 231 (procedure, registrazioni, contratti, report, evidenze di controllo) e alle informazioni detenute dalle funzioni aziendali;
- facoltà di richiedere informazioni e chiarimenti ai destinatari del Modello e di svolgere interviste/colloqui con il personale coinvolto nei processi oggetto di verifica;
- facoltà di effettuare verifiche e audit (anche a campione) e di richiedere l'esecuzione di controlli integrativi o approfondimenti;
- facoltà di avvalersi, nei limiti del budget assegnato, di consulenti esterni per attività specialistiche o istruttorie che richiedano competenze specifiche;
- potere di proporre misure correttive/migliorative e di formulare raccomandazioni all'Organo amministrativo e alle funzioni competenti.

L'OdV non irroga direttamente sanzioni disciplinari, ma può segnalare alle funzioni competenti e all'Organo amministrativo le violazioni rilevate e le criticità emerse, richiedendo evidenza delle azioni intraprese.

Il budget dell'OdV, definito in sede di nomina, deve consentire lo svolgimento delle attività pianificate (riunioni, audit, consulenze mirate, strumenti), prevedendo modalità di rendicontazione compatibili con l'esigenza di autonomia e riservatezza.

6.5 FUNZIONAMENTO (CENNI E PRINCIPI ORGANIZZATIVI)

Le modalità di funzionamento dell'OdV sono disciplinate da un Regolamento (predisposto separatamente e parte integrante del Modello di Organizzazione e Gestione), ferma la necessità, già in Parte Generale, di fissare i principi organizzativi essenziali:

- **programmazione:** definizione di un piano annuale di vigilanza e di obiettivi di verifica, con approccio risk-based;
- **periodicità**: convocazioni ordinarie con cadenza predefinita (almeno trimestrale) e convocazioni straordinarie in caso di urgenze o eventi rilevanti;
- verbalizzazione: redazione di verbali delle riunioni e delle attività svolte, con tracciabilità delle decisioni, delle evidenze esaminate e delle richieste inoltrate;
- follow-up: monitoraggio dello stato di attuazione delle azioni correttive e delle raccomandazioni, con escalation in caso di ritardi o inadempimenti;
- riservatezza: gestione protetta della documentazione e delle informazioni acquisite; trattamento dei dati personali nel rispetto della normativa applicabile (privacy/GDPR);
- gestione dei conflitti: obbligo di astensione e di informativa in caso di situazioni potenzialmente confliggenti.

Le attività dell'OdV devono essere svolte con criteri di imparzialità e con adeguata documentazione delle verifiche, così da rendere dimostrabile l'effettività della vigilanza.

6.6 FLUSSI INFORMATIVI E GESTIONE DELLE SEGNALAZIONI

Il Modello prevede obblighi informativi verso l'OdV (art. 6, co. 2, lett. d) D. Lgs. 231/2001). I flussi informativi costituiscono uno strumento essenziale per consentire all'OdV di svolgere la funzione di vigilanza e di intercettare tempestivamente criticità e scostamenti.

I flussi verso l'OdV si distinguono, in via generale, in:

- flussi periodici: informazioni strutturate e ricorrenti (report, indicatori, esiti controlli) utili a monitorare l'attuazione del Modello e lo stato dei presidi;
- flussi immediati/straordinari: informative senza ritardo relative a eventi anomali o potenzialmente rilevanti ai fini 231 (es. contestazioni/accertamenti da Autorità, violazioni del

Modello, incidenti rilevanti, anomalie significative in ambito documentale/contabile o di sicurezza).

Le modalità di invio, i formati, le frequenze e i responsabili dei flussi sono disciplinati nella matrice flussi e/o in apposite procedure, con tracciabilità dell'avvenuta trasmissione e dell'esame da parte dell'OdV.

Le segnalazioni (anche in ambito whistleblowing) che riguardino violazioni del Modello o condotte potenzialmente rilevanti ai fini 231 devono essere portate a conoscenza dell'OdV secondo le regole di riservatezza e di tutela previste dalla disciplina applicabile e dalle procedure interne.

6.7 REPORTING E RELAZIONI DELL'ODV

L'OdV riferisce all'Organo amministrativo in merito all'attività svolta, alle verifiche effettuate, alle criticità riscontrate e alle proposte di aggiornamento/miglioramento del Modello.

Il reporting avviene, in via ordinaria, con periodicità definita (almeno con relazione annuale), e in via straordinaria in presenza di eventi di particolare rilievo.

Le relazioni e le comunicazioni dell'OdV devono essere documentate e conservate in archivio riservato, unitamente alle evidenze delle attività svolte (verbali, report di audit).

Ove opportuno, l'OdV può interfacciarsi con gli ulteriori presidi di controllo (es. revisore legale) per il coordinamento su temi di comune interesse, nel rispetto della separazione dei ruoli e delle rispettive competenze, al fine di migliorare l'efficacia complessiva del sistema di controllo interno.

7. SISTEMA DISCIPLINARE E SANZIONATORIO

7.1 FINALITÀ E PRINCIPI (EFFETTIVITÀ DEL MODELLO)

Il sistema disciplinare e sanzionatorio costituisce requisito essenziale per l'efficace attuazione del Modello ai sensi dell'art. 6, comma 2, lett. e) e dell'art. 7, comma 4, lett. b) del D.Lgs. 231/2001. Esso assicura l'effettività delle regole del Modello, rafforza la cultura della legalità e rende concretamente sanzionabili le violazioni di principi, protocolli, procedure e obblighi informativi.

Il sistema disciplinare opera indipendentemente dall'instaurazione o dall'esito di un procedimento penale, nel rispetto delle garanzie previste dalla normativa lavoristica (in particolare art. 2106 c.c. ed art. 7 L. 300/1970) e dal CCNL applicabile, nonché dei principi di proporzionalità, gradualità e non discriminazione.

Principi applicativi:

- **tipicità e conoscibilità**: le condotte vietate e le relative conseguenze devono essere chiare, diffuse e accessibili ai destinatari;
- **proporzionalità e gradualità**: la sanzione è commisurata a gravità, dolo/colpa, ruolo, recidiva, danno/pregiudizio e livello di esposizione al rischio 231.
- **tracciabilità e motivazione**: contestazioni, istruttorie, decisioni e provvedimenti sono documentati e archiviati.
- **salvaguardia delle tutele**: garanzie difensive, contraddittorio, riservatezza e tutela dei segnalanti (divieto di ritorsione).

7.2 VIOLAZIONI RILEVANTI DEL MODELLO E CRITERI DI CLASSIFICAZIONE

Costituiscono violazioni disciplinarmente rilevanti, a titolo esemplificativo e non esaustivo:

- violazione di principi e regole del Modello, del Codice/Policy e dei protocolli applicabili;
- inosservanza di procedure operative e controlli interni (autorizzazioni, segregazione dei compiti, tracciabilità, riconciliazioni e verifiche);
- formazione/registrazioni: mancata partecipazione ingiustificata alle attività formative obbligatorie o mancata compilazione/conservazione delle evidenze richieste;

- flussi informativi: omessa, incompleta o tardiva comunicazione di informazioni dovute all'OdV oppure trasmissione di informazioni non veritiere;
- ostacolo ai controlli: rifiuto di collaborazione, impedimento o intralcio alle verifiche dell'OdV e/o degli organi di controllo, ovvero occultamento/distruzione di documenti;
- alterazione o falsificazione di documenti/registrazioni (es. ordini, DDT, fatture, registri, report, evidenze di controllo) o manomissione dei dati di sistema;
- violazioni del sistema di segnalazione: ritorsioni, discriminazioni o condotte intimidatorie verso segnalanti in buona fede; divulgazione indebita di identità; segnalazioni dolosamente infondate o calunniose;
- violazioni in materia di protezione dei dati e riservatezza quando incidano su presidi del Modello o su informazioni OdV.

Ai fini della graduazione, le violazioni sono valutate in base a: (i) intenzionalità (dolo/colpa); (ii) livello di rischio creato o danno; (iii) ruolo e responsabilità; (iv) recidiva; (v) eventuale coinvolgimento di terzi; (vi) tentativo di elusione dei controlli e qualità dell'occultamento.

7.3 MISURE VERSO DIPENDENTI (COERENZA CCNL)

Le sanzioni nei confronti dei lavoratori dipendenti sono applicate nel rispetto del CCNL e della disciplina di legge, secondo criteri di proporzionalità e gradualità. In via generale, possono essere previste (a titolo indicativo):

- richiamo verbale;
- richiamo scritto/censura;
- multa;
- sospensione dal lavoro e dalla retribuzione;
- licenziamento con preavviso o senza preavviso, nei casi di particolare gravità (es. condotte fraudolente, falsificazioni, appropriazioni, ritorsioni gravi, ostacolo sistematico ai controlli, reiterate violazioni deliberate).

La funzione competente cura la contestazione disciplinare e l'istruttoria; l'OdV è informato degli esiti nei casi rilevanti ai fini 231 e può richiedere approfondimenti o evidenze a supporto.

7.4 Misure verso dirigenti/quadri e responsabili

Per dirigenti, quadri e responsabili, le misure sono applicate in coerenza con l'inquadramento e con i contratti individuali, ferma la necessità di garantire l'effettività del Modello.

A titolo esemplificativo:

- richiamo formale e/o censura;
- sospensione o revoca di incarichi/attribuzioni, rimodulazione di deleghe e poteri;
- risoluzione del rapporto nei casi più gravi o in caso di reiterazione, nonché azioni risarcitorie ove ricorrano i presupposti.

7.5 Misure verso amministratori e soggetti apicali

In caso di violazioni del Modello da parte di amministratori o soggetti apicali, l'organo competente valuta e adotta misure proporzionate, nel rispetto delle disposizioni statutarie e di legge, quali, a titolo esemplificativo:

- contestazione formale e verbalizzazione;
- revoca o limitazione di deleghe/procure e rimodulazione dei poteri;
- sospensione dall'incarico o proposta di revoca/cessazione della carica, ove applicabile;
- promozione di azioni di responsabilità e richieste risarcitorie per danni arrecati alla Società;
- comunicazioni agli organi di controllo, ove previsti, e gestione dei conflitti di interesse.

Qualora la violazione riguardi componenti dell'OdV (se interni) o soggetti incaricati di funzioni di controllo, l'organo amministrativo procede alla valutazione di decadenza/revoca per giusta causa (es. perdita requisiti, conflitto di interessi, violazione riservatezza, negligenza grave), assicurando continuità di presidio.

7.6 Misure verso terze parti (clausole, risoluzione, penali)

Nei rapporti con fornitori, consulenti, trasportatori, partner e altri soggetti terzi, la Società può prevedere strumenti di tutela mediante clausole contrattuali e presidi di qualifica/monitoraggio.

In caso di violazioni rilevanti possono essere applicate, secondo contratto:

- diffida ad adempiere e richiesta di misure correttive;

- sospensione dell'esecuzione, sostituzione del personale impiegato dal terzo o limitazioni operative;
- diritto di audit/verifica e obbligo di collaborazione e messa a disposizione di evidenze;
- penali e risarcimento dei danni;
- risoluzione del rapporto per inadempimento o per giusta causa, nonché esclusione da successive qualifiche (ad. es. lista fornitori) nei casi più gravi o reiterati.

7.7 PROCESSO DISCIPLINARE E FLUSSI INFORMATIVI VERSO ODV

Il processo disciplinare è gestito secondo regole che assicurano tempestività, contraddittorio, imparzialità e tracciabilità.

In via generale:

- rilevazione della violazione (controlli di linea, audit, segnalazioni, verifiche dell'OdV);
- istruttoria preliminare e raccolta evidenze;
- contestazione formale e concessione dei termini a difesa secondo la normativa applicabile;
- valutazione e adozione del provvedimento disciplinare motivato;
- comunicazione degli esiti e archiviazione della documentazione.

Flussi verso l'OdV

L'OdV è informato, con cadenza almeno periodica e comunque senza ritardo in caso di fatti gravi, circa:

- violazioni significative del Modello;
- avvio ed esito di procedimenti disciplinari connessi a rischi 231;
- misure adottate e stato delle azioni correttive.

L'OdV può formulare raccomandazioni di miglioramento e richiedere l'aggiornamento di procedure/formazione quando emergano criticità ricorrenti.

La documentazione disciplinare è conservata con adeguati presidi di riservatezza e nel rispetto della normativa privacy, garantendo l'accesso ai soli soggetti autorizzati.

8. FORMAZIONE E COMUNICAZIONE

8.1 PRINCIPI E RESPONSABILITÀ DELLA DIREZIONE

La Società considera la formazione e la comunicazione sul Modello componenti essenziali dell' "efficace attuazione" ai sensi degli artt. 6–7 del D. Lgs. 231/2001: regole, procedure e controlli assumono reale efficacia preventiva solo se conosciuti, compresi e applicati dai Destinatari.
In tale prospettiva:

- l'Organo amministrativo/Direzione definisce gli indirizzi, assicura risorse e priorità, approva il piano formativo del proprio modelle di organizzazione e gestione e ne promuove l'attuazione;
- i responsabili di funzione/preposti garantiscono la partecipazione dei collaboratori e la corretta applicazione delle procedure pertinenti;
- l'OdV monitora l'adeguatezza del programma formativo segnalando se vi sono criticità e proponendo eventualmente integrazioni;
- tutti i Destinatari partecipano alla formazione assegnata, rispettano le regole del Modello e collaborano alle verifiche e ai flussi informativi di competenza.

Valenza 231: la formazione riduce il rischio di errori "inconsapevoli", rafforza la cultura dei controlli e della tracciabilità e rende effettivi i divieti fondamentali (ad es. elusione dei controlli, alterazione/falsificazione documentale, condotte opache).

8.2 PIANO FORMATIVO (INIZIALE, PERIODICO, MIRATO)

Il piano formativo è strutturato in modo proporzionato alla dimensione aziendale e ai processi sensibili, con approccio *risk-based*, distinguendo tra formazione iniziale, periodica e mirata per funzioni/ruoli maggiormente esposti.

8.2.1 Formazione iniziale

È erogata a neoassunti, neo-inseriti e collaboratori stabilmente integrati nei processi aziendali.
I contenuti minimi che la formazione sul MOG necessita sono i seguenti:

- principi del D. Lgs. 231/2001 e responsabilità dell'ente;

- struttura del Modello e regole/protocolli di competenza;
- canali di segnalazione e divieto di ritorsione;
- regole di tracciabilità documentale e presìdi di controllo pertinenti al ruolo (in particolare per le attività amministrative ed operative).

8.2.2 Formazione periodica

Prevede un "*refresh*" sui principi 231 e sugli aggiornamenti del Modello/policy/procedure, nonché moduli di richiamo sulla tracciabilità ed evidenze.

Ove opportuno, la formazione integra casi pratici e *lesson learned* derivanti da audit, non conformità, anomalie operative e segnalazioni (in forma anonimizzata quando necessario).

8.2.3 Formazione mirata per funzioni sensibili

Sono previsti moduli specifici per processi maggiormente esposti ai rischi-reato e/o ai rischi di non conformità, ad esempio:

- area amministrazione/finanza: riconciliazioni, incassi/pagamenti, archiviazione delle evidenze e controlli;
- area operativa/laboratorio: tracciabilità tecnica (pesi, saggiature, rese), gestione anomalie e registrazioni;
- logistica/trasporti: catena di custodia, consegne, documentazione e gestione scostamenti;
- sicurezza/ambiente (ove applicabile): DPI, emergenze/sversamenti, gestione autorizzativa e registrazioni;
- IT/Privacy: misure di sicurezza, gestione accessi, backup, autorizzazioni, principi GDPR.

L'approfondimento dei contenuti e la periodicità dei richiami sono determinati in funzione del rischio e del ruolo effettivamente svolto.

8.3 COMUNICAZIONE INTERNA DEL MODELLO

La comunicazione interna assicura la diffusione del Modello e delle regole applicabili, garantendo che i Destinatari dispongano di informazioni aggiornate e facilmente accessibili.

In particolare, la Società cura:

- comunicazione formale dell'adozione e degli aggiornamenti del Modello;

- disponibilità del documento (e delle parti pertinenti) in formato controllato e accessibile;
- comunicazione mirata ai ruoli sensibili (amministrazione, operazioni, logistica, ambiente/sicurezza, IT);
- richiamo periodico dei canali di segnalazione e del divieto di ritorsione.

Valenza 231: la comunicazione strutturata riduce "zone grigie" operative e favorisce comportamenti uniformi e tracciabili.

8.4 COMUNICAZIONE VERSO TERZE PARTI (CLAUSOLE E INFORMATIVA)

La Società informa, in misura proporzionata al rischio, anche le terze parti (fornitori, consulenti, trasportatori, partner, clienti) circa i principi di comportamento attesi e le regole rilevanti del proprio sistema di integrità.

In particolare, in fase di *onboarding*/qualifica e nei contratti possono essere previsti: impegni di conformità, obblighi di tracciabilità e collaborazione, divieti di condotte indebite, diritto di audit/verifica, penali e/o clausole risolutive per inadempimenti rilevanti.

8.5 REGISTRAZIONI: EVIDENZE FORMAZIONE E VALUTAZIONE EFFICACIA

Sono conservate, con adeguata tracciabilità e riservatezza, le evidenze del processo formativo e comunicativo (ad es. piano annuale, programmi, materiali, registri presenze, attestati, eventuali test/valutazioni).

L'efficacia è oggetto di riesame periodico anche alla luce di audit, non conformità, anomalie e segnalazioni, al fine di aggiornare contenuti e priorità formative.

9. WHISTLEBLOWING E GESTIONE SEGNALAZIONI

9.1 QUADRO NORMATIVO E PRINCIPI (RISERVATEZZA, DIVIETO RITORSIONE)

La Società adotta un sistema di segnalazione integrato nel Modello, ispirato ai principi di riservatezza, imparzialità e tutela del segnalante, nonché alla protezione del segnalato da accuse infondate.

Principi cardine:

- gestione riservata delle informazioni e limitazione degli accessi ai soli soggetti autorizzati;
- valutazione anche di segnalazioni anonime se circostanziate e supportate da elementi concreti;
- divieto di ritorsione verso chi segnala in buona fede;
- tutela del segnalato e garanzie di contraddittorio, ove compatibili con le esigenze istruttorie.

9.2 CANALI DI SEGNALAZIONE E ACCESSIBILITÀ

I canali di segnalazione sono resi noti ai Destinatari e garantiscono modalità idonee a preservare la riservatezza.

In coerenza con la procedura interna adottata dall'azienda, occorre la previsione di canali quali, ad esempio: cassetta interna, indirizzo specifico di posta elettronica per segnalazioni e modulo online sul sito aziendale, utilizzabile anche in forma anonima.

I canali sono accessibili, nei limiti applicabili, anche a terze parti che operano con/per la Società (es. fornitori, consulenti, trasportatori).

9.3 PROCESSO DI GESTIONE (RICEZIONE, ISTRUTTORIA, ESITO)

La gestione delle segnalazioni è affidata al soggetto incaricato secondo procedura interna, con presidi di riservatezza e imparzialità.

Il processo è strutturato in fasi:

1. ricezione e registrazione della segnalazione (con tracciatura degli step);
2. valutazione preliminare di ammissibilità e qualificazione (231/non 231; urgenza; rischio attuale);

3. eventuale approfondimento interno e raccolta evidenze;
4. definizione dell'esito e delle misure conseguenti (azioni correttive, segnalazioni alle funzioni competenti, eventuale attivazione disciplinare);
5. archiviazione riservata.

Valenza 231: un *workflow* formalizzato riduce il rischio di insabbiamento e rende dimostrabile la presa in carico delle anomalie.

9.4 TEMPI DI RISCONTRO E TRACCIABILITÀ

Nel rispetto delle regole di riservatezza, la Società assicura tempi di gestione proporzionati alla complessità del caso e traccia le attività svolte (ricezione, istruttoria, esito, misure adottate).
Ove applicabile, sono previsti: avviso di ricevimento al segnalante (se identificabile) e riscontro sugli esiti entro termini congrui, compatibilmente con la complessità dell'istruttoria e con i vincoli di riservatezza.

9.5 COORDINAMENTO CON ODV E CON IL SISTEMA DISCIPLINARE

Le segnalazioni relative a violazioni del Modello/protocolli 231, tentativi di elusione dei controlli, alterazioni o falsificazioni documentali e, più in generale, condotte potenzialmente rilevanti ai fini 231, devono essere portate a conoscenza dell'OdV secondo i flussi informativi previsti.
Qualora emergano profili disciplinari, la gestione della segnalazione si coordina con il sistema disciplinare (cap. 7), assicurando tracciabilità, proporzionalità e tutela delle parti coinvolte.

9.6 TRATTAMENTO DATI E ARCHIVIAZIONE

Il trattamento dei dati connessi alle segnalazioni avviene nel rispetto dei principi privacy (minimizzazione, limitazione degli accessi, misure tecniche e organizzative). La documentazione è conservata in archivi riservati per il tempo previsto dalla procedura interna e dalla normativa applicabile.

9.7 PROTEZIONE DEL SEGNALANTE E TUTELA DEL SEGNALATO

È vietata ogni forma di ritorsione (anche indiretta) nei confronti di chi segnala in buona fede. Sono parimenti vietate condotte che ostacolino o scoraggino la segnalazione.

Al contempo, il segnalato è tutelato da accuse infondate: sono garantiti, ove compatibili con l'istruttoria, contraddittorio e possibilità di fornire chiarimenti; sono previste conseguenze per segnalazioni manifestamente infondate presentate con dolo o colpa grave.

10. GESTIONE TERZE PARTI

10.1 Razionale e perimetro (fornitori, consulenti, partner, trasportatori, clienti)

Le terze parti (fornitori, consulenti, trasportatori, partner, clienti) possono incidere sui rischi 231 poiché operano "con/per" la Società e influenzano tracciabilità, autorizzazioni, sicurezza, ambiente e trattamento dati.

La gestione delle terze parti è, pertanto, improntata a diligenza preventiva, presidio contrattuale e monitoraggio in corso di rapporto, in modo proporzionato al rischio.

10.2 Qualifica e due diligence

La Società adotta un approccio *risk-based* alla qualifica delle controparti, che può includere, a seconda della tipologia di rapporto e della criticità, verifiche documentali e reputazionali, requisiti autorizzativi/abilitativi, coerenza dei pagamenti, nonché presidi su provenienza/liceità e coerenza delle operazioni.

Le controparti possono essere classificate per livelli di rischio (es. volume/criticità del servizio, accesso ad asset o dati, esposizione a rapporti con PA, impatto su processi sensibili) e assoggettate a riesame periodico.

10.3 Clausole contrattuali 231 e right to audit

Nei contratti con terze parti, in funzione del rischio, sono inserite clausole che disciplinano: impegno al rispetto di norme e principi etici; obblighi di collaborazione, tracciabilità e veridicità documentale; divieto di pratiche indebite; diritto di audit/verifica; penali e risoluzione per inadempimenti rilevanti.

10.4 Monitoraggi e controlli periodici

La Società effettua controlli proporzionati al rischio (anche a campione), volti a verificare coerenza tra attività svolte e documentazione/evidenze prodotte, nonché il rispetto di istruzioni operative e requisiti contrattuali.

Gli esiti dei monitoraggi e le eventuali non conformità rilevanti alimentano i flussi informativi verso l'OdV e possono determinare azioni correttive, aggiornamenti procedurali e/o interventi formativi mirati.

10.5 GESTIONE NON CONFORMITÀ E RISOLUZIONE RAPPORTI

In caso di violazioni o criticità rilevanti, la Società può attivare, in modo proporzionato, misure quali: richiesta di azioni correttive con evidenze, audit mirati, sospensione/limitazioni operative, sostituzione del personale del terzo, applicazione di penali, risoluzione per giusta causa e/o esclusione da successive qualifiche nei casi gravi o reiterati.

10.6 TERZE PARTI IT E SICUREZZA INFORMATICA (CENNI DI COORDINAMENTO)

Per fornitori IT e soggetti che trattano dati per conto della Società, la qualifica include requisiti di sicurezza e obblighi contrattuali coerenti con il sistema *privacy* e *cybersecurity* (istruzioni, misure tecniche e organizzative, gestione accessi, backup, gestione incidenti).

11. AGGIORNAMENTO E MIGLIORAMENTO DEL MODELLO

11.1 Principio di aggiornamento continuo e responsabilità

Il Modello è gestito secondo logica di miglioramento continuo, coerente con l'approccio per processi e con la metodologia PDCA (*Plan–Do–Check–Act*), assicurando aggiornamento, attuazione e tracciabilità delle evidenze.

L'Organo amministrativo assicura l'adeguatezza del Modello e ne approva gli aggiornamenti sostanziali; l'OdV monitora l'effettiva attuazione, segnala criticità e propone integrazioni; le funzioni operative curano l'implementazione delle azioni correttive e la produzione delle evidenze.

11.2 Trigger di aggiornamento (norme, organizzazione, violazioni, audit)

L'aggiornamento del Modello è attivato, a titolo esemplificativo, da: novità normative e di prassi; modifiche organizzative (ruoli, deleghe/procure, controlli); variazioni nelle attività/processi o nel contesto autorizzativo; violazioni significative del Modello; esiti di audit, non conformità, incidenti o segnalazioni rilevanti.

11.3 Gestione non conformità, azioni correttive e preventive

Le non conformità e le criticità di controllo sono gestite mediante: analisi delle cause, definizione di azioni correttive/preventive, assegnazione di responsabilità e tempistiche, verifica di efficacia e chiusura con evidenze.

L'Action Plan costituisce lo strumento operativo di pianificazione e follow-up, con monitoraggio dello stato di avanzamento e delle evidenze prodotte.

11.4 Riesame della direzione

Con periodicità almeno annuale (o al verificarsi di eventi rilevanti) la Direzione effettua il riesame del sistema 231, considerando: stato di attuazione del Modello; esiti di verifiche/audit e non conformità; stato dell'Action Plan; esiti aggregati delle segnalazioni; adeguatezza di formazione e comunicazione; necessità di aggiornamenti documentali.

11.5 MONITORAGGI E REPORTING

Sono utilizzati indicatori e reporting per misurare l'efficacia e intercettare trend di rischio, ad esempio:

- numero di non conformità su processi sensibili;
- scostamenti in riconciliazioni/quadrature;
- completamento formazione;
- tempi di gestione segnalazioni;
- esiti audit su processi di tracciabilità/catena di custodia.

Gli indicatori sono definiti in modo misurabile e documentabile e sono riesaminati periodicamente anche ai fini dell'aggiornamento del Modello.

11.6 GESTIONE DOCUMENTALE: REVISIONI, DISTRIBUZIONE E ARCHIVIAZIONE

La gestione documentale assicura controllo di versioni/revisioni, distribuzione controllata e archiviazione ordinata del Modello, delle policy/procedure e delle registrazioni, garantendo tracciabilità delle modifiche e accessibilità coerente ai destinatari interni ed esterni (limitata alle parti pertinenti).

È essenziale l'allineamento tra Modello, *policy*, procedure e modulistica, nonché la conservazione delle evidenze a supporto dell'effettiva attuazione nel tempo.