Documento	Modello 231 – Parte Speciale
Revisione	Rev. 00
Data di approvazione	08/10/2026
Organo approvante	Consiglio di Amministrazione
Entrata in vigore	23/10/2026

Premessa - Premessa della parte speciale

La presente sezione del Modello di organizzazione, gestione e controllo è dedicata alla raccolta e alla organizzazione delle Parti Speciali, ciascuna delle quali è riferita al singolo reato presupposto rilevante ai sensi del D.Lgs. 231/2001 e delle ulteriori disposizioni normative richiamate.

L'obiettivo delle Parti Speciali è quello di declinare, in relazione ai singoli ambiti di rischio, i principi generali del Modello in regole operative, presidi di controllo e comportamenti attesi, al fine di prevenire la commissione dei reati contemplati dalla normativa e garantire il rispetto dei principi di legalità, correttezza e trasparenza nell'operato dell'Ente.

A tal fine, per ogni singolo reato presupposto è stato adottato un approccio metodologico uniforme e strutturato, che consente una lettura organica e coerente dell'intero sistema di prevenzione. In particolare, ogni Parte Speciale è articolata secondo i seguenti elementi:

- **Inquadramento normativo**, volto a fornire una sintesi delle fattispecie di reato rilevanti e del relativo contesto giuridico
- **Mappatura delle attività sensibili e analisi del rischio**, sviluppata secondo una metodologia che identifica i processi aziendali maggiormente esposti e valuta i rischi di commissione dei reati
- **Individuazione delle attività sensibili**, con evidenza delle aree a rischio primario
- **Destinatari**, ossia i soggetti tenuti al rispetto delle prescrizioni contenute nella Parte Speciale
- **Principi generali di comportamento**, che definiscono le regole di condotta cui attenersi nello svolgimento delle attività a rischio
- **Sistema dei protocolli di controllo**, che disciplina i presidi organizzativi, procedurali e di controllo adottati dall'ente
- **Ruolo e controlli dell'Organismo di Vigilanza**, con riferimento alle attività di monitoraggio sull'efficace attuazione del Modello

L'impostazione adottata riflette un approccio integrato alla gestione del rischio 231, basato sulla stretta correlazione tra analisi dei processi aziendali, individuazione dei presidi di controllo e diffusione di una cultura della compliance all'interno dell'organizzazione.

Le Parti Speciali devono pertanto essere lette congiuntamente alla **Banca Dati Normativa**, che raccoglie il dettame normativo dei singoli reati presupposto, le fattispecie correlate e il relativo sistema sanzionatorio, ivi incluse le sanzioni interdittive, costituendo il riferimento di dettaglio per l'inquadramento giuridico delle tematiche trattate.

La Banca Dati Normativa è soggetta ad aggiornamento continuo in funzione dell'evoluzione legislativa e rappresenta, in tale prospettiva, uno strumento dinamico di supporto al Modello.

In coerenza con tale impostazione, anche le Parti Speciali sono oggetto di aggiornamento periodico e sistematico al mutare del dettame normativo e del perimetro dei reati presupposto, nonché in relazione all'evoluzione dell'assetto organizzativo e dei rischi aziendali.

Le Parti Speciali, in coordinamento con la Banca Dati Normativa, costituiscono pertanto un sistema organico e integrato di presidi volto alla prevenzione dei reati.

Art 24 - Indebita percezione di erogazioni

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 24 del D.Lgs. 231/2001, concernenti le fattispecie di indebita percezione di erogazioni pubbliche, truffa ai danni dello Stato o di un ente pubblico, o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di ente pubblico e frode nelle pubbliche forniture.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi ai rapporti con la Pubblica Amministrazione o dell'Unione Europea**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali connesse ai rapporti con la P.A. e Unione europea**

Le organizzazioni, indipendentemente dai settori in cui stabilmente operano, intrecciano quotidianamente rapporti con la P.A. ed eventualmente con l'Unione europea, per una miriade di attività che comportano un'interazione costante e strutturale con soggetti pubblici, autorità di controllo e organismi finanziatori, rendendo centrale la prevenzione dei reati contro la Pubblica Amministrazione.

L'art. 24 del D.Lgs. 231/2001 richiama, tra gli altri, i seguenti reati del codice penale e della legislazione speciale:

- Art. 316-bis c.p. – Malversazione di erogazioni pubbliche
- Art. 316-ter c.p. – Indebita percezione di erogazioni pubbliche
- Art. 353 c.p. – Turbata libertà degli incanti
- Art. 353-bis c.p. – Turbata libertà del procedimento di scelta del contraente
- Art. 356 c.p. – Frode nelle forniture pubbliche
- Art. 640 c.p. – Truffa
- Art. 640-bis c.p. – Truffa aggravata per il conseguimento di erogazioni pubbliche
- Art. 640-ter c.p. – Frode informatica
- Art. 640-quater c.p. – Applicabilità dell'art. 322-ter c.p.
- Art. 2 L. 898/1986 – Frode al Fondo Europeo Agricolo

In sintesi:

- Si ha **malversazione** quando contributi o finanziamenti pubblici, ottenuti legittimamente, vengono destinati a finalità diverse da quelle per cui sono stati concessi
- L'**indebita percezione** e la **truffa aggravata per il conseguimento di erogazioni pubbliche** si configurano quando contributi o finanziamenti vengono ottenuti mediante dichiarazioni false, documentazione non veritiera o omissioni rilevanti
- La **turbativa d'asta** e la **turbativa del procedimento di scelta del contraente** riguardano condotte idonee ad alterare la regolarità delle procedure di gara
- La **frode nelle pubbliche forniture** attiene all'inadempimento fraudolento nei contratti con la P.A
- La **frode informatica** si realizza, ad esempio, attraverso l'alterazione di sistemi informatici pubblici al fine di ottenere un ingiusto profitto

- La **Frode al Fondo Europeo Agricolo** si configura quando premi, aiuti, indennità, restituzioni contributi o altre erogazioni, a **carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale**, vengono ottenuti mediante dichiarazioni false, documentazione non veritiera o omissioni rilevanti

Per quelle imprese poi che operano stabilmente nel mercato degli appalti pubblici, tali fattispecie non rappresentano rischi astratti, ma ipotesi concretamente configurabili nelle diverse fasi del ciclo di vita della commessa pubblica: dalla gara, alla stipula, fino all'esecuzione e rendicontazione.

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.
Per "attività sensibili" si intendono quelle attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

Nel caso di Fondazione, il cui core business è fondato sulla partecipazione a finanziamenti pubblici ciò comporta:

- frequenti rapporti con stazioni appaltanti pubbliche
- interazioni con enti di controllo (Soprintendenze, ASL, Vigili del Fuoco, Ispettorato del Lavoro, INPS, INAIL, Agenzia delle Entrate, Guardia di Finanza)
- gestione di flussi finanziari legati a stati di avanzamento lavori (SAL), contributi, finanziamenti o anticipazioni pubbliche

Tale contesto impone una valutazione approfondita del rischio di commissione di reati contro la P.A., sia nelle attività direttamente esposte (attività sensibili), sia in quelle di supporto (attività strumentali).

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree.

a) Partecipazione a gare e procedure pubbliche

Questa fase rappresenta uno dei momenti a più elevato rischio-reato.
Il rischio può emergere:

- nella predisposizione della documentazione amministrativa e tecnica
- nella dichiarazione dei requisiti di ordine generale e speciale
- nella gestione dei rapporti con la stazione appaltante
- nella eventuale interlocuzione informale con funzionari pubblici

Condotte quali la presentazione di dichiarazioni non veritiere, l'alterazione di documenti, l'accordo collusivo con altri operatori economici o l'influenza indebita sul procedimento di gara possono integrare le fattispecie di turbativa o truffa.

Il principio guida in questa fase è: **ogni informazione resa alla P.A. deve essere completa, verificabile e documentalmente tracciabile**.

Una volta ottenuta la commessa, il rischio si sposta sulla fase esecutiva:

- rispetto delle specifiche tecniche
- qualità dei materiali impiegati
- corretta contabilizzazione dei lavori
- veridicità degli stati di avanzamento

La sostituzione di materiali con altri di qualità inferiore, la sovrafatturazione, la falsa attestazione di lavori non eseguiti o la richiesta di pagamenti non dovuti possono integrare la frode nelle pubbliche forniture o la truffa.

Il principio guida è: **piena corrispondenza tra quanto contrattualmente pattuito e quanto effettivamente realizzato e fatturato**.

Il rischio si articola in due momenti distinti:

1. **Fase genetica**: ottenimento del contributo (rischio di indebita percezione o truffa aggravata)
2. **Fase esecutiva**: utilizzo delle somme (rischio di malversazione)

Ogni contributo deve essere:

- richiesto sulla base di presupposti reali
- documentato in modo veritiero
- utilizzato esclusivamente per le finalità dichiarate

La tracciabilità delle spese e la separazione contabile delle risorse pubbliche rappresentano presidi essenziali.

Durante verifiche fiscali, previdenziali o in materia di sicurezza sul lavoro, è vietato:

- fornire documentazione alterata
- occultare informazioni rilevanti
- porre in essere condotte ostruzionistiche o ingannevoli

Il principio guida è la **leale collaborazione istituzionale**.

Anche attività apparentemente interne – quali selezione del personale, gestione dei fornitori, flussi finanziari, gestione del contenzioso – possono assumere rilievo strumentale alla commissione dei reati.

Ad esempio:

- l'assunzione di un soggetto su segnalazione indebita di un pubblico ufficiale
- il pagamento di consulenze fittizie destinate a veicolare utilità verso funzionari pubblici
- la creazione di fondi occulti

Pertanto, il rischio deve essere valutato in modo integrato lungo l'intera catena decisionale e finanziaria.

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività sensibili o strumentali: amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner commerciali, subappaltatori e fornitori.

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal ruolo effettivamente svolto nei processi aziendali.

I rapporti con la Pubblica Amministrazione devono essere improntati a:

- legalità
- trasparenza
- tracciabilità
- correttezza professionale

- separazione dei ruoli

È espressamente vietato:

- offrire o promettere denaro, regali o altri vantaggi a pubblici ufficiali o incaricati di pubblico servizio
- presentare dichiarazioni non veritiere per ottenere benefici pubblici
- destinare contributi pubblici a finalità diverse da quelle per cui sono stati concessi
- alterare documenti o sistemi informatici pubblici

Ogni dipendente o collaboratore che si trovi di fronte a richieste anomale o comportamenti sospetti deve attivare i canali di segnalazione previsti dal Modello.

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi, che disciplinano in modo analitico:

- il sistema di deleghe e procure
- la partecipazione e gestione di gare pubbliche
- la selezione e gestione di fornitori, consulenti e subappaltatori
- la gestione di contributi e finanziamenti pubblici
- la gestione del contenzioso
- la gestione delle verifiche ispettive
- la selezione e assunzione del personale
- la gestione di omaggi, liberalità e sponsorizzazioni

Tali protocolli devono essere letti come strumenti applicativi della presente Parte Speciale e costituiscono la traduzione operativa dei principi sopra enunciati.

L'attuazione efficace della presente Parte Speciale è sottoposta al controllo dell'Organismo di Vigilanza (OdV), istituito ai sensi dell'art. 6 del D.Lgs. 231/2001, al quale è attribuito il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del Modello.

Con specifico riferimento ai reati di cui all'art. 24 del D.Lgs. 231/2001, l'attività di controllo dell'OdV si concentra sulle aree aziendali caratterizzate da rapporti diretti o indiretti con la Pubblica Amministrazione, nonché sui processi che comportano la gestione di risorse pubbliche.

In particolare, l'OdV:

• verifica, anche a campione, la corretta applicazione dei protocolli relativi alla partecipazione a gare pubbliche, con attenzione alla veridicità delle dichiarazioni rese, alla completezza della documentazione e alla tracciabilità dei rapporti con la stazione appaltante

• monitora i processi di esecuzione dei contratti pubblici, al fine di accertare la coerenza tra prestazioni contrattuali, stati di avanzamento lavori, fatturazione e pagamenti ricevuti

• controlla la gestione di contributi, sovvenzioni e finanziamenti pubblici, verificando:

- la sussistenza dei requisiti per l'ottenimento
- la correttezza della documentazione presentata
- la destinazione delle risorse alle finalità dichiarate
- la tracciabilità dei flussi finanziari

• esamina i flussi informativi relativi ai rapporti con autorità di controllo e organi ispettivi, al fine di rilevare eventuali anomalie, criticità o comportamenti non conformi ai principi di trasparenza e collaborazione

• valuta l'adeguatezza del sistema delle deleghe e procure nelle aree a rischio, verificando la coerenza tra poteri attribuiti e responsabilità operative

• analizza eventuali segnalazioni (whistleblowing) relative a condotte potenzialmente rilevanti ai fini dei reati contro la Pubblica Amministrazione, garantendo la riservatezza del segnalante e promuovendo gli opportuni approfondimenti

• promuove interventi di formazione e sensibilizzazione del personale sulle tematiche connesse ai reati ex art. 24, anche sulla base delle criticità emerse in sede di controllo

L'OdV può richiedere alle funzioni aziendali competenti la trasmissione di documentazione, dati e informazioni rilevanti, nonché effettuare audizioni del personale coinvolto nei processi sensibili.

Particolare rilievo assumono i flussi informativi periodici verso l'OdV, che devono includere, tra l'altro:
• elenco delle gare pubbliche a cui la Fondazione ha partecipato
• stato di avanzamento delle commesse pubbliche
• contributi e finanziamenti pubblici richiesti e ottenuti
• esiti di eventuali verifiche ispettive
• anomalie riscontrate nei processi amministrativo-contabili

Gli esiti delle attività di controllo sono oggetto di report periodici agli organi societari competenti, contenenti eventuali rilievi, raccomandazioni e proposte di miglioramento del sistema di controllo interno.

In presenza di violazioni accertate o di significative carenze del Modello, l'OdV propone l'adozione di misure correttive, nonché l'eventuale attivazione del sistema disciplinare.

L'attività dell'Organismo di Vigilanza si configura, pertanto, come presidio essenziale per la prevenzione dei reati di cui all'art. 24, contribuendo in modo continuativo al rafforzamento della legalità, della trasparenza e della tracciabilità nei rapporti con la Pubblica Amministrazione.

La prevenzione dei reati contro la Pubblica Amministrazione non può essere affidata esclusivamente a regole formali. Essa richiede:

- consapevolezza diffusa dei rischi
- formazione continua del personale
- controlli effettivi e documentati
- una cultura dell'Ente orientata all'integrità

La presente Parte Speciale deve quindi essere intesa non solo come un documento di conformità normativa, ma come una guida operativa permanente per chiunque operi, direttamente o indirettamente, nei rapporti con la Pubblica Amministrazione.

Art 24-bis - Delitti informatici

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai **reati presupposto di cui all'art. 24-bis del D.Lgs. 231/2001**, concernenti i delitti informatici e il trattamento illecito di dati.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'utilizzo dei sistemi informatici, delle reti telematiche e dei dati digitali aziendali**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali che implicano l'uso di strumenti informatici**

Nell'attuale contesto economico e organizzativo, ogni impresa utilizza in modo strutturale **sistemi informatici, piattaforme digitali, infrastrutture telematiche e banche dati** per la gestione delle proprie attività operative, amministrative e commerciali.

Tali strumenti costituiscono un elemento essenziale per:

- la gestione dei processi aziendali
- la conservazione e l'elaborazione dei dati
- la comunicazione interna ed esterna
- i rapporti con clienti, fornitori, partner e Pubbliche Amministrazioni
- la gestione documentale e amministrativa

L'uso diffuso delle tecnologie informatiche comporta tuttavia l'esposizione a **specifici rischi di commissione di reati informatici**, sia mediante utilizzo improprio delle risorse aziendali sia attraverso comportamenti fraudolenti o abusivi posti in essere all'interno dell'organizzazione o nei confronti di soggetti terzi.

La prevenzione di tali reati richiede pertanto:

- adeguate **misure organizzative**
- **procedure di sicurezza informatica**
- sistemi di **tracciabilità e controllo degli accessi**
- una diffusa **cultura dell'Ente della sicurezza digitale**

Inquadramento normativo dei reati presupposto

L'art. 24-bis del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal codice penale e dalla normativa speciale in materia di sicurezza informatica.

Tra i principali reati rilevanti rientrano:

- Art. 491-bis c.p. – Documenti informatici
- Art. 615-ter c.p. – Accesso abusivo ad un sistema informatico o telematico
- Art. 615-quater c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

- Art. 617-bis c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche
- Art. 617-quater c.p. – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Art. 617-quinquies c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- Art. 617-sexies c.p. – Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
- Art. 629 c.p. – Estorsione (anche mediante strumenti informatici)
- Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici
- Art. 635-ter c.p. – Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico
- Art. 635-quater c.p. – Danneggiamento di sistemi informatici o telematici
- Art. 635-quater.1 c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Art. 635-quinquies c.p. – Danneggiamento di sistemi informatici di pubblico interesse
- Art. 640-ter c.p. – Frode informatica
- Art. 640-quinquies c.p. – Frode informatica del soggetto che presta servizi di certificazione di firma elettronica
- Art. 1 comma 11 D.L. 105/2019 – Disposizioni in materia di perimetro di sicurezza nazionale cibernetica

In sintesi:

- Si configura **l'accesso abusivo a sistema informatico** quando un soggetto si introduce in un sistema informatico o telematico protetto senza autorizzazione o eccedendo i limiti dell'autorizzazione ricevuta
- I reati di **intercettazione e interferenza nelle comunicazioni informatiche** riguardano l'acquisizione illecita, l'interruzione o l'alterazione di comunicazioni digitali tra soggetti
- I reati di **danneggiamento informatico** si verificano quando vengono distrutti, alterati o resi inutilizzabili dati, programmi o sistemi informatici
- La **frode informatica** consiste nell'alterazione di un sistema informatico o nell'intervento abusivo su dati o programmi allo scopo di procurare un ingiusto profitto aggravata se commessa da soggetto che presta servizi di certificazione di firma elettronica
- I reati relativi alla **detenzione o diffusione di strumenti informatici illeciti** riguardano la disponibilità o la distribuzione di password, software o dispositivi destinati a violare sistemi informatici
- La disciplina relativa al **perimetro di sicurezza nazionale cibernetica** introduce specifiche responsabilità per i soggetti che gestiscono infrastrutture informatiche critiche o strategiche

Per qualsiasi organizzazione che utilizzi strumenti digitali, tali fattispecie non rappresentano rischi meramente teorici, ma **ipotesi concretamente configurabili nello svolgimento delle**

attività aziendali, soprattutto con riferimento alla gestione dei sistemi informativi, dei dati e delle comunicazioni elettroniche.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati informatici sopra richiamati.

In qualsiasi organizzazione moderna, l'utilizzo di strumenti digitali interessa trasversalmente l'intera struttura dell'Ente:

- gestione amministrativa e contabile
- gestione documentale
- comunicazioni interne ed esterne
- gestione clienti e fornitori, partner e Pubbliche Amministrazioni
- gestione delle risorse umane
- attività commerciali e marketing
- gestione delle infrastrutture tecnologiche
- la gestione dei processi aziendali
- la conservazione e l'elaborazione dei dati

Pertanto, il rischio di commissione di reati informatici deve essere valutato **in modo trasversale**, considerando sia le attività direttamente connesse ai sistemi informativi sia quelle che utilizzano strumenti digitali come supporto operativo.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) **Gestione dei sistemi informativi**

La gestione dell'infrastruttura informatica rappresenta una delle aree più esposte al rischio di commissione di reati informatici.

Il rischio può emergere:

- nella gestione delle credenziali di accesso
- nella configurazione dei sistemi informatici
- nella gestione dei server e delle reti aziendali
- nell'installazione e aggiornamento di software
- nella gestione delle politiche di sicurezza informatica

Condotte quali l'utilizzo non autorizzato di credenziali di accesso, l'installazione di software non autorizzati, la diffusione di password o chiavi di accesso, la manipolazione dei sistemi informatici possono integrare i reati di accesso abusivo, diffusione di strumenti informatici illeciti o danneggiamento di sistemi.

Il principio guida in questa area è: **ogni accesso ai sistemi informatici deve essere autorizzato, tracciabile e coerente con le mansioni svolte.**

b) Gestione dei dati e dei documenti informatici

Le aziende gestiscono quotidianamente grandi quantità di dati digitali, documenti informatici e archivi elettronici.

Il rischio può emergere:

- nella creazione e gestione di documenti digitali
- nella conservazione di documentazione informatica
- nella modifica o cancellazione di dati
- nella trasmissione di informazioni digitali

L'alterazione, la falsificazione o la soppressione di documenti informatici possono integrare il reato relativo ai **documenti informatici**, nonché altre fattispecie di frode o danneggiamento informatico.

Il principio guida è: **integrità, autenticità e tracciabilità delle informazioni digitali.**

c) Gestione delle comunicazioni informatiche e telematiche

Le comunicazioni aziendali avvengono sempre più frequentemente mediante strumenti digitali quali posta elettronica, sistemi di messaggistica, piattaforme collaborative, reti aziendali e sistemi di videoconferenza

Il rischio può emergere in caso di:

- intercettazione abusiva di comunicazioni
- accesso non autorizzato a caselle di posta elettronica
- alterazione o soppressione di messaggi digitali
- interruzione intenzionale di comunicazioni informatiche

Il principio guida è: **le comunicazioni informatiche devono essere protette e accessibili esclusivamente ai soggetti autorizzati.**

d) Gestione delle relazioni digitali con soggetti esterni

Le imprese utilizzano sistemi informatici anche per interagire con soggetti esterni, quali clienti, fornitori, partner commerciali, consulenti e istituzioni pubbliche.

Il rischio può emergere nel caso di:

- utilizzo fraudolento di sistemi informatici per ottenere vantaggi economici
- manipolazione di dati trasmessi a soggetti esterni
- utilizzo illecito di piattaforme informatiche

In tali casi potrebbero configurarsi fattispecie di **frode informatica**.

Il principio guida è: **correttezza e trasparenza nell'utilizzo degli strumenti informatici nei rapporti con soggetti esterni.**

Attività strumentali

Anche alcune attività interne, pur non essendo direttamente informatiche, possono assumere rilievo strumentale alla commissione dei reati informatici.

Tra queste rientrano, ad esempio:

- la selezione del personale con accesso ai sistemi informatici

- la gestione dei fornitori di servizi IT
- l'acquisto di software e hardware
- la gestione degli accessi alle banche dati aziendali
- la gestione delle credenziali di autenticazione

Inoltre:

- la concessione di credenziali di accesso a soggetti non autorizzati
- l'utilizzo di software pirata o non autorizzati
- la mancata revoca degli accessi a personale cessato

possono facilitare la commissione di reati informatici.

Pertanto il rischio deve essere valutato **lungo l'intero ciclo di gestione delle risorse informatiche aziendali**.

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, utilizzano sistemi informatici o trattano dati digitali nell'ambito delle attività aziendali: amministratori, dirigenti, dipendenti, collaboratori, consulenti, fornitori di servizi informatici, partner tecnologici.

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivamente svolto nei processi aziendali che comportano l'utilizzo di strumenti informatici**.

Principi generali di comportamento

L'utilizzo dei sistemi informatici aziendali deve essere improntato ai principi di:

- legalità
- sicurezza informatica
- integrità dei dati
- tracciabilità delle operazioni
- responsabilità individuale nell'utilizzo delle risorse digitali

È espressamente vietato:

- accedere abusivamente a sistemi informatici o telematici
- utilizzare credenziali di accesso appartenenti ad altri soggetti
- diffondere password o strumenti di accesso ai sistemi informatici
- installare software non autorizzati o potenzialmente dannosi
- intercettare o interferire con comunicazioni informatiche
- alterare, distruggere o cancellare dati o programmi informatici senza autorizzazione
- utilizzare sistemi informatici per commettere frodi o ottenere vantaggi economici indebiti

Ogni dipendente o collaboratore che rilevi **anomalie, vulnerabilità o comportamenti sospetti nell'utilizzo dei sistemi informatici** è tenuto a segnalarli attraverso i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- la gestione della sicurezza informatica
- la gestione delle credenziali di accesso e dei sistemi di autenticazione
- la gestione degli accessi ai sistemi informativi
- la gestione e protezione dei dati aziendali
- la gestione della posta elettronica e delle comunicazioni digitali
- l'acquisto e l'installazione di software e hardware
- la gestione dei fornitori di servizi informatici
- la gestione degli incidenti di sicurezza informatica
- le procedure di backup e protezione dei dati

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV), istituito ai sensi dell'art. 6 del D.Lgs. 231/2001, al quale è attribuito il compito di verificare il funzionamento, l'osservanza e l'aggiornamento del Modello.

Con specifico riferimento ai reati di cui all'art. 24-bis del D.Lgs. 231/2001, l'attività di controllo dell'OdV si caratterizza per una particolare attenzione ai processi aziendali che implicano l'utilizzo di sistemi informatici, la gestione dei dati e la sicurezza delle infrastrutture digitali.

In particolare, l'OdV:

• verifica, anche mediante controlli a campione, la corretta applicazione dei protocolli di sicurezza informatica, con riferimento alla gestione degli accessi, delle credenziali di autenticazione e dei profili autorizzativi

• monitora i sistemi di tracciabilità degli accessi e delle operazioni (log), al fine di verificare la riconducibilità delle attività ai soggetti autorizzati e individuare eventuali anomalie o utilizzi impropri

• controlla i processi di gestione dei sistemi informativi aziendali, inclusi:

- configurazione e aggiornamento dei sistemi
- installazione di software
- gestione delle reti e dei dispositivi
- adozione di misure di protezione da accessi abusivi o malware

• verifica le modalità di gestione dei dati e dei documenti informatici, con particolare riferimento a:

- integrità e immodificabilità dei dati
- correttezza dei processi di archiviazione e conservazione
- tracciabilità delle modifiche e delle cancellazioni

• esamina i presidi adottati per la sicurezza delle comunicazioni informatiche e telematiche, inclusa la gestione della posta elettronica, delle piattaforme collaborative e degli strumenti di comunicazione digitale

• monitora i rapporti con fornitori di servizi informatici e partner tecnologici, verificando l'esistenza di adeguate clausole contrattuali in materia di sicurezza, riservatezza e protezione dei dati

• verifica la corretta gestione degli accessi in caso di cessazione o modifica del rapporto di lavoro o collaborazione, al fine di prevenire utilizzi indebiti dei sistemi informatici

• analizza eventuali segnalazioni (whistleblowing) relative a violazioni o anomalie in ambito informatico, garantendo la riservatezza del segnalante e promuovendo le opportune attività di verifica

• monitora la gestione degli incidenti di sicurezza informatica (es. data breach, accessi non autorizzati, perdita di dati), verificando la tempestività delle azioni correttive e la completezza della documentazione

• promuove iniziative di formazione e sensibilizzazione del personale sui rischi connessi ai reati informatici e sulle corrette modalità di utilizzo degli strumenti digitali

L'OdV può richiedere alle funzioni aziendali competenti l'accesso a documentazione tecnica, report di sicurezza, log di sistema e ogni altra informazione rilevante ai fini delle proprie attività di controllo, nonché effettuare audizioni del personale coinvolto nei processi sensibili.

Particolare rilevanza assumono i flussi informativi periodici verso l'OdV, che devono includere, tra l'altro:
• report sugli accessi ai sistemi informatici e sulle anomalie rilevate
• elenco degli incidenti di sicurezza informatica e delle misure adottate
• attività di aggiornamento dei sistemi e delle infrastrutture IT
• verifiche interne sulla sicurezza informatica
• utilizzo e gestione delle credenziali di accesso
• esiti di audit interni o esterni in materia di sicurezza dei sistemi informativi

Gli esiti delle attività di vigilanza sono oggetto di report periodici agli organi societari competenti, contenenti eventuali criticità riscontrate, raccomandazioni e proposte di miglioramento del sistema di controllo interno e dei presidi di sicurezza informatica.

In presenza di violazioni accertate, anomalie significative o carenze nei presidi di controllo, l'OdV propone l'adozione di misure correttive, nonché l'eventuale attivazione del sistema disciplinare.

L'attività dell'Organismo di Vigilanza costituisce pertanto un presidio essenziale per la prevenzione dei reati di cui all'art. 24-bis, contribuendo al rafforzamento della sicurezza informatica, della protezione dei dati e dell'utilizzo corretto delle tecnologie digitali all'interno dell'organizzazione.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati informatici non può essere affidata esclusivamente a soluzioni tecnologiche.

Essa richiede:

- una **governance chiara dei sistemi informativi**
- **procedure di sicurezza efficaci**
- **controlli tecnici e organizzativi documentati**
- **formazione continua del personale sulla sicurezza informatica**

- una **cultura dell'Ente orientata alla protezione dei dati e delle infrastrutture digitali**

La presente Parte Speciale deve pertanto essere intesa non solo come uno strumento di conformità normativa, ma come **una guida operativa per l'utilizzo corretto, sicuro e responsabile delle tecnologie informatiche all'interno dell'organizzazione**.

Art 24-ter - Criminalità organizzata

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'**art. 24-ter del D.Lgs. 231/2001**, concernenti i **delitti di criminalità organizzata**.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'eventuale infiltrazione o coinvolgimento della criminalità organizzata nelle attività economiche e imprenditoriali**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Nel contesto economico attuale, le organizzazioni criminali operano frequentemente attraverso attività apparentemente lecite, utilizzando Fondazione, fornitori, intermediari o collaboratori per realizzare attività illecite o infiltrarsi nei circuiti economici.

Le imprese possono essere esposte a tali rischi, ad esempio, attraverso:

· rapporti commerciali con fornitori o partner economici

· partecipazione a gare e appalti

· gestione di subappalti o servizi esternalizzati

· movimentazione di risorse finanziarie

· attività di intermediazione commerciale

· gestione delle relazioni con soggetti esterni

Tali contesti possono essere strumentalizzati da organizzazioni criminali per perseguire finalità illecite quali:

· il riciclaggio di proventi illeciti

· l'infiltrazione nell'economia legale

· il controllo indiretto di attività economiche

· l'ottenimento di vantaggi economici indebiti

La prevenzione dei reati di criminalità organizzata richiede pertanto:

· **adeguate misure organizzative**

· **procedure di selezione e controllo dei partner commerciali**

· **sistemi di tracciabilità dei rapporti economici**

· **una diffusa cultura dell'Ente orientata alla legalità e alla trasparenza**

Inquadramento normativo dei reati presupposto

L'**art. 24-ter del D.Lgs. 231/2001** richiama diverse fattispecie di reato previste dal codice penale e da normative speciali.

Tra i principali reati rilevanti rientrano:

· Art. 416 c.p. – Associazione per delinquere

· Art. 416-bis c.p. – Associazioni di tipo mafioso anche straniere

· Art. 416-ter c.p. – Scambio elettorale politico-mafioso

· Art. 630 c.p. – Sequestro di persona a scopo di estorsione

• Art. 74 D.P.R. 309/1990 – Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

In sintesi:

· Si configura il reato di associazione per delinquere quando **tre o più persone si associano stabilmente** allo scopo di commettere una serie indeterminata di delitti

· Il reato di associazione mafiosa si caratterizza per la **forza intimidatrice del vincolo associativo**

· Lo scambio elettorale politico-mafioso implica **accordi illeciti tra politica e criminalità**

· Il sequestro di persona a scopo di estorsione consiste nella **privazione della libertà per ottenere un vantaggio**

· L'associazione finalizzata al traffico di stupefacenti riguarda **strutture organizzate dedite ad attività illecite sistematiche**

Per un'impresa, tali fattispecie rappresentano prevalentemente un **rischio di coinvolgimento indiretto**, attraverso rapporti economici con soggetti collegati alla criminalità organizzata.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il **presupposto essenziale** per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali:

· **nel cui ambito potrebbero essere commessi i reati**

· **nelle quali l'organizzazione potrebbe essere strumentalizzata**

I principali processi esposti sono:

· selezione e gestione dei fornitori

· gestione di appalti e subappalti

· rapporti con partner e intermediari

· gestione delle risorse finanziarie

· rapporti con soggetti istituzionali

· selezione del personale

Attività sensibili: aree a rischio primario

a) Selezione e gestione di fornitori, partner e intermediari

Area ad **alto rischio di infiltrazione criminale**.

Il rischio può emergere:

· nella selezione di fornitori o subappaltatori

· nella stipula di contratti con consulenti

· nella gestione di partnership

Principio guida: verifica preventiva dell'affidabilità e reputazione.

b) Gestione dei flussi finanziari

Area critica per possibili **usi illeciti delle risorse economiche**.

Il rischio può emergere:

· nei pagamenti

· nella movimentazione di fondi

· nelle operazioni economiche

Principio guida: trasparenza, tracciabilità e giustificazione economica.

c) Gestione degli appalti e delle esternalizzazioni

Area esposta al rischio di **inserimento nella filiera di soggetti illeciti**.

Il rischio può emergere:

· nella selezione di subappaltatori

· nella gestione contrattuale

· nelle esternalizzazioni

Principio guida: controllo e trasparenza dei rapporti contrattuali.

d) Gestione dei rapporti istituzionali

Area sensibile sotto il profilo **reputazionale e relazionale**.

Il rischio può emergere:

· nelle relazioni con enti pubblici

· nelle iniziative territoriali

Principio guida: correttezza e trasparenza istituzionale.

Attività strumentali

Attività che possono facilitare indirettamente il rischio:

· la selezione del personale
· la gestione dei consulenti
· le procedure di acquisto
· la gestione contratti

Esempi di criticità:

· incarichi a soggetti non qualificati
· contratti senza reale utilità economica
· rapporti opachi

Destinatari

La presente Parte Speciale si applica ad **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner commerciali, fornitori e intermediari.**

Il rispetto del Modello dipende dal **ruolo effettivo svolto**.

Principi generali di comportamento

Tutti i rapporti devono essere improntati a:

· **legalità**
· **trasparenza**
· **correttezza professionale**
· **tracciabilità**
· **responsabilità**

È espressamente vietato:

· instaurare rapporti senza verifiche
· favorire organizzazioni criminali
· partecipare ad attività illecite
· facilitare comportamenti illegali
· utilizzare l'azienda per fini criminali

Obbligo di segnalazione in caso di anomalie.

Sistema dei protocolli di controllo

La Fondazione adotta protocolli relativi a:

· selezione fornitori
· gestione appalti
· procedure di acquisto
· consulenti e intermediari

· flussi finanziari
· partnership
· rapporti istituzionali
· controlli sulla filiera

I protocolli rappresentano la **traduzione operativa dei principi di controllo**.

I controlli dell'Organismo di Vigilanza

L'**Organismo di Vigilanza (OdV)** supervisiona l'efficace attuazione della presente Parte Speciale.

In particolare:

· verifica l'applicazione dei protocolli
· monitora appalti e fornitori
· controlla i flussi finanziari
· analizza operazioni anomale
· gestisce le segnalazioni
· promuove la formazione

L'OdV può:

· richiedere documentazione
· effettuare audizioni
· redigere report periodici

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati richiede:

- **trasparenza dei rapporti economici**
- **controllo dei soggetti esterni**
- **tracciabilità finanziaria**
- **consapevolezza dei rischi**
- **cultura della legalità**

La presente Parte Speciale rappresenta una **guida operativa** per garantire che le attività aziendali siano svolte nel rispetto dei principi di: **legalità, integrità e responsabilità**

Art 25 - Peculato e corruzione

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'**art. 25 del D.Lgs. 231/2001**, concernenti i **delitti contro la Pubblica Amministrazione**, con particolare riferimento a peculato, concussione, induzione indebita e corruzione.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi ai rapporti con la Pubblica Amministrazione e con soggetti che esercitano pubbliche funzioni**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Qualsiasi impresa, indipendentemente dal settore di attività, può trovarsi a interagire con la **Pubblica Amministrazione** o con soggetti che svolgono funzioni pubbliche, ad esempio in relazione a:

· procedimenti autorizzativi
· controlli amministrativi
· rapporti con enti pubblici
· attività ispettive
· partecipazione a gare o procedure pubbliche
· gestione di rapporti contrattuali con soggetti pubblici

In tali contesti possono emergere rischi connessi a comportamenti illeciti finalizzati ad ottenere vantaggi indebiti, quali:

· offerta o promessa di utilità a pubblici ufficiali
· richiesta indebita di vantaggi da parte di funzionari pubblici
· utilizzo distorto di risorse pubbliche
· partecipazione a gare o procedure pubbliche
· intermediazione illecita nei rapporti con la Pubblica Amministrazione

La prevenzione di tali reati richiede pertanto:

· **adeguate misure organizzative**
· **procedure chiare nei rapporti con la Pubblica Amministrazione**
· **sistemi di tracciabilità delle decisioni e dei flussi finanziari**
· **una cultura dell'Ente orientata alla legalità e all'integrità**

Inquadramento normativo dei reati presupposto

L'**art. 25 del D.Lgs. 231/2001** richiama diverse fattispecie di reato previste dal codice penale.

Tra i principali reati rilevanti rientrano:

· Art. 289-bis c.p.p. – Divieto temporaneo di trattare con la Pubblica Amministrazione

· Art. 314 c.p. – Peculato

· Art. 314-bis c.p. – Indebita destinazione di denaro o cose mobili

· Art. 316 c.p. – Peculato mediante profitto dell'errore altrui

· Art. 317 c.p. – Concussione

· Art. 318 c.p. – Corruzione per l'esercizio della funzione

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

· Art. 319-ter c.p. – Corruzione in atti giudiziari

· Art. 319-quater c.p. – Induzione indebita a dare o promettere utilità

· Art. 320 c.p. – Corruzione di persona incaricata di pubblico servizio

· Art. 322 c.p. – Istigazione alla corruzione

· Art. 322-bis c.p. – Estensione a funzionari esteri e internazionali

· Art. 346-bis c.p. – Traffico di influenze illecite

Inoltre, la commissione di tali reati può comportare **sanzioni interdittive**, tra cui il **divieto temporaneo di contrattare con la Pubblica Amministrazione**, con impatti rilevanti sull'operatività dell'Ente.

In sintesi:

· Il **peculato** riguarda l'appropriazione indebita di beni pubblici da parte di un soggetto qualificato

· La **concussione** si verifica quando il pubblico ufficiale costringe il privato a dare utilità

· La **corruzione** consiste nello scambio illecito tra privato e pubblico ufficiale

· L'**induzione indebita** si basa su una pressione non coercitiva ma abusiva

· Il **traffico di influenze illecite** riguarda l'intermediazione indebita verso pubblici funzionari

· Il **divieto di contrattare con la PA** rappresenta una misura interdittiva che può limitare significativamente l'attività dell'impresa

Per un'impresa, tali fattispecie si manifestano soprattutto nei **rapporti con la Pubblica Amministrazione**, in contesti caratterizzati da discrezionalità decisionale e gestione di risorse pubbliche.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il **presupposto essenziale** per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

I principali processi esposti sono:

· gestione dei rapporti con la Pubblica Amministrazione
· partecipazione a procedimenti amministrativi
· gestione di autorizzazioni e licenze
· gestione di controlli e verifiche ispettive
· gestione di consulenti e intermediari
· gestione di omaggi, sponsorizzazioni e liberalità
· gestione dei flussi finanziari

Attività sensibili: aree a rischio primario

a) Gestione dei rapporti con la Pubblica Amministrazione

Area a **elevato rischio corruttivo**.

Il rischio può emergere:

· nei procedimenti autorizzativi
· nella richiesta di concessioni o licenze
· nella gestione dei rapporti con funzionari pubblici

Principio guida: trasparenza, correttezza e tracciabilità dei rapporti.

b) Gestione di controlli e verifiche ispettive

Area critica in presenza di **poteri autoritativi e discrezionali**.

Il rischio può emergere:

· durante verifiche fiscali o ispettive
· nei rapporti con autorità di vigilanza

Principio guida: collaborazione leale e piena trasparenza.

c) Gestione di consulenti, intermediari e rappresentanti

Area a rischio di **intermediazione illecita**.

Il rischio può emergere:

· nell'affidamento di incarichi
· nella gestione di soggetti che operano verso la PA

Principio guida: due diligence e controllo dei soggetti terzi.

d) Gestione di omaggi, liberalità e sponsorizzazioni

Area sensibile per possibili **forme indirette di corruzione**.

Il rischio può emergere:

- nella concessione di regali
- nelle sponsorizzazioni

Principio guida: modico valore, liceità e tracciabilità.

Attività strumentali

Attività che possono agevolare condotte illecite:

- gestione dei flussi finanziari
- spese di rappresentanza
- procedure di acquisto
- relazioni istituzionali
- selezione del personale

Esempi di criticità:

- fondi non tracciati
- fatturazioni fittizie
- incarichi privi di utilità

Destinatari

La presente Parte Speciale si applica ad **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner e intermediari**

Il rispetto del Modello dipende dal **ruolo effettivo svolto**.

Principi generali di comportamento

I rapporti con la Pubblica Amministrazione devono essere improntati a:

- **legalità**
- **trasparenza**
- **correttezza professionale**
- **tracciabilità**

È espressamente vietato:

- offrire o promettere utilità indebite
- accettare richieste illecite
- utilizzare intermediari per fini illeciti

· influenzare indebitamente decisioni pubbliche
· creare fondi occulti

Obbligo di segnalazione in caso di comportamenti anomali.

Sistema dei protocolli di controllo

La Fondazione adotta protocolli relativi a:

· rapporti con la Pubblica Amministrazione
· autorizzazioni e licenze
· verifiche ispettive
· consulenti e intermediari
· spese di rappresentanza
· omaggi e sponsorizzazioni
· flussi finanziari
· rapporti istituzionali

I protocolli rappresentano la **traduzione operativa dei presidi di controllo**.

I controlli dell'Organismo di Vigilanza

L'**Organismo di Vigilanza (OdV)** vigila sull'efficace attuazione della presente Parte Speciale.

In particolare:

· verifica l'applicazione dei protocolli
· monitora i rapporti con la PA
· controlla verifiche ispettive e procedimenti
· analizza consulenti e intermediari
· verifica omaggi e spese
· controlla i flussi finanziari
· gestisce le segnalazioni
· promuove la formazione

L'OdV può:

· richiedere documentazione
· effettuare audizioni
· redigere report periodici

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati richiede:

- **trasparenza nei rapporti con la PA**
- **tracciabilità delle decisioni**
- **controllo dei soggetti terzi**
- **formazione continua**
- **cultura dell'integrità**

La presente Parte Speciale rappresenta una **guida operativa** per garantire che i rapporti con la Pubblica Amministrazione siano gestiti nel rispetto dei principi di: **legalità, correttezza e trasparenza**.

Art 25-bis - Falsità in monete

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai **reati presupposto di cui all'art. 25-bis del D.Lgs. 231/2001**, concernenti le fattispecie di falsificazione e utilizzo illecito di monete, carte di pubblico credito, valori di bollo, marchi e segni distintivi, nonché l'indebito utilizzo di strumenti di pagamento.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla circolazione e all'utilizzo di strumenti di pagamento, valori e segni distintivi**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Nel contesto economico attuale, tutte le organizzazioni gestiscono quotidianamente:

- flussi finanziari
- strumenti di pagamento
- documentazione commerciale
- prodotti contraddistinti da marchi o segni distintivi
- relazioni economiche con fornitori, clienti e intermediari

In tali contesti possono emergere rischi connessi a comportamenti illeciti quali:

- utilizzo o circolazione di moneta contraffatta
- utilizzo di valori di bollo falsificati
- utilizzo illecito di marchi o segni distintivi
- commercializzazione di prodotti con segni falsi
- utilizzo fraudolento di strumenti di pagamento

La prevenzione di tali reati richiede pertanto:

- adeguate **procedure di controllo sui flussi finanziari**
- sistemi di **verifica dei fornitori e dei prodotti acquistati**
- **tracciabilità delle operazioni economiche**
- una diffusa **cultura dell'Ente orientata alla legalità e alla tutela della proprietà industriale**

Inquadramento normativo dei reati presupposto

L'art. 25-bis del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal codice penale.

Tra i principali reati rilevanti rientrano:

- Art. 453 c.p. – Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate
- Art. 454 c.p. – Alterazione di monete
- Art. 455 c.p. – Spendita e introduzione nello Stato, senza concerto, di monete falsificate
- Art. 457 c.p. – Spendita di monete falsificate ricevute in buona fede

- Art. 459 c.p. – Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione e messa in circolazione di valori falsificati
- Art. 460 c.p. – Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo
- Art. 461 c.p. – Fabbricazione o detenzione di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata
- Art. 464 c.p. – Uso di valori di bollo contraffatti o alterati
- Art. 473 c.p. – Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni
- Art. 474 c.p. – Introduzione nello Stato e commercio di prodotti con segni falsi
- Art. 493-ter c.p. – Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti
- Art. 512-bis c.p. – Trasferimento fraudolento di valori

In sintesi:

- i reati di **falsificazione di monete e valori di bollo** riguardano la produzione, l'alterazione o la messa in circolazione di strumenti monetari o valori pubblici contraffatti
- i reati relativi ai **marchi e segni distintivi** riguardano la contraffazione o l'utilizzo illecito di marchi, brevetti, modelli o disegni tutelati
- il reato di **commercio di prodotti con segni falsi** si verifica quando vengono commercializzati prodotti che riportano marchi contraffatti o non autorizzati
- l'**indebito utilizzo di strumenti di pagamento** riguarda l'uso fraudolento di carte o altri strumenti elettronici di pagamento
- il **trasferimento fraudolento di valori** consiste nell'attribuzione fittizia della titolarità di beni o valori allo scopo di eludere la legge

Per qualsiasi impresa, tali fattispecie non rappresentano rischi esclusivamente teorici, ma ipotesi concretamente configurabili soprattutto nelle attività connesse alla **gestione dei pagamenti, alla commercializzazione di prodotti e alla gestione dei marchi e segni distintivi**.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione economica, alcune attività possono risultare maggiormente esposte al rischio di commissione di tali reati.

Tra queste:

- gestione dei pagamenti e degli incassi
- gestione degli strumenti di pagamento elettronici
- gestione dei rapporti con fornitori e distributori
- acquisto e commercializzazione di prodotti

- gestione di marchi e segni distintivi
- gestione della documentazione commerciale

Tale contesto richiede una valutazione attenta dei rischi connessi alla possibile introduzione nel circuito dell'Ente di strumenti monetari o prodotti contraffatti.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione dei pagamenti e degli incassi

La gestione dei flussi finanziari rappresenta una delle aree potenzialmente esposte al rischio di utilizzo di strumenti monetari o di pagamento falsificati.

Il rischio può emergere:

- nella gestione di pagamenti in contanti
- nella ricezione di incassi
- nella gestione di strumenti di pagamento elettronici
- nella gestione di carte di pagamento aziendali

L'utilizzo o la messa in circolazione di moneta falsificata o di strumenti di pagamento contraffatti può integrare le fattispecie di reato previste dalla normativa.

Principio guida: controllo e tracciabilità delle operazioni finanziarie e degli strumenti di pagamento utilizzati.

b) Gestione degli acquisti e dei rapporti con i fornitori

Il rischio di commercializzazione di prodotti contraffatti può emergere nelle attività di acquisto e approvvigionamento.

Il rischio può manifestarsi:

- nella selezione dei fornitori
- nell'acquisto di prodotti o componenti
- nella gestione della catena di distribuzione
- nella commercializzazione di prodotti

L'introduzione nel circuito commerciale di prodotti con marchi falsi può integrare le fattispecie di contraffazione o commercio di prodotti con segni falsi.

Principio guida: accurata verifica dell'affidabilità dei fornitori e dell'autenticità dei prodotti acquistati.

c) Gestione dei marchi, dei segni distintivi e della proprietà industriale

Le imprese possono essere titolari o utilizzatrici di marchi, brevetti, modelli o altri segni distintivi.

Il rischio può emergere:

- nell'utilizzo non autorizzato di marchi
- nella riproduzione non autorizzata di segni distintivi
- nella commercializzazione di prodotti con marchi non autentici

Principio guida: rispetto dei diritti di proprietà industriale e verifica della legittimità dell'utilizzo dei segni distintivi.

d) Gestione degli strumenti di pagamento elettronici

La diffusione di strumenti di pagamento digitali espone le organizzazioni al rischio di utilizzo fraudolento di tali strumenti.

Il rischio può emergere:

- nell'utilizzo di carte aziendali
- nella gestione dei pagamenti elettronici
- nella gestione di piattaforme di pagamento online

Principio guida: utilizzo responsabile e controllato degli strumenti di pagamento elettronici.

Attività strumentali

Anche alcune attività interne possono assumere rilievo strumentale rispetto ai reati sopra descritti.

Tra queste rientrano, ad esempio:

- la gestione delle procedure di acquisto
- la gestione dei pagamenti e della contabilità
- la gestione delle relazioni commerciali
- la gestione della documentazione commerciale

Esempi di criticità:

- l'acquisto di prodotti senza adeguata verifica del fornitore
- la gestione non tracciata dei pagamenti
- l'utilizzo di marchi senza autorizzazione

possono facilitare la commissione dei reati previsti dall'art. 25-bis.

Pertanto, il rischio deve essere valutato **lungo l'intero ciclo delle operazioni economiche e commerciali dell'organizzazione**.

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti, fornitori, partner commerciali**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivamente svolto nei processi aziendali connessi alla gestione delle operazioni economiche e commerciali**.

Principi generali di comportamento

Tutte le attività aziendali devono essere improntate ai principi di:

- **legalità**
- **trasparenza**
- **tracciabilità delle operazioni**

- **correttezza nei rapporti commerciali**
- **rispetto dei diritti di proprietà industriale**

È espressamente vietato:

- utilizzare o mettere in circolazione monete o valori falsificati
- utilizzare valori di bollo contraffatti o alterati
- commercializzare prodotti con marchi o segni distintivi falsi
- utilizzare marchi o brevetti senza autorizzazione
- utilizzare strumenti di pagamento in modo fraudolento
- porre in essere operazioni finalizzate al trasferimento fraudolento di valori

Ogni dipendente o collaboratore che rilevi **anomalie o situazioni sospette nella gestione dei pagamenti, dei prodotti o dei marchi** è tenuto a segnalarle attraverso i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- la gestione dei pagamenti e degli incassi
- la gestione degli strumenti di pagamento elettronici
- la selezione e qualifica dei fornitori
- la gestione delle procedure di acquisto
- la gestione dei marchi e dei segni distintivi
- la gestione della documentazione commerciale
- i controlli sulla catena di distribuzione dei prodotti

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV), istituito ai sensi dell'art. 6 del D.Lgs. 231/2001, cui è attribuito il compito di verificare il funzionamento, l'osservanza e l'aggiornamento del Modello.

Con specifico riferimento ai reati di cui all'art. 25-bis del D.Lgs. 231/2001, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi alla gestione dei flussi finanziari, degli strumenti di pagamento, dei rapporti commerciali e della gestione dei marchi e segni distintivi, al fine di prevenire il rischio di introduzione o utilizzo di strumenti o prodotti contraffatti.

In particolare, l'OdV:

• verifica, anche a campione, la corretta applicazione dei protocolli relativi alla gestione dei pagamenti e degli incassi, con particolare attenzione alla tracciabilità delle operazioni e all'utilizzo degli strumenti di pagamento

• monitora la gestione degli strumenti di pagamento elettronici, incluse carte aziendali e piattaforme digitali, al fine di rilevare eventuali utilizzi anomali o non autorizzati

• controlla i processi di selezione e qualifica dei fornitori, verificando l'adeguatezza delle procedure di due diligence e l'affidabilità dei soggetti coinvolti nella catena di approvvigionamento

• verifica i processi di acquisto e commercializzazione dei prodotti, al fine di accertare:

- la provenienza lecita dei beni
- l'autenticità dei prodotti e dei relativi marchi
- la coerenza tra documentazione commerciale e operazioni effettuate

• monitora la gestione dei marchi, dei segni distintivi e dei diritti di proprietà industriale, verificando la legittimità dell'utilizzo e l'assenza di utilizzi non autorizzati

• controlla la gestione della documentazione commerciale e amministrativa, al fine di accertarne la correttezza, completezza e tracciabilità

• verifica la coerenza e la tracciabilità dei flussi finanziari, al fine di individuare eventuali operazioni anomale o prive di adeguata giustificazione economica

• analizza eventuali segnalazioni (whistleblowing) relative a comportamenti sospetti, quali utilizzo di strumenti di pagamento irregolari, presenza di prodotti contraffatti o utilizzo illecito di marchi, garantendo la riservatezza del segnalante e promuovendo le opportune verifiche

• promuove iniziative di formazione e sensibilizzazione del personale sui rischi connessi ai reati di falsificazione, contraffazione e utilizzo illecito di strumenti di pagamento

L'OdV può richiedere alle funzioni aziendali competenti la trasmissione di documentazione contabile, contrattuale e commerciale, nonché ogni altra informazione rilevante ai fini delle attività di vigilanza, oltre a effettuare audizioni del personale coinvolto nei processi sensibili.

Particolare rilevanza assumono i flussi informativi periodici verso l'OdV, che devono includere, tra l'altro:

· dati relativi ai pagamenti e agli incassi effettuati

· utilizzo degli strumenti di pagamento aziendali

· elenco dei fornitori qualificati e relative verifiche effettuate

· informazioni sulla provenienza e autenticità dei prodotti commercializzati

· segnalazioni di anomalie nella gestione dei flussi finanziari o dei prodotti

· esiti di eventuali controlli interni sulla catena di approvvigionamento

Gli esiti delle attività di controllo sono oggetto di report periodici agli organi societari competenti, contenenti eventuali criticità riscontrate, raccomandazioni e proposte di miglioramento del sistema di controllo interno.

In presenza di violazioni accertate, anomalie significative o carenze nei presidi organizzativi, l'OdV propone l'adozione di misure correttive, nonché l'eventuale attivazione del sistema disciplinare.

L'attività dell'Organismo di Vigilanza costituisce pertanto un presidio essenziale per la prevenzione dei reati di cui all'art. 25-bis, contribuendo al rafforzamento della trasparenza, della tracciabilità e della correttezza nelle operazioni economiche e commerciali, nonché alla tutela della proprietà industriale e dei sistemi di pagamento.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati previsti dall'art. 25-bis richiede un approccio organizzativo fondato su:

- **controllo dei flussi finanziari**
- **verifica dell'affidabilità dei partner commerciali**
- **tutela della proprietà industriale**
- **tracciabilità delle operazioni economiche**
- **diffusione di una cultura dell'Ente orientata alla legalità**

La presente Parte Speciale deve pertanto essere intesa non solo come uno strumento di conformità normativa, ma come **una guida operativa per garantire la correttezza e la trasparenza delle attività economiche e commerciali svolte dall'organizzazione.**

Art 25-bis.1 - Delitti contro l'industria

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai **reati presupposto di cui all'art. 25-bis.1 del D.Lgs. 231/2001**, concernenti i delitti contro l'industria e il commercio.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi allo svolgimento delle attività economiche e commerciali**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Nel contesto economico e competitivo attuale, le imprese operano all'interno di mercati caratterizzati da rapporti complessi con clienti, fornitori, concorrenti e partner commerciali.

Tali relazioni possono esporre le organizzazioni al rischio di commissione di reati che incidono sulla **libertà dell'industria e del commercio**, sulla **correttezza delle pratiche commerciali** e sulla **tutela dei consumatori,** sulla **leale concorrenza** e, con particolare riferimento al settore alimentare, sulla genuinità, qualità, provenienza e tracciabilità dei prodotti.

In particolare, tali rischi possono emergere in relazione a:

- attività di produzione e commercializzazione di beni o servizi
- produzione, trasformazione, distribuzione e vendita di prodotti alimentari
- gestione dei rapporti con clienti, fornitori, distributori e partner commerciali
- utilizzo di marchi, segni distintivi, indicazioni geografiche e denominazioni di origine
- gestione delle attività commerciali, promozionali e di marketing
- rapporti con concorrenti e operatori del mercato
- gestione della qualità, della conformità e della tracciabilità dei prodotti

La prevenzione dei reati contro l'industria e il commercio richiede pertanto:

- adeguate **procedure di controllo delle attività commerciali**
- sistemi di **verifica della qualità, della conformità e della tracciabilità dei prodotti**
- corrette **procedure di utilizzo dei marchi, dei segni distintivi e delle indicazioni geografiche protette**
- **trasparenza nelle pratiche commerciali e nelle informazioni rese al mercato**
- efficaci s**istemi di controllo della filiera produttiva e distributiva**
- una **diffusa cultura dell'Ente orientata alla correttezza nei rapporti commerciali, alla tutela dei consumatori e alla valorizzazione della qualità dei prodotti**

Inquadramento normativo dei reati presupposto

L'art. 25-bis.1 del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal codice penale in materia di tutela dell'industria e del commercio.

Tra i principali reati rilevanti rientrano:

- Art. 513 c.p. – Turbata libertà dell'industria o del commercio
- Art. 513-bis c.p. – Illecita concorrenza con minaccia o violenza
- Art. 514 c.p. – Frodi contro le industrie nazionali

- Art. 515 c.p. – Frode nell'esercizio del commercio
- Art. 517 c.p. – Vendita di prodotti industriali con segni mendaci
- Art. 517-ter c.p. – Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale
- Art. 517-quater c.p. – Contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari
- Art. 517-sexies c.p. – Frode alimentare
- Art. 517-septies c.p. – Commercio di alimenti con segni mendaci
- Art. 517-octies c.p. – Pena accessoria e circostanze aggravanti

In sintesi:

- il reato di **turbata libertà dell'industria o del commercio** si verifica quando vengono utilizzati mezzi fraudolenti idonei a impedire o turbare il normale svolgimento delle attività economiche
- l'**illecita concorrenza con minaccia o violenza** riguarda comportamenti finalizzati ad ostacolare l'attività economica di concorrenti mediante intimidazione o coercizione
- la **frode nell'esercizio del commercio** consiste nella consegna al cliente di un prodotto diverso per origine, provenienza, qualità, quantità o altre caratteristiche essenziali, rispetto a quanto dichiarato o pattuito
- la **vendita di prodotti con segni mendaci** riguarda l'utilizzo di indicazioni, marchi o segni distintivi idonei a trarre in inganno il consumatore sull'origine, provenienza o qualità del prodotto
- i reati relativi alla **proprietà industriale** riguardano la fabbricazione o il commercio di beni realizzati in violazione di marchi, brevetti o altri diritti di proprietà industriale
- la **contraffazione** dei segni di indicazione geografica e di denominazione protetta riguarda l'utilizzo abusivo o ingannevole delle indicazioni geografiche e delle denominazioni di origine protette previste dalla normativa nazionale ed europea
- la **frode alimentare** riguarda le condotte fraudolente poste in essere nella produzione, trasformazione, commercializzazione o distribuzione degli alimenti, idonee a compromettere la genuinità, la qualità, la sicurezza o la corretta informazione del consumatore
- il **commercio di alimenti con segni mendaci** riguarda la commercializzazione di prodotti alimentari recanti indicazioni, segni, denominazioni o altre informazioni idonee a indurre in errore il consumatore in ordine alla provenienza, qualità, composizione o caratteristiche del prodotto
- le **circostanze aggravanti e le pene accessorie** previste dall'art. 517-octies assumono rilievo nelle ipotesi di particolare gravità delle condotte o di maggiore offensività nei confronti del mercato e dei consumatori

Per qualsiasi impresa operante nel mercato, tali fattispecie rappresentano rischi concretamente configurabili nelle attività connesse alla **produzione, trasformazione, commercializzazione, distribuzione e promozione di beni o servizi** e richiedono l'adozione di efficaci sistemi organizzativi, di controllo e di tracciabilità idonei a prevenire comportamenti illeciti.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione economica, il rischio di commissione di reati contro l'industria e il commercio può emergere in relazione a processi quali:

- produzione e commercializzazione di beni o servizi
- gestione delle attività di vendita
- gestione dei rapporti con clienti, fornitori, distributori e partner commerciali
- gestione della qualità, della conformità e della tracciabilità dei prodotti
- gestione dei marchi, dei segni distintivi, delle indicazioni geografiche e delle denominazioni di origine
- attività di marketing e comunicazione commerciale
- gestione della filiera produttiva e distributiva

Tali attività richiedono particolare attenzione al fine di garantire **correttezza nei rapporti di mercato, tutela dei consumatori, trasparenza delle informazioni commerciali e conformità dei prodotti alla normativa applicabile.**

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Produzione e commercializzazione di beni e servizi

Le attività di produzione e vendita rappresentano uno dei principali ambiti di rischio.

Il rischio può emergere:

- nella descrizione delle caratteristiche dei prodotti o servizi
- nella gestione delle specifiche qualitative dei prodotti
- nella consegna dei prodotti ai clienti
- nella commercializzazione di prodotti non conformi alle caratteristiche dichiarate

La consegna di prodotti diversi da quelli dichiarati o la fornitura di informazioni non veritiere può integrare la fattispecie di frode nell'esercizio del commercio.

Principio guida: piena corrispondenza tra quanto dichiarato al cliente e quanto effettivamente fornito.

b) Gestione dei marchi, dei segni distintivi e delle indicazioni geografiche

Le imprese possono utilizzare marchi, segni distintivi, indicazioni geografiche e denominazioni di origine nella produzione e commercializzazione dei propri prodotti.

Il rischio può emergere:

- nell'utilizzo improprio di marchi o segni distintivi
- nella riproduzione non autorizzata di titoli di proprietà industriale
- nell'utilizzo illecito di indicazioni geografiche o denominazioni di origine protette
- nell'impiego di segni o indicazioni idonei ad indurre in errore il consumatore

Principio guida: rispetto dei diritti di proprietà industriale e correttezza nell'utilizzo dei marchi, dei segni distintivi e delle indicazioni protette.

c) Gestione delle relazioni commerciali e della concorrenza

Le imprese operano in un contesto competitivo che richiede comportamenti improntati a correttezza e lealtà commerciale.

Il rischio può emergere:

- nella gestione dei rapporti con concorrenti
- nella gestione delle strategie commerciali
- nella gestione delle relazioni con distributori, intermediari o partner commerciali
- nell'adozione di pratiche commerciali scorrette idonee ad alterare il libero mercato

Comportamenti idonei ad ostacolare l'attività economica di concorrenti mediante mezzi fraudolenti, intimidatori o coercitivi **possono integrare le fattispecie di turbata libertà dell'industria o del commercio o di illecita concorrenza con minaccia o violenza.**

Principio guida: rispetto delle regole della concorrenza e correttezza nei rapporti di mercato.

d) Gestione della qualità, **della conformità e della tracciabilità dei prodotti**

La qualità, la conformità e la tracciabilità dei prodotti rappresentano elementi essenziali per la tutela dei consumatori e la correttezza delle attività commerciali.

Il rischio può emergere:

- nella gestione dei controlli di qualità
- nella gestione della tracciabilità dei prodotti
- nella gestione delle informazioni relative alla composizione, provenienza o caratteristiche dei prodotti
- nella gestione della documentazione attestante la conformità dei prodotti

Il principio guida è: garanzia della qualità, della conformità e della completa tracciabilità dei prodotti rispetto alle caratteristiche dichiarate.

e) Produzione e commercializzazione dei prodotti alimentari

Per le imprese operanti, anche indirettamente, nella filiera agroalimentare, particolare rilievo assumono le attività relative alla produzione, trasformazione, distribuzione e commercializzazione degli alimenti.

Il rischio può emergere:

- nella commercializzazione di alimenti recanti indicazioni false o ingannevoli
- nella gestione non conforme delle informazioni relative alla provenienza, composizione o qualità degli alimenti
- nell'utilizzo improprio di indicazioni geografiche o denominazioni di origine protette
- nella distribuzione di prodotti alimentari non conformi alla normativa applicabile

Le condotte fraudolente nella filiera alimentare possono integrare le fattispecie di frode alimentare o di commercio di alimenti con segni mendaci.

Principio guida: assicurare la genuinità, la qualità, la sicurezza, la corretta identificazione e la piena tracciabilità dei prodotti alimentari.

Attività strumentali

Anche alcune attività interne possono assumere rilievo strumentale rispetto ai reati sopra descritti.

Tra queste rientrano, ad esempio:

- la selezione e gestione dei fornitori
- la gestione delle procedure di acquisto
- la gestione della documentazione commerciale
- la gestione della documentazione tecnica relativa ai prodotti
- la gestione delle attività di marketing e comunicazione
- la gestione dei sistemi di controllo della qualità
- la gestione della tracciabilità dei prodotti e della filiera

Esempi di criticità:

- l'acquisto di prodotti o componenti privi di adeguata tracciabilità
- la diffusione di informazioni commerciali non veritiere o ingannevoli
- l'utilizzo non autorizzato di marchi, segni distintivi o indicazioni geografiche
- la carente gestione dei controlli di qualità
- l'inadeguata verifica della conformità dei prodotti

Tali situazioni possono agevolare la commissione dei reati previsti dall'art. 25-bis.1 del D.Lgs. 231/2001.

Pertanto, il rischio deve essere valutato **lungo l'intera filiera produttiva, commerciale e distributiva dell'organizzazione.**

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner commerciali, fornitori, distributori e ogni altro soggetto coinvolto nei processi produttivi, commerciali o promozionali dell'organizzazione.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivamente svolto nei processi aziendali connessi alle attività commerciali, produttive e di gestione della qualità dei prodotti.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità**
- **correttezza commerciale**
- **trasparenza nei rapporti con clienti, fornitori, distributori e partner commerciali**
- **tutela dei consumatori**
- **rispetto della proprietà industriale e dei diritti di terzi**
- **correttezza nell'utilizzo dei marchi, dei segni distintivi, delle indicazioni geografiche e delle denominazioni di origine protette**

- **qualità, conformità e tracciabilità dei prodotti**
- **lealtà nei rapporti con concorrenti e operatori economici**

È espressamente vietato:

- porre in essere comportamenti idonei ad ostacolare la libertà dell'industria o del commercio
- utilizzare minacce, violenza o indebite pressioni nei rapporti con concorrenti o operatori economici
- vendere o consegnare prodotti diversi per qualità, origine, provenienza, composizione, caratteristiche o quantità rispetto a quanto dichiarato o pattuito
- utilizzare marchi, brevetti, segni distintivi o altri diritti di proprietà industriale senza autorizzazione
- utilizzare indicazioni geografiche, denominazioni di origine protette o altri segni distintivi in modo ingannevole o non conforme alla normativa
- commercializzare prodotti recanti indicazioni false o idonee ad indurre in errore il consumatore
- porre in essere condotte fraudolente nella produzione, trasformazione, distribuzione o commercializzazione di prodotti alimentari
- diffondere informazioni commerciali non veritiere o comunque idonee ad alterare le corrette dinamiche del mercato

Ogni dipendente o collaboratore che rilevi **situazioni anomale, violazioni delle procedure aziendali o comportamenti potenzialmente ingannevoli nelle attività commerciali è tenuto a segnalarle attraverso i canali previsti dal Modello.**

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- a gestione delle attività commerciali
- la gestione della qualità, della conformità e della tracciabilità dei prodotti
- la gestione della filiera produttiva e distributiva
- la gestione dei marchi, dei segni distintivi, delle indicazioni geografiche e delle denominazioni di origine
- la gestione delle attività di marketing e comunicazione commerciale
- la selezione, qualificazione e monitoraggio dei fornitori e dei partner commerciali
- la gestione della documentazione commerciale e tecnica relativa ai prodotti
- la gestione dei controlli di qualità e delle verifiche di conformità
- la gestione dei reclami, delle non conformità e delle eventuali azioni correttive

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I protocolli devono garantire, in particolare:

- la tracciabilità delle attività commerciali e produttive
- la verificabilità delle informazioni rese ai clienti e al mercato
- la corretta gestione della documentazione relativa ai prodotti
- il rispetto della normativa in materia di proprietà industriale e tutela delle indicazioni geografiche

- adeguati livelli di controllo lungo l'intera filiera produttiva e commerciale
- la tempestiva gestione delle anomalie e delle non conformità riscontrate

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV), istituito ai sensi dell'art. 6 del D.Lgs. 231/2001, cui è attribuito il compito di verificare il funzionamento, l'osservanza e l'aggiornamento del Modello.

Con specifico riferimento ai reati di cui all'art. 25-bis.1 del D.Lgs. 231/2001, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi alla produzione, trasformazione, commercializzazione e promozione di beni e servizi, nonché sulla gestione dei rapporti con clienti, fornitori, distributori, partner commerciali e concorrenti, al fine di prevenire comportamenti idonei a compromettere la correttezza delle pratiche commerciali, la tutela dei consumatori, la libertà del mercato e la conformità dei prodotti alla normativa applicabile.

In particolare, l'OdV:

• verifica, anche a campione, la corretta applicazione dei protocolli relativi alla gestione delle attività commerciali, con particolare attenzione alla veridicità, completezza e trasparenza delle informazioni fornite ai clienti e al mercato

• monitora i processi di produzione, trasformazione, commercializzazione e distribuzione dei prodotti, al fine di accertare la coerenza tra le caratteristiche dichiarate e quanto effettivamente offerto o consegnato

• controlla la gestione della qualità, della conformità e della tracciabilità dei prodotti, verificando l'efficacia dei sistemi di controllo interno, la completezza della documentazione e la rispondenza alle specifiche dichiarate

• verifica la gestione dei marchi, dei segni distintivi, delle indicazioni geografiche e delle denominazioni di origine protette, accertando:

- la legittimità dell'utilizzo
- il rispetto dei diritti di proprietà industriale
- l'assenza di utilizzi ingannevoli o non autorizzati

• monitora le attività di marketing e comunicazione commerciale, al fine di verificare la correttezza, trasparenza e la non ingannevolezza delle informazioni diffuse al mercato

• controlla i rapporti con fornitori, distributori e partner commerciali, verificando l'adeguatezza delle procedure di selezione, qualificazione e monitoraggio, nonché la coerenza delle relazioni commerciali con i principi di correttezza e trasparenza

• monitora le relazioni con concorrenti e operatori economici, al fine di rilevare eventuali comportamenti anomali o non conformi ai principi della leale concorrenza

• verifica, ove applicabile, l'efficacia dei controlli adottati lungo la filiera produttiva e distributiva, con particolare riguardo alla qualità, conformità, identificazione e tracciabilità dei prodotti alimentari

• analizza eventuali segnalazioni (whistleblowing) relative a pratiche commerciali scorrette, comportamenti fraudolenti, utilizzi impropri di marchi, segni distintivi, indicazioni geografiche o denominazioni di origine protette, nonché a possibili violazioni della normativa in materia di

prodotti alimentari, garantendo la riservatezza del segnalante e promuovendo le opportune verifiche

• promuove iniziative di formazione e sensibilizzazione del personale sui rischi connessi ai reati contro l'industria e il commercio, con particolare riguardo alla tutela della proprietà industriale, alla correttezza delle pratiche commerciali, alla qualità dei prodotti e alla prevenzione delle frodi alimentari

L'OdV può richiedere alle funzioni aziendali competenti la trasmissione di documentazione commerciale, contrattuale e tecnica, nonché ogni altra informazione rilevante ai fini delle attività di vigilanza, oltre a effettuare audizioni del personale coinvolto nei processi sensibili.

Particolare rilevanza assumono i flussi informativi periodici verso l'OdV, che devono includere, tra l'altro:

- informazioni sulle attività commerciali e sulle campagne di marketing
- dati relativi alla qualità, conformità e tracciabilità dei prodotti
- informazioni sull'utilizzo dei marchi, dei segni distintivi, delle indicazioni geografiche e delle denominazioni di origine protette
- segnalazioni di non conformità, reclami dei clienti o contestazioni relative ai prodotti commercializzati
- informazioni sui rapporti con fornitori, distributori, partner commerciali e altri operatori della filiera
- esiti dei controlli interni sulla qualità, conformità e tracciabilità dei prodotti
- eventuali provvedimenti, contestazioni o verifiche da parte delle Autorità competenti

Gli esiti delle attività di controllo sono oggetto di report periodici agli organi societari competenti, contenenti eventuali criticità riscontrate, raccomandazioni e proposte di miglioramento del sistema di controllo interno.

In presenza di violazioni accertate, anomalie significative o carenze nei presidi organizzativi, l'OdV propone l'adozione delle opportune misure correttive, nonché l'eventuale attivazione del sistema disciplinare.

L'attività dell'Organismo di Vigilanza costituisce pertanto un presidio essenziale per la prevenzione dei reati di cui all'art. 25-bis.1 del D.Lgs. 231/2001, contribuendo al rafforzamento della correttezza commerciale, della trasparenza nei rapporti di mercato, della tutela dei consumatori, della protezione dei diritti di proprietà industriale e della conformità dei prodotti alle disposizioni normative applicabili.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati contro l'industria e il commercio richiede un approccio organizzativo fondato su:

- **trasparenza nelle pratiche commerciali**
- **controllo della qualità, della conformità e della tracciabilità dei prodotti**
- **rispetto dei diritti di proprietà industriale, delle indicazioni geografiche e delle denominazioni di origine protette**
- **correttezza nei rapporti con clienti, fornitori, concorrenti e operatori di mercato**
- **controllo della filiera produttiva e distributiva**

- **diffusione di una cultura dell'Ente orientata alla legalità, alla tutela dei consumatori e alla valorizzazione della qualità dei prodotti**

La presente Parte Speciale deve pertanto essere intesa non solo come uno strumento di conformità normativa, ma come **una guida operativa per garantire che le attività economiche e commerciali dell'organizzazione siano svolte nel pieno rispetto dei principi di correttezza, trasparenza, lealtà nel mercato e tutela dei consumatori, promuovendo la qualità, la sicurezza e la conformità dei prodotti lungo l'intera filiera produttiva e commerciale.**

Art 25-ter - Reati societari

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai **reati presupposto di cui all'art. 25-ter del D.Lgs. 231/2001**, concernenti i reati societari.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione della Fondazione, alla redazione di bilanci e alla conduzione delle operazioni dell'Ente**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività societarie e gestionali**

Nel contesto economico e competitivo attuale, le imprese operano in mercati caratterizzati da rapporti complessi con soci, amministratori, organi di controllo, creditori, partner commerciali e autorità di vigilanza.

Tali relazioni possono esporre le organizzazioni al rischio di commissione di reati che incidono sulla correttezza della gestione societaria, sulla trasparenza dei bilanci, sulla tutela dei soci e dei creditori.

In particolare, tali rischi possono emergere in relazione a:

- redazione e approvazione dei bilanci e delle comunicazioni
- gestione dei conferimenti, degli utili e delle riserve
- operazioni straordinarie e rapporti con soci e organi di controllo
- gestione dei conflitti di interesse
- relazioni con partner commerciali, società controllate e autorità di vigilanza
- operazioni finanziarie e patrimoniali interne

La prevenzione dei reati societari richiede pertanto:

- procedure di controllo interne e sistemi di verifica della correttezza dei bilanci e delle operazioni societarie
- trasparenza e tracciabilità delle operazioni societarie e finanziarie
- cultura dell'Ente orientata all'integrità e alla correttezza nei rapporti societari

Inquadramento normativo dei reati presupposto

L'art. 25-ter del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal codice civile e da norme speciali in materia societaria.

Tra i principali reati rilevanti rientrano:

- Art. 2621 c.c. – False comunicazioni sociali
- Art. 2622 c.c. – False comunicazioni sociali in danno della società, dei soci o dei creditori
- Art. 2625 c.c. – Impedito controllo
- Art. 2626 c.c. – Indebita restituzione dei conferimenti
- Art. 2627 c.c. – Illegale ripartizione degli utili e delle riserve

- Art. 2628 c.c. – Illecite operazioni sulle azioni o quote sociali o della società controllante
- Art. 2629 c.c. – Operazioni in pregiudizio dei creditori
- Art. 2629-bis c.c. – Omessa comunicazione del conflitto di interessi
- Art. 2632 c.c. – Formazione fittizia del capitale
- Art. 2633 c.c. – Indebita ripartizione dei beni sociali da parte dei liquidatori
- Art. 2635 c.c. – Corruzioni tra privati
- Art. 2635-bis c.c. – Istigazione alla corruzione tra privati
- Art. 2636 c.c. – Illecita influenza sull'assemblea
- Art. 2637 c.c. – Aggiotaggio
- Art. 2638 c.c. – Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza
- Art. 54 D.Lgs. 19/03/2023 – False o omesse dichiarazioni per il rilascio del certificato preliminare

In sintesi:

- le **false comunicazioni sociali** si verificano quando informazioni contenute in bilanci o relazioni societarie non rispecchiano la realtà patrimoniale o economica della Fondazione
- l'**impedito controllo** riguarda comportamenti volti a ostacolare l'attività di controllo di revisori e collegio sindacale
- la **ripartizione illecita di utili, conferimenti o beni sociali** può arrecare danno a soci o creditori
- l'**illecita influenza sull'assemblea**, le **operazioni in conflitto di interessi** compromettono equità e trasparenza della Fondazione
- la **corruzione tra privati** e l'**istigazione alla corruzione** configurano comportamenti illeciti tra soggetti privati
- le **false dichiarazioni per certificazioni preliminari** possono determinare vantaggi indebiti e pregiudizio per terzi

Per qualsiasi impresa, tali fattispecie rappresentano rischi concretamente configurabili nelle attività connesse alla gestione societaria, operazioni patrimoniali e finanziarie, redazione di bilanci e comunicazioni ai soci.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.
In qualsiasi organizzazione economica, il rischio di commissione di reati societari può emergere in relazione a processi quali:

- redazione e approvazione dei bilanci e delle relazioni
- gestione dei conferimenti, utili e riserve
- operazioni straordinarie e rapporti con soci, amministratori e organi di controllo
- gestione dei conflitti di interesse
- gestione delle relazioni con partner commerciali e società controllate

- gestione della tracciabilità dei flussi patrimoniali e finanziari

Tali attività richiedono particolare attenzione al fine di garantire trasparenza, correttezza e tutela dei soci e dei creditori.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Redazione e approvazione dei bilanci e delle comunicazioni

Il rischio può emergere:

- nella presentazione di dati contabili e patrimoniali non veritieri
- nella compilazione di relazioni societarie o bilanci infedeli
- nella trasmissione di informazioni incomplete a soci o creditori

Principio guida: piena corrispondenza tra quanto riportato nei documenti sociali e la reale situazione economico-patrimoniale.

b) Gestione dei conferimenti, utili e riserve

Il rischio può emergere:

- nella distribuzione illecita di utili o riserve
- nell'indebita restituzione di conferimenti
- nella formazione fittizia del capitale

Principio guida: rispetto delle norme civilistiche e tutela dei creditori.

c) Operazioni societarie e rapporti con organi di controllo

Il rischio può emergere:

- in operazioni societarie che ledono il patrimonio o i diritti dei soci
- nella mancata dichiarazione dei conflitti di interesse
- nell'ostacolo all'attività degli organi di controllo

Principio guida: trasparenza, correttezza e integrità nei rapporti

d) Gestione della corruzione tra privati e dell'istigazione

Il rischio può emergere:

- nella corruzione tra soci, amministratori o partner commerciali
- nell'istigazione alla corruzione tra privati

Principio guida: integrità e rispetto delle norme etiche interne ed esterne.

e) Relazioni con autorità di vigilanza

Il rischio può emergere:

- nella presentazione di dichiarazioni false o incomplete
- nell'ostacolo all'esercizio delle funzioni delle autorità di vigilanza

Principio guida: collaborazione, correttezza e trasparenza verso gli organi di controllo esterni.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati societari, tra cui:

- gestione contabile e flussi finanziari
- gestione documentale societaria e contrattuale
- gestione dei processi decisionali nelle operazioni straordinarie
- gestione delle relazioni con consulenti e revisori
- formazione del personale sui rischi societari

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori, membri degli organi di controllo, dirigenti, dipendenti, collaboratori, consulenti, partner commerciali e fornitori strategici.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivamente svolto nei processi societari.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e correttezza societaria**
- **trasparenza e veridicità delle comunicazioni sociali**
- **tutela dei soci e dei creditori**
- **rispetto della normativa patrimoniale e dei diritti dei terzi**
- **integrità e trasparenza nei rapporti interni ed esterni**

È espressamente vietato:

- fornire informazioni false o ingannevoli in bilanci, relazioni o certificazioni
- ostacolare il controllo degli organi societari
- operare in conflitto di interessi senza dichiarazione
- distribuire utili, riserve o beni sociali in violazione delle norme
- porre in essere corruzione o istigazione tra privati
- ostacolare l'esercizio delle funzioni delle autorità di vigilanza

Ogni dipendente o collaboratore che **rilevi anomalie o comportamenti sospetti** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- la redazione e approvazione dei bilanci e delle relazioni societarie
- la gestione dei conferimenti, utili e riserve
- le operazioni societarie straordinarie e i conflitti di interesse
- la gestione dei rapporti con organi di controllo, soci e partner commerciali
- la gestione della documentazione societaria e dei flussi patrimoniali
- la gestione delle relazioni con autorità di vigilanza
- la formazione del personale sulle procedure societarie e sui rischi legati ai reati

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'**Organismo di Vigilanza (OdV)**, istituito ai sensi dell'art. 6 del D.Lgs. 231/2001, cui è attribuito il compito di verificare il funzionamento, l'osservanza e l'aggiornamento del Modello.

Con specifico riferimento ai reati di cui all'art. 25-ter, l'attività di controllo dell'OdV si concentra sui processi societari sensibili al rischio di: falsi in bilancio, operazioni patrimoniali illecite, conflitti di interesse, corruzione tra privati e ostacolo ai controlli interni o esterni.

In particolare, l'OdV:

- verifica la correttezza e completezza dei bilanci e delle comunicazioni societarie
- monitora le operazioni sui conferimenti, utili, riserve e beni sociali
- controlla la gestione dei conflitti di interesse e delle relazioni con organi di controllo
- verifica le operazioni straordinarie e i rapporti con partner commerciali
- analizza le segnalazioni ricevute (whistleblowing) su comportamenti illeciti o non conformi
- promuove formazione e sensibilizzazione del personale sui rischi societari

L'OdV può richiedere documentazione e informazioni rilevanti, effettuare audizioni del personale coinvolto nei processi sensibili e redigere report periodici agli organi societari competenti, contenenti eventuali criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati societari richiede un approccio organizzativo fondato su:

- **trasparenza e correttezza nella gestione**
- **controllo e tracciabilità delle operazioni patrimoniali e finanziarie**
- **rispetto dei diritti dei soci e dei creditori**
- **integrità e collaborazione con organi di controllo interni ed esterni**
- **diffusione di una cultura dell'Ente orientata all'integrità e alla legalità**

La presente Parte Speciale deve essere intesa non solo come uno strumento di conformità normativa, ma come **guida operativa per garantire che la gestione societaria dell'organizzazione sia svolta nel pieno rispetto dei principi di correttezza, trasparenza e tutela dei soci e dei creditori.**

Art 25-quater - Reati di terrorismo

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-quater del D.Lgs. 231/2001, concernenti i reati di terrorismo o di eversione dell'ordinamento democratico.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla commissione di reati con finalità di terrorismo, anche internazionale**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Le organizzazioni operano oggi in contesti caratterizzati da rapporti con soggetti nazionali e internazionali, trasporti, infrastrutture critiche, fornitori, partner logistici e sistemi di pagamento.

Tali relazioni possono esporre l'impresa al rischio di commissione di reati di terrorismo, anche mediante il supporto logistico, finanziario o operativo ad associazioni o individui coinvolti.

In particolare, tali rischi possono emergere in relazione a:

- trasporto e gestione di merci o materiali sensibili
- gestione di infrastrutture critiche, impianti e strutture aziendali
- relazioni con partner commerciali, logistici e finanziari internazionali
- utilizzo di strumenti digitali o piattaforme di pagamento
- attività di formazione, addestramento o supporto tecnico
- trasferimenti di persone, beni o risorse con finalità illecite

La prevenzione dei reati di terrorismo richiede pertanto:

- procedure interne di controllo delle attività sensibili
- sistemi di verifica e tracciabilità di persone, materiali e risorse
- cultura dell'Ente orientata alla legalità, alla sicurezza e alla responsabilità sociale

Inquadramento normativo dei reati presupposto

L'art. 25-quater del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal codice penale e da leggi speciali in materia di terrorismo, anche internazionale.

Tra i principali reati rilevanti rientrano:

- Art. 270 c.p. – Associazioni sovversive
- Art. 270-bis c.p. – Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordinamento
- Art. 270-ter c.p. – Assistenza agli associati
- Art. 270-quater c.p. – Arruolamento con finalità di terrorismo anche internazionale
- Art. 270-quater.1 c.p. – Organizzazione di trasferimenti per finalità di terrorismo
- Art. 270-quinquies c.p. – Addestramento ad attività con finalità di terrorismo anche internazionale
- Art. 270-quinquies.1 c.p. – Finanziamento di condotte con finalità di terrorismo
- Art. 270-quinquies.2 c.p. – Sottrazione di beni o denaro sottoposti a sequestro

- Art. 270-quinquies.3 c.p. – Detenzione di materiale con finalità di terrorismo
- Art. 270-sexies c.p. – Condotte con finalità di terrorismo
- Art. 280 c.p. – Attentato per finalità terroristiche o di eversione
- Art. 280-bis c.p. – Atto di terrorismo con ordigni micidiali o esplosivi
- Art. 280-ter c.p. – Atto di terrorismo nucleare
- Art. 289-bis c.p. – Sequestro di persona a scopo di terrorismo o di eversione
- Art. 289-ter c.p. – Sequestro di persona a scopo di coazione
- Art. 302 c.p. – Istigazione a commettere uno dei delitti (previsti dai Capi I e II) contro la personalità dello Stato
- Art. 304 c.p. – Cospirazione politica mediante accordo
- Art. 305 c.p. – Cospirazione politica mediante associazione
- Art. 306 c.p. – Banda armata: formazione e partecipazione
- Art. 307 c.p. – Assistenza ai partecipi di cospirazione o di banda armata
- Art. 435 c.p. – Fabbricazione o detenzione di materie esplodenti
- Artt. 1 e 2 L. 342/1976 –Impossessamento, dirottamento e distruzione di un aereo o danneggiamento installazioni a terra
- Art. 3 L. 422/1989 –Impossessamento, dirottamento e distruzione o danneggiamento delle installazioni di una nave

In sintesi:

- le **associazioni sovversive e terroristiche** prevedono la partecipazione a organizzazioni finalizzate a commettere atti di terrorismo
- l'**assistenza agli associati, l'arruolamento e l'addestramento** costituiscono supporto operativo diretto a fini terroristici
- il **finanziamento e la gestione di trasferimenti illeciti** agevolano condotte terroristiche, nazionali o internazionali
- le **condotte materiali**, come attentati, sequestro di persona, uso di ordigni esplosivi o nucleari, costituiscono azioni concrete di terrorismo
- le **attività di fabbricazione o detenzione di materiale esplodente e infrastrutture critiche** aumentano la pericolosità dei reati

Per qualsiasi impresa, tali fattispecie rappresentano rischi concretamente configurabili nella gestione di infrastrutture, trasporti, logistica, risorse umane e rapporti finanziari.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione economica, il rischio di commissione di reati di terrorismo può emergere in relazione a processi quali:

- gestione di trasporti, logistica e infrastrutture critiche
- gestione e addestramento di personale interno o esterno

- trasferimento di risorse, denaro o materiali sensibili
- gestione dei rapporti con partner commerciali, fornitori o autorità pubbliche
- utilizzo di strumenti informatici e piattaforme digitali
- attività formative, tecniche o operative correlate a infrastrutture e sicurezza

Tali attività richiedono particolare attenzione al fine di garantire sicurezza, trasparenza e rispetto della normativa nazionale e internazionale.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione di infrastrutture critiche e trasporti
Il rischio può emergere:

- nella gestione di aeroporti, porti, navi, aerei e impianti industriali
- nella sicurezza dei materiali trasportati
- nella sorveglianza delle strutture aziendali

Principio guida: garanzia della sicurezza, integrità e rispetto delle normative vigenti.

b) Supporto operativo e logistico a soggetti esterni
Il rischio può emergere:

- nell'assistenza a individui o gruppi con finalità terroristiche
- nella partecipazione a addestramento o trasferimenti illeciti
- nella fornitura di risorse, denaro o strumenti

Principio guida: assenza di qualsiasi supporto a condotte terroristiche o sovversive.

c) Gestione di materiali esplosivi o pericolosi
Il rischio può emergere:

- nella fabbricazione, detenzione o trasporto di materie esplodenti
- nell'uso improprio di ordigni o materiali a rischio nucleare

Principio guida: conformità rigorosa alle norme di sicurezza e prevenzione rischi esplosivi.

d) Relazioni con autorità, partner e fornitori
Il rischio può emergere:

- nella mancata comunicazione o collaborazione con autorità competenti
- nell'interazione con soggetti esterni a finalità illecite

Principio guida: trasparenza, tracciabilità e controllo delle relazioni esterne.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di terrorismo, tra cui:

- gestione documentale e dei flussi di trasporto
- gestione delle risorse finanziarie e dei trasferimenti internazionali
- sorveglianza di infrastrutture critiche
- formazione e addestramento del personale sulla sicurezza

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori, dirigenti, dipendenti operativi in aree sensibili, collaboratori, consulenti e partner logistici o commerciali, fornitori strategici, personale addetto alla sicurezza e ai trasporti.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nei processi sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e sicurezza**
- **trasparenza e tracciabilità dei processi sensibili**
- **assoluta assenza di supporto a condotte terroristiche o eversione dell'ordine democratico**
- **rispetto delle norme nazionali e internazionali**
- **responsabilità e integrità nelle relazioni con partner e fornitori**

È espressamente vietato:

- fornire supporto, risorse o addestramento a soggetti con finalità terroristiche
- partecipare ad associazioni o cospirazioni finalizzate a condotte terroristiche
- detenzione, trasporto o utilizzo illecito di esplosivi o materiali pericolosi
- ostacolare l'azione delle autorità di vigilanza o sicurezza

Ogni dipendente o collaboratore che **rilevi anomalie o comportamenti sospetti** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione delle infrastrutture critiche, trasporti e logistica
- controllo su materiali pericolosi o esplosivi
- gestione dei trasferimenti di persone e risorse
- gestione delle relazioni con partner commerciali e fornitori internazionali
- gestione delle procedure di addestramento e formazione del personale
- gestione della documentazione e dei flussi informativi con autorità

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'**Organismo di Vigilanza (OdV)**, istituito ai sensi dell'art. 6 del D.Lgs. 231/2001.

Con specifico riferimento ai reati di cui all'art. 25-quater, l'attività di controllo dell'OdV si concentra sui processi aziendali sensibili, al fine di prevenire supporto a condotte terroristiche, gestione illecita di materiali pericolosi o ostacolo all'azione delle autorità.

In particolare, l'OdV:

- verifica la corretta applicazione dei protocolli di gestione delle infrastrutture critiche e dei trasporti
- monitora la gestione dei materiali pericolosi, dei flussi di risorse e dei trasferimenti
- controlla la formazione e l'addestramento del personale
- verifica le relazioni con partner commerciali, fornitori e autorità competenti
- analizza le segnalazioni (whistleblowing) su comportamenti sospetti, garantendo la riservatezza
- promuove formazione e sensibilizzazione del personale sui rischi legati al terrorismo

L'OdV può richiedere documentazione e informazioni, effettuare audizioni e redigere report periodici agli organi societari, contenenti eventuali criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di terrorismo richiede un approccio organizzativo fondato su:

- **sicurezza e trasparenza nelle operazioni sensibili**
- **controllo e tracciabilità dei materiali e delle risorse**
- **assenza di supporto a condotte terroristiche**
- **responsabilità, legalità e integrità nelle relazioni interne ed esterne**
- **diffusione di una cultura dell'Ente orientata alla sicurezza e alla legalità**

La presente Parte Speciale deve essere intesa non solo come uno strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di sicurezza, trasparenza e responsabilità.**

Art 25-quater.1 - Mutilazione genitali femminili

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-quater.1 del D.Lgs. 231/2001, concernenti le **mutilazioni genitali femminili (MGF)**.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla commissione di condotte di mutilazione degli organi genitali femminili**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e relazionali**

Le organizzazioni, in particolare quelle con rapporti internazionali, comunità multiculturali o attività nel settore sanitario, educativo e sociale, possono trovarsi esposte al rischio di commissione o concorso in pratiche di MGF.

In particolare, tali rischi possono emergere in relazione a:

- gestione di attività sanitarie, sociali o educative
- rapporti con comunità, associazioni o partner internazionali
- gestione di programmi di supporto a minori e adolescenti
- formazione, informazione e comunicazione su temi culturali e sanitari
- viaggi, trasferimenti o attività in contesti a rischio

La prevenzione dei reati di MGF richiede pertanto:

- procedure di controllo interne per attività sensibili
- formazione e sensibilizzazione del personale su norme e diritti delle persone
- sistemi di segnalazione e whistleblowing sicuri
- una cultura dell'Ente orientata alla tutela della salute, dei minori e dei diritti umani

Inquadramento normativo dei reati presupposto

L'art. 25-quater.1 del D.Lgs. 231/2001 richiama la fattispecie prevista dall'art. 583-bis c.p., che punisce le pratiche di mutilazione degli organi genitali femminili.

In sintesi:

- il reato si configura quando chiunque **cagioni mutilazioni agli organi genitali femminili, anche se giustificate da motivi culturali, religiosi o tradizionali**
- la normativa tutela in particolare la **salute fisica e psichica delle ragazze e delle donne**, indipendentemente dal consenso dei familiari o della vittima stessa
- tali **comportamenti sono sempre illeciti e sanzionati penalmente, sia nel territorio nazionale sia nei casi connessi a trasferimenti o pratiche effettuate all'estero su cittadine italiane o residenti**

Per qualsiasi organizzazione che operi in contesti internazionali, sociali o sanitari, la fattispecie rappresenta un rischio concreto, specialmente in attività di supporto, mediazione culturale o relazioni con comunità a rischio.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di MGF può emergere in relazione a processi quali:

- gestione di attività sanitarie, educative e sociali
- programmi di assistenza a minori o adolescenti
- gestione dei rapporti con famiglie, comunità e associazioni culturali
- formazione e sensibilizzazione del personale

Tali attività richiedono particolare attenzione al fine di garantire la tutela della salute, dei diritti fondamentali e della sicurezza delle persone coinvolte.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione di attività sanitarie e assistenziali
Il rischio può emergere:

- nell'erogazione di servizi sanitari a minori e adolescenti
- nella gestione di programmi di prevenzione e controllo sanitario
- nella collaborazione con medici, operatori e strutture esterne

Principio guida: tutela della salute, integrità fisica e psicologica delle ragazze.

b) Relazioni con comunità e partner culturali
Il rischio può emergere:

- nell'interazione con famiglie o comunità che possano praticare MGF
- nella gestione di programmi educativi o sociali in contesti a rischio

Principio guida: assoluta assenza di supporto o tolleranza verso pratiche mutilative.

c) Formazione, sensibilizzazione e informazione
Il rischio può emergere:

- nella gestione di corsi o attività informative che non rispettino norme o diritti
- nella mancata informazione delle vittime o famiglie sui rischi sanitari e legali

Principio guida: promozione della consapevolezza, della prevenzione e dei diritti umani.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di MGF, tra cui:

- gestione documentale di attività educative e sanitarie
- verifica e selezione di collaboratori e partner operanti in contesti a rischio
- gestione di segnalazioni o reclami da parte di minori o famiglie
- formazione del personale sulla normativa e sui protocolli di prevenzione

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori, dirigenti, dipendenti e collaboratori coinvolti in attività educative, sanitarie o sociali, consulenti e partner operativi, personale addetto alla formazione, prevenzione e sensibilizzazione**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e tutela dei diritti umani**
- **protezione della salute fisica e psichica delle ragazze**
- **trasparenza e assenza di condotte collusive o permissive verso pratiche mutilative**
- **rispetto delle norme nazionali e internazionali**
- **responsabilità e integrità nelle relazioni interne ed esterne**

È espressamente vietato:

- praticare, favorire o tollerare mutilazioni genitali femminili
- ostacolare l'azione delle autorità competenti
- omettere la segnalazione di comportamenti a rischio
- fornire supporto logistico, informativo o organizzativo a chi intenda commettere MGF

Ogni dipendente o collaboratore che **rilevi anomalie o comportamenti sospetti** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione di attività sanitarie, educative e sociali
- gestione dei rapporti con comunità, famiglie e partner culturali
- formazione e sensibilizzazione del personale
- gestione dei flussi informativi e documentali
- procedure di segnalazione e whistleblowing

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'**Organismo di Vigilanza (OdV)**, istituito ai sensi dell'art. 6 del D.Lgs. 231/2001.

Con specifico riferimento ai reati di MGF, l'attività di controllo dell'OdV si concentra sui processi aziendali sensibili, al fine di prevenire condotte illecite o omissioni.

In particolare, l'OdV:

- verifica la corretta applicazione dei protocolli relativi a attività sanitarie, educative e sociali
- monitora la gestione dei rapporti con famiglie, comunità e partner culturali

- controlla la formazione e sensibilizzazione del personale
- analizza segnalazioni (whistleblowing) e reclami relativi a comportamenti a rischio
- promuove iniziative formative sulla normativa e sui protocolli di prevenzione

L'OdV può richiedere documentazione e informazioni, effettuare audizioni e redigere report periodici agli organi societari, contenenti eventuali criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di mutilazioni genitali femminili richiede un approccio organizzativo fondato su:

- **tutela della salute e integrità fisica e psicologica delle ragazze**
- **controllo dei rapporti con partner, famiglie e comunità**
- **assoluta assenza di supporto o tolleranza verso pratiche mutilative**
- **responsabilità, legalità e integrità nelle relazioni interne ed esterne**
- **diffusione di una cultura dell'Ente orientata ai diritti umani e alla prevenzione**

La presente Parte Speciale deve essere intesa non solo come uno strumento di conformità normativa, ma **come guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di tutela, legalità e protezione delle persone vulnerabili.**

Art 25-quinquies - Delitti contro la personalità

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto previsti dall'art. 25-quinquies del D.Lgs. 231/2001, relativi ai delitti contro la personalità individuale, con particolare riguardo alla tutela dei diritti fondamentali della persona, soprattutto nei confronti di minori e soggetti vulnerabili.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla commissione di condotte lesive della libertà e dignità individuale**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e sociali**

Le organizzazioni, specialmente quelle con rapporti internazionali, nel settore turistico, sanitario, educativo, sociale o nei servizi di mediazione, possono trovarsi esposte al rischio di commissione o concorso in delitti che violano la personalità e i diritti fondamentali delle persone.

In particolare, tali rischi possono emergere in relazione a:

- gestione di programmi educativi e sociali
- gestione di servizi per minori, persone vulnerabili o migranti
- attività turistiche, culturali o ricreative coinvolgenti minori
- rapporti con fornitori, partner o collaboratori esterni
- gestione di dati sensibili e documentazione relativa a persone vulnerabili
- la prevenzione dei reati contro la personalità richiede pertanto:
- procedure di controllo interno mirate a protezione di soggetti vulnerabili
- formazione e sensibilizzazione del personale su norme, diritti umani e segnalazione di abusi
- sistemi di whistleblowing sicuri e riservati
- diffusione di una cultura dell'Ente orientata alla tutela della dignità e alla legalità

Inquadramento normativo dei reati presupposto

L'art. 25-quinquies del D.Lgs. 231/2001 richiama le seguenti fattispecie penali:

- Art. 600 c.p. – Riduzione o mantenimento in schiavitù o in servitù
- Art. 600-bis c.p. – Prostituzione minorile
- Art. 600-ter c.p. – Pornografia minorile
- Art. 600-quater c.p. – Detenzione o accesso a materiale pornografico
- Art. 600-quater.1 c.p. – Pornografia virtuale
- Art. 600-quinquies c.p. – Iniziative turistiche volte allo sfruttamento della prostituzione minorile
- Art. 601 c.p. – Tratta di persone
- Art. 601-bis c.p. – Traffico di organi prelevati da persona vivente
- Art. 602 c.p. – Acquisto e alienazione di schiavi
- Art. 603-bis c.p. – Intermediazione illecita e sfruttamento del lavoro
- Art. 609-undecies c.p. – Adescamento di minorenni

- Art. 613-bis c.p. – Tortura
- Art. 613-ter c.p. – Istigazione del pubblico ufficiale a commettere tortura

In sintesi:

- i delitti previsti tutelano l**a libertà, la dignità, l'integrità fisica e psicologica delle persone, con particolare attenzione ai minori e soggetti vulnerabili**
- le condotte illecite includono **riduzione in schiavitù, sfruttamento sessuale, pornografia, traffico di persone o organi, lavoro forzato, adescamento, tortura e istigazione alla tortura**
- tali comportamenti sono **sempre illeciti, indipendentemente dal consenso o da pratiche culturali, e comportano sanzioni penali gravi**

Per qualsiasi organizzazione operante in contesti sociali, educativi, turistici o internazionali, le fattispecie rappresentano rischi concreti che richiedono prevenzione e monitoraggio costante.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di delitti contro la personalità può emergere in relazione a processi quali:

- gestione di servizi educativi, ricreativi o sociali per minori e soggetti vulnerabili
- gestione di programmi turistici, culturali o ricreativi coinvolgenti minori
- gestione di dati e documentazione personale
- gestione dei rapporti con fornitori, partner e collaboratori esterni
- organizzazione di viaggi, trasferimenti o attività internazionali

Tali attività richiedono particolare attenzione al fine di garantire la protezione dei soggetti vulnerabili e il rispetto della legalità.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione di servizi a minori e soggetti vulnerabili

Il rischio può emergere:

- nella somministrazione di attività educative, sanitarie o ricreative
- nella selezione e supervisione del personale a contatto con minori
- nella gestione dei rapporti con famiglie e comunità

Principio guida: tutela della libertà, dignità e sicurezza dei minori e dei soggetti vulnerabili.

b) Gestione di attività turistiche e culturali

Il rischio può emergere:

- nell'organizzazione di viaggi, iniziative ricreative o turistiche

- nella promozione di servizi rivolti a minori o persone vulnerabili
- nella gestione di partner e fornitori esterni

Principio guida: assoluta assenza di supporto a pratiche di sfruttamento o abusi.

c) Gestione della documentazione e dei dati sensibili

Il rischio può emergere:

- nella conservazione o accesso a dati personali di minori
- nella diffusione non autorizzata di immagini o materiali sensibili
- nella gestione di sistemi informativi o archivi documentali

Principio guida: riservatezza, protezione dei dati e prevenzione di abusi.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai delitti contro la personalità, tra cui:

- gestione documentale e archiviazione di dati sensibili
- selezione e monitoraggio di collaboratori, partner e fornitori
- gestione di segnalazioni e whistleblowing
- formazione del personale su normativa, diritti umani e prevenzione

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori a contatto con minori o soggetti vulnerabili, consulenti e partner operativi, personale addetto a gestione dati, servizi educativi, sociali o turistici.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e tutela dei diritti fondamentali delle persone**
- **protezione fisica e psicologica dei minori e soggetti vulnerabili**
- **trasparenza e assenza di comportamenti collusivi verso sfruttamento o abusi**
- **rispetto delle norme nazionali e internazionali**
- **responsabilità e integrità nelle relazioni interne ed esterne**

È espressamente vietato:

- ridurre, mantenere o sfruttare persone in schiavitù o servitù
- favorire prostituzione minorile, pornografia o traffico di persone
- porre in essere o agevolare condotte di tortura o trattamenti inumani
- istigare un pubblico ufficiale a commettere atti di tortura
- ostacolare l'azione delle autorità competenti
- omettere la segnalazione di condotte illecite o comportamenti a rischio

Ogni dipendente o collaboratore che **rilevi anomalie o comportamenti sospetti** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione di servizi educativi, sociali e turistici
- gestione dei rapporti con minori, famiglie e soggetti vulnerabili
- gestione di fornitori e partner esterni
- gestione di dati sensibili e documentazione
- procedure di formazione, sensibilizzazione e segnalazione

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-quinquies, l'attività di controllo dell'OdV si concentra sui processi aziendali sensibili, al fine di prevenire condotte illecite e omissioni, incluse quelle riconducibili alla tortura e alla sua istigazione.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi a servizi educativi, sociali e turistici
- monitora la gestione dei rapporti con minori, famiglie e partner esterni
- controlla la gestione dei dati sensibili e della documentazione
- analizza segnalazioni e reclami relativi a comportamenti a rischio
- promuove iniziative formative sulla normativa, diritti umani e prevenzione

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei delitti contro la personalità richiede un approccio organizzativo fondato su:

- **tutela della libertà, dignità e integrità dei minori e soggetti vulnerabili**
- **controllo dei rapporti con partner, famiglie e collaboratori esterni**
- **assoluta assenza di supporto a pratiche di sfruttamento, abuso o tortura**
- **responsabilità, legalità e integrità nelle relazioni interne ed esterne**
- **diffusione di una cultura dell'Ente orientata alla protezione, alla prevenzione e ai diritti umani**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di tutela, legalità e protezione delle persone vulnerabili.**

Art 25-sexies - Abuso di mercato

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-sexies del D.Lgs. 231/2001, concernenti l'abuso di mercato,* l'abuso di informazioni privilegiate, la comunicazione illecita di informazioni privilegiate e la manipolazione del mercato.

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla commissione di comportamenti illeciti sui mercati finanziari**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e finanziarie**

Le organizzazioni che operano in contesti finanziari, bancari o di gestione patrimoniale possono essere esposte al rischio di comportamenti idonei a compromettere l'integrità dei mercati, utilizzare o divulgare informazioni privilegiate, ovvero porre in essere condotte finalizzate alla manipolazione degli strumenti finanziari, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- gestione di strumenti finanziari, titoli e azioni
- gestione di informazioni sensibili o privilegiate
- operazioni di trading e investimento
- rapporti con clienti, investitori, intermediari finanziari e partner commerciali
- attività di consulenza e comunicazione finanziaria

La prevenzione dei reati di abuso di mercato richiede pertanto:

- procedure di controllo interno sui flussi informativi sensibili
- formazione del personale su normative, regolamenti europei e principi di trasparenza
- sistemi di monitoraggio delle operazioni finanziarie e dei movimenti di mercato
- una cultura dell'Ente orientata alla legalità, correttezza e trasparenza

Inquadramento normativo dei reati presupposto

L'art. 25-sexies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- **Art. 184 TUF – Abuso di informazioni privilegiate e comunicazione illecita di informazioni privilegiate**
- **Art. 185 TUF – Manipolazione del mercato**
- **Art. 187-bis TUF – Abuso e comunicazione illecita di informazioni privilegiate**
- **Art. 187-ter TUF – Manipolazione del mercato**
- **Art. 187-ter.1 TUF – Sanzioni relative alle violazioni delle disposizioni del Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio del 16 aprile 2014**
- **Art. 187-quinquies TUF – Responsabilità dell'ente**
- **Art. 89 Reg. UE n. 1114/2023 – Divieto di manipolazione del mercato**
- **Art. 90 Reg. UE n. 1114/2023 – Divieto di abuso di informazioni privilegiate**

- **Art. 91 Reg. UE n. 1114/2023 – Divieto di divulgazione illecita di informazioni privilegiate**

In sintesi:

- i reati di abuso di mercato tutelano l**a trasparenza, la correttezza e l'integrità dei mercati finanziari**
- le condotte illecite **includono trading basato su informazioni privilegiate, diffusione non autorizzata di informazioni sensibili e manipolazione dei prezzi**
- tali comportamenti possono **determinare gravi conseguenze per l'ente, gli investitori e l'ordinamento finanziario**

Per qualsiasi organizzazione operante nel settore finanziario, bancario o di gestione patrimoniale, le fattispecie rappresentano rischi concreti e richiedono sistemi di prevenzione e controllo efficaci.

A seguito delle più recenti evoluzioni normative, Il **D.Lgs. n. 128 del 25 giugno 2026**, recante attuazione della delega per la riforma organica e il riordino del sistema sanzionatorio previsto dal **Testo Unico delle disposizioni in materia di intermediazione finanziaria (D.Lgs. n. 58/1998 - TUF)**, ha modificato gli **artt. 187-ter.1 e 187-quinquies del TUF**, disposizioni rilevanti nell'ambito della disciplina degli abusi di mercato richiamata dall'art. 25-sexies del D.Lgs. 231/2001.

Gli interventi hanno riguardato esclusivamente il coordinamento normativo e l'aggiornamento della disciplina sanzionatoria applicabile agli abusi di mercato, senza modificare le fattispecie rilevanti ai fini della responsabilità amministrativa degli enti prevista dal D.Lgs. 231/2001.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione finanziaria, il rischio di commissione di delitti di abuso di mercato può emergere in relazione a processi quali:

- gestione e scambio di strumenti finanziari, titoli e azioni
- accesso e trattamento di informazioni privilegiate o riservate
- comunicazioni finanziarie verso investitori, clienti e partner
- attività di trading, consulenza o investimento
- gestione dei rapporti con intermediari, autorità di vigilanza e mercati regolamentati

Tali attività richiedono particolare attenzione per garantire la trasparenza, la legalità e la correttezza delle operazioni finanziarie.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione e utilizzo di informazioni privilegiate
Il rischio può emergere:

- nella ricezione e trattamento di informazioni riservate relative a società quotate o strumenti finanziari
- nella divulgazione non autorizzata di informazioni sensibili
- nell'uso delle informazioni per trading o operazioni personali

Principio guida: accesso e utilizzo delle informazioni solo secondo le norme vigenti, con assoluta riservatezza e trasparenza.

b) Operazioni sui mercati finanziari
Il rischio può emergere:

- nella negoziazione di titoli o strumenti finanziari a rischio manipolazione
- nella promozione di attività di investimento ingannevoli o non trasparenti

Principio guida: rispetto delle regole di integrità dei mercati e correttezza nelle operazioni.

c) Comunicazioni finanziarie e relazioni con investitori
Il rischio può emergere:

- nella comunicazione di dati finanziari non corretti o parziali
- nella raccomandazione o induzione di altri a comportamenti illeciti
- nella gestione dei canali di informazione verso il pubblico o partner finanziari

Principio guida: trasparenza, correttezza e accuratezza delle informazioni diffuse.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai delitti di abuso di mercato, tra cui:

- gestione di sistemi informativi e piattaforme di trading
- gestione documentale e archiviazione di dati finanziari sensibili
- selezione e monitoraggio di partner, consulenti e intermediari finanziari
- formazione e sensibilizzazione del personale su normative, regolamenti e comportamenti leciti

Destinatari
La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori addetti a gestione titoli, trading e comunicazioni finanziarie, consulenti, partner e intermediari finanziari, personale con accesso a dati riservati o privilegiati.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal ruolo effettivo nelle attività sensibili.

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e trasparenza dei mercati finanziari**
- **riservatezza e correttezza nella gestione delle informazioni privilegiate**
- **integrità, lealtà e trasparenza nelle comunicazioni finanziarie**
- **responsabilità nella negoziazione e gestione di strumenti finanziari**
- **assoluta assenza di comportamenti finalizzati a manipolazioni o abusi di mercato**

È espressamente vietato:

- utilizzare informazioni privilegiate per trading o operazioni personali
- divulgare dati sensibili non autorizzati
- indurre terzi a violare le norme sui mercati finanziari
- manipolare prezzi, indici o strumenti finanziari

Ogni dipendente o collaboratore **che rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione di informazioni privilegiate e riservate
- monitoraggio e controllo delle operazioni sui mercati finanziari
- comunicazioni verso investitori, clienti e partner
- selezione e gestione di consulenti, intermediari e partner finanziari
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-sexies, l'attività di controllo dell'OdV si concentra sui processi sensibili di mercato, al fine di prevenire comportamenti illeciti.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi a informazioni privilegiate e riservate
- monitora le operazioni finanziarie e i flussi di mercato
- controlla la correttezza e trasparenza delle comunicazioni verso investitori e partner
- analizza segnalazioni e reclami relativi a condotte sospette
- promuove iniziative formative su normativa, regolamenti UE e corrette pratiche di mercato

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei delitti di abuso di mercato richiede un approccio organizzativo fondato su:

- **trasparenza e correttezza nelle operazioni finanziarie**
- **gestione prudente e riservata delle informazioni privilegiate**
- **rispetto delle regole di integrità dei mercati e dei regolamenti UE**
- **responsabilità e trasparenza nelle comunicazioni verso investitori e partner**
- **diffusione di una cultura dell'Ente orientata alla legalità, correttezza e tutela del mercato finanziario**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di correttezza, integrità e trasparenza nei mercati finanziari.**

Art 25-septies - Omicidio colposo sul lavoro

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-septies del D.Lgs. 231/2001, concernenti l'omicidio colposo e le lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione della salute e sicurezza nei luoghi di lavoro**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Le organizzazioni, indipendentemente dal settore di attività, sono esposte al rischio di eventi lesivi derivanti da carenze organizzative, tecniche o procedurali in materia di sicurezza sul lavoro, con conseguenti gravi responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- gestione degli ambienti di lavoro e delle infrastrutture
- utilizzo di macchinari, attrezzature e impianti
- organizzazione delle attività operative e dei turni di lavoro
- gestione dei rischi interferenziali e degli appalti
- formazione, informazione e addestramento del personale
- gestione delle emergenze e dei dispositivi di protezione

La prevenzione dei reati in materia di salute e sicurezza richiede pertanto:

- un sistema strutturato di valutazione e gestione dei rischi
- l'adozione di misure tecniche, organizzative e procedurali adeguate
- la formazione continua del personale
- sistemi di controllo e monitoraggio delle condizioni di sicurezza
- una cultura dell'Ente orientata alla tutela della persona e alla prevenzione degli infortuni

Inquadramento normativo dei reati presupposto

L'art. 25-septies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- Art. 589 c.p. – Omicidio colposo
- Art. 590 c.p. – Lesioni personali colpose

In relazione alla responsabilità dell'ente, tali reati assumono rilevanza quando sono commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro e per la tutela della salute e sicurezza dei lavoratori.

Il quadro normativo di riferimento comprende, inoltre:

- D.Lgs. 81/2008 (Testo Unico sulla salute e sicurezza sul lavoro)
- normative tecniche e regolamentari applicabili agli specifici settori
- standard e linee guida in materia di prevenzione e protezione

Il sistema di prevenzione dell'Ente ricomprende anche gli obblighi di tutela della salute e sicurezza dei lavoratori che svolgono la prestazione in modalità di lavoro agile, secondo quanto previsto dalla normativa vigente e dalle successive modifiche intervenute, comprese quelle introdotte dalla Legge n. 34/2026.

In sintesi:

- **i reati tutelano la vita, l'integrità fisica e la salute dei lavoratori**
- **le condotte illecite consistono in negligenza, imprudenza, imperizia o violazione di norme antinfortunistiche**
- **la responsabilità dell'ente deriva da carenze organizzative e gestionali**

Per qualsiasi organizzazione, tali fattispecie rappresentano rischi concreti e richiedono sistemi di prevenzione e controllo efficaci.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione dei reati in materia di sicurezza sul lavoro può emergere in relazione a processi quali:

- progettazione e organizzazione delle attività lavorative
- gestione operativa dei processi produttivi o di servizio
- manutenzione di impianti, macchinari e attrezzature
- gestione degli appalti e dei fornitori
- gestione della sicurezza nei luoghi di lavoro
- sorveglianza sanitaria e gestione delle idoneità

Tali attività richiedono particolare attenzione per garantire la tutela della salute e dell'integrità fisica dei lavoratori.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione della sicurezza e valutazione dei rischi
Il rischio può emergere:

- nella mancata o incompleta valutazione dei rischi
- nell'assenza o inadeguatezza del Documento di Valutazione dei Rischi (DVR)
- nella mancata individuazione delle misure di prevenzione e protezione

Principio guida: identificazione sistematica dei rischi e adozione di misure adeguate a eliminarli o ridurli.

b) Gestione operativa delle attività lavorative
Il rischio può emergere:

- nell'utilizzo improprio di macchinari o attrezzature

- nella mancata applicazione delle procedure di sicurezza
- nell'organizzazione del lavoro in condizioni pericolose

Principio guida: svolgimento delle attività nel rispetto delle procedure e delle norme di sicurezza.

c) Formazione, informazione e addestramento

Il rischio può emergere:

- nella mancata formazione dei lavoratori
- nella carenza di informazione sui rischi specifici
- nell'assenza di addestramento pratico

Principio guida: garantire che ogni lavoratore sia adeguatamente formato e consapevole dei rischi.

d) Gestione degli appalti e dei fornitori

Il rischio può emergere:

- nella mancata verifica dell'idoneità tecnico-professionale
- nella gestione inadeguata dei rischi interferenziali
- nella carenza di coordinamento tra le parti

Principio guida: assicurare il rispetto delle norme di sicurezza anche nei rapporti con terzi.

e) Gestione della salute e sicurezza nel lavoro agile

Il rischio può emergere:

- nella mancata valutazione dei rischi connessi alle attività svolte in modalità agile
- nell'omessa informazione del lavoratore sui rischi generali e specifici
- nella mancata adozione delle misure organizzative idonee a garantire condizioni di lavoro sicure
- nella carente definizione delle responsabilità e delle modalità operative del lavoro agile

Principio guida: assicurare che anche le attività svolte in modalità agile siano organizzate e gestite nel rispetto della normativa in materia di salute e sicurezza.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati, tra cui:

- gestione documentale in materia di sicurezza
- monitoraggio e audit interni
- gestione dei dispositivi di protezione individuale (DPI)
- gestione delle emergenze e del primo soccorso
- sistemi di segnalazione di incidenti, near miss e non conformità

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **datori di lavoro, dirigenti e preposti, dipendenti e lavoratori, responsabili del servizio di prevenzione e protezione (RSPP), consulenti, appaltatori e fornitori, personale con responsabilità in materia di sicurezza.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **tutela della salute e sicurezza dei lavoratori**
- **prevenzione degli infortuni e delle malattie professionali**
- **rispetto delle norme e delle procedure di sicurezza**
- **responsabilità e collaborazione tra tutti i soggetti coinvolti**
- **miglioramento continuo delle condizioni di lavoro**
- **garantire la tutela della salute e sicurezza anche dei lavoratori che operano in modalità agile, mediante adeguata informazione, formazione e organizzazione delle attività**

È espressamente vietato:

- omettere o eludere misure di prevenzione e protezione
- utilizzare macchinari o attrezzature in modo non sicuro
- non utilizzare i dispositivi di protezione individuale
- ignorare segnalazioni di pericolo o situazioni di rischio
- adottare comportamenti imprudenti o negligenti

Ogni dipendente o collaboratore **che rilevi situazioni di rischio** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- valutazione e aggiornamento dei rischi (DVR)
- gestione delle misure di prevenzione e protezione
- formazione e addestramento del personale
- gestione degli appalti e dei rischi interferenziali
- manutenzione di impianti e attrezzature
- gestione delle emergenze e degli infortuni
- gestione della salute e sicurezza dei lavoratori in modalità agile
- informativa sui rischi connessi al lavoro agile
- monitoraggio periodico delle misure organizzative adottate per il lavoro agile

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con specifico riferimento ai reati di cui all'art. 25-septies, l'attività di controllo dell'OdV si concentra sui processi sensibili in materia di sicurezza sul lavoro.

In particolare, l'OdV:

- verifica l'applicazione delle procedure di sicurezza
- monitora l'aggiornamento del DVR e delle misure di prevenzione
- analizza gli infortuni, i near miss e le segnalazioni
- controlla i flussi informativi verso gli organi competenti
- promuove iniziative formative in materia di sicurezza
- verifica l'applicazione delle procedure di sicurezza relative al lavoro agile
- monitora l'aggiornamento delle procedure e delle informative in materia di lavoro agile

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di omicidio colposo e lesioni personali colpose richiede un approccio organizzativo fondato su:

- **centralità della sicurezza nei processi aziendali**
- **gestione sistematica e documentata dei rischi**
- **rispetto delle normative e delle buone prassi**
- **coinvolgimento attivo di tutti i soggetti aziendali**
- **diffusione di una cultura della sicurezza**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto della tutela della salute, della sicurezza e della dignità dei lavoratori, indipendentemente dalle modalità di svolgimento della prestazione lavorativa, ivi compreso il lavoro agile.**

Art 25-octies - Riciclaggio

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-octies del D.Lgs. 231/2001, concernenti la ricettazione, il riciclaggio, l'impiego di denaro, beni o utilità di provenienza illecita, nonché l'autoriciclaggio.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione di risorse finanziarie, beni o utilità di provenienza illecita**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e finanziarie**

Le organizzazioni, indipendentemente dal settore di attività, possono essere esposte al rischio di coinvolgimento, anche inconsapevole, in operazioni di ricettazione, riciclaggio o autoriciclaggio, con conseguenti gravi responsabilità penali e amministrative.

Tali rischi assumono particolare rilievo nell'ambito dei rapporti economici e commerciali con soggetti terzi, della gestione dei flussi finanziari, dell'acquisizione di beni e servizi e delle operazioni aventi ad oggetto risorse economiche o patrimoniali, rispetto alle quali è necessario assicurare adeguati livelli di trasparenza, tracciabilità e verifica della provenienza lecita.

In particolare, tali rischi possono emergere in relazione a:

- gestione di flussi finanziari e operazioni di pagamento
- rapporti con clienti, fornitori, partner commerciali, consulenti e intermediari
- gestione di contratti, appalti e operazioni commerciali
- acquisizione, alienazione o utilizzo di beni, materiali e altre utilità
- operazioni straordinarie, investimenti e movimentazioni di capitale
- gestione di beni aziendali e risorse economiche

La prevenzione dei reati di cui all'art. 25-octies richiede pertanto:

- procedure di controllo sui flussi finanziari e sulla tracciabilità delle operazioni
- adeguata verifica dell'identità, dell'affidabilità e della reputazione delle controparti
- controlli sull'origine lecita di denaro, beni e altre utilità oggetto delle operazioni aziendali
- formazione del personale sui rischi di riciclaggio e sulle normative applicabili
- sistemi di monitoraggio delle operazioni anomale o sospette
- una cultura dell'Ente orientata alla legalità, alla trasparenza, alla correttezza e alla collaborazione con le Autorità competenti

Inquadramento normativo dei reati presupposto

L'art. 25-octies del D.Lgs. 231/2001 richiama le seguenti fattispecie penali:

- Art. 648 c.p. – Ricettazione
- Art. 648-bis c.p. – Riciclaggio
- Art. 648-ter c.p. – Impiego di denaro, beni o utilità di provenienza illecita
- Art. 648-ter.1 c.p. – Autoriciclaggio

In sintesi:

- il **reato di ricettazione** punisce le condotte di acquisto, ricezione, occultamento, intermediazione o comunque di gestione di denaro, beni o altre utilità provenienti da delitto, quando tali attività siano poste in essere nella consapevolezza della provenienza illecita e al fine di trarne profitto per sé o per altri
- il **riciclaggio** consiste nella sostituzione, nel trasferimento o nel compimento di altre operazioni su denaro, beni o altre utilità provenienti da delitto, idonee ad ostacolare l'identificazione della loro origine delittuosa
- il **reato di impiego di denaro, beni o utilità di provenienza illecita** riguarda l'utilizzo di risorse di provenienza delittuosa nell'ambito di attività economiche, finanziarie, imprenditoriali o speculative
- l'**autoriciclaggio** consiste nell'impiego, sostituzione, trasferimento o utilizzo, in attività economiche, finanziarie, imprenditoriali o speculative, dei proventi derivanti da delitti commessi dallo stesso autore, in modo da ostacolarne concretamente l'identificazione della provenienza delittuosa

I reati sopra indicati sono finalizzati a contrastare l'immissione nel circuito economico legale di capitali, beni o altre utilità derivanti da attività delittuose e mirano a garantire la trasparenza e la liceità delle transazioni economiche e finanziarie.

Per qualsiasi organizzazione, tali fattispecie rappresentano rischi concreti, in particolare nelle attività caratterizzate da movimentazioni finanziarie, rapporti con soggetti esterni, acquisizione di beni o servizi e gestione di operazioni economiche, richiedendo adeguati presidi organizzativi, procedure di controllo e sistemi di tracciabilità idonei a garantire la liceità delle operazioni e la corretta verifica delle controparti.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio può emergere in relazione a processi quali:

- gestione di incassi, pagamenti e flussi finanziari
- gestione di rapporti contrattuali con clienti, fornitori, partner commerciali e consulenti
- operazioni di investimento e movimentazione di capitali
- gestione di appalti, forniture e consulenze
- acquisizione, cessione e gestione di beni aziendali o altre utilità
- utilizzo di conti correnti, strumenti finanziari e mezzi di pagamento

Tali attività richiedono particolare attenzione al fine di garantire la tracciabilità delle operazioni, la verifica dell'identità e dell'affidabilità delle controparti e la provenienza lecita delle risorse economiche, dei beni e delle utilità oggetto delle operazioni aziendali.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione dei flussi finanziari
Il rischio può emergere:

- nella gestione di pagamenti e incassi non adeguatamente tracciati
- nell'utilizzo di conti correnti, strumenti finanziari o mezzi di pagamento non trasparenti
- nella gestione di operazioni frazionate, anomale o prive di adeguata giustificazione economica
- nell'esecuzione di operazioni che possano ostacolare la ricostruzione dei flussi finanziari

Principio guida: tracciabilità, trasparenza, verificabilità e coerenza economica di tutte le operazioni finanziarie.

b) Gestione dei rapporti con controparti
Il rischio può emergere:

- nella selezione di fornitori, clienti, partner commerciali o consulenti non adeguatamente verificati
- nella stipula di contratti con soggetti coinvolti, anche indirettamente, in attività illecite
- nella gestione di intermediari o soggetti che operino con modalità non trasparenti
- nell'omessa verifica dell'identità, dell'affidabilità o della reputazione delle controparti

Principio guida: adeguata conoscenza della controparte, verifica dell'affidabilità e della liceità delle attività svolte.

c) Operazioni economiche e investimenti
Il rischio può emergere:

- nella realizzazione di operazioni economiche complesse o non adeguatamente giustificate
- nell'impiego di risorse finanziarie di dubbia provenienza
- nella gestione di operazioni straordinarie o investimenti privi di adeguata trasparenza
- nell'acquisizione di partecipazioni, beni o attività senza adeguata verifica della provenienza delle risorse impiegate

Principio guida: coerenza economica, trasparenza e liceità delle operazioni.

d) Acquisizione e gestione di beni, materiali e altre utilità
L'acquisizione o la gestione di beni aziendali può costituire un'area di rischio qualora non siano adeguatamente verificate la provenienza e la legittima disponibilità dei beni o delle utilità oggetto delle operazioni.

Il rischio può emergere:

- nell'acquisto di beni a condizioni economiche anomale o non coerenti con il valore di mercato
- nella ricezione di beni o utilità privi di adeguata documentazione
- nella gestione di beni provenienti da soggetti non adeguatamente identificati
- nell'omessa verifica della regolarità della documentazione relativa ai beni acquisiti

Principio guida: garantire la liceità, la tracciabilità e la verificabilità della provenienza dei beni, delle utilità e delle risorse economiche.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-octies, tra cui:

- gestione amministrativa, contabile e finanziaria
- gestione documentale e archiviazione dei flussi economici
- selezione, qualificazione e monitoraggio di fornitori, partner commerciali, consulenti e intermediari
- gestione dei sistemi informativi e dei mezzi di pagamento
- gestione degli acquisti e delle procedure di approvvigionamento
- gestione dei beni aziendali
- formazione del personale sui rischi di ricettazione, riciclaggio e autoriciclaggio

Particolare attenzione deve essere posta:

- alla corretta identificazione delle controparti
- alla conservazione della documentazione giustificativa delle operazioni
- alla verifica della coerenza economica delle transazioni
- alla tracciabilità dei pagamenti e degli incassi
- alla documentazione attestante la provenienza lecita dei beni e delle utilità acquisite

Tali attività costituiscono presidi essenziali per prevenire l'utilizzo dell'organizzazione quale strumento, anche inconsapevole, per operazioni di ricettazione, riciclaggio, impiego di beni di provenienza illecita o autoriciclaggio.

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti nella gestione finanziaria, amministrativa e contrattuale, consulenti, partner commerciali e intermediari, personale con accesso a risorse economiche, beni aziendali e flussi finanziari.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal ruolo effettivo nelle attività sensibili.

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e correttezza nella gestione delle risorse economiche**
- **trasparenza e tracciabilità dei flussi finanziari**
- **verifica dell'origine lecita di denaro, beni e utilità**
- **adeguata conoscenza e valutazione dell'affidabilità delle controparti**
- **responsabilità nella gestione dei rapporti economici e contrattuali**
- **assoluta assenza di comportamenti finalizzati alla ricettazione, al riciclaggio, all'impiego di denaro, beni o utilità di provenienza illecita e all'autoriciclaggio**

È espressamente vietato:

- acquistare, ricevere, detenere o utilizzare denaro, beni o altre utilità di provenienza illecita
- porre in essere operazioni idonee a ostacolare l'identificazione della provenienza delittuosa di denaro, beni o altre utilità
- impiegare risorse economiche di provenienza illecita in attività economiche, finanziarie o imprenditoriali
- effettuare operazioni simulate o prive di adeguata giustificazione economica
- instaurare rapporti contrattuali con controparti senza le verifiche previste dalle procedure aziendali
- omettere o alterare la documentazione necessaria a garantire la tracciabilità delle operazioni economiche e finanziarie
- frazionare artificiosamente operazioni economiche o finanziarie allo scopo di eludere i controlli interni

Ogni dipendente o collaboratore che rilevi anomalie, operazioni sospette o comportamenti non coerenti con i principi della presente Parte Speciale è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione e tracciabilità dei flussi finanziari
- verifica, selezione e monitoraggio delle controparti contrattuali
- gestione delle operazioni economiche, degli investimenti e delle operazioni straordinarie
- gestione dell'acquisizione, utilizzo e cessione di beni aziendali
- controllo delle operazioni anomale o sospette
- conservazione della documentazione a supporto delle operazioni economiche e finanziarie
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

In particolare, i protocolli devono garantire:

- la completa tracciabilità delle operazioni economiche e finanziarie
- la verificabilità dell'identità e dell'affidabilità delle controparti
- la documentazione della provenienza e della destinazione dei flussi finanziari
- la verifica della provenienza lecita dei beni e delle utilità oggetto delle operazioni aziendali
- la segregazione delle funzioni nelle attività maggiormente esposte al rischio
- la tempestiva individuazione e gestione di operazioni anomale o non coerenti con il profilo economico dell'operazione

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con specifico riferimento ai reati di cui all'art. 25-octies, l'attività di controllo dell'OdV si concentra sui processi aziendali sensibili, al fine di prevenire operazioni di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alla gestione e alla tracciabilità dei flussi finanziari
- monitora le operazioni economiche, finanziarie e patrimoniali, verificando la presenza di adeguati presidi di controllo
- controlla la correttezza dei rapporti con clienti, fornitori, partner commerciali, consulenti e intermediari
- verifica l'adeguatezza delle procedure di identificazione e valutazione delle controparti
- monitora le modalità di acquisizione, gestione e utilizzo di beni e altre utilità, verificando la presenza di adeguata documentazione sulla provenienza
- analizza segnalazioni, anomalie e operazioni potenzialmente sospette relative a movimentazioni finanziarie o rapporti economici con soggetti terzi
- verifica il rispetto delle procedure interne relative alla gestione dei pagamenti, degli incassi e degli strumenti finanziari
- promuove iniziative formative e di sensibilizzazione in materia di prevenzione della ricettazione, del riciclaggio, dell'impiego di beni di provenienza illecita e dell'autoriciclaggio

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Particolare rilevanza assumono i flussi informativi periodici verso l'OdV, che devono includere, tra l'altro:

- informazioni relative alle operazioni finanziarie maggiormente rilevanti
- segnalazioni di anomalie o operazioni non coerenti con le procedure aziendali
- informazioni relative alla gestione dei rapporti con controparti considerate maggiormente sensibili
- dati relativi ad acquisizioni, cessioni o movimentazioni di beni e altre utilità di particolare rilevanza economica
- esiti dei controlli interni sulla tracciabilità delle operazioni e sulla corretta gestione della documentazione

Gli esiti delle attività di controllo sono oggetto di report periodici agli organi societari competenti, contenenti eventuali criticità riscontrate, raccomandazioni e proposte di miglioramento del sistema di controllo interno.

In presenza di violazioni accertate, anomalie significative o carenze nei presidi organizzativi, l'OdV propone l'adozione delle opportune misure correttive, nonché l'eventuale attivazione del sistema disciplinare.

L'attività dell'Organismo di Vigilanza costituisce pertanto un presidio essenziale per la prevenzione dei reati di cui all'art. 25-octies del D.Lgs. 231/2001, contribuendo al rafforzamento della trasparenza, della tracciabilità delle operazioni economiche e della corretta gestione delle risorse finanziarie, dei beni e delle utilità aziendali.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio richiede un approccio organizzativo fondato su:

- **tracciabilità e trasparenza delle operazioni finanziarie**
- **verifica dell'affidabilità, dell'identità e della liceità delle controparti**
- **controllo della provenienza dei beni, delle risorse economiche e delle utilità gestite dall'organizzazione**
- **documentazione e verificabilità delle operazioni economiche e contrattuali**
- **responsabilità e correttezza nella gestione delle risorse aziendali**
- **diffusione di una cultura dell'Ente orientata alla legalità, alla trasparenza e alla prevenzione dei fenomeni di riciclaggio**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, trasparenza, correttezza economica e tracciabilità delle operazioni, prevenendo qualsiasi utilizzo dell'organizzazione quale strumento per la gestione o l'impiego di denaro, beni o utilità di provenienza illecita.**

Art 25-octies.1 - Strumenti di pagamento

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-octies.1 del D.Lgs. 231/2001, concernenti i delitti in materia di strumenti di pagamento diversi dai contanti e il trasferimento fraudolento di valori.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'utilizzo illecito di strumenti di pagamento e alle frodi informatiche e finanziarie**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e delle operazioni economico-finanziarie**

Le organizzazioni, in considerazione della crescente digitalizzazione dei sistemi di pagamento e della diffusione di strumenti elettronici, possono essere esposte al rischio di utilizzo fraudolento di strumenti di pagamento, nonché di coinvolgimento in operazioni illecite di trasferimento di valori.

In particolare, tali rischi possono emergere in relazione a:

- utilizzo di carte di pagamento, strumenti elettronici e sistemi digitali
- gestione di credenziali di accesso e strumenti di autenticazione
- operazioni di pagamento e incasso tramite piattaforme informatiche
- gestione dei sistemi informativi e delle infrastrutture IT
- rapporti con clienti, fornitori, intermediari e partner tecnologici

La prevenzione dei reati di cui all'art. 25-octies.1 richiede pertanto:

- procedure di controllo sull'utilizzo degli strumenti di pagamento
- sistemi di sicurezza informatica e protezione delle credenziali
- formazione del personale sui rischi di frodi digitali e finanziarie
- monitoraggio delle operazioni anomale e dei flussi finanziari
- una cultura dell'Ente orientata alla sicurezza, legalità e trasparenza

Inquadramento normativo dei reati presupposto

L'art. 25-octies.1 del D.Lgs. 231/2001 richiama le seguenti fattispecie penali:

- Art. 493-ter c.p. – Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti
- Art. 493-quater c.p. – Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti
- Art. 512-bis c.p. – Trasferimento fraudolento di valori
- Art. 640-ter c.p. – Frode informatica

In sintesi:

- i reati sopra indicati sono finalizzati a **tutelare la sicurezza dei sistemi di pagamento e la correttezza delle transazioni economiche**

- le condotte illecite includono **l'utilizzo indebito di carte o strumenti elettronici, la falsificazione, la detenzione di dispositivi fraudolenti e le manipolazioni informatiche**
- tali comportamenti possono **determinare rilevanti danni economici e reputazionali per l'ente e per i soggetti coinvolti**

Per qualsiasi organizzazione che utilizzi strumenti di pagamento elettronici o sistemi informatici, tali fattispecie rappresentano rischi concreti e richiedono adeguati sistemi di prevenzione e controllo.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica
La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di reati in materia di strumenti di pagamento e frodi informatiche può emergere in relazione a processi quali:

- gestione di pagamenti elettronici e strumenti di incasso
- utilizzo e gestione di credenziali di accesso ai sistemi
- gestione di sistemi informativi e piattaforme digitali
- operazioni finanziarie tramite canali telematici
- gestione dei rapporti con fornitori di servizi tecnologici

Tali attività richiedono particolare attenzione al fine di garantire la sicurezza dei sistemi e la legittimità delle operazioni effettuate.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione degli strumenti di pagamento elettronici
Il rischio può emergere:

- nell'utilizzo improprio di carte di pagamento o strumenti digitali
- nella gestione non sicura delle credenziali e dei dispositivi di accesso
- nella mancata tracciabilità delle operazioni di pagamento

Principio guida: utilizzo corretto, sicuro e tracciabile degli strumenti di pagamento.

b) Gestione dei sistemi informatici e delle credenziali
Il rischio può emergere:

- nell'accesso non autorizzato ai sistemi informativi
- nella diffusione o detenzione di software o dispositivi illeciti
- nella carenza di misure di sicurezza informatica

Principio guida: protezione dei sistemi e delle credenziali mediante adeguati presidi di sicurezza.

c) Operazioni economico-finanziarie e trasferimento di valori
Il rischio può emergere:

- nella realizzazione di operazioni fraudolente o non trasparenti
- nel trasferimento fittizio o simulato di beni o valori
- nella gestione di operazioni economiche prive di giustificazione

Principio guida: trasparenza, liceità e tracciabilità delle operazioni economiche.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-octies.1, tra cui:

- gestione dei sistemi IT e delle infrastrutture digitali
- gestione delle credenziali e dei profili di accesso
- gestione documentale e archiviazione dei dati
- selezione e monitoraggio di fornitori tecnologici e partner
- formazione del personale in materia di sicurezza informatica

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti nella gestione di pagamenti e sistemi informatici, consulenti, partner e fornitori tecnologici, personale con accesso a sistemi informativi e strumenti di pagamento.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e correttezza nell'utilizzo degli strumenti di pagamento**
- **sicurezza e protezione dei sistemi informatici**
- **tracciabilità e trasparenza delle operazioni economiche**
- **responsabilità nella gestione delle credenziali e degli accessi**
- **prevenzione di qualsiasi forma di frode informatica o finanziaria**

È espressamente vietato:

- utilizzare indebitamente strumenti di pagamento altrui o falsificati
- detenere o diffondere dispositivi o software destinati a commettere reati
- effettuare operazioni fraudolente o manipolare sistemi informatici
- realizzare trasferimenti fittizi o simulati di valori

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione e utilizzo degli strumenti di pagamento elettronici
- sicurezza dei sistemi informatici e protezione delle credenziali
- monitoraggio delle operazioni finanziarie e delle anomalie

- selezione e gestione di fornitori tecnologici e partner
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con specifico riferimento ai reati di cui all'art. 25-octies.1, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi all'utilizzo di strumenti di pagamento e sistemi informatici, al fine di prevenire condotte illecite.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi ai sistemi di pagamento e IT
- monitora le operazioni economiche e le attività digitali
- controlla la gestione delle credenziali e degli accessi
- analizza segnalazioni e anomalie relative a comportamenti sospetti
- promuove iniziative formative in materia di sicurezza informatica e prevenzione delle frodi

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di strumenti di pagamento e trasferimento fraudolento di valori richiede un approccio organizzativo fondato su:

- **sicurezza e protezione dei sistemi informatici**
- **corretto utilizzo degli strumenti di pagamento elettronici**
- **tracciabilità e trasparenza delle operazioni economiche**
- **controllo dei processi digitali e dei flussi finanziari**
- **diffusione di una cultura dell'Ente orientata alla legalità e alla sicurezza**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di sicurezza, trasparenza e correttezza nelle operazioni economico-finanziarie.**

Art 25-octies.2 - Violazione misure restrittive UE

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-octies.2 del D.Lgs. 231/2001, concernenti la violazione delle misure restrittive adottate dall'Unione Europea.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla violazione di sanzioni economiche, finanziarie e commerciali imposte dall'Unione Europea**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e dei rapporti internazionali**

Le organizzazioni che operano in contesti internazionali o intrattengono rapporti con controparti estere possono essere esposte al rischio di violazione di misure restrittive (sanzioni), con conseguenti rilevanti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- rapporti commerciali con controparti estere o soggetti sottoposti a sanzioni
- operazioni di import/export di beni, servizi o tecnologie
- trasferimenti finanziari internazionali
- utilizzo di intermediari, distributori o partner commerciali
- gestione di autorizzazioni e licenze per attività soggette a restrizioni

La prevenzione dei reati di cui all'art. 25-octies.2 richiede pertanto:

- procedure di controllo sulle controparti e sulle operazioni internazionali
- verifica delle liste sanzionatorie e delle normative UE applicabili
- formazione del personale sui regimi sanzionatori europei
- monitoraggio dei flussi commerciali e finanziari transnazionali
- una cultura dell'Ente orientata alla legalità, trasparenza e conformità normativa

Inquadramento normativo dei reati presupposto

L'art. 25-octies.2 del D.Lgs. 231/2001 richiama le seguenti fattispecie penali:

- Art. 275-bis c.p. – Violazione delle misure restrittive dell'Unione europea
- Art. 275-ter c.p. – Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione europea
- Art. 275-quater c.p. – Violazione delle condizioni dell'autorizzazione allo svolgimento di attività
- Art. 275-quinquies c.p. – Violazione colposa di misure restrittive dell'Unione europea

In sintesi:

- i reati sopra indicati sono **finalizzati a garantire l'effettività delle misure restrittive adottate dall'Unione Europea**
- le condotte illecite **includono la violazione di divieti di commercio, trasferimento di fondi, prestazione di servizi o obblighi informativi**

- rilevano sia le condotte **dolose sia quelle colpose, con particolare riferimento alla mancata verifica delle restrizioni applicabili**

Per qualsiasi organizzazione operante a livello internazionale, tali fattispecie rappresentano rischi concreti e richiedono adeguati presidi di controllo e verifica.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 23.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di violazione delle misure restrittive UE può emergere in relazione a processi quali:

- gestione di operazioni commerciali internazionali
- gestione di forniture e approvvigionamenti da paesi esteri
- trasferimenti finanziari e operazioni bancarie internazionali
- gestione di autorizzazioni e licenze
- rapporti con intermediari, agenti e partner commerciali

Tali attività richiedono particolare attenzione al fine di garantire la conformità alle normative europee e internazionali.

Attività sensibili: aree a rischio primario
Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione dei rapporti con controparti estere
Il rischio può emergere:

- nella selezione di partner, clienti o fornitori soggetti a sanzioni
- nella mancata verifica delle liste restrittive UE
- nella gestione di rapporti indiretti tramite intermediari

Principio guida: verifica preventiva e continua dell'affidabilità e della liceità delle controparti.

b) Operazioni commerciali e trasferimenti internazionali
Il rischio può emergere:

- nell'esecuzione di operazioni vietate o soggette a restrizioni
- nel trasferimento di fondi verso soggetti sanzionati
- nella movimentazione di beni o tecnologie soggette a divieti

Principio guida: piena conformità alle restrizioni UE e tracciabilità delle operazioni.

c) Gestione delle autorizzazioni e degli obblighi informativi
Il rischio può emergere:

- nel mancato rispetto delle condizioni previste da autorizzazioni
- nell'omissione o incompletezza degli obblighi informativi
- nella gestione non conforme delle comunicazioni alle autorità

Principio guida: rispetto rigoroso delle autorizzazioni e degli obblighi informativi previsti dalla normativa.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-octies.2, tra cui:

- gestione dei flussi finanziari internazionali
- gestione documentale e archiviazione delle operazioni commerciali
- selezione e monitoraggio di partner e intermediari
- gestione dei sistemi informativi e delle banche dati sanzionatorie
- formazione del personale su normative UE e regimi sanzionatori

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti in attività commerciali e finanziarie internazionali, consulenti, partner e intermediari, personale addetto alla gestione di operazioni estere e autorizzazioni.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **rispetto delle misure restrittive dell'Unione Europea**
- **trasparenza e correttezza nei rapporti internazionali**
- **verifica preventiva delle controparti e delle operazioni**
- **tracciabilità dei flussi commerciali e finanziari**
- **responsabilità nella gestione delle attività soggette a restrizioni**

È espressamente vietato:

- intrattenere rapporti con soggetti sottoposti a misure restrittive
- effettuare operazioni vietate o in violazione delle sanzioni UE
- omettere obblighi informativi o fornire informazioni non corrette
- violare le condizioni previste da autorizzazioni o licenze

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- verifica delle controparti rispetto alle liste sanzionatorie
- gestione delle operazioni commerciali e finanziarie internazionali
- controllo delle autorizzazioni e degli obblighi informativi
- monitoraggio delle operazioni a rischio e delle anomalie
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con specifico riferimento ai reati di cui all'art. 25-octies.2, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi alle operazioni internazionali e ai rapporti con controparti estere.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alle misure restrittive UE
- monitora le operazioni commerciali e finanziarie internazionali
- controlla la gestione delle autorizzazioni e degli obblighi informativi
- analizza segnalazioni e anomalie relative a possibili violazioni
- promuove iniziative formative in materia di sanzioni internazionali

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di violazione delle misure restrittive dell'Unione Europea richiede un approccio organizzativo fondato su:

- **verifica sistematica delle controparti e delle operazioni**
- **rispetto rigoroso delle normative e delle sanzioni UE**
- **controllo dei flussi commerciali e finanziari internazionali**
- **gestione corretta delle autorizzazioni e degli obblighi informativi**
- **diffusione di una cultura dell'Ente orientata alla compliance e alla legalità internazionale**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, trasparenza e conformità alle normative europee e internazionali.**

Art 25-novies - Diritto d'autore

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-novies del D.Lgs. 231/2001, concernenti i delitti in materia di violazione del diritto d'autore.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'utilizzo illecito di opere dell'ingegno, contenuti digitali e materiali protetti dal diritto d'autore**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali e nella gestione di contenuti e strumenti informatici**

Le organizzazioni, in considerazione dell'ampio utilizzo di contenuti digitali, software, banche dati e materiali protetti, possono essere esposte al rischio di violazione della normativa sul diritto d'autore, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- utilizzo di software, banche dati e contenuti digitali
- gestione di siti web, piattaforme e canali di comunicazione
- produzione, diffusione e condivisione di materiali informativi e multimediali
- utilizzo di opere protette per finalità commerciali o promozionali
- gestione di archivi digitali e documentazione dell'Ente

La prevenzione dei reati di cui all'art. 25-novies richiede pertanto:

- procedure di controllo sull'utilizzo di contenuti e software
- verifica delle licenze e dei diritti di utilizzo
- formazione del personale sul rispetto della normativa sul diritto d'autore
- monitoraggio dei sistemi informativi e dei contenuti pubblicati
- una cultura dell'Ente orientata alla legalità e al rispetto della proprietà intellettuale

Inquadramento normativo dei reati presupposto

L'art. 25-novies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- Art. 171, comma 1, lett. a-bis) e a-ter) e comma 3, Legge 633/1941 – Messa a disposizione del pubblico di un'opera dell'ingegno protetta o parte di essa
- Art. 171-bis Legge 633/1941 – Abusiva pubblicazione contenuta in supporti non contrassegnati ai sensi della Legge n.166/2024
- Art. 171-ter Legge 633/1941 – Abusiva duplicazione di opere dell'ingegno destinate al circuito televisivo, cinematografico, etc.
- Art. 171-septies Legge 633/1941 – Mancata comunicazione dei dati di identificazione dei supporti ai sensi della Legge n.166/2024
- Art. 171-octies Legge 633/1941 – Fraudolenta produzione, vendita o importazione di apparati di decodifica
- Art. 174-ter Legge 633/1941 –Utilizzare, duplicare, riprodurre in modo abusivo opere o materiali protetti

- Art. 174-sexies Legge 633/1941 – Obblighi di segnalazione e notificazione

In sintesi:

- i reati sopra indicati **tutelano i diritti patrimoniali e morali degli autori e dei titolari di diritti connessi**
- le condotte illecite **includono la riproduzione, diffusione, messa a disposizione del pubblico e utilizzo abusivo di opere protette**
- tali comportamenti possono determinare **rilevanti danni economici e reputazionali per l'ente**

Per qualsiasi organizzazione che utilizzi contenuti digitali o opere dell'ingegno, tali fattispecie rappresentano rischi concreti e richiedono adeguati sistemi di prevenzione e controllo.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di reati in materia di diritto d'autore può emergere in relazione a processi quali:

- utilizzo e gestione di software e banche dati
- produzione e diffusione di contenuti digitali
- gestione di siti web e canali di comunicazione dell'Ente
- utilizzo di materiali protetti per attività commerciali o promozionali
- gestione di archivi documentali e digitali

Tali attività richiedono particolare attenzione al fine di garantire il rispetto dei diritti di proprietà intellettuale.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione di software e banche dati
Il rischio può emergere:

- nell'utilizzo di software non licenziati o non autorizzati
- nella duplicazione o distribuzione abusiva di programmi informatici
- nella gestione non conforme di banche dati

Principio guida: utilizzo esclusivo di software e banche dati regolarmente licenziati.

b) Gestione di contenuti digitali e multimediali
Il rischio può emergere:

- nella pubblicazione non autorizzata di opere protette
- nella diffusione di contenuti senza il consenso dei titolari dei diritti
- nell'utilizzo di materiali protetti per finalità commerciali

Principio guida: rispetto dei diritti di utilizzo e delle licenze dei contenuti.

c) Gestione delle comunicazioni e dei canali digitali
Il rischio può emergere:

- nella pubblicazione di contenuti su siti web o piattaforme aziendali
- nella condivisione di materiali protetti tramite strumenti digitali
- nella gestione non conforme delle comunicazioni pubbliche

Principio guida: verifica preventiva dei diritti di utilizzo prima della diffusione dei contenuti.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-novies, tra cui:

- gestione dei sistemi informativi e delle piattaforme digitali
- gestione documentale e archiviazione dei contenuti
- selezione e gestione di fornitori di contenuti e servizi digitali
- controllo delle licenze software e dei diritti di utilizzo
- formazione del personale sul diritto d'autore

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti nella gestione di contenuti e sistemi informatici, consulenti, partner e fornitori di servizi digitali, personale con accesso a software, banche dati e materiali protetti.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **rispetto della normativa sul diritto d'autore**
- **utilizzo lecito e autorizzato di opere dell'ingegno**
- **trasparenza nella gestione dei contenuti e dei materiali digitali**
- **responsabilità nella diffusione di informazioni e materiali**
- **prevenzione di qualsiasi forma di utilizzo abusivo**

È espressamente vietato:

- duplicare, riprodurre o diffondere opere protette senza autorizzazione
- utilizzare software privi di licenza o contraffatti
- mettere a disposizione del pubblico contenuti senza i necessari diritti
- utilizzare materiali protetti per finalità commerciali senza autorizzazione

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione delle licenze software e dei diritti di utilizzo
- controllo dei contenuti digitali e delle pubblicazioni
- verifica dei fornitori di contenuti e servizi
- monitoraggio dei sistemi informativi e delle attività digitali
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-novies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi all'utilizzo di contenuti, software e sistemi informatici.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi al diritto d'autore
- monitora l'utilizzo di software e contenuti digitali
- controlla la gestione delle licenze e dei diritti di utilizzo
- analizza segnalazioni e anomalie relative a possibili violazioni
- promuove iniziative formative in materia di proprietà intellettuale

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di violazione del diritto d'autore richiede un approccio organizzativo fondato su:

- **rispetto dei diritti di proprietà intellettuale**
- **controllo dell'utilizzo di software e contenuti digitali**
- **verifica delle licenze e dei diritti di utilizzo**
- **responsabilità nella diffusione di materiali e informazioni**
- **diffusione di una cultura dell'Ente orientata alla legalità e alla tutela delle opere dell'ingegno**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, correttezza e tutela della proprietà intellettuale.**

Art 25-decies - Induzione a dichiarazioni mendaci

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-decies del D.Lgs. 231/2001, concernenti l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi a comportamenti che possano ostacolare l'attività dell'autorità giudiziaria**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nella gestione di rapporti con autorità giudiziarie e procedimenti legali**

Le organizzazioni possono essere esposte al rischio che soggetti apicali o subordinati pongano in essere condotte finalizzate a influenzare indebitamente dichiarazioni rese nell'ambito di procedimenti giudiziari, con conseguenti rilevanti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- gestione di contenziosi giudiziari o procedimenti penali
- rapporti con dipendenti, collaboratori o terzi coinvolti in procedimenti
- attività di audit interno e raccolta di informazioni
- gestione di segnalazioni e indagini interne
- rapporti con consulenti legali e difensori

La prevenzione dei reati di cui all'art. 25-decies richiede pertanto:

- procedure di gestione dei rapporti con l'autorità giudiziaria
- formazione del personale sui comportamenti da adottare in caso di procedimenti
- tracciabilità delle comunicazioni e delle attività rilevanti
- sistemi di segnalazione e gestione delle anomalie
- una cultura dell'Ente orientata alla legalità, trasparenza e collaborazione con le autorità

Inquadramento normativo dei reati presupposto

L'art. 25-decies del D.Lgs. 231/2001 richiama la seguente fattispecie penale:

- Art. 377-bis c.p. – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

In sintesi:

- il reato punisce chi, con **violenza, minaccia, offerta o promessa di denaro o altra utilità, induce taluno a non rendere dichiarazioni o a renderle mendaci davanti all'autorità giudiziaria**
- la tutela è rivolta al **corretto funzionamento della giustizia e alla genuinità delle dichiarazioni rese nei procedimenti**
- tali condotte possono compromettere **l'accertamento della verità e determinare gravi responsabilità per l'ente**

Per qualsiasi organizzazione coinvolta, anche indirettamente, in procedimenti giudiziari, tali fattispecie rappresentano rischi concreti e richiedono adeguati presidi di prevenzione.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione del reato di cui all'art. 377-bis c.p. può emergere in relazione a processi quali:

- gestione di procedimenti giudiziari e contenziosi
- rapporti con soggetti chiamati a rendere dichiarazioni
- gestione di indagini interne e audit
- comunicazioni con consulenti legali e difensori
- gestione di informazioni rilevanti per procedimenti giudiziari

Tali attività richiedono particolare attenzione al fine di garantire la correttezza dei comportamenti e il rispetto dell'autonomia delle dichiarazioni rese.

Attività sensibili: aree a rischio primario
Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione dei procedimenti giudiziari
Il rischio può emergere:

- nella gestione dei rapporti con soggetti coinvolti in procedimenti
- nella predisposizione di strategie difensive non conformi alla legge
- nella pressione su soggetti chiamati a rendere dichiarazioni

Principio guida: pieno rispetto dell'autonomia e della libertà delle dichiarazioni rese all'autorità giudiziaria.

b) Rapporti con dipendenti, collaboratori e terzi
Il rischio può emergere:

- nella richiesta o sollecitazione di dichiarazioni non veritiere
- nella promessa di vantaggi o utilità in cambio di dichiarazioni
- nella gestione non trasparente delle informazioni

Principio guida: correttezza, trasparenza e assenza di qualsiasi forma di pressione o induzione.

c) Gestione delle informazioni e delle indagini interne
Il rischio può emergere:

- nella manipolazione o omissione di informazioni rilevanti
- nella gestione non corretta di audit o verifiche interne
- nella comunicazione impropria con soggetti coinvolti

Principio guida: integrità, completezza e veridicità delle informazioni.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto al reato di cui all'art. 25-decies, tra cui:

- gestione documentale e archiviazione delle informazioni
- gestione dei flussi informativi verso consulenti legali
- selezione e monitoraggio di consulenti e difensori
- gestione dei sistemi di segnalazione (whistleblowing)
- formazione del personale sui rapporti con l'autorità giudiziaria

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti in procedimenti o audit, consulenti legali e professionisti esterni, personale con accesso a informazioni rilevanti.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto dell'autorità giudiziaria**
- **trasparenza e correttezza nelle dichiarazioni e nei comportamenti**
- **integrità e veridicità delle informazioni fornite**
- **rispetto dell'autonomia dei soggetti coinvolti nei procedimenti**
- **collaborazione con le autorità competenti**

È espressamente vietato:

- indurre taluno a non rendere dichiarazioni o a renderle mendaci
- esercitare pressioni, minacce o promesse di utilità
- alterare o manipolare informazioni rilevanti per procedimenti giudiziari
- ostacolare l'attività dell'autorità giudiziaria

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione dei rapporti con l'autorità giudiziaria
- gestione dei procedimenti e delle attività difensive
- tracciabilità delle comunicazioni e delle informazioni rilevanti
- selezione e gestione dei consulenti legali
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-decies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi ai rapporti con l'autorità giudiziaria e alla gestione delle informazioni rilevanti.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi ai procedimenti giudiziari
- monitora la gestione dei rapporti con soggetti coinvolti
- controlla la tracciabilità delle comunicazioni e delle informazioni
- analizza segnalazioni e anomalie relative a possibili condotte illecite
- promuove iniziative formative in materia di legalità e rapporti con l'autorità giudiziaria

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci richiede un approccio organizzativo fondato su:

- **rispetto dell'autonomia dei soggetti coinvolti nei procedimenti**
- **correttezza e trasparenza nella gestione delle informazioni**
- **tracciabilità delle comunicazioni e delle attività**
- **collaborazione con le autorità giudiziarie**
- **diffusione di una cultura dell'Ente orientata alla legalità e all'integrità**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, trasparenza e correttezza nei rapporti con l'autorità giudiziaria.**

Art 25-undecies - Reati ambientali

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-undecies del D.Lgs. 231/2001, concernenti i reati in materia ambientale.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla commissione di reati che possano arrecare danno all'ambiente**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali con impatto ambientale**

Le organizzazioni, in relazione alle proprie attività produttive, logistiche o di servizio, possono essere esposte al rischio di violazioni della normativa ambientale, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- gestione dei rifiuti e delle sostanze potenzialmente inquinanti
- gestione di impianti, processi produttivi e attività con impatto ambientale
- emissioni in atmosfera, scarichi idrici e contaminazione del suolo
- produzione, utilizzo, movimentazione e commercializzazione di prodotti potenzialmente inquinanti
- trasporto, recupero, trattamento e smaltimento dei rifiuti
- gestione delle autorizzazioni ambientali e dei rapporti con le autorità competenti

La prevenzione dei reati ambientali richiede pertanto:

- procedure di controllo sulla gestione ambientale
- valutazione e monitoraggio degli impatti ambientali
- rispetto delle prescrizioni autorizzative e normative applicabili
- tracciabilità dei rifiuti, delle sostanze e dei materiali gestiti
- formazione del personale sulla normativa ambientale
- una cultura dell'Ente orientata alla tutela dell'ambiente e alla responsabilità nella gestione delle attività aziendali

La tutela ambientale costituisce un elemento essenziale del sistema organizzativo dell'Ente e richiede un approccio preventivo fondato sull'individuazione dei rischi, sull'adozione di adeguate misure di controllo e sul costante monitoraggio delle attività potenzialmente impattanti.

Inquadramento normativo dei reati presupposto

L'art. 25-undecies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- Art. 452-bis c.p. – Inquinamento ambientale
- Art. 452-bis.1 c.p. – Commercio di prodotti inquinanti
- Art. 452-ter c.p. – Morte o lesioni come conseguenza del delitto di inquinamento ambientale e di commercio di prodotti inquinanti
- Art. 452-quater c.p. – Disastro ambientale

- Art. 452-quinquies c.p. – Delitti colposi contro l'ambiente
- Art. 452-sexies c.p. – Traffico e abbandono di materiale ad alta radioattività
- Art. 452-septies c.p. – Impedimento del controllo
- Art. 452-terdecies c.p. – Omessa bonifica
- Art. 452-quaterdecies c.p. – Attività organizzate per il traffico illecito di rifiuti
- Art. 452-quinquiesdecies c.p. – Nozione di abusività
- Art. 452-sexiesdecies c.p. – Circostanze aggravanti
- Art. 727-bis c.p. – Uccisione, distruzione, cattura, prelievo, detenzione e commercio di esemplari di specie animali o vegetali selvatiche protette
- Art. 255 D.Lgs. 152/2006 – Abbandono di rifiuti
- Art. 255-bis D.Lgs. 152/2006 – Abbandono di rifiuti non pericolosi in casi particolari
- Art. 255-ter D.Lgs. 152/2006 – Abbandono di rifiuti pericolosi
- Art. 256 D.Lgs. 152/2006 – Attività di gestione di rifiuti non autorizzata
- Art. 256-bis D.Lgs. 152/2006 – Combustione illecita di rifiuti
- Art. 257 D.Lgs. 152/2006 – Bonifica dei siti
- Art. 258 D.Lgs. 152/2006 – Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
- Art. 259 D.Lgs. 152/2006 – Spedizione illegale di rifiuti
- Art. 260-bis D.Lgs. 152/2006 – Sistema di tracciabilità dei rifiuti
- Art. 8 D.Lgs. 202/2007 – Inquinamento doloso provocato da navi
- Art. 9 D.Lgs. 202/2007 – Inquinamento colposo provocato da navi
- Art. 1, 2, 3-bis e 6 L. 150/1992 – Commercio internazionale delle specie di flora e fauna selvaggia
- Art. 9, comma 1, lett. a), L. 146/2006 – Operazioni sotto copertura

In relazione agli aggiornamenti normativi intervenuti, il sistema di prevenzione dei reati ambientali deve considerare anche le nuove fattispecie introdotte dalla normativa europea di tutela penale dell'ambiente, recepite nell'ordinamento nazionale, che ampliano la rilevanza penale delle condotte lesive dell'ambiente e rafforzano la responsabilità degli enti in presenza di carenze organizzative e gestionali.

In particolare, assumono rilievo:

- le condotte di inquinamento ambientale con conseguenze aggravate sulla salute e sull'integrità delle persone
- la commercializzazione di prodotti inquinanti in violazione delle disposizioni applicabili
- la gestione abusiva di attività aventi impatto ambientale
- le circostanze aggravanti connesse alla particolare gravità del danno ambientale o delle conseguenze derivanti dalle condotte illecite

In sintesi:

- i reati ambientali tutelano **l'ambiente, la salute pubblica, la biodiversità e il patrimonio naturale**
- le condotte illecite includono **inquinamento, gestione illecita dei rifiuti, traffico illecito, commercio di prodotti inquinanti, mancata bonifica e violazione degli obblighi di controllo**
- tali comportamenti possono determinare **gravi danni ambientali e rilevanti responsabilità per l'ente**

Per qualsiasi organizzazione con attività aventi potenziale impatto ambientale, tali fattispecie rappresentano rischi concreti e richiedono sistemi di prevenzione e controllo efficaci.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di reati ambientali può emergere in relazione a processi quali:

- gestione dei rifiuti e delle sostanze potenzialmente pericolose
- gestione degli impianti e delle attività produttive aventi impatto ambientale
- gestione delle emissioni in atmosfera, degli scarichi idrici e della tutela del suolo
- produzione, utilizzo, movimentazione e commercializzazione di prodotti potenzialmente inquinanti
- trasporto, recupero, trattamento e smaltimento dei rifiuti
- gestione delle autorizzazioni ambientali e dei rapporti con le autorità competenti

Tali attività richiedono particolare attenzione al fine di garantire la conformità alla normativa ambientale, la prevenzione degli impatti negativi sull'ambiente e il rispetto degli obblighi di controllo e tracciabilità.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione dei rifiuti

Il rischio può emergere:

- nella gestione dei rifiuti in assenza delle necessarie autorizzazioni
- nell'abbandono, deposito incontrollato o smaltimento illecito dei rifiuti
- nella mancata corretta classificazione, registrazione o tracciabilità dei rifiuti
- nell'affidamento delle attività di trasporto, recupero o smaltimento a soggetti non adeguatamente autorizzati

Principio guida: gestione conforme, autorizzata e tracciata dei rifiuti, attraverso il controllo dell'intero ciclo di gestione.

b) Gestione degli impianti e degli impatti ambientali

Il rischio può emergere:

- nel superamento dei limiti previsti per emissioni e scarichi
- nella gestione non conforme degli impianti o dei processi produttivi
- nella mancata manutenzione, verifica o controllo delle apparecchiature con rilevanza ambientale
- nell'adozione di comportamenti idonei a determinare fenomeni di inquinamento ambientale

Principio guida: rispetto dei limiti normativi, corretta gestione degli impianti e monitoraggio continuo degli impatti ambientali.

c) Gestione delle autorizzazioni e dei controlli ambientali
Il rischio può emergere:

- nella violazione delle prescrizioni contenute nelle autorizzazioni ambientali
- nella gestione di attività in assenza dei necessari titoli autorizzativi
- nella mancata comunicazione di informazioni richieste dalle autorità competenti
- nell'impedimento o ostacolo alle attività di controllo e vigilanza

Principio guida: piena collaborazione con le autorità competenti, trasparenza delle informazioni e rispetto delle autorizzazioni ambientali.

d) Gestione di prodotti e materiali potenzialmente inquinanti

Il rischio può emergere:

- nella produzione, commercializzazione o gestione di prodotti non conformi alla normativa ambientale
- nella mancata verifica delle caratteristiche e degli effetti ambientali dei prodotti trattati
- nella gestione non corretta di materiali o sostanze potenzialmente idonee a provocare danni ambientali
- nella mancata adozione di misure preventive e di controllo

Principio guida: assicurare che la gestione dei prodotti e dei materiali avvenga nel rispetto della normativa ambientale applicabile e dei principi di prevenzione del danno ambientale.

e) Gestione delle situazioni di contaminazione e bonifica ambientale

Il rischio può emergere:

- nella mancata adozione degli interventi necessari in presenza di contaminazioni ambientali
- nell'omessa comunicazione agli enti competenti delle situazioni di potenziale rischio
- nella mancata esecuzione delle attività di ripristino o bonifica previste dalla normativa

Principio guida: tempestiva gestione delle situazioni di rischio ambientale e adozione delle misure di prevenzione, contenimento e ripristino.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati ambientali, tra cui:

- gestione documentale e archiviazione delle autorizzazioni ambientali
- gestione dei registri, formulari e sistemi di tracciabilità dei rifiuti
- selezione, qualificazione e monitoraggio dei fornitori ambientali e dei trasportatori
- gestione dei sistemi informativi utilizzati per gli adempimenti ambientali
- gestione dei controlli periodici e delle verifiche interne
- formazione e sensibilizzazione del personale in materia ambientale
- gestione delle segnalazioni relative a possibili anomalie o violazioni ambientali

Le attività strumentali sopra individuate assumono particolare rilevanza in quanto una carente gestione organizzativa e documentale può incidere sull'efficacia del sistema di prevenzione dei rischi ambientali.

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, dipendenti e collaboratori coinvolti in attività con impatto ambientale, consulenti e fornitori operanti nel settore ambientale, personale addetto alla gestione degli impianti, dei rifiuti e delle attività soggette a controllo ambientale.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo ricoperto nell'ambito delle attività sensibili e dalle responsabilità concretamente esercitate.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- rispetto della normativa ambientale e delle autorizzazioni applicabili
- prevenzione dell'inquinamento e tutela dell'ambiente
- gestione corretta, controllata e tracciabile dei rifiuti e delle sostanze potenzialmente impattanti
- valutazione preventiva degli effetti ambientali derivanti dalle attività aziendali
- responsabilità nella gestione delle risorse naturali e dei materiali utilizzati
- collaborazione e trasparenza nei rapporti con le autorità competenti
- diffusione di una cultura dell'Ente orientata alla sostenibilità e alla tutela ambientale

È espressamente vietato:

- effettuare scarichi, emissioni o attività con impatto ambientale in assenza delle necessarie autorizzazioni o in violazione dei limiti previsti
- gestire, trasportare o smaltire rifiuti in modo illecito o non tracciato
- affidare attività ambientali a soggetti privi dei necessari requisiti autorizzativi
- impedire, ostacolare o rendere difficoltose le attività di controllo delle autorità competenti
- omettere interventi necessari di prevenzione, contenimento, ripristino o bonifica ambientale
- commercializzare o gestire prodotti potenzialmente inquinanti in violazione della normativa applicabile
- alterare, omettere o fornire informazioni non corrette negli adempimenti e nelle comunicazioni ambientali

Ogni dipendente o collaboratore **che rilevi anomalie, situazioni di rischio ambientale o possibili violazioni della normativa** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione dei rifiuti e delle sostanze potenzialmente pericolose
- classificazione, registrazione e tracciabilità dei rifiuti
- gestione dei sistemi di controllo e monitoraggio ambientale

- controllo delle emissioni, degli scarichi e degli impatti ambientali
- gestione delle autorizzazioni ambientali e delle relative prescrizioni
- selezione e controllo dei fornitori, trasportatori e soggetti terzi coinvolti in attività ambientali
- gestione delle situazioni di contaminazione, emergenza ambientale e interventi di ripristino
- gestione della documentazione e degli adempimenti ambientali
- formazione, sensibilizzazione e gestione delle segnalazioni in materia ambientale

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

La Fondazione assicura inoltre il costante aggiornamento dei presidi organizzativi e procedurali in relazione all'evoluzione della normativa ambientale e ai cambiamenti nelle attività aziendali aventi impatto sull'ambiente.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-undecies, l'attività di controllo dell'OdV si concentra sui processi aziendali con impatto ambientale e sui relativi sistemi di prevenzione e controllo.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli e delle procedure ambientali
- monitora la gestione dei rifiuti, delle emissioni e degli altri aspetti con rilevanza ambientale
- controlla la conformità delle attività aziendali rispetto alle autorizzazioni e alle prescrizioni ambientali applicabili
- analizza segnalazioni, anomalie e non conformità relative a possibili violazioni ambientali
- verifica la corretta gestione dei flussi informativi relativi alle attività a rischio
- monitora l'aggiornamento delle procedure aziendali in materia ambientale
- promuove iniziative formative e informative in materia ambientale

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati ambientali richiede un approccio organizzativo fondato su:

- **rispetto della normativa e delle autorizzazioni ambientali**
- **gestione sistematica e documentata dei rischi ambientali**
- **controllo delle attività aventi impatto sull'ambiente**
- **gestione corretta e tracciata dei rifiuti, dei materiali e delle sostanze utilizzate**
- **responsabilità nella tutela dell'ambiente e nella prevenzione del danno ambientale**
- **coinvolgimento attivo di tutti i soggetti aziendali**

- **diffusione di una cultura dell'Ente orientata alla sostenibilità e alla responsabilità ambientale**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di tutela ambientale, legalità e responsabilità, attraverso un sistema organizzativo fondato sulla prevenzione, sul controllo continuo e sul miglioramento delle modalità operative.**

Art 25-duodecies - Impiego irregolare cittadini paesi terzi

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-duodecies del D.Lgs. 231/2001, concernenti l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare e i delitti connessi all'immigrazione clandestina.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'impiego irregolare di lavoratori stranieri e alle violazioni della normativa sull'immigrazione**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nella gestione dei rapporti di lavoro e delle attività aziendali**

Le organizzazioni possono essere esposte al rischio di impiegare lavoratori stranieri privi di valido titolo di soggiorno o di essere coinvolte, anche indirettamente, in attività connesse all'immigrazione irregolare, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- processi di selezione e assunzione del personale
- gestione amministrativa dei rapporti di lavoro
- utilizzo di lavoratori tramite appalti, somministrazione o cooperative
- rapporti con fornitori e partner operativi
- gestione della documentazione relativa ai lavoratori stranieri

La prevenzione dei reati di cui all'art. 25-duodecies richiede pertanto:

- procedure di verifica dei requisiti di soggiorno dei lavoratori
- controlli sulla documentazione e sulla regolarità dei rapporti di lavoro
- monitoraggio dei fornitori e delle catene di appalto
- formazione del personale sulle normative in materia di immigrazione
- una cultura dell'Ente orientata alla legalità e al rispetto dei diritti dei lavoratori

Inquadramento normativo dei reati presupposto

L'art. 25-duodecies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- Art. 12, commi 1, 1-bis, 3, 3-bis, 3-ter, 3-quinquies, 4, 4-bis, 4-ter e 5, D.Lgs. 286/1998 – Disposizioni contro le immigrazioni clandestine
- Art. 12-bis D.Lgs. 286/1998 – Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina

In sintesi:

- i reati sopra indicati tutelano il **controllo dei flussi migratori e i diritti fondamentali delle persone**
- le condotte illecite includono il **favoreggiamento dell'ingresso o permanenza illegale, nonché l'impiego di lavoratori stranieri irregolari**
- sono previste aggravanti in caso di **sfruttamento, numero elevato di persone coinvolte o conseguenze gravi per l'incolumità**

Per qualsiasi organizzazione che gestisca rapporti di lavoro o collaborazioni, tali fattispecie rappresentano rischi concreti e richiedono adeguati sistemi di prevenzione e controllo.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione dei reati di cui all'art. 25-duodecies può emergere in relazione a processi quali:

- selezione e assunzione del personale
- gestione amministrativa e contrattuale dei lavoratori
- gestione di appalti e subappalti
- verifica della documentazione dei lavoratori stranieri
- gestione dei rapporti con fornitori di manodopera

Tali attività richiedono particolare attenzione al fine di garantire la regolarità dei rapporti di lavoro e il rispetto della normativa vigente.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Selezione e assunzione del personale
Il rischio può emergere:

- nella mancata verifica del permesso di soggiorno
- nell'assunzione di lavoratori privi di titolo valido
- nella gestione non conforme delle procedure di assunzione

Principio guida: verifica preventiva e continua della regolarità del lavoratore.

b) Gestione dei rapporti di lavoro e della documentazione
Il rischio può emergere:

- nella mancata conservazione o aggiornamento dei documenti
- nella gestione non conforme delle pratiche amministrative
- nell'omissione di controlli periodici

Principio guida: tracciabilità, aggiornamento e correttezza della documentazione.

c) Gestione di appalti, fornitori e partner
Il rischio può emergere:

- nell'utilizzo di fornitori che impiegano lavoratori irregolari
- nella mancata verifica della regolarità dei partner
- nella gestione non trasparente delle catene di appalto

Principio guida: controllo e responsabilizzazione della filiera contrattuale.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-duodecies, tra cui:

- gestione documentale e archiviazione dei dati dei lavoratori
- gestione dei sistemi informativi HR
- selezione e monitoraggio di fornitori e appaltatori
- gestione dei flussi informativi verso enti e autorità
- formazione del personale in materia di immigrazione e lavoro

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali**, amministratori e dirigenti, personale delle risorse umane, dipendenti e collaboratori coinvolti nella gestione dei rapporti di lavoro, consulenti, fornitori e partner operativi.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **rispetto della normativa in materia di immigrazione e lavoro**
- **tutela dei diritti dei lavoratori stranieri**
- **trasparenza e correttezza nella gestione dei rapporti di lavoro**
- **tracciabilità delle procedure di assunzione e gestione**
- **responsabilità nella selezione e gestione dei partner**

È espressamente vietato:

- impiegare lavoratori stranieri privi di permesso di soggiorno valido
- favorire l'ingresso o la permanenza irregolare di cittadini stranieri
- omettere controlli sulla documentazione dei lavoratori
- utilizzare fornitori o partner non conformi alla normativa

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- verifica dei requisiti di soggiorno dei lavoratori
- gestione dei processi di assunzione e amministrazione del personale
- controllo dei fornitori e delle catene di appalto
- monitoraggio della documentazione e degli aggiornamenti
- formazione, sensibilizzazione e gestione delle segnalazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-duodecies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi alla gestione del personale e dei rapporti di lavoro.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alla gestione dei lavoratori stranieri
- monitora la regolarità della documentazione
- controlla i rapporti con fornitori e appaltatori
- analizza segnalazioni e anomalie relative a possibili violazioni
- promuove iniziative formative in materia di immigrazione e lavoro

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di impiego di cittadini di paesi terzi irregolari richiede un approccio organizzativo fondato su:

- **verifica sistematica della regolarità dei lavoratori**
- **controllo dei processi di assunzione e gestione del personale**
- **monitoraggio dei fornitori e delle catene di appalto**
- **tutela dei diritti dei lavoratori**
- **diffusione di una cultura dell'Ente orientata alla legalità e alla responsabilità sociale**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, correttezza e tutela dei diritti dei lavoratori**

Art 25-terdecies - Razzismo e xenofobia

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-terdecies del D.Lgs. 231/2001, concernenti i delitti di razzismo e xenofobia, con particolare riferimento alla fattispecie di cui all'art. 604-bis c.p., relativa alla propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi a comportamenti discriminatori, anche indiretti, che possano configurare responsabilità per l'ente**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nella gestione delle attività aziendali, al fine di prevenire fenomeni di discriminazione, odio o intolleranza**

Le organizzazioni possono essere esposte al rischio di porre in essere, anche inconsapevolmente, comportamenti discriminatori o di favorire la diffusione di contenuti offensivi o incitanti all'odio, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- gestione delle risorse umane e dei rapporti interpersonali
- comunicazione interna ed esterna
- utilizzo di strumenti informatici e piattaforme digitali
- attività di marketing e pubblicità
- rapporti con clienti, fornitori e stakeholder

La prevenzione dei reati di cui all'art. 25-terdecies richiede pertanto:

- promozione di una cultura dell'Ente inclusiva e rispettosa delle diversità
- adozione di codici di comportamento chiari contro ogni forma di discriminazione
- controllo dei contenuti comunicativi e informativi
- formazione del personale sui temi della diversità e dell'inclusione
- sistemi di segnalazione e gestione delle condotte discriminatorie

Inquadramento normativo dei reati presupposto

L'art. 25-terdecies del D.Lgs. 231/2001 richiama la seguente fattispecie normativa:

- Art. 604-bis c.p. – Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa

In sintesi:

- punisce la **propaganda di idee fondate sulla superiorità o sull'odio razziale o etnico**
- sanziona **l'istigazione a commettere e la commissione di atti di discriminazione per motivi razziali, etnici, nazionali o religiosi**
- sanziona altresì **l'istigazione a commettere e la commissione di atti di violenza per i medesimi motivi**

- rileva anche quando le **condotte sono realizzate mediante strumenti idonei alla diffusione nei confronti di un pubblico indeterminato**
- prevede circostanze **aggravanti nei casi espressamente previsti dalla legge**

Per qualsiasi organizzazione, tali fattispecie rappresentano un rischio concreto, soprattutto in contesti caratterizzati da interazioni sociali, comunicazione diffusa e gestione del personale.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione dei reati di cui all'art. 25-terdecies può emergere in relazione a processi quali:

- gestione delle relazioni tra dipendenti e collaboratori
- comunicazione dell'Ente interna ed esterna
- gestione dei contenuti digitali e social media
- attività commerciali e di marketing
- selezione e gestione dei fornitori e partner

Tali attività richiedono particolare attenzione al fine di garantire il rispetto dei principi di uguaglianza, dignità e non discriminazione.

a) Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione delle risorse umane e dei rapporti interni

Il rischio può emergere:

- in comportamenti discriminatori nei confronti di dipendenti o candidati
- nella creazione di ambienti di lavoro ostili o offensivi
- nella tolleranza di linguaggi o atteggiamenti inappropriati

Principio guida: rispetto, inclusione e pari opportunità.

b) Comunicazione interna ed esterna

Il rischio può emergere:

- nella diffusione di contenuti discriminatori o offensivi
- nell'utilizzo improprio dei canali aziendali (e-mail, intranet, social media)
- nella pubblicazione di messaggi non conformi ai valori aziendali

Principio guida: responsabilità e controllo dei contenuti comunicativi.

c) Attività di marketing e promozione

Il rischio può emergere:

- nella creazione di campagne pubblicitarie con contenuti stereotipati o discriminatori
- nell'utilizzo di immagini o messaggi offensivi

- nella mancata verifica dei contenuti prima della diffusione

Il principio guida è: comunicazione etica e rispettosa.

d) Gestione dei rapporti con terzi

Il rischio può emergere:

- nella collaborazione con soggetti che adottano comportamenti discriminatori
- nella mancata vigilanza sui partner commerciali
- nella gestione non conforme delle relazioni con clienti o fornitori

Principio guida: coerenza etica lungo tutta la filiera relazionale.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-terdecies, tra cui:

- gestione dei sistemi informativi e delle comunicazioni digitali
- gestione dei contenuti web e social
- processi di selezione e valutazione del personale
- organizzazione di eventi aziendali
- formazione e comunicazione interna

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, personale delle risorse umane, dipendenti e collaboratori, addetti alla comunicazione e al marketing, consulenti, fornitori e partner.**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **rispetto della dignità umana e delle diversità**
- **uguaglianza e non discriminazione**
- **correttezza e responsabilità nelle comunicazioni**
- **inclusione e valorizzazione delle differenze**
- **prevenzione di ogni forma di odio o intolleranza**

È espressamente vietato:

- diffondere idee basate sulla superiorità o sull'odio razziale o etnico
- porre in essere comportamenti discriminatori per motivi razziali, etnici o religiosi
- utilizzare linguaggi offensivi o incitanti all'odio
- tollerare comportamenti discriminatori all'interno dell'organizzazione
- diffondere contenuti non conformi ai principi di inclusione e rispetto

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione dei comportamenti e delle relazioni interne
- controllo dei contenuti comunicativi e promozionali
- utilizzo corretto degli strumenti informatici e digitali
- selezione e monitoraggio dei partner
- formazione e sensibilizzazione sui temi della diversità e inclusione
- gestione delle segnalazioni e delle violazioni

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-terdecies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi alla gestione delle relazioni interne ed esterne e delle comunicazioni.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alla prevenzione delle discriminazioni
- monitora i contenuti comunicativi e i comportamenti organizzativi
- controlla i sistemi di segnalazione e gestione delle violazioni
- analizza eventuali episodi di discriminazione o condotte inappropriate
- promuove iniziative formative sui temi dell'inclusione e del rispetto

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di razzismo e xenofobia richiede un approccio organizzativo fondato su:

- **promozione attiva di una cultura inclusiva**
- **controllo dei comportamenti e delle comunicazioni**
- **formazione continua del personale**
- **gestione efficace delle segnalazioni**
- **coerenza etica nei rapporti interni ed esterni**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di uguaglianza, dignità e rispetto reciproco.**

Art 25-quaterdecies - Frode in competizioni sportive

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-quaterdecies del D.Lgs. 231/2001, concernenti la frode in competizioni sportive e l'esercizio abusivo di attività di gioco o di scommessa, con riferimento alle fattispecie previste dalla L. 401/1989.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi a comportamenti illeciti nell'ambito delle competizioni sportive e delle attività di gioco e scommessa**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Le organizzazioni possono essere esposte al rischio di coinvolgimento, diretto o indiretto, in condotte che alterano il regolare svolgimento di competizioni sportive o che integrano esercizio abusivo di attività di gioco o scommessa, con conseguenti responsabilità penali e amministrative.

In particolare, tali rischi possono emergere in relazione a:

- sponsorizzazioni e rapporti con società sportive
- organizzazione o partecipazione a eventi sportivi
- gestione di attività promozionali e commerciali collegate al gioco
- utilizzo di piattaforme digitali e strumenti di pagamento
- rapporti con partner commerciali operanti nel settore del gioco e delle scommesse

La prevenzione dei reati di cui all'art. 25-quaterdecies richiede pertanto:

- verifica della legalità delle attività sportive e di gioco con cui l'ente interagisce
- controllo dei partner e delle controparti commerciali
- trasparenza nelle sponsorizzazioni e nei rapporti con il mondo sportivo
- formazione del personale sui rischi specifici del settore
- adozione di procedure di controllo e monitoraggio

Inquadramento normativo dei reati presupposto

L'art. 25-quaterdecies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- Art. 1 L. 401/1989 – Frode in competizioni sportive
- Art. 4 L. 401/1989 – Esercizio abusivo di attività di giuoco o di scommessa

In sintesi:

- la frode in competizioni sportive si configura in caso di **offerta, promessa o dazione di denaro o altra utilità finalizzata ad alterare il risultato di una competizione sportiva**
- rientrano nella medesima fattispecie anche le condotte di **accettazione o comunque di partecipazione alla manipolazione dell'evento sportivo**
- l'esercizio abusivo di attività di gioco o di scommessa si configura in caso di **organizzazione, gestione o esercizio non autorizzato di giochi o scommesse**

- assumono rilievo, a tal fine, anche **la raccolta abusiva di scommesse nonché l'utilizzo di apparecchi o piattaforme non conformi alla normativa vigente**
- le fattispecie sopra indicate risultano **aggravate in presenza di modalità organizzate ovvero di coinvolgimento di una pluralità di soggetti**

Per qualsiasi organizzazione, tali fattispecie rappresentano rischi concreti soprattutto in presenza di relazioni con il settore sportivo o con operatori del gioco.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione dei reati di cui all'art. 25-quaterdecies può emergere in relazione a processi quali:

- gestione di rapporti con enti sportivi
- sponsorizzazioni e partnership commerciali
- organizzazione di eventi e iniziative promozionali
- gestione di piattaforme digitali e transazioni economiche
- selezione e monitoraggio di fornitori e partner

Tali attività richiedono particolare attenzione al fine di garantire la legalità e la trasparenza delle operazioni.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Sponsorizzazioni e rapporti con il settore sportivo

Il rischio può emergere:

- nell'utilizzo delle sponsorizzazioni per finalità illecite
- nella gestione non trasparente dei rapporti con società o atleti
- nel coinvolgimento in pratiche di alterazione delle competizioni
- **Principio guida: trasparenza e integrità nei rapporti sportivi.**

b) Organizzazione e partecipazione a eventi sportivi

Il rischio può emergere:

- nella manipolazione dei risultati sportivi
- nella gestione non conforme degli eventi
- nel coinvolgimento di soggetti non qualificati o non autorizzati

Principio guida: correttezza e regolarità delle competizioni.

c) Attività legate al gioco e alle scommesse

Il rischio può emergere:

- nell'organizzazione o promozione di attività di gioco non autorizzate

- nella raccolta abusiva di scommesse
- nell'utilizzo di apparecchi o piattaforme non conformi

Principio guida: legalità e autorizzazione delle attività di gioco.

d) Gestione dei rapporti con partner e fornitori

Il rischio può emergere:

- nella collaborazione con operatori non autorizzati
- nella mancata verifica dei requisiti dei partner
- nella gestione non trasparente delle relazioni commerciali

Principio guida: selezione e controllo delle controparti.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-quaterdecies, tra cui:

- gestione dei flussi finanziari
- gestione dei contratti e delle sponsorizzazioni
- utilizzo dei sistemi informativi e delle piattaforme digitali
- attività di marketing e comunicazione
- gestione delle autorizzazioni e delle verifiche di conformità

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, personale coinvolto nella gestione commerciale e marketing, dipendenti e collaboratori, addetti alla gestione finanziaria, consulenti, fornitori e partner**

L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto della normativa in materia di sport e gioco**
- **trasparenza nelle relazioni commerciali**
- **correttezza e integrità nelle competizioni sportive**
- **tracciabilità delle operazioni**
- **responsabilità nella selezione dei partner**

È espressamente vietato:

- offrire o accettare denaro o utilità per alterare competizioni sportive
- partecipare a pratiche di manipolazione dei risultati
- esercitare attività di gioco o scommessa in assenza di autorizzazione
- utilizzare apparecchi o strumenti non conformi alla normativa
- collaborare con soggetti coinvolti in attività illecite

Ogni dipendente o collaboratore che **rilevi anomalie o condotte sospette** è tenuto a segnalarle tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione delle sponsorizzazioni e dei rapporti sportivi
- verifica della legalità delle attività di gioco e scommessa
- controllo dei partner e dei fornitori
- tracciabilità dei flussi finanziari
- monitoraggio delle attività promozionali
- formazione e sensibilizzazione del personale
- gestione delle segnalazioni e delle anomalie

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con specifico riferimento ai reati di cui all'art. 25-quaterdecies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi ai rapporti con il settore sportivo e alle attività di gioco e scommessa.

In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alle sponsorizzazioni e agli eventi sportivi
- monitora la regolarità delle attività connesse al gioco e alle scommesse
- controlla i rapporti con partner e fornitori
- analizza eventuali segnalazioni di anomalie o comportamenti illeciti
- promuove iniziative formative sui rischi specifici

L'OdV può richiedere documentazione, effettuare audizioni e redigere report periodici agli organi societari competenti, contenenti criticità, raccomandazioni e misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati in materia di frodi sportive e gioco abusivo richiede un approccio organizzativo fondato su:

- **trasparenza e correttezza nei rapporti con il settore sportivo**
- **controllo delle attività di gioco e scommessa**
- **verifica dei partner e delle controparti**
- **monitoraggio dei flussi finanziari**
- **formazione continua del personale**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che le attività aziendali siano svolte nel pieno rispetto dei principi di legalità, integrità e correttezza.**

Art 25-quinquiesdecies - Reati tributari

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-quinquiesdecies del D.Lgs. 231/2001, concernenti i reati tributari disciplinati dal D.Lgs. n. 74/2000.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi fiscali e tributari connessi alla gestione dell'Ente**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nella gestione degli adempimenti fiscali e contabili**

Qualsiasi impresa, indipendentemente dal settore di attività, è esposta al rischio di commissione di reati tributari, in relazione a:

- predisposizione e presentazione delle dichiarazioni fiscali
- gestione della contabilità generale e fiscale
- registrazione delle fatture attive e passive
- gestione dei rapporti con consulenti fiscali e revisori
- gestione dei crediti d'imposta e compensazioni
- conservazione della documentazione contabile

In tali contesti possono emergere rischi connessi a comportamenti illeciti finalizzati ad ottenere vantaggi fiscali indebiti, quali:

- utilizzo di fatture per operazioni inesistenti
- alterazione dei dati contabili
- sotto-dichiarazione dei ricavi
- indebita compensazione di crediti fiscali
- occultamento o distruzione di documentazione
- sottrazione fraudolenta al pagamento delle imposte

La prevenzione di tali reati richiede pertanto:

- adeguate misure organizzative
- procedure contabili e fiscali formalizzate
- sistemi di controllo interno e tracciabilità
- una cultura dell'Ente orientata alla correttezza fiscale

Inquadramento normativo dei reati presupposto

L'art. 25-quinquiesdecies del D.Lgs. 231/2001 richiama diverse fattispecie di reato previste dal D.Lgs. n. 74/2000.

Tra i principali reati rilevanti rientrano:

- Art. 2 D.Lgs. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- Art. 3 D.Lgs. 74/2000 – Dichiarazione fraudolenta mediante altri artifici
- Art. 4 D.Lgs. 74/2000 – Dichiarazione infedele
- Art. 5 D.Lgs. 74/2000 – Omessa dichiarazione

- Art. 8 D.Lgs. 74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti
- Art. 10 D.Lgs. 74/2000 – Occultamento o distruzione di documenti contabili
- Art. 10-quater D.Lgs. 74/2000 – Indebita compensazione
- Art. 11 D.Lgs. 74/2000 – Sottrazione fraudolenta al pagamento di imposte

La commissione di tali reati può comportare rilevanti sanzioni pecuniarie e interdittive, con impatti significativi sulla continuità dell'Ente.

In sintesi:

- La dichiarazione fraudolenta implica **l'uso di elementi falsi o artifici per ridurre il carico fiscale**
- La dichiarazione infedele consiste **nell'indicazione non veritiera dei dati fiscali**
- L'omessa dichiarazione riguarda la **mancata presentazione delle dichiarazioni obbligatorie**
- **L'emissione o utilizzo di fatture false** costituisce una delle principali modalità fraudolente
- **L'occultamento documentale** ostacola le attività di controllo
- **L'indebita compensazione** riguarda l'utilizzo non spettante di crediti fiscali
- **La sottrazione fraudolenta** mira a evitare il pagamento delle imposte

Per un'impresa, tali fattispecie si manifestano soprattutto nei processi amministrativo-contabili e fiscali.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

I principali processi esposti sono:

- gestione della contabilità generale
- predisposizione delle dichiarazioni fiscali
- gestione delle fatture attive e passive
- gestione dei rapporti con consulenti fiscali
- gestione dei crediti d'imposta
- gestione delle compensazioni fiscali
- archiviazione e conservazione documentale

Attività sensibili: aree a rischio primario

a) Gestione della contabilità e delle dichiarazioni fiscali
Area a elevato rischio di manipolazione dei dati.

Il rischio può emergere:

- nella registrazione delle operazioni contabili
- nella predisposizione delle dichiarazioni fiscali
- nella determinazione del reddito imponibile

Principio guida: veridicità, completezza e tracciabilità dei dati contabili.

b) Gestione delle fatture attive e passive
Area critica per l'utilizzo o emissione di documenti inesistenti.

Il rischio può emergere:

- nella registrazione di fatture per operazioni inesistenti
- nella creazione di costi fittizi

Principio guida: effettività delle operazioni e controlli documentali.

c) Gestione dei crediti d'imposta e compensazioni
Area a rischio di indebita compensazione.

Il rischio può emergere:

- nell'utilizzo di crediti non spettanti
- nella compensazione oltre i limiti consentiti

Principio guida: legittimità e verifica preventiva dei crediti.

d) Conservazione della documentazione contabile
Area sensibile per possibili condotte di occultamento.

Il rischio può emergere:

- nella distruzione o mancata conservazione dei documenti
- nell'alterazione della documentazione

Principio guida: integrità, completezza e accessibilità della documentazione.

Attività strumentali

Attività che possono agevolare condotte illecite:

- gestione dei flussi finanziari
- procedure di acquisto
- gestione dei fornitori
- selezione e gestione dei consulenti
- gestione dei sistemi informativi contabili

Esempi di criticità:

- fatturazioni fittizie
- registrazioni contabili non corrette
- utilizzo improprio di crediti fiscali
- carenza di controlli interni

Destinatari

La presente Parte Speciale si applica **ad amministratori, dirigenti, dipendenti, collaboratori, consulenti e partner.**

Il rispetto del Modello dipende **dal ruolo effettivo svolto**, con particolare riferimento alle funzioni amministrative, contabili e fiscali.

Principi generali di comportamento

La gestione degli adempimenti fiscali deve essere improntata a:

- **legalità**

- **trasparenza**
- **correttezza contabile**
- **tracciabilità**

È espressamente vietato:

- utilizzare fatture o documenti per operazioni inesistenti
- alterare dati contabili o fiscali
- omettere dichiarazioni obbligatorie
- effettuare compensazioni indebite
- occultare o distruggere documentazione

Ogni dipendente o collaboratore che **rilevi anomalie o irregolarità** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo

La Fondazione adotta protocolli relativi a:

- gestione della contabilità
- predisposizione delle dichiarazioni fiscali
- gestione delle fatture
- gestione dei crediti d'imposta
- compensazioni fiscali
- conservazione documentale
- rapporti con consulenti fiscali

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza (OdV) vigila sull'efficace attuazione della presente Parte Speciale.

In particolare:

- verifica la corretta applicazione dei protocolli
- monitora i processi contabili e fiscali
- controlla la gestione delle dichiarazioni
- analizza i rapporti con consulenti fiscali
- verifica la tracciabilità dei flussi finanziari
- gestisce le segnalazioni
- promuove la formazione

L'OdV può:

- richiedere documentazione
- effettuare verifiche e audit
- redigere report periodici

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati tributari richiede:

- **trasparenza nei processi contabili**
- **tracciabilità delle operazioni**
- **controlli interni efficaci**

- **verifica dei soggetti terzi**
- **formazione continua**

La presente Parte Speciale rappresenta una guida operativa per garantire che la gestione fiscale e contabile avvenga nel rispetto dei principi di: **legalità, correttezza e trasparenza.**

Art 25-sexiesdecies - Contrabbando

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-sexiesdecies del D.Lgs. 231/2001, concernenti i reati di contrabbando e le violazioni in materia di accise.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione delle merci, dei flussi doganali e dei prodotti soggetti ad accisa**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività logistiche, commerciali e fiscali**

Nel contesto economico attuale, caratterizzato da mercati globalizzati e catene di approvvigionamento complesse, le imprese operano attraverso importazioni, esportazioni e movimentazioni di merci soggette a controlli doganali e fiscali.

Tali attività espongono le organizzazioni al rischio di commissione di reati connessi al contrabbando, alla sottrazione al pagamento di diritti doganali e accise, nonché alla gestione irregolare di prodotti soggetti a regime fiscale speciale (quali prodotti energetici, alcolici e tabacchi).

In particolare, tali rischi possono emergere in relazione a:

- operazioni di importazione ed esportazione di merci
- gestione dei prodotti soggetti ad accisa
- dichiarazioni doganali e documentazione commerciale
- movimentazione e stoccaggio delle merci
- rapporti con autorità doganali e fiscali
- gestione dei fornitori e dei partner logistici

La prevenzione dei reati di contrabbando richiede pertanto:

- procedure di controllo interne sui flussi di merci e documenti doganali
- tracciabilità delle operazioni commerciali e logistiche
- corretta gestione fiscale dei prodotti soggetti ad accisa
- cultura dell'Ente orientata alla legalità e al rispetto delle normative doganali e tributarie

Inquadramento normativo dei reati presupposto

L'art. 25-sexiesdecies del D.Lgs. 231/2001 richiama le fattispecie di contrabbando previste dalla normativa doganale e dalle disposizioni in materia di accise.

Tra i principali reati rilevanti rientrano:

- Art. 78 D.Lgs. n. 141/2024 – Contrabbando per omessa dichiarazione
- Art. 79 D.Lgs. n. 141/2024 – Contrabbando per dichiarazione infedele
- Art. 80 D.Lgs. n. 141/2024 – Contrabbando nel movimento delle merci marittimo, aereo e nei laghi di confine
- Art. 81 D.Lgs. n. 141/2024 – Contrabbando per indebito uso di merci importate con riduzione totale o parziale dei diritti

- Art. 82 D.Lgs. n. 141/2024 – Contrabbando nell'esportazione di merci ammesse a restituzione di diritti
- Art. 83 D.Lgs. n. 141/2024 – Contrabbando nell'esportazione temporanea e nei regimi di uso particolare e di perfezionamento
- Art. 84 D.Lgs. n. 141/2024 – Contrabbando di tabacchi lavorati
- Art. 86 D.Lgs. n. 141/2024 – Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati

Nonché le fattispecie previste dal Testo Unico delle Accise (D.Lgs. n. 504/1995):

- Art. 40 – Sottrazione all'accertamento o al pagamento dell'accisa sui prodotti energetici
- Art. 40-bis – Sottrazione all'accertamento o al pagamento dell'accisa sui tabacchi lavorati
- Art. 40-quinquies – Vendita di tabacchi lavorati senza autorizzazione o acquisto da persone non autorizzate alla vendita
- Art. 41 – Fabbricazione clandestina di alcole e bevande alcoliche
- Art. 42 – Associazione a scopo di fabbricazione clandestina di alcole e di bevande alcoliche
- Art. 43 – Sottrazione all'accertamento ed al pagamento dell'accisa sull'alcole e bevande alcoliche
- Art. 46 – Alterazione di congegni, impronte e contrassegni
- Art. 47 – Deficienze ed eccedenze nel deposito e nella circolazione dei prodotti soggetti ad accisa
- Art. 48 – Irregolarità nell'esercizio degli impianti di lavorazione e di deposito di prodotti sottoposti ad accisa
- Art. 49 – Irregolarità nella circolazione

In sintesi:

- il contrabbando si configura quando **merci vengono introdotte o sottratte ai controlli doganali senza corretta dichiarazione o pagamento dei diritti**
- le **dichiarazioni infedeli o incomplete** possono determinare indebiti vantaggi economici
- la **gestione irregolare** dei prodotti soggetti ad accisa comporta evasione fiscale
- la **fabbricazione clandestina e la distribuzione non autorizzata** alterano il mercato e ledono gli interessi erariali
- **l'alterazione di strumenti di controllo e la falsificazione dei contrassegni** compromettono il sistema di vigilanza fiscale

Per qualsiasi impresa coinvolta in attività logistiche, commerciali o produttive, tali fattispecie rappresentano rischi concretamente configurabili.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio di commissione di reati di contrabbando può emergere in relazione a processi quali:

- gestione delle operazioni di import/export
- predisposizione delle dichiarazioni doganali
- gestione dei prodotti soggetti ad accisa
- movimentazione, deposito e trasporto delle merci
- rapporti con spedizionieri, doganalisti e autorità competenti
- gestione della documentazione commerciale e fiscale

Tali attività richiedono particolare attenzione al fine di garantire legalità, trasparenza e corretto adempimento degli obblighi fiscali.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione delle operazioni di importazione ed esportazione

Il rischio può emergere:

- nell'omessa dichiarazione delle merci
- nella dichiarazione infedele del valore, quantità o natura delle merci
- nell'uso improprio di regimi doganali agevolati

Principio guida: correttezza, completezza e veridicità delle dichiarazioni doganali.

b) Gestione dei prodotti soggetti ad accisa

Il rischio può emergere:

- nella sottrazione al pagamento delle accise
- nella gestione irregolare dei depositi fiscali
- nella circolazione non autorizzata dei prodotti

Principio guida: rispetto rigoroso della normativa fiscale e tracciabilità dei prodotti.

c) Movimentazione e deposito delle merci

Il rischio può emergere:

- in difformità tra giacenze fisiche e contabili
- in movimentazioni non tracciate
- in utilizzo di documentazione non conforme

Principio guida: tracciabilità completa dei flussi logistici.

d) Rapporti con partner logistici e fornitori

Il rischio può emergere:

- nell'affidamento a operatori non qualificati
- nella partecipazione indiretta a operazioni illecite
- nell'assenza di controlli sui partner commerciali

Principio guida: selezione e monitoraggio dei partner secondo criteri di affidabilità e compliance.

e) Relazioni con autorità doganali e fiscali

Il rischio può emergere:

- nella trasmissione di dati incompleti o non veritieri
- nell'ostacolo ai controlli
- nella mancata collaborazione con le autorità

Principio guida: trasparenza, collaborazione e correttezza istituzionale.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di contrabbando, tra cui:

- gestione amministrativa e fiscale
- gestione documentale e archiviazione
- controllo dei flussi logistici
- selezione e gestione dei fornitori
- formazione del personale in ambito doganale e accise

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito delle attività aziendali, quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner logistici e fornitori.**

L'obbligo di conformarsi al Modello 231 deriva dal **ruolo svolto nei processi sensibili, indipendentemente dalla qualifica formale.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto delle normative doganali e fiscali**
- **trasparenza e tracciabilità delle operazioni commerciali**
- **correttezza nelle dichiarazioni e nei rapporti con le autorità**
- **integrità nella gestione dei prodotti soggetti ad accisa**
- **controllo e responsabilità nei processi logistici**

È espressamente vietato:

- omettere o alterare dichiarazioni doganali
- sottrarre merci al controllo o al pagamento dei diritti
- gestire prodotti soggetti ad accisa in violazione delle norme
- utilizzare documentazione falsa o incompleta
- ostacolare le attività di controllo delle autorità
- intrattenere rapporti con operatori coinvolti in attività illecite

Ogni soggetto che **rilevi anomalie o comportamenti sospetti** è tenuto a segnalarli attraverso i canali previsti dal Modello.

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano:

- la gestione delle operazioni doganali e delle dichiarazioni
- la gestione dei prodotti soggetti ad accisa

- la tracciabilità dei flussi logistici e documentali
- la selezione e il controllo dei partner logistici
- la gestione dei rapporti con autorità doganali e fiscali
- la conservazione della documentazione
- la formazione del personale sui rischi di contrabbando

Tali protocolli rappresentano la traduzione operativa dei principi di prevenzione.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con riferimento ai reati di cui all'art. 25-sexiesdecies, l'attività dell'OdV si concentra sui processi sensibili al rischio di contrabbando e violazioni in materia di accise.

In particolare, l'OdV:

- verifica la correttezza delle operazioni doganali
- monitora la gestione dei prodotti soggetti ad accisa
- controlla la tracciabilità dei flussi logistici
- analizza i rapporti con partner e fornitori
- esamina le segnalazioni ricevute (whistleblowing)
- promuove attività di formazione e sensibilizzazione

L'OdV può richiedere documentazione, effettuare verifiche e predisporre report periodici con eventuali misure correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di contrabbando richiede un approccio organizzativo fondato su:

- **trasparenza nelle operazioni commerciali e doganali**
- **controllo e tracciabilità dei flussi di merci**
- **corretta gestione fiscale dei prodotti soggetti ad accisa**
- **collaborazione con le autorità competenti**
- **diffusione di una cultura dell'Ente orientata alla legalità**

La presente Parte Speciale rappresenta uno **strumento operativo volto a garantire che tutte le attività aziendali siano svolte nel rispetto delle normative doganali e fiscali, tutelando l'impresa dai rischi di responsabilità amministrativa e contribuendo a un sistema economico corretto e trasparente.**

Art 25-septiesdecies - Reati contro il patrimonio culturale

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-septiesdecies del D.Lgs. 231/2001, concernenti i delitti contro il patrimonio culturale.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione, circolazione, acquisizione e valorizzazione dei beni culturali**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali che possano incidere sul patrimonio culturale**

Nel contesto attuale, le imprese possono entrare in contatto con beni culturali in molteplici ambiti, quali operazioni commerciali, attività immobiliari, sponsorizzazioni, gestione di eventi, interventi edilizi o rapporti con enti pubblici e privati.

Tali interazioni espongono le organizzazioni al rischio di commissione di reati che incidono sulla tutela, conservazione e corretta circolazione dei beni culturali e paesaggistici.

In particolare, tali rischi possono emergere in relazione a:

- acquisto, vendita o detenzione di beni culturali
- gestione di opere d'arte o beni di valore storico-artistico
- operazioni di importazione ed esportazione
- interventi su immobili sottoposti a vincoli culturali o paesaggistici
- gestione documentale e certificativa relativa ai beni culturali
- rapporti con autorità di tutela e organismi pubblici

La prevenzione dei reati contro il patrimonio culturale richiede pertanto:

- procedure di controllo sulla provenienza, autenticità e legittima disponibilità dei beni culturali
- tracciabilità delle operazioni di acquisto, vendita, trasferimento e movimentazione
- verifica della conformità normativa nelle operazioni nazionali e internazionali
- controllo dell'affidabilità dei soggetti terzi coinvolti nelle operazioni aventi ad oggetto beni culturali
- cultura dell'Ente orientata alla tutela e al rispetto del patrimonio culturale

L'aggiornamento della presente Parte Speciale tiene conto delle modifiche normative intervenute sulla disciplina dei delitti contro il patrimonio culturale, con particolare riferimento all'art. 518-quater c.p. – Ricettazione di beni culturali, modificato dal Decreto-Legge 24 febbraio 2026, n. 23, convertito con Legge 24 aprile 2026, n. 54.

Tale aggiornamento comporta un rafforzamento dell'attenzione sui processi aziendali nei quali possano verificarsi attività di acquisizione, ricezione, detenzione, intermediazione o trasferimento di beni culturali, con particolare riguardo alla verifica della provenienza lecita dei beni e alla corretta identificazione delle controparti coinvolte.

Inquadramento normativo dei reati presupposto

L'art. 25-septiesdecies del D.Lgs. 231/2001 richiama le fattispecie di reato introdotte nel codice penale a tutela del patrimonio culturale.

Tra i principali reati rilevanti rientrano:

- Art. 518-bis c.p. – Furto di beni culturali
- Art. 518-ter c.p. – Appropriazione indebita di beni culturali
- Art. 518-quater c.p. – Ricettazione di beni culturali
- Art. 518-octies c.p. – Falsificazione in scrittura privata relativa a beni culturali
- Art. 518-novies c.p. – Violazioni in materia di alienazione di beni culturali
- Art. 518-decies c.p. – Importazione illecita di beni culturali
- Art. 518-undecies c.p. – Uscita o esportazione illecite di beni culturali
- Art. 518-duodecies c.p. – Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici
- Art. 518-quaterdecies c.p. – Contraffazione di opere d'arte

In sintesi:

- **il furto e l'appropriazione indebita riguardano la sottrazione o l'acquisizione illegittima di beni culturali**
- **la ricettazione concerne l'acquisto, la ricezione, la detenzione o l'intermediazione nella circolazione di beni culturali di provenienza illecita, anche attraverso condotte finalizzate a consentirne la successiva immissione nel mercato**
- **le falsificazioni documentali incidono sulla tracciabilità, autenticità e corretta rappresentazione delle informazioni relative ai beni culturali**
- **le violazioni nelle alienazioni compromettono la legittima circolazione dei beni culturali**
- **l'importazione ed esportazione illecita aggirano i controlli pubblici e le procedure autorizzative previste dalla normativa**
- **la distruzione o il deterioramento arrecano danni al patrimonio culturale e paesaggistico**
- **la contraffazione altera il mercato e compromette l'autenticità delle opere d'arte**

Per qualsiasi impresa, tali fattispecie rappresentano rischi concretamente configurabili, soprattutto in presenza di attività che coinvolgano beni di valore artistico, storico, archeologico o culturale.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

L'identificazione delle attività sensibili consente alla Fondazione di individuare i processi maggiormente esposti al rischio di commissione dei reati contro il patrimonio culturale e di predisporre adeguati presidi organizzativi e procedurali finalizzati alla prevenzione degli illeciti.

In qualsiasi organizzazione, il rischio di commissione di reati contro il patrimonio culturale può emergere in relazione a processi quali:

- acquisto e vendita di beni mobili o immobili di valore culturale
- gestione, conservazione e movimentazione di opere d'arte o beni storici
- organizzazione di eventi, mostre, esposizioni o iniziative di valorizzazione culturale
- interventi edilizi, manutentivi o conservativi su beni sottoposti a vincoli culturali o paesaggistici
- gestione delle operazioni nazionali e internazionali di trasferimento di beni culturali
- gestione della documentazione relativa alla provenienza, autenticità, titolarità e disponibilità dei beni
- gestione dei rapporti con intermediari, consulenti, operatori specializzati e soggetti coinvolti nella circolazione dei beni culturali

Tali attività richiedono particolare attenzione al fine di garantire legalità, tutela del patrimonio culturale e rispetto delle normative vigenti, assicurando che ogni operazione sia supportata da adeguata documentazione e da verifiche preventive sulla provenienza e legittimità dei beni coinvolti.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Acquisto, vendita e detenzione di beni culturali

Il rischio può emergere:

- nell'acquisto di beni culturali di provenienza illecita o privi di adeguata documentazione attestante la provenienza
- nella ricezione o detenzione di beni culturali derivanti da reato
- nella vendita o trasferimento di beni in violazione delle disposizioni normative previste a tutela del patrimonio culturale
- nell'acquisizione inconsapevole di beni contraffatti, rubati o oggetto di illecita circolazione

Particolare attenzione deve essere posta alle attività di verifica preventiva delle controparti, dei fornitori, degli intermediari e dei soggetti coinvolti nelle operazioni di acquisizione o trasferimento dei beni.

La Fondazione deve garantire che ogni operazione sia preceduta dalla verifica della provenienza lecita del bene, della documentazione disponibile e della legittimità della relativa circolazione.

Principio guida: verifica della provenienza lecita, dell'autenticità e della regolarità giuridica dei beni.

b) Gestione della documentazione e autenticità

Il rischio può emergere:

- nella falsificazione o alterazione di certificazioni, dichiarazioni o documenti relativi ai beni culturali
- nella rappresentazione non veritiera delle informazioni relative alla provenienza, proprietà o autenticità dei beni
- nell'utilizzo di documentazione incompleta, irregolare o non verificata
- nella mancata conservazione delle informazioni necessarie a ricostruire la storia del bene e le relative movimentazioni

La documentazione relativa ai beni culturali deve essere gestita secondo criteri di completezza, accuratezza, verificabilità e conservazione nel tempo.

Particolare rilevanza assume la corretta gestione delle informazioni relative alla provenienza dei beni, al fine di prevenire condotte riconducibili alla ricettazione di beni culturali o ad altre fattispecie previste dagli artt. 518-bis e seguenti del codice penale.

Principio guida: autenticità, completezza, integrità e verificabilità della documentazione.

c) Operazioni di importazione ed esportazione

Il rischio può emergere:

- nell'esportazione di beni culturali in assenza delle autorizzazioni previste
- nell'importazione di beni culturali provenienti da circuiti illeciti
- nell'utilizzo di documentazione non corretta o incompleta nelle procedure doganali e amministrative
- nell'aggiramento dei controlli previsti dalle autorità competenti

Le operazioni internazionali aventi ad oggetto beni culturali devono essere effettuate nel rispetto delle disposizioni nazionali e internazionali applicabili, verificando preventivamente la documentazione autorizzativa e la legittima provenienza dei beni.

Principio guida: rispetto delle procedure autorizzative e delle normative nazionali e internazionali applicabili.

d) Interventi su beni culturali e paesaggistici

Il rischio può emergere:

- in lavori eseguiti senza le necessarie autorizzazioni su beni sottoposti a tutela
- nel danneggiamento, deterioramento o alterazione di beni culturali o paesaggistici
- nell'utilizzo improprio di immobili o beni sottoposti a vincolo
- nella mancata osservanza delle prescrizioni impartite dalle autorità competenti

Gli interventi su beni culturali o paesaggistici devono essere preceduti dalla verifica dei vincoli esistenti e dall'acquisizione delle eventuali autorizzazioni richieste dalla normativa vigente.

Principio guida: tutela, conservazione e rispetto dei vincoli normativi applicabili.

e) Gestione di opere d'arte e mercato artistico

Il rischio può emergere:

- nella commercializzazione o acquisizione di opere contraffatte
- nella partecipazione a circuiti di circolazione illecita di beni culturali

- nell'assenza di adeguati controlli sugli intermediari e sui soggetti coinvolti nelle operazioni
- nella mancata verifica dell'affidabilità delle controparti commerciali

La gestione di opere d'arte e beni culturali deve essere improntata a criteri di trasparenza, correttezza e adeguata verifica delle informazioni relative ai beni oggetto di trattativa.

Particolare attenzione deve essere riservata ai rapporti con galleristi, intermediari, consulenti, case d'asta e altri operatori specializzati, assicurando la raccolta e conservazione della documentazione relativa alle operazioni effettuate.

Principio guida: integrità, trasparenza e controllo nella gestione del mercato dei beni culturali.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati contro il patrimonio culturale, tra cui:

- gestione amministrativa e contrattuale relativa all'acquisto, vendita o trasferimento di beni
- gestione documentale e archiviazione delle informazioni relative ai beni culturali
- selezione, qualificazione e gestione di fornitori, intermediari e consulenti
- gestione delle operazioni internazionali e dei relativi adempimenti autorizzativi
- gestione dei rapporti con autorità pubbliche e organismi di tutela
- formazione del personale sui rischi legali e culturali connessi alle attività aziendali

La Fondazione assicura che tali attività siano svolte secondo principi di segregazione dei compiti, tracciabilità delle decisioni e adeguata documentazione delle operazioni.

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito delle attività aziendali potenzialmente rilevanti ai fini della normativa in materia di tutela del patrimonio culturale, quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner commerciali e intermediari.**

I destinatari della presente Parte Speciale sono tenuti a conoscere e rispettare i principi, le regole di comportamento e i protocolli di controllo previsti dal Modello 231, **in relazione al ruolo ricoperto e alle attività svolte.**

L'obbligo di conformarsi al Modello 231 deriva dal coinvolgimento, diretto o indiretto, nei processi sensibili individuati e dalla necessità di assicurare che ogni attività dell'Ente sia svolta nel rispetto della normativa vigente e dei principi di tutela del patrimonio culturale.

In particolare, i soggetti coinvolti in attività di acquisizione, gestione, trasferimento, conservazione o valorizzazione di beni culturali devono operare garantendo:

- la verifica preventiva della provenienza e della legittima disponibilità dei beni
- la completezza e correttezza della documentazione relativa ai beni e alle operazioni effettuate
- la trasparenza nei rapporti con soggetti terzi, intermediari e operatori specializzati
- la tempestiva segnalazione di eventuali anomalie o situazioni potenzialmente rilevanti sotto il profilo normativo

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto della normativa in materia di beni culturali**
- **trasparenza e tracciabilità delle operazioni**
- **verifica della provenienza, autenticità e legittima circolazione dei beni**
- **tutela e valorizzazione del patrimonio culturale**
- **correttezza nei rapporti con autorità pubbliche, enti di tutela e soggetti terzi**
- **integrità nella gestione delle operazioni aventi ad oggetto beni culturali**
- **affidabilità e qualificazione dei soggetti coinvolti nei processi sensibili**

La Fondazione adotta misure organizzative volte a prevenire il rischio che, anche indirettamente, possano essere acquistati, ricevuti, detenuti, trasferiti o commercializzati beni culturali di provenienza illecita o privi di adeguata documentazione attestante la loro origine e legittima circolazione.

È espressamente vietato:

- acquistare, ricevere o detenere beni culturali di provenienza illecita o privi di adeguate verifiche sulla provenienza
- utilizzare, produrre o fornire documentazione falsa, alterata o non veritiera relativa ai beni culturali
- effettuare operazioni di importazione o esportazione di beni culturali senza le necessarie autorizzazioni
- porre in essere attività finalizzate ad aggirare i controlli delle autorità competenti
- danneggiare, deteriorare, alterare o utilizzare illecitamente beni culturali o paesaggistici
- commercializzare, acquistare o trasferire opere contraffatte o di dubbia autenticità
- instaurare rapporti con soggetti terzi privi di adeguata affidabilità o senza effettuare le necessarie verifiche preventive

Ogni soggetto destinatario della presente Parte Speciale è tenuto a **segnalare eventuali anomalie, irregolarità o comportamenti sospetti che possano assumere rilevanza ai fini della normativa in materia di delitti contro il patrimonio culturale.**

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi finalizzati alla prevenzione dei reati contro il patrimonio culturale.

Tali protocolli disciplinano in particolare:

- la verifica preventiva della provenienza, autenticità e disponibilità giuridica dei beni culturali
- la raccolta, verifica e conservazione della documentazione relativa ai beni acquisiti, trasferiti o gestiti
- la tracciabilità delle operazioni di acquisto, vendita, movimentazione e trasferimento
- la gestione delle operazioni di importazione ed esportazione e dei relativi adempimenti autorizzativi
- la verifica della conformità normativa degli interventi effettuati su beni sottoposti a vincoli culturali o paesaggistici

- la selezione e il controllo degli intermediari, fornitori, consulenti e partner commerciali coinvolti nelle attività sensibili
- la verifica dell'affidabilità delle controparti nelle operazioni aventi ad oggetto beni culturali
- la conservazione delle informazioni e della documentazione necessaria a ricostruire la storia delle operazioni effettuate
- la formazione del personale sui rischi specifici connessi ai delitti contro il patrimonio culturale

Con particolare riferimento al rischio di ricettazione di beni culturali di cui all'art. 518-quater c.p., la Fondazione assicura l'adozione di procedure volte a impedire l'ingresso nel proprio patrimonio o nei propri processi aziendali di beni di provenienza illecita, prevedendo adeguati controlli sulla documentazione disponibile, sulle controparti coinvolte e sulle modalità di acquisizione o trasferimento dei beni.

I protocolli adottati rappresentano **strumenti fondamentali di prevenzione e consentono di assicurare che le attività aziendali siano svolte secondo criteri di legalità, trasparenza e tracciabilità.**

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con riferimento ai reati di cui all'art. 25-septiesdecies del D.Lgs. 231/2001, l'attività dell'OdV si concentra sul monitoraggio dei processi sensibili maggiormente esposti al rischio di violazioni in materia di tutela del patrimonio culturale.

In particolare, l'OdV:

- verifica l'effettiva applicazione dei protocolli aziendali relativi alla gestione dei beni culturali
- controlla la corretta gestione della documentazione relativa alla provenienza, autenticità e disponibilità dei beni
- monitora le operazioni di acquisizione, trasferimento, importazione ed esportazione di beni culturali
- verifica la presenza di adeguati controlli sugli intermediari e sui soggetti terzi coinvolti
- analizza eventuali segnalazioni ricevute relative a comportamenti anomali o potenzialmente rilevanti
- verifica l'efficacia delle attività formative rivolte al personale coinvolto nei processi sensibili
- propone eventuali interventi correttivi o migliorativi del sistema di controllo interno

L'OdV può effettuare verifiche periodiche, richiedere documentazione, acquisire informazioni dai soggetti coinvolti nei processi sensibili e proporre alla Fondazione eventuali azioni correttive qualora siano rilevate criticità nell'applicazione delle procedure adottate.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati contro il patrimonio culturale richiede un approccio organizzativo fondato su:

- **trasparenza nelle operazioni e nella gestione documentale**
- **controllo della provenienza, autenticità e legittimità dei beni**
- **rispetto delle normative nazionali e internazionali applicabili**
- **adeguata verifica dei soggetti coinvolti nelle operazioni**
- **collaborazione con le autorità competenti e gli organismi di tutela**
- **diffusione di una cultura dell'Ente orientata alla responsabilità e alla protezione del patrimonio culturale**

La presente Parte Speciale rappresenta uno **strumento operativo volto a garantire che le attività aziendali si svolgano nel rispetto della normativa vigente, contribuendo alla tutela e valorizzazione del patrimonio culturale e prevenendo il rischio di responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001.**

Art 25-duodevicies - Riciclaggio beni culturali

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-duodevicies del D.Lgs. 231/2001, concernenti il riciclaggio di beni culturali e i delitti di devastazione e saccheggio di beni culturali e paesaggistici.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione e circolazione dei beni culturali, anche sotto il profilo della loro possibile provenienza illecita**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali che possano incidere sulla tutela del patrimonio culturale**

Nel contesto economico attuale, caratterizzato da una crescente circolazione internazionale di opere d'arte e beni culturali, le imprese possono trovarsi coinvolte, anche indirettamente, in operazioni che riguardano beni di provenienza illecita o che incidono sulla conservazione del patrimonio culturale e paesaggistico.

Tali attività espongono le organizzazioni al rischio di commissione di reati particolarmente gravi, che ledono interessi di rilevanza pubblica e collettiva.

In particolare, tali rischi possono emergere in relazione a:

- acquisto, vendita o intermediazione di beni culturali
- gestione di operazioni internazionali di trasferimento di opere
- rapporti con intermediari, collezionisti e operatori del mercato dell'arte
- attività immobiliari o interventi su beni di valore culturale o paesaggistico
- gestione di eventi, mostre o attività espositive
- gestione documentale relativa alla provenienza dei beni

La prevenzione dei reati richiede pertanto:

- verifiche approfondite sulla provenienza lecita dei beni
- tracciabilità delle operazioni e dei flussi finanziari
- controlli sui partner commerciali e intermediari
- cultura dell'Ente orientata alla tutela del patrimonio culturale

Inquadramento normativo dei reati presupposto

L'art. 25-duodevicies del D.Lgs. 231/2001 richiama specifiche fattispecie del codice penale introdotte a tutela del patrimonio culturale.

Tra i principali reati rilevanti rientrano:

- Art. 518-sexies c.p. – Riciclaggio di beni culturali
- Art. 518-terdecies c.p. – Devastazione e saccheggio di beni culturali e paesaggistici

In sintesi:

- **il riciclaggio di beni culturali si configura quando beni di provenienza illecita vengono sostituiti, trasferiti o impiegati al fine di ostacolarne l'identificazione**
- **la devastazione e il saccheggio riguardano condotte di distruzione, depredazione o grave danneggiamento di beni culturali o paesaggistici**
- **tali reati presentano un elevato disvalore sociale in quanto incidono su beni di interesse collettivo e identitario**
- **anche il coinvolgimento indiretto, tramite intermediari o operazioni commerciali, può determinare responsabilità per l'ente**

Per le imprese, tali fattispecie rappresentano rischi concreti soprattutto nei settori che operano con beni di valore storico-artistico o in contesti territoriali di particolare rilevanza culturale.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio può emergere in relazione a processi quali:

- acquisto e vendita di beni culturali
- intermediazione commerciale nel mercato dell'arte
- gestione di operazioni internazionali
- gestione dei flussi finanziari connessi alle operazioni
- rapporti con partner, consulenti e intermediari
- interventi su beni immobili di valore culturale o paesaggistico

Tali attività richiedono particolare attenzione al fine di garantire legalità, trasparenza e tutela del patrimonio.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Acquisto, vendita e intermediazione di beni culturali

Il rischio può emergere:

- nell'acquisto o vendita di beni di provenienza illecita
- nell'intermediazione in operazioni di riciclaggio
- nella mancata verifica della provenienza dei beni

Principio guida: due diligence rigorosa sulla provenienza e liceità dei beni.

b) Gestione dei flussi finanziari

Il rischio può emergere:

- nell'utilizzo di strumenti finanziari per occultare l'origine illecita dei beni
- in operazioni economiche non tracciate o anomale
- nella mancanza di controlli sui pagamenti

Principio guida: tracciabilità e trasparenza dei flussi finanziari.

c) Operazioni internazionali e trasferimento di beni

Il rischio può emergere:

- nel trasferimento transfrontaliero di beni illeciti
- nell'utilizzo di intermediari opachi
- nell'aggiramento dei controlli normativi

Principio guida: rispetto delle normative nazionali e internazionali.

d) Interventi su beni culturali e paesaggistici

Il rischio può emergere:

- in attività che comportano danneggiamento o distruzione
- in interventi non autorizzati
- in utilizzi incompatibili con la tutela dei beni

Principio guida: salvaguardia e conservazione del patrimonio.

e) Rapporti con partner e intermediari

Il rischio può emergere:

- nel coinvolgimento di soggetti operanti in contesti illeciti
- nell'assenza di controlli reputazionali
- nella partecipazione indiretta a condotte criminose

Principio guida: selezione e monitoraggio dei partner.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati in esame, tra cui:

- gestione amministrativa e contabile
- gestione dei contratti e delle operazioni commerciali
- gestione documentale e archiviazione
- controllo dei flussi finanziari
- formazione del personale sui rischi legali

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito delle attività aziendali, quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti e partner commerciali.**

L'obbligo di conformarsi al Modello 231 deriva dal **ruolo svolto nei processi sensibili.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto della normativa in materia di beni culturali**
- **trasparenza e tracciabilità delle operazioni**
- **tutela del patrimonio culturale e paesaggistico**
- **correttezza nei rapporti con soggetti terzi**
- **integrità nella gestione delle operazioni economiche**

È espressamente vietato:

- acquistare, vendere o intermediare beni culturali di provenienza illecita
- porre in essere operazioni di riciclaggio
- utilizzare strumenti finanziari per occultare attività illecite
- danneggiare, distruggere o saccheggiare beni culturali o paesaggistici
- intrattenere rapporti con soggetti coinvolti in attività illecite
- aggirare i controlli normativi e autorizzativi

Ogni soggetto è tenuto a **segnalare eventuali anomalie o comportamenti sospetti.**

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano:

- la verifica della provenienza dei beni culturali
- la tracciabilità dei flussi finanziari
- la gestione delle operazioni commerciali e internazionali
- la selezione e il monitoraggio dei partner
- la gestione documentale
- la conservazione delle informazioni
- la formazione del personale

Tali protocolli costituiscono strumenti fondamentali di prevenzione.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

Con riferimento ai reati di cui all'art. 25-duodevicies, l'attività dell'OdV si concentra sui processi sensibili al rischio di riciclaggio di beni culturali e devastazione o saccheggio.

In particolare, l'OdV:

- verifica la regolarità delle operazioni sui beni culturali
- controlla la tracciabilità dei flussi finanziari
- monitora le operazioni internazionali
- analizza i rapporti con partner e intermediari
- esamina le segnalazioni ricevute
- promuove attività formative

L'OdV può effettuare verifiche, richiedere documentazione e proporre azioni correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei reati di cui alla presente Parte Speciale richiede un approccio organizzativo fondato su:

- **trasparenza nelle operazioni e nei flussi finanziari**
- **controllo della provenienza dei beni**
- **rispetto delle normative nazionali e internazionali**
- **tutela attiva del patrimonio culturale e paesaggistico**
- **diffusione di una cultura dell'Ente orientata alla legalità**

La presente Parte Speciale rappresenta uno **strumento operativo volto a garantire che le attività aziendali siano svolte nel rispetto dei principi di tutela del patrimonio culturale,**

prevenendo il rischio di coinvolgimento in condotte di riciclaggio, devastazione o saccheggio e contribuendo alla salvaguardia di beni di valore collettivo.

Art 25-undevicies - Delitti contro gli animali

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-undevicies del D.Lgs. 231/2001, concernenti i delitti contro gli animali.*

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi alla gestione di attività che possano coinvolgere animali**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nello svolgimento delle attività aziendali**

Nel contesto attuale, le imprese possono entrare in contatto con animali in molteplici ambiti, quali attività produttive, logistiche, commerciali, eventi, ricerca, trasporto o gestione di forniture.

Tali attività espongono le organizzazioni al rischio di commissione di reati che incidono sul benessere e sulla tutela degli animali.

In particolare, tali rischi possono emergere in relazione a:

- gestione diretta o indiretta di animali
- organizzazione di eventi o attività che coinvolgono animali
- rapporti con fornitori, allevatori o trasportatori
- attività di trasporto e custodia
- utilizzo di animali in attività promozionali o produttive
- gestione di strutture o ambienti che ospitano animali

La prevenzione dei reati contro gli animali richiede pertanto:

- procedure di controllo sul benessere animale
- selezione qualificata dei fornitori e dei partner
- rispetto delle normative in materia di tutela degli animali
- cultura dell'Ente orientata al rispetto degli esseri viventi

Inquadramento normativo dei reati presupposto

L'art. 25-undevicies del D.Lgs. 231/2001 richiama le principali fattispecie di reato previste dal codice penale in materia di tutela degli animali.

Tra i principali reati rilevanti rientrano:

- Art. 544-bis c.p. – Uccisione di animali
- Art. 544-ter c.p. – Maltrattamento di animali
- Art. 544-quater c.p. – Spettacoli o manifestazioni vietati
- Art. 544-quinquies c.p. – Divieto di combattimenti tra animali
- Art. 638 c.p. – Uccisione o danneggiamento di animali altrui

In sintesi:

- **l'uccisione di animali è punita quando avviene senza necessità o per crudeltà**
- **il maltrattamento comprende comportamenti che cagionano sofferenze o lesioni**

- **gli spettacoli vietati includono eventi che comportano sevizie o sfruttamento**
- **i combattimenti tra animali costituiscono condotte particolarmente gravi**
- **il danneggiamento di animali altrui incide sul patrimonio e sulla tutela degli stessi**

Per qualsiasi impresa, tali fattispecie rappresentano rischi concreti laddove vi sia anche un coinvolgimento indiretto nella gestione o utilizzo di animali.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati.

In qualsiasi organizzazione, il rischio può emergere in relazione a processi quali:

- gestione e custodia di animali
- trasporto di animali vivi
- organizzazione di eventi o attività promozionali
- rapporti con fornitori e partner operanti nel settore animale
- gestione di strutture e ambienti
- attività operative che possono incidere indirettamente sugli animali

Tali attività richiedono particolare attenzione al fine di garantire il rispetto delle normative e del benessere animale.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Gestione e custodia di animali

Il rischio può emergere:

- in condizioni di detenzione non adeguate
- in comportamenti che causano sofferenza o lesioni
- nella mancata adozione di misure di tutela

Principio guida: rispetto del benessere animale e delle condizioni di vita adeguate.

b) Trasporto di animali

Il rischio può emergere:

- in modalità di trasporto non conformi
- in condizioni che causano stress o sofferenza
- nella violazione delle normative specifiche

Principio guida: sicurezza, dignità e tutela durante il trasporto.

c) Organizzazione di eventi o attività

Il rischio può emergere:

- nell'utilizzo improprio di animali

- nella partecipazione a spettacoli vietati
- in attività che comportano sfruttamento o maltrattamento

Principio guida: divieto di utilizzo degli animali in contesti lesivi.

d) Rapporti con fornitori e partner

Il rischio può emergere:

- nell'affidamento a soggetti non qualificati
- nel coinvolgimento in pratiche illecite
- nell'assenza di controlli sulla filiera

Principio guida: selezione e monitoraggio dei partner.

e) Attività operative e ambientali

Il rischio può emergere:

- in attività che causano danni indiretti agli animali
- in utilizzo improprio di strumenti o sostanze
- nella mancata prevenzione di situazioni di rischio

Principio guida: prevenzione e minimizzazione degli impatti sugli animali.

Attività strumentali

Alcune attività interne possono assumere rilievo strumentale rispetto ai reati contro gli animali, tra cui:

- gestione amministrativa e contrattuale
- gestione dei fornitori
- controllo operativo e logistico
- gestione della sicurezza
- formazione del personale

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito delle attività aziendali, quali **amministratori, dirigenti, dipendenti, collaboratori, consulenti e partner commerciali.**

L'obbligo di conformarsi al Modello 231 deriva dal **ruolo svolto nei processi sensibili**.

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto delle normative sulla tutela degli animali**
- **attenzione al benessere animale**
- **responsabilità nelle attività operative**
- **trasparenza nei rapporti con terzi**
- **integrità e rispetto degli esseri viventi**

È espressamente vietato:

- uccidere animali senza giustificazione
- maltrattare o causare sofferenze
- organizzare o partecipare a spettacoli vietati

- promuovere o favorire combattimenti tra animali
- danneggiare animali altrui
- collaborare con soggetti che pongano in essere tali condotte

Ogni soggetto è tenuto a **segnalare eventuali anomalie o comportamenti sospetti.**

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano:

- la gestione e custodia degli animali
- le modalità di trasporto
- la selezione e il controllo dei fornitori
- la gestione delle attività e degli eventi
- la prevenzione dei rischi operativi
- la formazione del personale
- la tracciabilità delle attività rilevanti

Tali protocolli rappresentano strumenti operativi di prevenzione.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza dell'Organismo di Vigilanza (OdV).

Con riferimento ai reati di cui all'art. 25-undevicies, l'attività dell'OdV si concentra sui processi sensibili al rischio di violazioni in materia di tutela degli animali.

In particolare, l'OdV:

- verifica la conformità delle attività aziendali
- controlla i rapporti con fornitori e partner
- monitora le attività operative
- analizza le segnalazioni ricevute
- promuove attività formative e di sensibilizzazione

L'OdV può effettuare verifiche, richiedere documentazione e proporre azioni correttive.

Conclusione: la prevenzione come processo organizzativo

La prevenzione dei delitti contro gli animali richiede un approccio organizzativo fondato su:

- **rispetto del benessere animale**
- **controllo delle attività e dei processi**
- **selezione responsabile dei partner**
- **formazione e sensibilizzazione del personale**
- **diffusione di una cultura dell'Ente etica**

La presente Parte Speciale rappresenta uno **strumento operativo volto a garantire che le attività aziendali siano svolte nel rispetto degli animali, prevenendo comportamenti illeciti e contribuendo a un modello organizzativo responsabile e sostenibile.**

Articolo 25-vicies - Reati commessi con l'uso di sistemi di intelligenza artificiale

> La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 25-vicies del D.Lgs. 231/2001, concernenti i reati commessi con l'uso di sistemi di intelligenza artificiale, con particolare riferimento alle fattispecie previste dagli artt. 437-bis e 612-quater del codice penale.

L'obiettivo di questa sezione è duplice:

1. **Fornire a tutti i destinatari del Modello una chiara comprensione dei rischi connessi all'utilizzo di sistemi di intelligenza artificiale e alle possibili condotte illecite realizzabili attraverso tali strumenti**
2. **Indicare in modo concreto e operativo i comportamenti da adottare e quelli da evitare nell'utilizzo, nella gestione e nel controllo dei sistemi di intelligenza artificiale**

Le organizzazioni possono essere esposte al rischio di coinvolgimento, diretto o indiretto, in condotte illecite connesse alla progettazione, allo sviluppo, all'addestramento, alla produzione, all'immissione sul mercato e all'utilizzo di sistemi di intelligenza artificiale, nonché alla diffusione di contenuti falsificati o alterati mediante tali sistemi.
In particolare, tali rischi possono emergere in relazione a:

- progettazione, sviluppo e addestramento di sistemi di intelligenza artificiale
- utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio
- gestione e supervisione dei sistemi di intelligenza artificiale
- adozione delle misure tecniche e organizzative di sicurezza
- utilizzo di sistemi di intelligenza artificiale nei processi aziendali
- produzione e diffusione di immagini, video, audio o altri contenuti generati o alterati mediante sistemi di intelligenza artificiale
- attività di marketing, comunicazione e gestione dei contenuti digitali
- gestione dei rapporti con fornitori e sviluppatori di sistemi di intelligenza artificiale
- utilizzo di piattaforme e strumenti di intelligenza artificiale messi a disposizione di dipendenti e collaboratori

La prevenzione dei reati di cui all'art. 25-vicies richiede pertanto:

- **adozione di adeguate misure tecniche e organizzative di sicurezza**
- **adeguata supervisione umana dei sistemi di intelligenza artificiale ad alto rischio**
- **controllo degli accessi e degli utilizzi dei sistemi di intelligenza artificiale**
- **verifica dei fornitori e dei sistemi utilizzati dall'organizzazione**
- **tracciabilità delle attività svolte mediante sistemi di intelligenza artificiale**
- **formazione del personale sui rischi connessi all'utilizzo dell'intelligenza artificiale**
- **adozione di procedure per la gestione e la diffusione dei contenuti generati o alterati mediante sistemi di intelligenza artificiale**

Inquadramento normativo dei reati presupposto
L'art. 25-vicies del D.Lgs. 231/2001 richiama le seguenti fattispecie normative:

- **Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi**

- **Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale**

Ai sensi dell'art. 25-vicies:

- in relazione al delitto di cui all'**art. 437-bis c.p.**, all'ente si applica la **sanzione pecuniaria da 600 a 1.000 quote**
- in relazione al delitto di cui all'**art. 612-quater c.p.**, all'ente si applica la **sanzione pecuniaria da 200 a 700 quote**
- nei casi previsti dai commi 1 e 2 si applicano inoltre le **sanzioni interdittive previste dall'art. 9, comma 2, lettere b), c), d) ed e), del D.Lgs. 231/2001**

In sintesi:

- l'**art. 437-bis c.p.** punisce, tra l'altro, l'omessa adozione delle necessarie misure tecniche di sicurezza e di **sorveglianza umana** relative ai sistemi di intelligenza artificiale ad alto rischio, quando da tali omissioni derivi un pericolo per la vita o l'incolumità pubblica o individuale
- la medesima disposizione disciplina anche l'**alterazione illecita di sistemi di intelligenza artificiale ad alto rischio**, quando da tale condotta derivi un pericolo per la vita o l'incolumità pubblica o individuale
- le condotte assumono maggiore gravità quando dal fatto deriva un **pericolo per la sicurezza dello Stato**
- l'art. 437-bis c.p. disciplina inoltre specificamente la condotta dell'**utilizzatore professionale** di sistemi di intelligenza artificiale ad alto rischio che ometta intenzionalmente di adottare le necessarie misure di sorveglianza umana
- l'**art. 612-quater c.p.** punisce la diffusione, senza il consenso della persona interessata, di **immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale**, quando tali contenuti siano idonei a indurre in inganno sulla loro genuinità e dalla condotta derivi un danno ingiusto alla persona
- il delitto di cui all'art. 612-quater c.p. è, di regola, **punibile a querela della persona offesa**, salvo i casi nei quali la legge prevede la procedibilità d'ufficio

Per qualsiasi organizzazione, tali fattispecie rappresentano rischi concreti soprattutto in presenza di un **utilizzo significativo di sistemi di intelligenza artificiale**, in particolare nei processi caratterizzati da elevati livelli di automazione, trattamento di dati, generazione di contenuti o impiego di sistemi ad alto rischio.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili costituisce il presupposto essenziale per l'efficace attuazione del Modello 231.

Per attività sensibili si intendono le attività aziendali nel cui ambito potrebbe essere commesso uno dei reati sopra richiamati, anche mediante l'utilizzo di sistemi, piattaforme o strumenti di intelligenza artificiale.

In qualsiasi organizzazione, il rischio di commissione dei reati di cui all'art. 25-vicies può emergere in relazione a processi quali:

- progettazione, sviluppo e addestramento di sistemi di intelligenza artificiale
- utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio
- gestione della sicurezza e della supervisione dei sistemi

- produzione, elaborazione e diffusione di contenuti mediante sistemi di intelligenza artificiale
- attività di marketing, comunicazione e gestione dei canali digitali
- selezione e gestione dei fornitori di tecnologie e servizi di intelligenza artificiale
- gestione degli accessi e delle autorizzazioni all'utilizzo degli strumenti di intelligenza artificiale

Tali attività richiedono particolare attenzione al fine di garantire **sicurezza, supervisione, tracciabilità, correttezza e rispetto dei diritti delle persone**.

Attività sensibili: aree a rischio primario
Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:
a) Progettazione, sviluppo e gestione di sistemi di intelligenza artificiale
Il rischio può emergere:

- nell'omessa adozione delle necessarie **misure tecniche di sicurezza**
- nell'assenza o nell'inadeguatezza dei sistemi di controllo e monitoraggio
- nella mancata prevenzione di malfunzionamenti o alterazioni del sistema
- nell'utilizzo di sistemi ad alto rischio senza adeguate misure di sicurezza
- nella gestione non corretta delle fasi di progettazione, addestramento e produzione

Principio guida: sicurezza, affidabilità e controllo dei sistemi di intelligenza artificiale.

b) Sorveglianza umana e utilizzo professionale dei sistemi di IA
Il rischio può emergere:

- nell'omessa predisposizione di adeguate procedure di **sorveglianza umana**
- nell'utilizzo professionale di sistemi ad alto rischio senza adeguato controllo
- nell'eccessiva delega di decisioni rilevanti ai sistemi automatizzati
- nella mancata verifica degli output prodotti dal sistema
- nell'assenza di soggetti responsabili del monitoraggio e dell'intervento umano

Principio guida: supervisione umana e responsabilità nell'utilizzo dell'intelligenza artificiale.

c) Alterazione e modifica dei sistemi di intelligenza artificiale
Il rischio può emergere:

- nella modifica non autorizzata dei sistemi
- nell'alterazione dei parametri o delle funzionalità dei sistemi ad alto rischio
- nell'accesso ai sistemi da parte di soggetti non autorizzati
- nella manipolazione del funzionamento dei sistemi
- nell'utilizzo di modifiche non adeguatamente verificate o documentate

Principio guida: integrità, controllo degli accessi e tracciabilità delle modifiche.

d) Produzione e diffusione di contenuti generati o alterati mediante IA
Il rischio può emergere:

- nella creazione di **immagini, video o voci falsificati o alterati**
- nella diffusione di contenuti senza il consenso della persona interessata
- nell'utilizzo di contenuti generati artificialmente per finalità illecite
- nella pubblicazione di contenuti idonei a essere confusi con contenuti autentici
- nell'utilizzo improprio di sistemi di generazione e manipolazione dei contenuti

Principio guida: correttezza, trasparenza e rispetto dei diritti delle persone nella gestione dei contenuti generati mediante IA.

e) Marketing, comunicazione e gestione dei contenuti digitali
Il rischio può emergere:

- nell'utilizzo di contenuti artificialmente generati o modificati nelle comunicazioni aziendali
- nella pubblicazione di immagini, video o audio senza adeguate verifiche
- nell'utilizzo di strumenti di IA per attività di comunicazione esterna
- nella diffusione di contenuti suscettibili di arrecare un danno ingiusto a terzi
- nella mancata verifica dei contenuti prima della loro pubblicazione

Principio guida: controllo dei contenuti e responsabilità nella comunicazione digitale.

f) Gestione dei rapporti con fornitori e partner tecnologici
Il rischio può emergere:

- nella collaborazione con fornitori che non garantiscano adeguati livelli di sicurezza
- nella mancata verifica delle caratteristiche dei sistemi di IA utilizzati
- nell'affidamento a terzi di attività sensibili senza adeguati controlli
- nella mancata definizione delle responsabilità relative alla sicurezza e alla supervisione dei sistemi
- nella gestione non trasparente dei rapporti contrattuali

Principio guida: selezione, qualificazione e controllo delle controparti tecnologiche.

Attività strumentali
Alcune attività interne possono assumere rilievo strumentale rispetto ai reati di cui all'art. 25-vicies, tra cui:

- gestione degli accessi ai sistemi informatici e di intelligenza artificiale
- gestione delle credenziali e delle autorizzazioni
- gestione dei sistemi informativi e delle infrastrutture tecnologiche
- gestione dei fornitori e dei contratti relativi ai sistemi di IA
- gestione dei dati utilizzati per l'addestramento e il funzionamento dei sistemi
- gestione dei contenuti digitali e delle attività di comunicazione
- gestione della sicurezza informatica
- formazione e gestione delle competenze del personale
- monitoraggio e registrazione delle attività svolte mediante sistemi di intelligenza artificiale

Destinatari
La presente Parte Speciale si applica a tutti i soggetti che, a qualsiasi titolo, operano nell'ambito delle attività aziendali quali **amministratori e dirigenti, personale IT e tecnico, personale coinvolto nello sviluppo o nell'utilizzo di sistemi di intelligenza artificiale, personale delle funzioni marketing e comunicazione, dipendenti e collaboratori, consulenti, fornitori e partner tecnologici**.
L'obbligo di conformarsi al Modello 231 non dipende dalla qualifica formale, ma dal **ruolo effettivo nelle attività sensibili e dal livello di accesso o utilizzo dei sistemi di intelligenza artificiale**.

Principi generali di comportamento
Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto della normativa applicabile ai sistemi di intelligenza artificiale**
- **sicurezza e affidabilità dei sistemi**
- **supervisione e controllo umano**
- **trasparenza nell'utilizzo dell'intelligenza artificiale**
- **tracciabilità delle attività e delle modifiche**
- **protezione dei diritti e degli interessi delle persone**
- **responsabilità nella gestione dei contenuti generati o alterati mediante IA**
- **correttezza nella selezione e gestione dei fornitori tecnologici**

È espressamente vietato:

- omettere consapevolmente le misure di sicurezza previste per i sistemi di intelligenza artificiale ad alto rischio
- omettere le necessarie misure di **sorveglianza umana** quando richieste
- alterare illecitamente sistemi di intelligenza artificiale ad alto rischio
- consentire l'accesso ai sistemi a soggetti non autorizzati
- utilizzare sistemi di intelligenza artificiale per realizzare condotte idonee a mettere in pericolo la vita o l'incolumità delle persone
- diffondere, senza il consenso dell'interessato, **immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale** quando dalla diffusione possa derivare un danno ingiusto
- utilizzare o diffondere contenuti generati o alterati mediante IA senza le necessarie verifiche e autorizzazioni
- eludere i sistemi di controllo e monitoraggio predisposti dall'organizzazione
- collaborare con soggetti che utilizzino sistemi di intelligenza artificiale in violazione delle procedure aziendali o della normativa applicabile

Ogni dipendente o collaboratore che **rilevi anomalie, utilizzi non autorizzati, alterazioni dei sistemi o contenuti potenzialmente illeciti** è tenuto a segnalarli tramite i canali previsti dal Modello.

Sistema dei protocolli di controllo
A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi che disciplinano in modo analitico:

- gestione e utilizzo dei sistemi di intelligenza artificiale
- classificazione e individuazione dei sistemi ad alto rischio
- adozione e verifica delle misure tecniche di sicurezza
- gestione della **sorveglianza umana**
- controllo degli accessi e delle autorizzazioni
- gestione e tracciabilità delle modifiche ai sistemi
- verifica e monitoraggio dei sistemi di IA
- gestione dei contenuti generati o alterati mediante intelligenza artificiale
- controllo delle attività di comunicazione e pubblicazione dei contenuti
- selezione e monitoraggio dei fornitori e dei partner tecnologici
- formazione e sensibilizzazione del personale
- gestione delle segnalazioni e delle anomalie

Tali protocolli costituiscono **strumenti applicativi della presente Parte Speciale** e rappresentano la traduzione operativa dei principi sopra indicati.

I controlli dell'Organismo di Vigilanza
L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV)**.
Con specifico riferimento ai reati di cui all'art. 25-vicies, l'attività di controllo dell'OdV si concentra sui processi aziendali connessi allo sviluppo, alla gestione e all'utilizzo dei sistemi di intelligenza artificiale, nonché alla produzione e diffusione di contenuti mediante tali sistemi.
In particolare, l'OdV:

- verifica l'applicazione dei protocolli relativi alla gestione e all'utilizzo dei sistemi di intelligenza artificiale
- monitora l'adozione delle misure tecniche e organizzative di sicurezza
- verifica la presenza e l'effettiva applicazione delle procedure di **sorveglianza umana**
- controlla la gestione degli accessi e delle autorizzazioni
- verifica la tracciabilità delle modifiche apportate ai sistemi
- monitora le attività di produzione e diffusione di contenuti generati o alterati mediante IA
- controlla i rapporti con fornitori e partner tecnologici
- analizza eventuali segnalazioni relative a utilizzi impropri o anomalie dei sistemi
- promuove iniziative formative sui rischi specifici connessi all'intelligenza artificiale

L'OdV può richiedere documentazione, effettuare audizioni e verifiche, acquisire informazioni dai responsabili delle funzioni aziendali interessate e redigere report periodici agli organi societari competenti, contenenti **criticità, raccomandazioni e misure correttive**.

Conclusione: la prevenzione come processo organizzativo
La prevenzione dei reati connessi all'utilizzo di sistemi di intelligenza artificiale richiede un approccio organizzativo fondato su:

- **sicurezza e affidabilità dei sistemi di intelligenza artificiale**
- **adeguata supervisione e controllo umano**
- **prevenzione degli accessi e delle alterazioni non autorizzate**
- **tracciabilità delle attività e delle modifiche**
- **controllo dei contenuti generati o alterati mediante IA**
- **verifica dei fornitori e delle controparti tecnologiche**
- **formazione continua del personale**

La presente Parte Speciale deve essere intesa non solo come strumento di conformità normativa, ma come **guida operativa per garantire che l'utilizzo dei sistemi di intelligenza artificiale avvenga in condizioni di sicurezza, trasparenza, controllo e responsabilità**, prevenendo condotte che possano determinare i rischi previsti dagli artt. 437-bis e 612-quater del codice penale.

Art 26 - Delitti tentati

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 26 del D.Lgs. 231/2001, concernenti i delitti tentati, in relazione a tutte le fattispecie di reato rilevanti ai fini della responsabilità amministrativa degli enti.*

L'obiettivo di questa sezione è duplice:

1. **Fornire ai destinatari del Modello una chiara comprensione della rilevanza penalistica delle condotte tentate**
2. **Definire comportamenti e presidi idonei a prevenire anche fasi prodromiche o non consumate di reati**

Nel sistema del D.Lgs. 231/2001, infatti, la responsabilità dell'ente può sorgere non solo quando il reato è consumato, ma anche quando lo stesso rimane allo stadio di tentativo, purché siano integrati gli estremi previsti dalla normativa penale.

Nel contesto operativo dell'Ente, ciò implica che anche comportamenti non portati a compimento – ma idonei e diretti in modo non equivoco alla realizzazione di un reato – possono esporre l'ente a responsabilità.

In particolare, tali rischi possono emergere in relazione a:

- attività negoziali e contrattuali
- processi decisionali e autorizzativi
- gestione delle risorse finanziarie
- rapporti con la Pubblica Amministrazione
- gestione dei fornitori e partner
- attività commerciali e promozionali

La prevenzione dei delitti tentati richiede pertanto:

- attenzione alle fasi iniziali e intermedie dei processi aziendali
- controlli preventivi e non solo successivi
- tracciabilità delle decisioni e delle operazioni
- diffusione di una cultura della legalità orientata alla prevenzione del rischio anche potenziale

Inquadramento normativo dei reati presupposto

L'art. 26 del D.Lgs. 231/2001 stabilisce che, nei casi di commissione nelle forme del tentativo dei delitti rilevanti ai fini del decreto, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà.

Il riferimento normativo principale è rappresentato dall'art. 56 del Codice Penale:

- Art. 56 c.p. – Delitto tentato

Ai sensi di tale disposizione:

- risponde di delitto tentato chi compie atti idonei diretti in modo non equivoco a commettere un delitto

- quando l'azione non si compie o l'evento non si verifica

La norma prevede inoltre che:

- la pena è diminuita rispetto al delitto consumato
- non è punibile chi volontariamente desiste dall'azione
- se il soggetto impedisce l'evento, si applica la pena per il tentativo ridotta

In sintesi:

- il tentativo punisce **comportamenti già pericolosi, anche se non conclusi**
- rileva **l'idoneità degli atti e la direzione univoca verso il reato**
- la **responsabilità può emergere anche in assenza di danno effettivo**
- la desistenza volontaria e il ravvedimento attivo hanno **effetti attenuanti o escludenti**

Per le imprese, ciò comporta che il rischio 231 si configura anche in presenza di attività preparatorie o interrotte, se qualificabili come tentativo di reato.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili assume un ruolo particolarmente rilevante in relazione ai delitti tentati, in quanto il rischio si manifesta spesso nelle fasi preliminari dei processi.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbero essere posti in essere atti idonei e diretti in modo non equivoco alla commissione di un reato.

Il rischio può emergere trasversalmente rispetto a tutte le aree aziendali già esposte ai reati presupposto, con particolare riferimento a:

- fasi di pianificazione e negoziazione
- attività autorizzative
- operazioni economico-finanziarie
- gestione delle relazioni esterne

Tali attività richiedono un **approccio preventivo rafforzato.**

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Processi decisionali e autorizzativi
Il rischio può emergere:

- nella predisposizione di atti finalizzati a un comportamento illecito
- nell'autorizzazione di operazioni non conformi
- nella mancanza di controlli preventivi

Principio guida: segregazione delle funzioni e controllo ex ante.

b) Attività negoziali e contrattuali
Il rischio può emergere:

- nella definizione di accordi finalizzati a condotte illecite
- nella predisposizione di documentazione non veritiera
- in trattative orientate a violare norme di legge

Principio guida: correttezza, trasparenza e verificabilità dei contenuti contrattuali.

c) Gestione delle risorse finanziarie
Il rischio può emergere:

- nella predisposizione di operazioni finanziarie illecite non completate
- nell'avvio di flussi economici non giustificati
- in tentativi di distrazione o impiego illecito di fondi

Principio guida: tracciabilità e giustificazione economica delle operazioni.

d) Rapporti con la Pubblica Amministrazione
Il rischio può emergere:

- in tentativi di corruzione o induzione indebita non perfezionati
- nella predisposizione di documentazione falsa
- in condotte dirette a influenzare indebitamente funzionari pubblici

Principio guida: integrità e legalità nei rapporti istituzionali.

e) Gestione dei fornitori e partner
Il rischio può emergere:

- nella selezione di soggetti coinvolti in attività illecite
- nella partecipazione a operazioni non trasparenti
- in accordi preparatori di reati non consumati

Principio guida: due diligence e monitoraggio continuo dei partner.

Attività strumentali

Rilevano altresì attività interne quali:

- gestione amministrativa e contabile
- gestione documentale
- sistemi di controllo interno
- formazione del personale
- gestione dei flussi informativi

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito dell'organizzazione dell'Ente, tra cui **amministratori, dirigenti, dipendenti, collaboratori, consulenti e partner.**

L'obbligo di conformarsi al Modello riguarda anche **comportamenti non portati a compimento ma potenzialmente idonei a integrare fattispecie di tentativo.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto delle norme penali**
- **prevenzione del rischio anche nelle fasi preliminari**
- **trasparenza e tracciabilità delle operazioni**
- **responsabilità individuale nei processi decisionali**
- **controllo preventivo delle attività sensibili**

È espressamente vietato:

- porre in essere atti idonei e diretti alla commissione di reati
- avviare operazioni prive di giustificazione economica o giuridica
- predisporre documentazione falsa o fuorviante
- intraprendere trattative finalizzate a comportamenti illeciti
- eludere i controlli interni nelle fasi iniziali dei processi

È fatto **obbligo di segnalare tempestivamente eventuali comportamenti anomali o tentativi di illecito**

Sistema dei protocolli di controllo

La Fondazione adotta protocolli specifici volti a prevenire anche il rischio di delitti tentati, tra cui:

- procedure autorizzative multilivello
- controlli preventivi sulle operazioni sensibili
- tracciabilità delle decisioni e delle attività
- verifica della coerenza economica delle operazioni
- due diligence su controparti e partner
- sistemi di segnalazione interna (whistleblowing)
- formazione sui rischi di responsabilità anche in forma tentata

Tali protocolli mirano a **intercettare il rischio prima della consumazione del reato**.

I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza (OdV) verifica l'efficace attuazione della presente Parte Speciale anche con riferimento ai delitti tentati.

In particolare, l'OdV:

- monitora i processi a rischio nelle fasi preliminari
- verifica l'efficacia dei controlli preventivi
- analizza anomalie e segnali di rischio
- promuove la cultura della prevenzione
- propone eventuali misure correttive

L'OdV può effettuare verifiche mirate su operazioni non concluse ma potenzialmente rilevanti.

Conclusione: la prevenzione come presidio anticipato

La prevenzione dei delitti tentati richiede un approccio anticipatorio fondato su:

- **controllo delle fasi iniziali dei processi**
- **tracciabilità delle decisioni**
- **trasparenza nelle attività aziendali**
- **responsabilizzazione dei soggetti coinvolti**
- **diffusione di una cultura della legalità preventiva**

La presente Parte Speciale costituisce uno **strumento volto a intercettare il rischio prima che il reato si realizzi, rafforzando il sistema di controllo interno e tutelando l'ente da responsabilità derivanti anche da condotte non consumate.**

Art 12 Legge n.9/2013 - Responsabilità degli enti

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto richiamati dall'art. 12 della L. n. 9/2013, concernenti la responsabilità degli enti per reati in materia di sicurezza alimentare, genuinità dei prodotti, tutela dei consumatori e protezione dei segni distintivi e delle indicazioni di origine.*

L'obiettivo di questa sezione è duplice:

1. **Fornire ai destinatari del Modello una chiara comprensione dei rischi connessi alla produzione, commercializzazione e distribuzione di prodotti alimentari e industriali**
2. **Individuare comportamenti e presidi operativi idonei a prevenire fenomeni di adulterazione, contraffazione e frode commerciale**

Nel contesto economico attuale, caratterizzato da filiere produttive articolate e mercati globalizzati, le imprese sono esposte a rischi significativi legati alla qualità, autenticità e sicurezza dei prodotti immessi sul mercato.

In particolare, tali rischi possono emergere in relazione a:

- produzione e trasformazione di alimenti
- approvvigionamento di materie prime
- etichettatura e presentazione dei prodotti
- utilizzo di marchi, brevetti e denominazioni
- distribuzione e vendita dei prodotti
- gestione della supply chain

La prevenzione dei reati ambientali richiede pertanto:

- controlli rigorosi sulla qualità e provenienza dei prodotti
- tracciabilità delle filiere produttive e distributive
- correttezza delle informazioni commerciali
- tutela della proprietà industriale e dei segni distintivi
- diffusione di una cultura dell'Ente orientata alla sicurezza alimentare e alla lealtà commerciale

Inquadramento normativo dei reati presupposto

L'art. 12 della L. n. 9/2013 ha esteso la responsabilità amministrativa degli enti a una serie di reati previsti dal Codice Penale in materia di sicurezza alimentare, frodi e contraffazione.

- Art. 440 c.p. – Adulterazione e contraffazione di sostanze alimentari
- Art. 442 c.p. – Commercio di sostanze alimentari contraffatte o adulterate
- Art. 444-ter c.p. – Commercio di sostanze alimentari nocive
- Art. 473 c.p. – Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni
- Art. 474 c.p. – Introduzione nello Stato e commercio di prodotti con segni falsi
- Art. 515 c.p. – Frode nell'esercizio del commercio
- Art. 516 c.p. – Vendita di sostanze alimentari non genuine come genuine

- Art. 517 c.p. – Vendita di prodotti industriali con segni mendaci
- Art. 517-quater c.p. – Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari

In sintesi:

- l'adulterazione e contraffazione incidono sulla **sicurezza e genuinità degli alimenti**
- la commercializzazione di **prodotti non conformi o nocivi mette a rischio la salute pubblica**
- la contraffazione di marchi e segni distintivi **lede la proprietà industriale e la concorrenza**
- le frodi commerciali alterano la **trasparenza del mercato**
- l'uso indebito di indicazioni geografiche **compromette la tutela delle eccellenze agroalimentari**

Per le imprese operanti nei settori alimentare, industriale e commerciale, tali fattispecie rappresentano rischi concreti e rilevanti ai fini della responsabilità 231.

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili rappresenta un elemento essenziale per la prevenzione dei reati in esame.

Per **attività sensibili** si intendono le attività aziendali nel cui ambito potrebbero essere commessi i reati sopra indicati.

Il rischio può emergere in relazione a processi quali:

- approvvigionamento delle materie prime
- produzione e trasformazione
- controllo qualità
- etichettatura e confezionamento
- gestione dei marchi e dei segni distintivi
- distribuzione e vendita
- gestione dei fornitori e dei partner commerciali

Tali attività richiedono elevati standard di controllo, qualità e trasparenza.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Produzione e trasformazione alimentare
Il rischio può emergere:

- nell'utilizzo di ingredienti non conformi o adulterati
- nella manipolazione dei prodotti
- nella violazione degli standard igienico-sanitari

Principio guida: sicurezza, qualità e conformità normativa dei processi produttivi.

b) Controllo qualità e sicurezza alimentare
Il rischio può emergere:

- nell'omissione o alterazione dei controlli

- nella mancata individuazione di prodotti nocivi
- nella falsificazione dei risultati di analisi

Principio guida: indipendenza, rigorosità e tracciabilità dei controlli.

c) Etichettatura, confezionamento e comunicazione commerciale
Il rischio può emergere:

- in informazioni ingannevoli o non veritiere
- nell'uso improprio di denominazioni di origine
- nella presentazione fuorviante dei prodotti

Principio guida: trasparenza e veridicità delle informazioni al consumatore.

d) Gestione dei marchi e della proprietà industriale
Il rischio può emergere:

- nell'utilizzo di marchi contraffatti o non autorizzati
- nella violazione di brevetti o modelli
- nella commercializzazione di prodotti con segni falsi

Principio guida: rispetto dei diritti di proprietà industriale.

e) Distribuzione e commercializzazione dei prodotti
Il rischio può emergere:

- nella vendita di prodotti non genuini o contraffatti
- nella frode sulle caratteristiche del prodotto
- nell'immissione sul mercato di prodotti nocivi

Principio guida: correttezza e lealtà nelle pratiche commerciali.

f) Gestione dei fornitori e della filiera
Il rischio può emergere:

- nell'approvvigionamento da fornitori non affidabili
- nella mancata verifica della provenienza dei prodotti
- nella partecipazione a filiere irregolari

Principio guida: tracciabilità e qualificazione della supply chain.

Attività strumentali

Assumono rilievo anche:

- gestione documentale e certificazioni
- sistemi di controllo interno
- audit e verifiche ispettive
- formazione del personale
- gestione dei reclami e dei richiami di prodotto

Destinatari

La presente Parte Speciale si applica a tutti i soggetti che operano nell'ambito dell'organizzazione dell'Ente, inclusi **amministratori, dirigenti, dipendenti, collaboratori, consulenti, fornitori e partner commerciali.**

L'obbligo di conformità riguarda tutte le attività **connesse alla produzione, distribuzione e commercializzazione dei prodotti.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **tutela della salute e sicurezza dei consumatori**
- **qualità e genuinità dei prodotti**
- **trasparenza e correttezza commerciale**
- **rispetto della proprietà industriale**
- **tracciabilità e controllo della filiera**

È espressamente vietato:

- adulterare o contraffare prodotti alimentari
- commercializzare prodotti nocivi o non conformi
- utilizzare marchi o segni distintivi falsi o non autorizzati
- fornire informazioni ingannevoli sui prodotti
- vendere prodotti non genuini come genuini
- utilizzare indebitamente denominazioni di origine

È fatto obbligo di **segnalare tempestivamente eventuali anomalie o non conformità.**

Sistema dei protocolli di controllo

A presidio delle aree di rischio sopra individuate, la Fondazione adotta specifici protocolli operativi tra cui:

- sistemi di controllo qualità e sicurezza alimentare (es. HACCP)
- procedure di tracciabilità e rintracciabilità dei prodotti
- controlli su etichettatura e comunicazione commerciale
- verifiche sulla proprietà industriale e sui marchi
- qualifica e monitoraggio dei fornitori
- audit interni e controlli ispettivi
- sistemi di gestione dei reclami e dei ritiri dal mercato
- formazione del personale

Tali protocolli costituiscono **strumenti essenziali di prevenzione**.

I controlli dell'Organismo di Vigilanza

L'efficace attuazione della presente Parte Speciale è sottoposta alla vigilanza **dell'Organismo di Vigilanza (OdV).**

In particolare, l'OdV:

- monitora i processi produttivi e commerciali
- verifica l'efficacia dei controlli qualità
- analizza i flussi della filiera
- controlla l'uso dei marchi e delle denominazioni
- esamina le segnalazioni ricevute
- promuove attività di formazione e sensibilizzazione

L'OdV può effettuare verifiche, richiedere documentazione e proporre azioni correttive.

Conclusione: la prevenzione come garanzia di qualità e legalità

La prevenzione dei reati in materia di sicurezza alimentare, contraffazione e frodi commerciali richiede un approccio organizzativo fondato su:

- **controllo della qualità e della sicurezza dei prodotti**
- **tracciabilità della filiera**
- **trasparenza nelle informazioni al consumatore**
- **tutela della proprietà industriale**
- **responsabilità e formazione del personale**

La presente Parte Speciale rappresenta uno strumento operativo volto a garantire che tutte le attività aziendali siano svolte nel **rispetto delle normative, tutelando la salute dei consumatori, la correttezza del mercato e l'integrità dell'impresa.**

Art. 10 Legge n.146/2006 - Reati transnazionali

Introduzione alla Parte Speciale

> *La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati presupposto di cui all'art. 10 della Legge n. 146/2006, concernenti i reati transnazionali.*

L'obiettivo di questa sezione è duplice:

1. **Fornire ai destinatari del Modello una chiara comprensione dei rischi connessi allo svolgimento di attività con profili internazionali**
2. **Individuare comportamenti e presidi idonei a prevenire il coinvolgimento, anche indiretto, in attività criminali organizzate a carattere transnazionale**

Nel contesto economico attuale, caratterizzato da globalizzazione, mobilità dei capitali e interconnessione dei mercati, le imprese operano frequentemente oltre i confini nazionali, instaurando rapporti con controparti estere, partner commerciali e intermediari internazionali.

Tale operatività espone le organizzazioni al rischio di essere coinvolte, anche inconsapevolmente, in attività illecite di natura transnazionale, spesso riconducibili a fenomeni di criminalità organizzata.

In particolare, tali rischi possono emergere in relazione a:

- operazioni commerciali e finanziarie internazionali
- gestione di fornitori e partner esteri
- movimentazione di merci e capitali oltre confine
- gestione di personale e collaboratori in contesti internazionali
- rapporti con autorità giudiziarie e investigative

La prevenzione dei reati transnazionali richiede pertanto:

- adeguata conoscenza delle controparti (know your counterparty)
- tracciabilità dei flussi finanziari e commerciali
- controlli sui rapporti internazionali
- cooperazione con le autorità
- diffusione di una cultura dell'Ente orientata alla legalità globale

Inquadramento normativo dei reati presupposto

L'art. 10 della Legge n. 146/2006 prevede la responsabilità amministrativa degli enti per una serie di reati, quando gli stessi presentano carattere transnazionale.

Un reato si considera transnazionale quando:

- è punito con pena non inferiore nel massimo a quattro anni
- coinvolge più di uno Stato (per commissione, preparazione, pianificazione o effetti)
- oppure è commesso da un gruppo criminale organizzato operante in più Stati

Tra i principali reati rilevanti rientrano:

- Art. 377-bis c.p. – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- Art. 378 c.p. – Favoreggiamento personale

- Art. 416 c.p. – Associazione per delinquere
- Art. 416-bis c.p. – Associazioni di tipo mafioso anche straniere
- Art. 12, commi 3, 3-bis, 3-ter e 5, D.Lgs. 286/1998 – Disposizioni contro le immigrazioni clandestine
- Art. 74 D.P.R. 309/1990 – Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope
- Art. 86 D.Lgs. n. 141/2024 – Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati

In sintesi:

- i reati transnazionali sono spesso **connessi alla criminalità organizzata**
- presentano una **dimensione internazionale e strutturata**
- possono coinvolgere **flussi finanziari, traffici illeciti e reti criminali**
- il rischio per l'impresa può derivare anche da **rapporti indiretti con soggetti coinvolti**

Mappatura delle attività sensibili e analisi del rischio

Premessa metodologica

La mappatura delle attività sensibili è fondamentale per individuare i processi aziendali esposti al rischio di reati transnazionali.

Per **attività sensibili** si intendono le attività nel cui ambito l'ente potrebbe essere coinvolto, anche indirettamente, in condotte illecite a carattere internazionale.

Il rischio può emergere in relazione a:

- operazioni commerciali con controparti estere
- trasferimenti di denaro e operazioni finanziarie internazionali
- gestione della supply chain globale
- rapporti con intermediari, agenti e consulenti esteri
- gestione delle spedizioni e dei flussi logistici

Tali attività richiedono controlli rafforzati e un approccio basato sul rischio.

Attività sensibili: aree a rischio primario

Le principali attività sensibili possono essere ricondotte alle seguenti macro-aree:

a) Operazioni commerciali e contrattuali internazionali
Il rischio può emergere:

- nella conclusione di contratti con controparti collegate a organizzazioni criminali
- nella partecipazione a operazioni economiche illecite
- nella mancanza di verifiche sull'identità e affidabilità dei partner

Principio guida: due diligence e trasparenza delle relazioni commerciali.

b) Gestione dei flussi finanziari internazionali
Il rischio può emergere:

- in trasferimenti di fondi verso soggetti sospetti
- nell'utilizzo di canali non tracciati
- nella partecipazione a operazioni di riciclaggio o finanziamento illecito

Principio guida: tracciabilità e controllo delle operazioni finanziarie.

c) Gestione della supply chain e dei trasporti
Il rischio può emergere:

- nel coinvolgimento in traffici illeciti (merci, stupefacenti, tabacchi)
- nell'utilizzo di vettori o intermediari non affidabili
- nella movimentazione internazionale non controllata

Principio guida: controllo e monitoraggio della filiera logistica.

d) Gestione del personale e mobilità internazionale
Il rischio può emergere:

- in pratiche irregolari di immigrazione o impiego di personale
- nel coinvolgimento in attività illecite connesse allo sfruttamento
- nella mancata verifica della regolarità dei rapporti

Principio guida: rispetto delle normative sull'immigrazione e sul lavoro.

e) Rapporti con autorità giudiziarie e investigative
Il rischio può emergere:

- in condotte di favoreggiamento
- nell'induzione a rendere dichiarazioni mendaci
- nell'ostacolo alle indagini

Principio guida: collaborazione, trasparenza e correttezza istituzionale.

Attività strumentali

Rilevano altresì:

- gestione amministrativa e contabile
- sistemi di controllo interno
- gestione documentale
- audit e verifiche interne
- formazione del personale

Destinatari

La presente Parte Speciale si applica a tutti i soggetti operanti per conto della Fondazione, inclusi **amministratori, dirigenti, dipendenti, collaboratori, consulenti, partner e intermediari, in particolare quelli coinvolti in attività internazionali.**

Principi generali di comportamento

Le attività aziendali devono essere improntate ai principi di:

- **legalità e rispetto delle normative nazionali e internazionali**
- **trasparenza nei rapporti commerciali e finanziari**
- **tracciabilità delle operazioni**
- **collaborazione con le autorità**
- **prevenzione del coinvolgimento in attività criminali**

È espressamente vietato:

- intrattenere rapporti con organizzazioni criminali
- partecipare, anche indirettamente, ad attività illecite transnazionali
- effettuare operazioni finanziarie non tracciabili

- favorire soggetti coinvolti in reati
- ostacolare l'attività delle autorità giudiziarie
- indurre a dichiarazioni mendaci o reticenti

È obbligatorio **segnalare tempestivamente qualsiasi anomalia o sospetto.**

Sistema dei protocolli di controllo

La Fondazione adotta protocolli specifici volti a prevenire i reati transnazionali, tra cui:

- procedure di due diligence su clienti, fornitori e partner
- controlli sui flussi finanziari internazionali
- tracciabilità delle operazioni commerciali e logistiche
- verifiche sulla regolarità dei rapporti di lavoro
- sistemi di segnalazione interna (whistleblowing)
- audit periodici sui processi a rischio
- formazione del personale sui rischi internazionali

Tali protocolli rappresentano **strumenti essenziali di prevenzione.**

I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza (OdV) vigila sull'efficace attuazione della presente Parte Speciale.

In particolare, l'OdV:

- monitora le attività con profili internazionali
- verifica l'efficacia dei controlli sui partner esteri
- analizza i flussi finanziari e logistici
- esamina le segnalazioni ricevute
- promuove la cultura della legalità internazionale
- propone eventuali azioni correttive

L'OdV può effettuare verifiche specifiche e richiedere documentazione.

Conclusione: la prevenzione come presidio globale

La prevenzione dei reati transnazionali richiede un approccio organizzativo fondato su:

- **controllo dei rapporti internazionali**
- **tracciabilità dei flussi finanziari e commerciali**
- **selezione accurata delle controparti**
- **collaborazione con le autorità**
- **diffusione di una cultura della legalità globale**

La presente Parte Speciale costituisce uno **strumento operativo volto a prevenire il coinvolgimento dell'ente in fenomeni di criminalità organizzata transnazionale, tutelando l'impresa e contribuendo alla legalità dei mercati internazionali.**