Settore: Trasporto merci e logistica

1. Finalità

La presente Parte Speciale ha lo scopo di individuare e descrivere i presidi organizzativi, gestionali e di controllo adottati dalla Società per prevenire la commissione dei reati presupposto rilevanti ai sensi del D.lgs. 231/2001, nell'ambito delle attività specifiche del settore trasporti e logistica.

2. Reati rilevanti per il settore

Settore: Trasporto merci e logistica
Focus: Punti di esposizione al rischio (PEE) e misure preventive per singolo reato

Art. 24 – Indebita percezione di erogazioni pubbliche / Truffa ai danni dello Stato

Punti di Esposizione al Rischio (PEE):

- - Predisposizione domande per contributi pubblici
- - Partecipazione a bandi pubblici
- - Dichiarazioni di requisiti tecnici ed economici non veritieri

Misure / Azioni di Prevenzione:

- - Verifica preliminare requisiti da parte dell'Ufficio Amministrazione
- - Controllo formale della documentazione da parte del Responsabile Legale
- - Approvazione con firma congiunta del Direttore Generale e Legale Rappresentante
- - Archiviazione digitale della domanda e allegati su sistema tracciabile
- - Divieto assoluto di dichiarazioni non veritiere o incomplete

Art. 24-BisPunti di esposizione al rischio per reati informatici

- Gestione degli accessi ai sistemi informatici
- Trattamento e archiviazione di dati sensibili o riservati
- Utilizzo della posta elettronica aziendale e strumenti di comunicazione
- Gestione della sicurezza informatica
- Gestione degli utenti esterni / fornitori IT
- Cessazione del rapporto di lavoro o collaborazione

Misure /Azioni di Prevenzione

1. Gestione degli accessi ai sistemi

- Politiche aziendali per la gestione degli accessi (principio del "minimo privilegio").
- Password complesse e obbligo di cambio periodico.
- Procedure di attivazione/disattivazione degli utenti.

2. Amministratori di sistema e infrastruttura IT

- Nomina formale degli amministratori di sistema.
- Registro delle attività svolte dagli utenti con privilegi elevati.
- Segregazione dei compiti tra utenti normali e amministratori.

3. Trattamento e archiviazione dei dati

- Classificazione delle informazioni per livello di riservatezza.
- Crittografia dei dati sensibili.
- Policy per la gestione dei dati personali (adeguamento GDPR).

4. Utilizzo di e-mail e comunicazioni

- Regolamento interno sull'uso della posta elettronica e di internet.
- Filtri antispam e antivirus attivi sui server di posta.
- Divieti espliciti per invio/condivisione non autorizzata di dati.

5. Sicurezza informatica

- Adozione di un sistema antivirus e firewall costantemente aggiornati.
- Monitoraggio continuo delle vulnerabilità.
- Piano di backup periodico e test di ripristino.

6. Sviluppo e manutenzione software

- Procedure per il rilascio controllato di aggiornamenti.
- Test e verifica delle modifiche ai software prima del rilascio.
- Registro delle modifiche (versioning, audit trail).

7. Dispositivi mobili e supporti rimovibili

- Blocco dell'utilizzo di dispositivi USB non autorizzati.
- Policy BYOD con condizioni tecniche e di sicurezza.
- Obbligo di cifratura dei dispositivi portatili.

8. Fornitori IT e utenti esterni

- Accordi contrattuali con clausole di riservatezza e sicurezza.
- Autorizzazioni specifiche per l'accesso ai sistemi.
- Supervisione degli interventi tecnici esterni.

9. Monitoraggio e logging

- Attivazione dei log per tutte le operazioni rilevanti.
- Conservazione dei log per un tempo congruo.
- Verifiche periodiche sugli accessi e sulle anomalie.

10. Cessazione dei rapporti

- Revoca immediata di credenziali e accessi al termine del rapporto.
- Recupero e disattivazione di dispositivi aziendali.
- Verifica dell'integrità dei dati prima della chiusura dell'utenza.

Art. 25 – Corruzione e concussione

Punti di Esposizione al Rischio (PEE):

- - Gestione rapporti con funzionari pubblici
- - Ottenimento di autorizzazioni o agevolazioni fiscali
- - Partecipazione a conferenze dei servizi o tavoli di trattativa pubblica

Misure / Azioni di Prevenzione:

- - Registro degli incontri con PA e verbalizzazione obbligatoria
- - Presenza di almeno due soggetti aziendali a ogni incontro istituzionale
- - Divieto di omaggi o regalie superiori al valore simbolico (<50 euro)
- - Formazione annuale obbligatoria su anticorruzione
- - Clausola di integrità nei contratti pubblici

Art. 25-ter – Reati societari (falsità in bilancio, false comunicazioni sociali)

Punti di Esposizione al Rischio (PEE):

- - Redazione bilancio d'esercizio
- - Relazioni di gestione e note integrative
- - Gestione contabilità generale e scritture accessorie

Misure / Azioni di Prevenzione:

- - Sistema contabile integrato e validato da revisori
- - Procedure di quadratura contabile trimestrali
- - Firma congiunta per operazioni bancarie superiori a 5.000 €
- - Divieto di contabilità extracontabile
- - Revisione legale affidata a società esterna indipendente

Art. 25-septies – Omicidio colposo / lesioni per violazioni sicurezza sul lavoro

Punti di Esposizione al Rischio (PEE):

- - Pianificazione turni autisti
- - Movimentazione merci e carico/scarico
- - Controllo e manutenzione dei mezzi

Misure / Azioni di Prevenzione:

- - Aggiornamento DVR con analisi specifica per autisti e magazzinieri
- - Controlli pre-turno su alcol e droghe con strumenti omologati
- - Check-list giornaliera veicoli prima dell'utilizzo
- - Formazione biennale su sicurezza, con focus su guida e movimentazione
- - Registro infortuni con analisi cause e misure correttive obbligatorie

Art. 25-undecies – Reati ambientali

Punti di Esposizione al Rischio (PEE):

- - Gestione rifiuti da officina e magazzino
- - Smaltimento acque reflue e lavaggio mezzi
- - Emissioni in atmosfera da impianti interni

Misure / Azioni di Prevenzione:

- - Tenuta registro carico-scarico rifiuti secondo normativa vigente
- - Accordi solo con ditte iscritte all'Albo Gestori Ambientali
- - Controllo annuale delle autorizzazioni ambientali (AUA, AIA)
- - Formazione ambientale per magazzinieri e addetti manutenzione
- - Audit ambientali interni semestrali

Art. 25-octies – Riciclaggio e autoriciclaggio

Punti di Esposizione al Rischio (PEE):

- - Movimentazioni finanziarie in contanti
- - Incassi/rimborsi da soggetti esteri
- - Pagamenti a fornitori non tracciati

Misure / Azioni di Prevenzione:

- - Divieto assoluto di utilizzo contante > soglia normativa
- - Verifica preventiva dei fornitori tramite vendor list qualificata
- - Controlli incrociati tra IBAN e intestatari fatture
- - Segnalazione operazioni sospette all'OdV

- Approvazione a doppia firma per transazioni > 3.000

3. Aree a rischio e protocolli di prevenzione

Questa sezione individua le attività aziendali più esposte a rischi di commissione dei reati 231 e le misure preventive associate.

A. Rapporti con la Pubblica Amministrazione

Punti di Esposizione al Rischio (PEE):

- Predisposizione e invio di documentazione per gare e bandi pubblici
- Contatti diretti con funzionari pubblici per richieste di autorizzazioni, licenze o concessioni
- Redazione di dichiarazioni e certificazioni per la partecipazione a procedure pubbliche
- Gestione di contenziosi o trattative con enti pubblici

Attività a rischio:

- Partecipazione a bandi pubblici e procedure a evidenza pubblica
- Richieste di contributi, incentivi, autorizzazioni amministrative o permessi ambientali

Misure di prevenzione e controllo:

- Autorizzazioni multilivello obbligatorie per ogni partecipazione a gare pubbliche, con coinvolgimento del Responsabile Legale e del Direttore Generale
- Registro informatico dei contatti con Enti Pubblici, aggiornato settimanalmente, con indicazione del soggetto incontrato, oggetto e finalità
- Controllo documentale ex ante a cura del Responsabile Legale per tutti i documenti ufficiali da presentare alla PA
- Controlli a campione ex post da parte del Responsabile Amministrativo su almeno il 20% delle pratiche trasmesse nel trimestre
- Codice Etico aziendale vincolante per dipendenti, collaboratori e consulenti esterni, con esplicito divieto di elargizioni indebite o comportamenti elusivi nei rapporti con la PA
- Formazione annuale obbligatoria per tutto il personale coinvolto nei rapporti con enti pubblici, focalizzata su normativa anticorruzione e trasparenza
- Clausola 231 di integrità da includere in ogni contratto o convenzione con la PA

B. Sicurezza sul lavoro e circolazione stradale

Punti di Esposizione al Rischio (PEE):

- **Pianificazione turni e turnazioni di guida:**
  - L'organizzazione dei turni può comportare un rischio per la sicurezza stradale, qualora non venga rispettato il riposo sufficiente per gli autisti. La stanchezza e la fatica prolungata aumentano il rischio di incidenti stradali.
- **Carico/scarico merci in magazzino:**
  - Operazioni di carico e scarico inadeguate possono risultare in infortuni sul lavoro, danni ai materiali, ma anche incidenti stradali se le merci non sono stivate in modo sicuro.

Attività a rischio:

- **Pianificazione turni e turnazioni di guida:**
  - Rischi derivanti dal sovraccarico di lavoro e dalla stanchezza degli autisti, che può comprometterne la concentrazione e i riflessi.
- **Carico/scarico merci in magazzino:**
  - Incidenti durante le operazioni di movimentazione merci, con il rischio di lesioni fisiche per i lavoratori e danni ai mezzi e ai carichi.

Misure di prevenzione e controllo:

1. **DVR (Documento di Valutazione dei Rischi) aggiornato e procedure antinfortunistiche**
   - Ogni azienda deve avere un Documento di Valutazione dei Rischi (DVR) che includa specifici rischi relativi alla sicurezza stradale e alla movimentazione di merci.
   - Il DVR deve essere aggiornato periodicamente, con particolare attenzione alla sicurezza nei turni di guida e nelle operazioni di carico/scarico. Le procedure devono essere chiare e dettagliate, comprese le normative antinfortunistiche e le pratiche di sicurezza durante le operazioni di movimentazione merci.
2. **Formazione periodica degli autisti**
   - Gli autisti devono essere sottoposti a formazione periodica riguardante la sicurezza stradale, la gestione dei turni, e la prevenzione dei rischi legati alla fatica.
   - La formazione deve includere tecniche per prevenire incidenti stradali, riconoscere i segnali di affaticamento e rispettare le normative relative ai tempi di guida e riposo.
   - Ogni autista deve essere consapevole dei propri limiti e delle responsabilità riguardo alla sicurezza durante la guida.
3. **Controlli alcolemici e test per cannabis random**
   - Per prevenire incidenti dovuti a consumo di alcol o sostanze stupefacenti, l'azienda deve attuare controlli periodici e random sui propri autisti.

- I test alcolemici e per cannabis devono essere eseguiti a campione, in modo da dissuadere eventuali comportamenti rischiosi e garantire la sicurezza del personale e degli utenti della strada.

4. **Check-list di controllo mezzi**
   -
   - Prima di ogni viaggio, deve essere effettuato un controllo di sicurezza completo sui mezzi. Questo controllo dovrebbe riguardare gli aspetti meccanici e di sicurezza del veicolo, come i freni, le luci, gli pneumatici, e i sistemi di carico.
   - Una check-list standardizzata deve essere utilizzata da ogni autista per garantire che ogni mezzo sia in perfette condizioni prima di partire. Eventuali anomalie o guasti devono essere immediatamente segnalati e risolti.
5. **Gestione dei turni e riposi obbligatori**
   - La programmazione dei turni deve essere fatta in modo da garantire un adeguato riposo tra le ore di guida e turni lavorativi, nel rispetto delle normative sulla sicurezza stradale. È fondamentale evitare turni troppo lunghi o inadeguati che possano compromettere la capacità di concentrazione dell'autista.
   - Vanno monitorati attentamente i tempi di guida, utilizzando tachigrafi digitali che permettano di registrare e controllare il rispetto dei tempi di riposo e lavoro.
6. **Procedure di emergenza per incidenti stradali**
   - In caso di incidente stradale, devono essere previste procedure chiare e dettagliate su come comportarsi, inclusi i passaggi per la gestione del sinistro, la segnalazione alle autorità competenti e l'assistenza sanitaria ai feriti.
   - È necessario che ogni dipendente sia formato su come attivare l'assicurazione aziendale, compilare il modulo di incidente e seguire le normative locali riguardo agli incidenti stradali.
7. **Utilizzo di dispositivi di protezione individuale (DPI)**
   - Per la parte legata alla sicurezza sul lavoro, è fondamentale fornire ai dipendenti attrezzature e dispositivi di protezione adeguati, come guanti, caschi, scarpe antinfortunistiche, e dispositivi di protezione per il carico/scarico delle merci.
   - L'azienda deve garantire che i dipendenti siano adeguatamente equipaggiati e che utilizzino sempre i DPI necessari durante le operazioni di magazzino e trasporto.

Conclusioni:

Queste misure sono essenziali per ridurre al minimo i rischi legati alla sicurezza stradale e alla sicurezza sul lavoro. Una corretta implementazione di queste azioni preventive contribuirà significativamente a garantire la sicurezza degli autisti e a ridurre gli incidenti e le problematiche legate alle operazioni di carico e scarico merci.

C. Reati ambientali

Punti di Esposizione al Rischio (PEE):

- **Gestione rifiuti (oli esausti, pneumatici):**
  - La gestione non corretta dei rifiuti pericolosi, come oli esausti, pneumatici usati e altri materiali industriali, può comportare gravi danni all'ambiente e alle persone. La non osservanza delle normative di smaltimento può portare a multe pesanti e danni reputazionali.
- **Scarichi industriali o emissioni di lavaggio:**
  - Lo smaltimento non conforme di scarichi industriali o emissioni derivanti da attività di lavaggio (ad esempio, scarichi di acque reflue da impianti industriali) può contaminare il suolo, le acque e l'aria, con conseguenti violazioni delle normative ambientali. Questo tipo di attività è strettamente regolato e richiede costante monitoraggio.

Attività a rischio:

- **Gestione rifiuti (oli esausti, pneumatici):**
  - Stoccaggio, trasporto e smaltimento improprio di rifiuti pericolosi come oli esausti, pneumatici usati e batterie.
  - Trattamenti non autorizzati o non registrati di rifiuti, con rischio di sversamenti o dispersione di sostanze pericolose nell'ambiente.
- **Scarichi industriali o emissioni di lavaggio:**
  - Emissioni incontrollate da impianti di lavaggio o scarichi industriali non trattati che violano le normative locali e europee in materia di tutela dell'ambiente.

Misure di prevenzione e controllo:

1. **Registro carico/scarico rifiuti aggiornato**
   - È obbligatorio mantenere un registro aggiornato delle operazioni di carico e scarico di rifiuti, inclusi oli esausti, pneumatici usati e altri rifiuti industriali. Questo registro deve includere dettagli sui quantitativi, le tipologie di rifiuti, i destinatari e la destinazione finale (ad esempio, il centro di trattamento o smaltimento).
   - Il registro deve essere conservato per un periodo minimo di 5 anni e deve essere disponibile per la verifica da parte delle autorità competenti.
2. **Affidamento solo a fornitori autorizzati**
   - Per evitare il rischio di smaltimento illecito o di violazioni ambientali, l'azienda deve affidarsi solo a fornitori che siano regolarmente autorizzati per la gestione dei rifiuti. I fornitori devono possedere le necessarie licenze e certificazioni per operare in conformità con le normative locali e europee.
   - Gli accordi con i fornitori di servizi di smaltimento devono essere formalizzati attraverso contratti che specificano le modalità di gestione dei rifiuti, le procedure di monitoraggio e gli obblighi reciproci.

- Prima di qualsiasi incarico, l'azienda deve eseguire verifiche periodiche sullo status di autorizzazione dei fornitori e sulla loro capacità di garantire il corretto smaltimento.

3. **Audit ambientali periodici**
   - Gli audit ambientali sono fondamentali per monitorare e valutare la conformità dell'azienda alle normative ambientali e per identificare eventuali aree di rischio. Gli audit devono essere eseguiti almeno una volta all'anno da un ente esterno indipendente o da una figura interna con esperienza.
   - Durante gli audit, viene esaminata la gestione dei rifiuti, gli scarichi industriali, e le emissioni. È fondamentale che le azioni correttive vengano intraprese tempestivamente per ridurre al minimo i rischi ambientali e legali.
4. **Autorizzazioni integrate e controlli ISPRA**
   - L'azienda deve ottenere tutte le necessarie autorizzazioni integrate ambientali per le attività che coinvolgono scarichi industriali, emissioni atmosferiche e gestione di rifiuti pericolosi. Queste autorizzazioni sono rilasciate dalle autorità locali competenti, ma devono essere conformi alle normative ambientali nazionali ed europee.
   - È fondamentale che l'azienda si sottoponga ai controlli periodici da parte dell'ISPRA (Istituto Superiore per la Protezione e la Ricerca Ambientale) e delle autorità locali. L'ISPRA è incaricato di monitorare e controllare le attività industriali per garantire che vengano rispettate le leggi relative alla protezione dell'ambiente.
   - L'azienda deve essere preparata a fornire la documentazione richiesta durante i controlli e a cooperare con gli ispettori, garantendo che tutte le operazioni siano conformi alle normative.
5. **Monitoraggio delle emissioni e scarichi**
   - L'azienda deve monitorare costantemente le emissioni di gas e le acque di scarico provenienti dalle attività industriali, registrando e analizzando i dati raccolti. Gli impianti di trattamento devono essere sottoposti a manutenzione regolare per garantire che siano efficienti e in grado di ridurre al minimo l'impatto ambientale.
   - Le analisi delle acque reflue devono essere eseguite da laboratori accreditati e i risultati devono essere riportati alle autorità competenti, se richiesto dalla legge.
6. **Formazione ambientale per il personale**
   - È necessario fornire formazione continua a tutti i dipendenti coinvolti nella gestione dei rifiuti e nelle operazioni che possono comportare un impatto ambientale (come lo scarico delle acque reflue o il trattamento dei rifiuti).
   - La formazione deve riguardare la corretta gestione dei rifiuti, la sicurezza durante le operazioni di smaltimento, le normative ambientali e le procedure da seguire in caso di emergenza ambientale.
7. **Gestione dei rifiuti pericolosi e protocolli di emergenza**
   - L'azienda deve stabilire protocolli chiari e pratici per la gestione dei rifiuti pericolosi e per le emergenze ambientali, come sversamenti di sostanze chimiche o fuoriuscite di rifiuti industriali.
   - I dipendenti devono essere addestrati a rispondere prontamente a qualsiasi incidente ambientale, minimizzando i danni e riportando tempestivamente l'incidente alle autorità competenti.
8. **Verifica della conformità alle normative**
   - L'azienda deve garantire che tutte le sue attività siano conformi alle normative locali e internazionali in materia di protezione ambientale. Ciò include la verifica della

corretta applicazione delle normative europee in materia di rifiuti, emissioni e scarichi, nonché delle normative nazionali sull'ambiente.

Conclusioni: Implementando queste misure preventive e di controllo, l'azienda sarà in grado di ridurre significativamente i rischi legati ai reati ambientali, proteggere l'ambiente e garantire la conformità alle normative. Queste pratiche sono fondamentali non solo per evitare sanzioni legali, ma anche per promuovere una gestione responsabile e sostenibile delle risorse e dei rifiuti.

D. Reati societari e fiscali

Punti di Esposizione al Rischio (PEE):

- **Redazione del bilancio:**
  - La redazione del bilancio è uno degli aspetti più delicati della gestione aziendale. La mancata o scorretta registrazione di operazioni aziendali, la falsificazione dei dati contabili o l'omissione di informazioni essenziali può configurare un reato societario e fiscale. Errori deliberati o non intenzionali nella redazione del bilancio, ad esempio per ridurre l'imposta sul reddito o nascondere passività, possono portare a gravi sanzioni penali e danni reputazionali.
- **Operazioni extra-contabili:**
  - Le operazioni non registrate o occultate, come transazioni non documentate o trasferimenti di denaro "in nero" (ad esempio, attraverso cassa contante non dichiarata), sono rischiose per l'azienda. Queste pratiche possono essere utilizzate per evadere il fisco, alterare i bilanci aziendali o occultare operazioni illecite, esponendo l'azienda a procedimenti penali.

Attività a rischio:

- **Redazione del bilancio:**
  - Alterazione delle voci di bilancio con l'intento di manipolare il risultato economico o la posizione patrimoniale dell'azienda.
  - Falsificazione dei dati contabili per ridurre la base imponibile o migliorare artificialmente i risultati finanziari.
- **Operazioni extra-contabili:**
  - Gestione di fondi o transazioni non registrati nei libri contabili ufficiali.
  - L'omissione di ricavi o costi in modo da ridurre il carico fiscale o nascondere operazioni non legittime.

Misure di prevenzione e controllo:

1. **Contabilità trasparente e tracciata**
   - La contabilità deve essere completamente trasparente, con ogni transazione aziendale debitamente registrata e tracciata nel sistema contabile. Ogni entrata e uscita deve essere giustificata da documentazione adeguata, come fatture, contratti o ricevute. Le registrazioni contabili devono essere effettuate tempestivamente e in modo accurato per garantire che il bilancio rispecchi fedelmente la situazione finanziaria dell'azienda.

- L’azienda deve utilizzare software di contabilità che permettano di tracciare tutte le operazioni finanziarie e garantire la completezza dei dati. I bilanci devono essere facilmente verificabili e prontamente disponibili per eventuali audit interni o esterni.

2. **Firma congiunta su movimentazioni > soglia**
   - Per prevenire movimenti di denaro o operazioni fuori dal controllo, è necessario che tutte le movimentazioni superiori a una determinata soglia (ad esempio, una cifra significativa come 10.000 euro) vengano approvate da almeno due figure autorizzate, come il Direttore Finanziario e il CEO o il Consiglio di Amministrazione. Questo sistema di firma congiunta riduce il rischio di operazioni non autorizzate e crea una protezione contro abusi da parte di singoli individui.
   - Le movimentazioni finanziarie significative, come pagamenti o trasferimenti bancari, devono essere tracciabili e supportate da documentazione che giustifichi il loro scopo e l’esistenza di un contratto o accordo formale.
3. **Controlli del revisore indipendente**
   - L’azienda deve nominare un revisore indipendente che verifichi regolarmente la correttezza e la trasparenza del bilancio. Il revisore esterno ha il compito di esaminare le operazioni aziendali e assicurarsi che le pratiche contabili siano conformi alle leggi fiscali e societarie. La revisione esterna aiuta a identificare anomalie o errori nei bilanci e a garantire che non ci siano operazioni sospette o fraudolente.
   - Il revisore deve essere scelto tra professionisti indipendenti e deve avere il potere di accedere a tutta la documentazione necessaria per una verifica approfondita. L’audit esterno è cruciale per evitare il rischio di frodi o manipolazioni contabili.
4. **Divieto di contabilità parallela**
   - È vietato tenere una contabilità parallela o non ufficiale. Tutte le operazioni economiche e finanziarie devono essere registrate nel sistema contabile ufficiale dell’azienda. La creazione di contabilità parallele, che possano essere utilizzate per nascondere transazioni o operazioni non dichiarate, è un reato grave e rappresenta un rischio significativo per l’azienda.
   - L’azienda deve stabilire politiche rigorose contro la gestione di fondi non registrati o di “scorte nere” e deve vigilare affinché ogni dipendente o collaboratore rispetti le linee guida in materia contabile. Le pratiche di contabilità parallela sono illegali e possono causare pesanti sanzioni penali e fiscali.
   - Ogni operazione che possa sembrare fuori dall'ordinario o non registrata deve essere oggetto di audit e indagine interna per garantire che non si stiano occultando attività illecite.
5. **Obbligo di documentazione e tracciamento delle operazioni**
   - Ogni transazione deve essere correttamente documentata e archiviata in un sistema facilmente accessibile per eventuali controlli. Le fatture, gli estratti bancari, le ricevute e qualsiasi altro documento giustificativo devono essere conservati in conformità alle normative fiscali e societarie.
   - L’azienda deve mantenere un sistema di archiviazione elettronica dei documenti che consenta la tracciabilità delle operazioni e la facile consultazione in caso di audit o ispezioni da parte delle autorità fiscali o regolamentari.
6. **Formazione periodica sul rischio fiscale e societario**
   - Il personale coinvolto nella gestione delle attività contabili, fiscali e finanziarie deve essere formato periodicamente sulle normative fiscali e societarie, nonché sui rischi legati alla manipolazione del bilancio o alla realizzazione di operazioni extra-contabili.

- La formazione dovrebbe includere gli aspetti della legislazione fiscale, le tecniche di rilevamento delle frodi, la gestione delle dichiarazioni fiscali e l'importanza di una contabilità corretta e trasparente.

7. **Politiche interne di integrità e comportamento etico**
   - L'azienda deve implementare politiche interne chiare per prevenire il coinvolgimento dei dipendenti in pratiche fraudolente. Queste politiche dovrebbero includere un codice etico che vieta qualsiasi tipo di attività illecita, comprese la manipolazione dei bilanci, l'occultamento di ricavi o la registrazione di operazioni non autorizzate.
   - L'azienda deve promuovere un ambiente di lavoro in cui l'integrità e la trasparenza siano i principi guida. I dipendenti devono essere incentivati a segnalare comportamenti sospetti senza timore di ritorsioni.

Conclusioni:
Le misure preventive e di controllo descritte sopra sono fondamentali per evitare reati societari e fiscali, che potrebbero compromettere gravemente la reputazione, la solidità economica e la posizione legale dell'azienda. L'implementazione di una contabilità trasparente, l'introduzione di pratiche di controllo rigorose e la formazione costante del personale sono strumenti essenziali per ridurre i rischi di frodi e manipolazioni contabili.

E. Selezione e gestione dei fornitori

Punti di Esposizione al Rischio (PEE):

- **Affidamento trasporti o manutenzioni:**
  - Il rischio associato alla selezione e alla gestione dei fornitori, in particolare per i servizi di trasporto e manutenzione, è legato all'affidamento di appalti a soggetti che potrebbero non rispettare le normative di sicurezza, ambientali, fiscali o etiche. L'azienda può trovarsi esposta a rischi legali, economici e reputazionali se i fornitori non operano in conformità con gli obblighi normativi o se sono coinvolti in pratiche fraudolente.
  - Le attività di manutenzione e trasporto coinvolgono anche il rischio di danneggiare beni aziendali, compromettere la sicurezza e l'efficienza operativa, nonché esporre l'azienda a sanzioni per il mancato rispetto delle normative ambientali e di sicurezza sul lavoro.

Attività a rischio:

- **Affidamento trasporti o manutenzioni:**
  - Affidamento di appalti per servizi di trasporto, spedizioni, manutenzione dei mezzi o impianti a fornitori che non soddisfano i requisiti legali o operativi richiesti.
  - Selezione di fornitori non qualificati o non verificati che potrebbero non rispettare le normative di sicurezza sul lavoro, ambientali, fiscali, o in materia di protezione dei dati.
  - Concludere contratti senza garantire la protezione dell'azienda da eventuali danni, ritardi o non conformità delle prestazioni.

Misure di prevenzione e controllo:

1. **Vendor list con qualifica e verifiche DURC**
   - L'azienda deve mantenere una **vendor list** aggiornata, che contenga solo fornitori qualificati che soddisfano determinati criteri di selezione. I fornitori devono essere accuratamente valutati prima di essere inclusi nella lista e devono possedere tutte le certificazioni necessarie relative alla loro attività (ad esempio, ISO 9001 per la qualità, ISO 14001 per l'ambiente, e OHSAS 18001 per la sicurezza sul lavoro).
   - La qualifica dei fornitori deve essere basata su una valutazione dettagliata delle loro capacità operative, dei riferimenti commerciali e della loro esperienza. In particolare, nel settore dei trasporti e delle manutenzioni, è fondamentale che il fornitore rispetti gli standard di sicurezza, efficienza e compliance alle normative.
   - Prima di affidare un contratto, l'azienda deve richiedere e verificare il **DURC** (Documento Unico di Regolarità Contributiva) del fornitore, che attesta la regolarità fiscale e contributiva del fornitore, assicurando che quest'ultimo sia in regola con il pagamento di contributi previdenziali, assistenziali e assicurativi.
2. **Contratti con clausole 231**
   - Ogni contratto stipulato con un fornitore deve includere **clausole 231**, che obbligano il fornitore a rispettare il modello organizzativo e di gestione dell'azienda in conformità con la **Legge 231/2001**. Le clausole devono coprire vari aspetti, tra cui la prevenzione di reati societari, fiscali, ambientali e di sicurezza sul lavoro.
   - Le clausole 231 sono essenziali per garantire che i fornitori adottino e rispettino comportamenti conformi alle normative e alle politiche aziendali. Queste clausole devono esplicitamente indicare le sanzioni e le azioni correttive in caso di violazioni.
   - Le principali aree da coprire nelle clausole 231 sono:
     - **Prevenzione di reati**: come frodi fiscali, violazioni delle normative ambientali o di sicurezza sul lavoro.
     - **Compliance legale**: assicurarsi che i fornitori operino nel rispetto delle leggi nazionali e internazionali applicabili.
     - **Gestione dei subappaltatori**: i fornitori devono garantire che anche i subappaltatori siano in possesso dei requisiti legali e operativi.
   - Inoltre, la stipulazione di contratti con clausole 231 rafforza il sistema di governance aziendale, poiché impone la necessità di controlli costanti sui fornitori e sulle loro attività.
3. **Controllo documentazione Albo Gestori Ambientali**
   - Quando l'azienda si avvale di fornitori che operano in ambito ambientale, come quelli coinvolti nella gestione dei rifiuti, dei trasporti o della manutenzione di impianti industriali, è fondamentale verificare che i fornitori siano iscritti all'**Albo Nazionale Gestori Ambientali**. Questo Albo contiene l'elenco ufficiale delle imprese che sono autorizzate a gestire rifiuti e altre attività ambientali.
   - I fornitori che operano nel settore dei trasporti devono avere tutte le licenze necessarie, in particolare quelle relative al trasporto di materiali pericolosi, e devono rispettare le normative ambientali in vigore. Le aziende devono effettuare una verifica periodica dello stato di registrazione e della conformità di questi fornitori con le normative ambientali.
   - Un controllo continuo della documentazione richiesta, che include il possesso delle licenze, delle certificazioni ambientali e delle polizze assicurative, è cruciale per ridurre i rischi legati all'affidamento di attività sensibili a fornitori non conformi alle normative.

4. **Controlli di conformità periodici**
   - È necessario che l'azienda effettui controlli di conformità periodici sui fornitori, per garantire che continuino a soddisfare gli standard di qualità e le normative legali in vigore. Questi controlli devono essere pianificati e condotti annualmente o con frequenza maggiore, in base alla criticità dell'attività del fornitore.
   - I controlli devono includere:
     - Verifica della regolarità fiscale e contributiva (esame del DURC).
     - Verifica dell'iscrizione all'Albo Nazionale Gestori Ambientali, se applicabile.
     - Monitoraggio della documentazione relativa alla sicurezza sul lavoro e alle certificazioni di qualità.
     - Verifica delle attività legate al rispetto delle normative ambientali (ad esempio, emissioni, gestione dei rifiuti, rispetto delle normative sull'inquinamento).
5. **Audit sul ciclo di vita del contratto con i fornitori**
   - L'azienda deve condurre audit a cadenza periodica sull'intero ciclo di vita dei contratti con i fornitori, dal processo di selezione all'esecuzione del contratto. Questi audit devono coprire tutti gli aspetti relativi alla gestione del fornitore, comprese le performance, la compliance alle leggi e la qualità dei servizi prestati.
   - Gli audit possono essere svolti da un team interno specializzato o da un ente esterno indipendente, che fornisca una valutazione oggettiva e imparziale del rispetto delle condizioni contrattuali e delle normative di settore.
6. **Politiche interne di selezione e monitoraggio dei fornitori**
   - L'azienda deve stabilire politiche interne chiare e rigorose per la selezione, la gestione e il monitoraggio dei fornitori. Le politiche devono includere linee guida precise su come selezionare i fornitori (criteri di qualità, sicurezza, conformità legale), su come monitorarli durante la durata del contratto e su come intervenire in caso di non conformità.
   - Le politiche devono essere comunicate a tutti i livelli aziendali e integrate nel processo di approvvigionamento.
7. **Obbligo di compliance etica e sociale**
   - Le politiche aziendali devono includere anche un codice etico che i fornitori devono rispettare. Questo codice dovrebbe coprire temi come il rispetto dei diritti umani, la lotta contro la corruzione, la parità di trattamento e la responsabilità sociale d'impresa.
   - L'azienda deve garantire che i fornitori operino in modo etico e che non siano coinvolti in pratiche di corruzione, sfruttamento del lavoro o altre attività illegali o immorali.

Conclusioni:
La selezione e gestione dei fornitori sono attività fondamentali per prevenire rischi legali, fiscali e reputazionali. L'implementazione di misure rigorose, come la creazione di una vendor list qualificata, l'inclusione di clausole 231 nei contratti, e il controllo continuo della documentazione, è cruciale per garantire che l'azienda operi in conformità con le normative e promuova pratiche etiche e sicure. L'approccio sistematico e la vigilanza costante sulla conformità dei fornitori riducono sensibilmente il rischio di incorrere in reati societari e fiscali, così come in violazioni delle normative ambientali e di sicurezza.

F. Reati informatici

1. GESTIONE DEGLI ACCESSI AI SISTEMI INFORMATIVI

Punto di esposizione: utilizzo, assegnazione e controllo delle credenziali di accesso ai sistemi informatici aziendali.

Attività a rischio:

- Attivazione o mancata disattivazione di utenti su server, gestionali, posta elettronica.
- Accesso abusivo a sistemi o dati da parte di soggetti interni o esterni.

Misure di prevenzione:

- Politica di accesso basata sul principio del minimo privilegio.
- Autenticazione forte (es. multifattore).
- Registrazione e approvazione formale per la creazione e modifica degli account.
- Procedure di revoca immediata degli accessi a seguito di cessazione del rapporto.

2. AMMINISTRAZIONE DI SISTEMA E INFRASTRUTTURE IT

Punto di esposizione: gestione tecnica dei sistemi aziendali da parte di personale IT interno o esterno.

Attività a rischio:

- Accessi illimitati ai server e alle applicazioni gestionali.
- Alterazioni fraudolente dei log, dati o funzionalità di sistema.

Misure di prevenzione:

- Nomina formale degli amministratori di sistema.
- Registro degli accessi privilegiati.
- Segregazione dei compiti tra amministrazione e controllo.
- Monitoraggio continuo delle attività amministrative.

3. TRATTAMENTO E CONSERVAZIONE DI DATI SENSIBILI

Punto di esposizione: archiviazione, modifica e trasferimento di dati personali, aziendali o strategici.

Attività a rischio:

- Trattamento non autorizzato di dati personali (violazioni GDPR).
- Distruzione o alterazione dolosa di file aziendali.

Misure di prevenzione:

- Classificazione dei dati e accesso riservato in base al ruolo.
- Crittografia dei dati sensibili.
- Backup giornalieri e test periodici di ripristino.
- Tracciamento e logging delle operazioni critiche.

4. UTILIZZO DELLA POSTA ELETTRONICA E DEI SISTEMI DI COMUNICAZIONE

Punto di esposizione: impiego di strumenti aziendali di comunicazione per fini illeciti.

Attività a rischio:

- Invio non autorizzato di documenti aziendali riservati.
- Intercettazione e manipolazione di comunicazioni aziendali.

Misure di prevenzione:

- Policy sull'utilizzo degli strumenti di comunicazione aziendali.
- Sistemi di cifratura delle e-mail sensibili.
- Antivirus, antiphishing e sistemi di prevenzione delle intrusioni.
- Monitoraggio delle comunicazioni in entrata e uscita con sistemi SIEM.

5. SICUREZZA DEI SISTEMI INFORMATIVI

Punto di esposizione: vulnerabilità tecnologiche, software obsoleti, configurazioni deboli.

Attività a rischio:

- Introduzione di malware o software dannoso.
- Mancato aggiornamento di patch critiche di sicurezza.
- Attacchi esterni (es. ransomware, DDoS).

Misure di prevenzione:

- Aggiornamento regolare di software e firmware.
- Firewall e sistemi antivirus professionali.
- Vulnerability assessment periodici e penetration test.
- Piano di disaster recovery e business continuity.

6. SVILUPPO E MANUTENZIONE DI SOFTWARE AZIENDALE

Punto di esposizione: modifiche al codice o ai sistemi gestionali aziendali.

Attività a rischio:

- Manipolazione fraudolenta dei flussi informativi.
- Introduzione intenzionale di funzionalità occulte.

Misure di prevenzione:

- Documentazione formale del ciclo di sviluppo software (SDLC).
- Verifica e approvazione delle modifiche da parte di almeno due soggetti.
- Test di sicurezza e funzionalità su ambienti di staging.
- Log delle modifiche e audit trail.

7. UTILIZZO DI DISPOSITIVI MOBILI E SUPPORTI REMOVIBILI

Punto di esposizione: uso di dispositivi mobili aziendali o personali, chiavette USB, hard disk esterni.

Attività a rischio:

- Esfiltrazione di dati aziendali.
- Accesso ai sistemi tramite dispositivi smarriti o compromessi.

Misure di prevenzione:

- Blocco dell'uso di dispositivi non autorizzati.
- Crittografia automatica dei supporti rimovibili.
- MDM (Mobile Device Management) per dispositivi mobili.
- Policy BYOD con requisiti di sicurezza minimi.

8. GESTIONE DEI FORNITORI INFORMATICI E DI SERVIZI IN OUTSOURCING

Punto di esposizione: rapporti contrattuali con consulenti, manutentori o partner IT.

Attività a rischio:

- Accesso incontrollato ai dati o ai sistemi da parte di terzi.
- Utilizzo improprio di credenziali condivise.

Misure di prevenzione:

- Contratti con clausole di riservatezza e responsabilità specifica.
- Profilazione e limitazione degli accessi concessi ai fornitori.
- Supervisione degli interventi tramite logging e audit.
- Rotazione periodica delle credenziali condivise.

9. MONITORAGGIO, LOGGING E CONSERVAZIONE DELLE EVIDENZE DIGITALI

Punto di esposizione: gestione inadeguata dei sistemi di tracciamento delle attività.

Attività a rischio:

- Cancellazione o manomissione dei file di log.
- Impossibilità di ricostruire eventi a fini investigativi.

Misure di prevenzione:

- Attivazione dei log su server, gestionali, firewall.
- Conservazione per almeno 12 mesi in formato immodificabile.
- Accesso ai log riservato a soggetti autorizzati.
- Audit periodici sui file di log da parte dell'OdV o IT Security.

10. CESSAZIONE DEI RAPPORTI DI LAVORO O COLLABORAZIONE

Punto di esposizione: fase di uscita di dipendenti o collaboratori.

Attività a rischio:

- Uso delle credenziali aziendali da parte di ex collaboratori.
- Atti ritorsivi: cancellazione o danneggiamento di file.

Misure di prevenzione:

- Checklist di uscita con disattivazione immediata degli account.
- Restituzione e verifica dei dispositivi aziendali.
- Backup preventivo dei dati gestiti dal soggetto uscente.
- Audit sui log delle attività recenti.

Conclusioni

L'introduzione dell'art. 24-bis nel D.Lgs. 231/2001 ha segnato un passaggio cruciale nel riconoscimento della vulnerabilità digitale delle imprese e della crescente rilevanza delle minacce informatiche nel contesto della responsabilità amministrativa degli enti. I reati informatici, per loro

natura, presentano caratteristiche particolarmente insidiose: si sviluppano in tempi rapidi, possono essere perpetrati a distanza e spesso sfuggono al controllo immediato delle strutture organizzative tradizionali.

In tale contesto, **l'approccio preventivo** rappresenta la principale strategia difensiva. Il Modello 231 deve evolversi includendo presidi tecnici e organizzativi che siano in grado non solo di rispondere agli obblighi normativi, ma anche di riflettere una cultura della sicurezza informatica diffusa e concreta. L'adozione di politiche di accesso rigorose, l'implementazione di sistemi di logging, il monitoraggio degli utenti privilegiati e la protezione delle informazioni sensibili costituiscono misure minime, ma imprescindibili, per ridurre il rischio di commissione di reati informatici.

Il **fattore umano** continua a rappresentare un punto debole: la consapevolezza dei dipendenti e la loro formazione continua restano strumenti chiave per mitigare comportamenti colposi o dolosi. Occorre altresì valorizzare il ruolo dell'Organismo di Vigilanza (OdV) nel controllo dell'adeguatezza delle misure adottate, promuovendo una sinergia costante con la funzione IT e con l'ufficio legale.

Infine, si sottolinea come l'ambito cyber debba essere oggetto di una **valutazione dinamica del rischio**, soggetta a revisione periodica. Le minacce informatiche evolvono con estrema rapidità, e con esse devono evolversi anche i presidi aziendali. Solo attraverso un monitoraggio costante, una pronta risposta agli incidenti e un aggiornamento continuo delle misure tecniche e procedurali, l'impresa può costruire una **difesa effettiva e credibile** nell'ambito del Modello 231.

4. Obblighi informativi verso l'Organismo di Vigilanza (OdV)

Punti di Esposizione al Rischio (PEE):

Gli obblighi informativi verso l'**Organismo di Vigilanza (OdV)** sono cruciali per il corretto funzionamento del Modello 231 e per garantire che l'azienda mantenga un sistema di gestione e controllo efficace in relazione ai rischi legali, normativi e operativi. I punti di esposizione al rischio legati agli obblighi informativi riguardano principalmente la **comunicazione tempestiva e trasparente delle anomalie, degli incidenti e dei procedimenti amministrativi** che potrebbero influire sulla conformità aziendale e sulla prevenzione di reati.

Un'adeguata informazione all'OdV è essenziale per prevenire la possibilità di responsabilità penale dell'ente, poiché consente di monitorare in tempo reale il rispetto delle normative e delle politiche aziendali, e garantisce la trasparenza nell'individuazione di eventuali irregolarità o violazioni.

Attività a rischio:

1. **Report periodici su anomalie, ispezioni, multe:**
   - **Rischio di non comunicazione:** Se l'azienda non informa regolarmente l'OdV su anomalie, ispezioni, e multe ricevute, si può creare un vuoto informativo che impedisce all'OdV di svolgere adeguatamente il suo compito di supervisione e monitoraggio.
   - **Rischio di mancato aggiornamento:** La mancata comunicazione di ispezioni o verifiche da parte degli enti competenti può portare all'insorgere di situazioni di non conformità non rilevate tempestivamente.
   - **Rischio di azioni correttive non tempestive:** L'assenza di report periodici sugli eventi sopra descritti limita la capacità dell'azienda di implementare azioni correttive rapide ed efficaci.
2. **Comunicazione incidenti e infortuni gravi:**
   - **Rischio di mancata segnalazione:** Se incidenti gravi o infortuni non vengono segnalati immediatamente all'OdV, si perde l'opportunità di analizzare le cause e adottare misure preventive per evitare il ripetersi dell'evento.
   - **Rischio di violazioni delle normative sulla sicurezza:** La mancata comunicazione di incidenti e infortuni gravi potrebbe esporre l'azienda a sanzioni per la non conformità alle normative in materia di sicurezza sul lavoro e salute dei dipendenti.
3. **Notifica avvii di procedimenti amministrativi:**
   - **Rischio di non conformità procedurale:** Se l'azienda non comunica tempestivamente l'avvio di procedimenti amministrativi, l'OdV potrebbe non essere in grado di adottare azioni correttive per proteggere l'ente da potenziali sanzioni legali o danni reputazionali.
   - **Rischio di responsabilità penale:** La mancata notifica di procedimenti amministrativi può comportare il rischio che l'azienda non adotti tempestivamente misure correttive, aumentando la probabilità che si verifichino violazioni legali che potrebbero comportare la responsabilità dell'ente.

Misure di prevenzione e controllo:

1. **Report periodici su anomalie, ispezioni, multe:**
   - **Sistema di registrazione delle anomalie e sanzioni:** L'azienda deve attivare un sistema di registrazione centrale per raccogliere informazioni su tutte le anomalie, le ispezioni ricevute e le multe comminate, in modo che siano facilmente accessibili per l'OdV. Ogni evento (anomalie o ispezioni) deve essere documentato con il dettaglio del fatto, l'entità della violazione, le azioni correttive intraprese e gli eventuali risvolti legali o amministrativi.
   - **Report periodici all'OdV:** L'azienda deve stabilire una **frequenza periodica** per inviare all'OdV un report dettagliato su tutte le ispezioni e le multe ricevute, nonché su qualsiasi anomalia riscontrata nelle attività aziendali. Questi report devono essere forniti con cadenza almeno mensile o trimestrale, a seconda delle dimensioni e della complessità dell'azienda. Il report deve essere completo, obiettivo e accompagnato da un'analisi delle azioni correttive adottate e dei risultati ottenuti.
   - **Piani di azione correttivi e follow-up:** In ogni report, l'azienda deve includere informazioni riguardo le azioni correttive messe in atto per risolvere le anomalie e le violazioni, e un piano di monitoraggio per garantire che i problemi non si ripetano. L'OdV deve essere coinvolto nel processo di valutazione e approvazione dei piani di azione.
2. **Comunicazione incidenti e infortuni gravi:**
   - **Sistema di segnalazione immediata:** L'azienda deve disporre di un sistema interno di **segnalazione immediata** degli incidenti e degli infortuni gravi, che consenta ai responsabili di informare tempestivamente l'OdV e le autorità competenti. Questo sistema deve essere strutturato in modo tale da garantire che ogni evento sia segnalato entro un tempo molto breve dalla sua occorrenza (ad esempio, entro 24 ore).
   - **Indagine immediata sugli incidenti:** Dopo ogni incidente grave, deve essere avviata un'indagine interna per determinare le cause e le circostanze che hanno portato all'infortunio. L'indagine deve essere documentata e i risultati devono essere condivisi con l'OdV.
   - **Report sugli infortuni:** L'azienda deve redigere un **report periodico sugli incidenti** e infortuni gravi, che includa dettagli sull'incidente, la natura dell'infortunio, le cause riscontrate, le misure correttive adottate e le azioni preventive per evitare il ripetersi del fatto. L'OdV deve essere messo al corrente di tutte le indagini e delle azioni correttive, per monitorare l'efficacia delle misure adottate.
   - **Formazione sulla sicurezza e prevenzione degli infortuni:** L'azienda deve assicurarsi che tutti i dipendenti e collaboratori ricevano una formazione continua sulla sicurezza sul lavoro, affinché siano in grado di prevenire incidenti e infortuni e segnalare tempestivamente qualsiasi problema.
3. **Notifica avvii di procedimenti amministrativi:**
   - **Sistema di notifica tempestiva:** L'azienda deve attivare un sistema che garantisca la **notifica tempestiva** all'OdV dell'avvio di qualsiasi procedimento amministrativo che possa implicare l'azienda. Ciò include notifiche relative a procedimenti di tipo fiscale, ambientale, di sicurezza sul lavoro, o relativi a violazioni contrattuali.
   - **Monitoraggio dei procedimenti:** Una volta avviato un procedimento amministrativo, l'azienda deve monitorarlo costantemente, tenendo l'OdV aggiornato sull'evoluzione della situazione, sulle azioni intraprese per risolvere la

questione, e sugli esiti. Questo monitoraggio deve essere continuo e regolarmente riportato all'OdV tramite meeting periodici o report.

- **Coordinamento con il team legale:** L'azienda deve coinvolgere il team legale in ogni fase del procedimento amministrativo, per garantire che tutte le azioni siano in linea con le normative e per gestire la difesa dell'azienda in modo adeguato. L'OdV deve essere informato su tutte le fasi critiche del procedimento, come la ricezione di sanzioni o la necessità di avviare negoziati con le autorità.

Best practices:

- **Trasparenza totale con l'OdV**: La comunicazione con l'OdV deve essere sempre trasparente, tempestiva e completa. L'azienda deve garantire che l'OdV sia sempre informato su tutti gli aspetti rilevanti che potrebbero implicare rischi di responsabilità, sia per l'azienda che per i suoi dipendenti.
- **Utilizzo di software gestionali**: Per semplificare e automatizzare i report periodici, le comunicazioni degli incidenti e la gestione dei procedimenti amministrativi, l'azienda può dotarsi di software gestionali che permettano di tracciare in modo accurato tutte le informazioni e di generarne report in tempo reale. Questo strumento consente all'OdV di avere un accesso diretto e immediato ai dati rilevanti.

Conclusioni:
La comunicazione tempestiva e precisa all'Organismo di Vigilanza è fondamentale per garantire che l'azienda rimanga in linea con il Modello 231 e per prevenire possibili responsabilità penali o amministrative. Ogni segnalazione di anomalie, incidenti, infortuni o procedimenti amministrativi deve essere trattata con la massima serietà e trasparenza, in modo che l'OdV possa agire prontamente per evitare danni legali o reputazionali. Le misure preventive e di controllo devono essere rigorose e sistematiche, con l'implementazione di sistemi di reportistica periodica e l'adozione di buone pratiche di gestione delle informazioni.

5. Sistema disciplinare

Il **Sistema Disciplinare** è una componente essenziale del Modello 231 e serve a garantire che le **violazioni** ai **protocolli** e alle **procedure** stabilite dalla Parte Speciale siano affrontate in modo sistematico e che siano adottate le necessarie **misure correttive** per mantenere l'efficacia del Modello stesso. La sua funzione primaria è quella di evitare che comportamenti illeciti o negligenza nella gestione delle attività aziendali possano pregiudicare la conformità dell'azienda alle normative e ai principi contenuti nel Modello 231.

Le **violazioni ai protocolli** e alle **procedure** devono essere trattate con un sistema di **sanzioni disciplinari** che sia **giusto**, **graduato** e **proporzionato** in base alla **gravità** della violazione e alla **posizione** del soggetto responsabile (dipendente, dirigente, terzo). Il sistema deve essere strutturato in modo da **prevenire** comportamenti scorretti e di garantire che vengano adottate le giuste azioni in caso di violazioni.

Punti di esposizione al rischio (PEE):

1. **Violazioni ai protocolli interni e alle procedure della Parte Speciale:**
   - **Rischio di inadeguata gestione delle sanzioni:** Se il sistema disciplinare non è adeguato o applicato correttamente, le violazioni possono rimanere impunite o non affrontate in modo tempestivo, mettendo a rischio l'efficacia del Modello 231.
   - **Rischio di trattamento incoerente:** Se le sanzioni non sono proporzionate alla gravità delle violazioni o non applicate in modo coerente tra tutti i soggetti (dipendenti, dirigenti, terzi), si può compromettere l'integrità e la credibilità del sistema disciplinare.
   - **Rischio di mancato monitoraggio:** L'azienda potrebbe non avere un sistema di monitoraggio per valutare l'efficacia delle sanzioni e il loro impatto sui comportamenti aziendali, perdendo così l'opportunità di migliorare continuamente i suoi processi interni.
2. **Mancata differenziazione delle sanzioni per ruolo (dipendente, dirigente, terzo):**
   - **Rischio di mancanza di adeguate misure per i dirigenti:** I dirigenti hanno un ruolo di responsabilità superiore rispetto ai dipendenti, quindi le violazioni a loro carico dovrebbero essere trattate in modo diverso, con sanzioni che riflettano la loro posizione e responsabilità.
   - **Rischio di incoerenza nelle sanzioni per i terzi:** Le violazioni commesse dai terzi (fornitori, consulenti, partner) potrebbero essere trattate con minore severità o senza le dovute azioni correttive. La mancanza di un approccio chiaro e uniforme rischia di minare la responsabilità dell'azienda nei confronti della legge.
3. **Mancanza di formazione adeguata sul sistema disciplinare:**
   - **Rischio di scarsa consapevolezza:** Se i dipendenti, dirigenti e terzi non sono correttamente formati sul sistema disciplinare e sulle sanzioni previste, le violazioni potrebbero verificarsi con maggiore frequenza, poiché il personale non è consapevole delle conseguenze derivanti dai comportamenti illeciti.
   - **Rischio di ignorare le procedure disciplinari:** La mancanza di un sistema di comunicazione chiaro riguardo le sanzioni potrebbe condurre a un disinteresse per le procedure e a una scarsa motivazione nel rispettare i protocolli aziendali.

Misure preventive e di controllo:

1. **Definizione chiara del sistema disciplinare:**
   - **Norme e regolamenti scritti:** L'azienda deve stabilire e documentare un sistema disciplinare chiaro e completo che preveda il trattamento delle violazioni in modo coerente e trasparente. Questo sistema deve essere redatto in modo che tutti i dipendenti, i dirigenti e i terzi siano pienamente informati delle regole e delle sanzioni applicabili. Le norme disciplinari devono essere integrate con i principi del Modello 231 e adattate alle specificità aziendali e alle normative legali.
   - **Comunicazione chiara e trasparente:** L'azienda deve garantire che tutte le persone coinvolte nell'attività aziendale, inclusi i terzi, siano informate del sistema disciplinare e delle conseguenze delle violazioni. Questo può avvenire tramite la distribuzione del codice etico, la pubblicazione del sistema disciplinare sui canali aziendali ufficiali, e la formazione continua.
2. **Graduazione delle sanzioni in base alla gravità delle violazioni:**
   - **Sanzioni per dipendenti:** Per i dipendenti, il sistema disciplinare deve prevedere **sanzioni proporzionate** alla gravità della violazione. Le sanzioni possono variare da **richiami verbali o scritti** per le violazioni minori fino a **sospensioni** o **licenziamenti** per le violazioni gravi. Ogni sanzione deve essere applicata in modo equo, tenendo conto di fattori come la ripetitività dell'infrazione e la responsabilità del dipendente.
   - **Sanzioni per dirigenti:** Le sanzioni per i dirigenti devono essere particolarmente severe in quanto queste figure ricoprono un ruolo di **leadership** e **responsabilità** all'interno dell'azienda. In caso di violazioni gravi, i dirigenti possono essere soggetti a **sospensioni** o, in casi estremi, al **licenziamento**. La gravità della violazione sarà legata al danno che essa ha causato all'azienda e alla sua posizione gerarchica.
   - **Sanzioni per terzi:** I terzi (fornitori, partner commerciali, consulenti, ecc.) devono essere inclusi nel sistema disciplinare attraverso **contratti** che specifichino le sanzioni in caso di violazioni delle normative aziendali. Le sanzioni per i terzi possono includere la **risoluzione del contratto**, la **sospensione dei pagamenti** o l'esclusione da future gare o contratti con l'azienda. È importante che queste disposizioni siano chiaramente indicate nei contratti e che le violazioni siano monitorate regolarmente.
3. **Controllo e monitoraggio delle sanzioni:**
   - **Registro delle violazioni e delle sanzioni:** L'azienda deve mantenere un **registro completo** di tutte le violazioni riscontrate, delle azioni disciplinari adottate e delle misure correttive. Questo registro deve essere costantemente aggiornato e utilizzato per **monitorare l'efficacia** delle sanzioni nel prevenire future violazioni. Deve essere previsto un sistema di revisione periodica per analizzare i casi di sanzioni applicate e per apportare eventuali modifiche alle politiche disciplinari.
   - **Audit interno e report all'OdV:** L'azienda deve istituire un sistema di **audit interno** per verificare che le sanzioni siano applicate correttamente e in modo proporzionato. L'Organismo di Vigilanza (OdV) deve ricevere regolarmente report su come il sistema disciplinare viene applicato, per garantire che le procedure siano seguite in modo adeguato e per prevenire eventuali abusi.
4. **Formazione continua sui protocolli e sulle sanzioni:**

- **Corsi di formazione:** L'azienda deve organizzare corsi di **formazione periodici** per tutti i dipendenti, dirigenti e terzi sui protocolli e le procedure previsti dalla Parte Speciale del Modello 231. Durante questi corsi, devono essere chiaramente illustrate le **sanzioni disciplinari** per le violazioni dei protocolli e la gravità delle conseguenze derivanti da comportamenti illeciti.
- **Simulazioni e casi pratici:** È utile organizzare sessioni di formazione pratiche, con **simulazioni di violazioni** e l'analisi di casi concreti in modo che i partecipanti possano comprendere come il sistema disciplinare opera nella pratica e quale comportamento è richiesto per evitare sanzioni.

Best practices:

- **Eguaglianza e trasparenza:** La coerenza nell'applicazione delle sanzioni è fondamentale per mantenere l'integrità del sistema disciplinare. Ogni violazione, indipendentemente dal ruolo del soggetto (dipendente, dirigente, terzo), deve essere trattata in modo equo e in base alla gravità del fatto.
- **Prevenzione e consapevolezza:** Il miglior modo per applicare il sistema disciplinare è prevenire le violazioni attraverso una **formazione continua**, una **comunicazione trasparente** e una **cultura aziendale** che promuova la conformità e l'integrità.