Comodepur scpa

MAPPATURA SINTETICA DEI RISCHI

(D.LGS 231/2001)

Edizione approvata dal Consiglio di Amministrazione
del 19 Settembre 2018

Il Consiglio di Amministrazione
Il Presidente

Avv. Alberto Grandi

SOMMARIO

1. FINALITÀ DELLA MAPPATURA DELLE AREE A RISCHIO E MODALITÀ PER L'IDENTIFICAZIONE

La mappatura delle Aree di Rischio ha il fine di evidenziare in quale area, processo, attività e secondo quali modalità potrebbero essere commessi reati presupposto.
La mappatura deve essere aggiornata a seguito di modifiche legislative o organizzative interne.

2. APPROCCIO UTILIZZATO

L'analisi dei rischi si fonda sulle risultanze delle interviste condotte ai Responsabili di funzione, sia in termini di attività svolte dalle singole funzioni, sia di potenziali possibilità di commettere reato presupposto nell'esecuzione di tali attività.
Il rischio è stato classificato in alto, medio, basso, molto basso, inesistente. L'attribuzione del grado di rischio si fonda sul rischio potenzialmente insito in ciascuna attività, messo in relazione con i seguenti principi generali di controllo, generalmente in grado di mitigare il rischio stesso:

- Segregazione funzionale fra coloro che svolgono attività di un processo a rischio.
- Chiara attribuzione di poteri e responsabilità.
- Disciplina interna o esterna.
- Tracciabilità delle operazioni, chiarezza e trasparenza della documentazione.

Per quanto riguarda i reati in materia di sicurezza sul lavoro, la puntuale analisi dei rischi richiede il rinvio a parametri più idonei rispetto ai processi aziendali, quali strutture, tecnologie, ambienti di lavoro e fattori di rischio. Tale analisi viene, più propriamente, effettuata nell'ambito del Documento di Valutazione dei Rischi (DVR), al quale integralmente si rinvia.

3. RISULTATI DELL'ANALISI

All'esito della Mappatura delle aree a rischio e con specifico riferimento all'attività esercitata da Comodepur scpa ai reati presupposto è stato assegnato il seguente livello di rischio:

Rischio Alto:

- Reato di omicidio colposo e lesioni colpose, gravi o gravissime, connessi con la violazione delle norme antinfortunistiche e della tutela dell'igiene e della salute sul lavoro
- Reati ambientali

Rischio Medio:

- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico
- Concussione, induzione indebita a dare o promettere utilità e corruzione
- Reati societari previsti dal Codice Civile

Rischio Basso:

- Delitti informatici e trattamento illecito dei dati

Rischio Molto Basso:

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
- Delitti contro la personalità individuale
- Delitti contro l'industria e il commercio
- Abusi di mercato
- Delitti in materia di violazione del diritto d'autore
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Rischio per il quale non sussistono in società i presupporti (rischio inesistente):

- Delitti di criminalità organizzata
- Reati transnazionali
- Razzismo e xenofobia
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali
- Pratiche di mutilazione degli organi genitali femminili.

Qui di seguito sono presentate le attività sensibili alla commissione di reati presupposto qualificati alti, medi e bassi.

4. ATTIVITÀ SENSIBILI ALLA COMMISSIONE DI REATI PRESUPPOSTO

I sotto paragrafi che seguono sono dedicati alle attività a rischio per talune famiglie di reato presupposto.

4.1 Attività sensibili al reato di omicidio colposo o lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

La puntuale analisi dei rischi in materia di salute e sicurezza sul lavoro richiede il rinvio a parametri più idonei, quali strutture, tecnologie, ambienti di lavoro e fattori di rischio. Tale analisi viene, più propriamente, effettuata nell'ambito del Documento di Valutazione dei Rischi (DVR), al quale integralmente si rinvia.

4.2 Attività sensibili ai reati ambientali

L'attività esercitata dalla società porta ad attribuire alla famiglia dei reati ambientali previsti dall'art. 25 undecies un livello di rischio elevato.
Devono riternesi prevalentemente a rischio le seguenti aree aziendali:
- gestione impianto e fanghi;
- laboratori;
- gestione risorse umane;
- gestione acquisti;
- amministrazione e finanza;
- gestione sistema informativo.

Si richiama in ogni caso il documento "Analisi ambientale" del Sistema di Gestione Integrato, allegato 14 – AMR120111.

4.3 Attività sensibili al rischio di indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico

La natura dell'attività svolta da Comodepur scpa induce ad assegnare a tale famiglia di reati un livello di rischio medio, legato alla possibilità di conseguire incentivi attraverso l'indebita percezione di erogazioni pubbliche. E' necessario che tali condotte comportino un vantaggio per la Società.

In relazione ai reati di cui al presente paragrafo e in base ad una valutazione prognostica devono ritenersi prevalentemente a rischio le seguenti aree:

- Amministrazione e Finanza, HR (risorse umane), in relazione ad aspetti fiscali, previdenziali, documentali legati all'amministrazione e al reclutamento del personale.
- Gestione degli aspetti documentali legati agli adempimenti sulla salute e sicurezza sul lavoro e all'ambiente. Questi ultimi connessi con le precisazioni previste dalle autorizzazioni.

In relazione ai soli reati di abuso di indebita percezione e/o truffa ai danni dello Stato deve inoltre ritenersi a rischio l'area Amministrazione e Finanza, in relazione alla gestione delle pratiche volte all'ottenimento di eventuali incentivi o contributi.

4.4 Attività sensibili al rischio di Concussione, induzione indebita a dare o promettere utilità e corruzione

La natura dell'attività svolta da Comodepur scpa induce ad assegnare a tale famiglia di reati un livello di rischio medio legato, in particolare, ai rapporti intrattenuti dalla Società con enti pubblici. Affinché sia possibile configurare responsabilità ai fini del Decreto 231 è necessario che la condotta conferisca un vantaggio per la Società. In base ad una valutazione prognostica devono ritenersi prevalentemente a rischio le seguenti aree:

- Amministrazione e Finanza, per il rischio legato alla gestione dei pagamenti come mezzo per costituire riserve destinate a fini corruttivi, nonché per il rischio legato ad atti corruttivi realizzati tramite la gestione degli incassi e della tesoreria della Società.
- Gestione Risorse Umane, per il rischio di instaurare rapporti di lavoro o di riconoscere benefici di varia natura (avanzamenti di carriera, retribuzioni, erogazione bonus, etc.) a persona legata a soggetti pubblici.
- Ispezioni ed Autorizzazioni, per il rischio di atti corruttivi nei confronti dei soggetti appartenenti a Enti Pubblici che effettuano materialmente l'ispezione.
- Gestione impianto per il rischio di atti corruttivi realizzati nell'ambito dei rapporti con i fornitori per gli acquisti di opere, beni, servizi.

4.5 Attività sensibili al rischio di reati societari

Le caratteristiche della Società inducono ad assegnare a questa famiglia di reati un livello di rischio medio.
Ragionevolmente e in base ad una valutazione prognostica devono ritenersi prevalentemente a rischio le seguenti aree:

- Amministrazione e Finanza, per il rischio di:
  - Errata rappresentazione della situazione patrimoniale, economica e finanziaria della Società attraverso la contabilizzazione di valori errati o artefatti o l'omessa contabilizzazione di valori effettivi.
- Acquisti, per il rischio di:
  - Contabilizzazione di valori errati o artefatti o l'omessa contabilizzazione degli stessi in relazione a spese di consulenza, a costi assicurativi e a costi in genere.
- HR, per il rischio di:
  - Contabilizzazione di valori errati o artefatti od omessa contabilizzazione degli stessi, in relazione ai costi per il personale

4.6 Delitti informatici e trattamento dati

Le modalità operative della società e la configurazione organizzativa inducono ad assegnare a questa famiglia di reati un rischio basso.

4.6.1 Attività sensibili al rischio di delitti informatici e di trattamento dati

Tutte le aree aziendali possono considerarsi a rischio.

4.6.2 Precisazioni sui reati informatici

La legge 18.3.2008 n. 48, entrata in vigore il 5.4.2008, ha introdotto nell'ordinamento italiano una serie di nuove fattispecie di reato che possono essere commesse attraverso un illecito utilizzo di documenti informatici e/o di sistemi informatici.
Tale legge ha altresì introdotto nel D.Lgs. 231/01 il nuovo art. 24bis, che estende alle società, ricorrendone i presupposti, la responsabilità amministrativa per i reati sopra indicati.
La natura informatica che qualifica questi reati può riguardare le modalità di realizzazione della condotta, il suo oggetto materiale, il bene giuridico tutelato o la natura dei mezzi di prova.
Al fine di meglio comprendere l'ambito di responsabilità delle persone giuridiche verranno di seguito descritte le diverse condotte integranti le singole fattispecie di reato rilevanti ex D.Lgs. 231/2001.
Preliminarmente, al fine di agevolare la lettura delle norme, vengono di seguito fornite le definizioni di documento informatico e di sistema informatico.

Documento informatico: per documento informatico si intende "la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti" secondo quanto previsto dal Codice dell'Amministrazione Digitale ex D.Lgs. 82/2005;

Sistema informatico: per sistema informatico si intende, secondo la Convenzione di Budapest, "qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compie un'elaborazione automatica di dati".

- **491 bis** c.p. **Documenti informatici**

Tale norma, di portata generale, estende le sanzioni previste per le falsità degli atti pubblici e privati, alle falsità riguardanti, rispettivamente, un documento informatico pubblico o privato avente efficacia probatoria.

- **615 ter c.p. Accesso abusivo ad un sistema informatico o telematico**

La norma in esame punisce l'accesso non autorizzato ad un sistema informatico o telematico altrui, protetto da misure di sicurezza interne al medesimo, siano esse di tipo *hardware* o *software*.
La condotta illecita può concretizzarsi sia in un'attività di "introduzione" che di "permanenza" abusiva nel sistema informatico o telematico del proprietario del medesimo.
Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.
Il reato in questione, ad esempio, contrasta il fenomeno dei c.d. "*hackers*", e cioè di quei soggetti che si introducono nei sistemi informatici altrui, attraverso le reti telematiche, aggirando le protezioni elettroniche create dai proprietari di tali sistemi per tutelarsi dagli accessi indesiderati.

- **615 quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**

La norma in esame, tutelando la riservatezza dei codici di accesso, punisce la condotta di chi si procura illecitamente codici, parole chiave o altri mezzi idonei per accedere ad un sistema informatico o telematico protetto da misure di sicurezza.
Tra le condotte illecite tipizzate dalla norma rientrano anche le attività di diffusione, comunicazione o consegna a terzi dei predetti codici idonei all'accesso, nonché di comunicazione di indicazioni o istruzioni idonee al predetto scopo.
La norma sanziona solo le condotte prodromiche e preparatorie all'accesso abusivo al sistema informatico o telematico.
Il reato, ad esempio, è integrato qualora un soggetto ceda illecitamente ad un terzo la propria *password* di accesso alle banche dati cui abitualmente si collega.

- **615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico e telematico**

La norma in esame sanziona quelle condotte abusive che si sostanziano nella diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
L'ipotesi tipica è quella di creazione dei c.d. "programmi virus", che diffondendosi e riproducendosi minano la funzionalità dei sistemi ove riescano ad introdursi.

- **617 quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**

La norma in esame, tutelando la genuinità e la riservatezza delle comunicazioni, punisce le condotte di intercettazione, impedimento o interruzione delle comunicazioni telematiche, poste in essere all'insaputa del soggetto che trasmette la comunicazione.
La formula normativa di "comunicazioni telematiche" si presta ad abbracciare qualunque forma e qualunque strumento di divulgazione, ivi compresa la stessa via telematica, e quindi anche la diffusione del testo della comunicazione via Internet o attraverso qualsiasi altra rete.
Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

- **617 quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**

La norma in esame punisce la condotta di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, posta in essere al di fuori dei casi espressamente consentiti dalla legge.

- **635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici**

La norma punisce esclusivamente il danneggiamento di informazioni, dati e programmi informatici altrui.

Nella nozione di danneggiamento rientrano le condotte di distruzione, deterioramento, cancellazione, alterazione e soppressione.
Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

- **635 ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità**

La norma in questione al primo comma punisce le condotte prodromiche e preparatorie al danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635 *bis* c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità.
La concreta realizzazione del danno, invece, integra un'autonoma ipotesi di reato, sanzionata più pesantemente nel comma 2 della norma in commento.

- **635 quater c.p. Danneggiamento di sistemi informatici o telematici**

La norma in questione punisce le condotte di danneggiamento di cui all'art. 635 *bis* c.p. aventi ad oggetto il funzionamento di un sistema informatico.
Tra le condotte di danneggiamento punite dalla norma rientra, oltre a quella di "rendere in tutto od in parte inservibile" il sistema informatico, anche quella di averne "ostacolato gravemente" il funzionamento.
Il riferimento al fatto che il danneggiamento punito possa essere commesso anche attraverso "l'introduzione o la trasmissione di dati" dimostra l'attenzione del Legislatore alla punizione delle condotte che si concretizzano nella diffusione di virus informatici.

- **635 quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità**

La norma in questione punisce i fatti di danneggiamento previsti dall'art. 635 *quater* c.p. riguardanti i sistemi informatici o telematici di pubblica utilità.
Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

- **640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica**

La norma in esame punisce la frode informatica commessa esclusivamente dal soggetto che presta servizi di certificazione di firma elettronica ovvero fornisce altri servizi connessi con quest'ultimo, secondo quanto previsto dal Codice dell'Amministrazione Digitale ex D.Lgs. 82/2005.
La condotta punita penalmente consiste nella violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato: si tratta, in particolare, degli obblighi di controllo e garanzia previsti dal predetto D.Lgs. 82/2005.

4.7 Attività sensibili ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Trattasi di rischi ritenuti in Comodepur molto bassi.

I rischi connessi alla famiglia in epigrafe potrebbero essere correlati alla:
- Non adeguata verifica della controparte.
- Gestione non corretta della fatturazione e delle risorse finanziarie.
- Acquisizione di beni e servizi provenienti da attività illecite.

Ragionevolmente e in base ad una valutazione prognostica devono ritenersi prevalentemente a rischio le seguenti aree:
- Acquisto di beni e servizi:
  - Per il rischio di ricorrere a fornitori coinvolti in episodi di riciclaggio o ricettazione.
- Amministrazione Finanza e Controllo:
  - Per il rischio di impiegare proventi di origine delittuosa attraverso movimenti bancari.
- Gestione Risorse Umane, per il rischio di utilizzare proventi illeciti nelle retribuzioni del personale.

4.7.1 Precisazioni su ricettazione, riciclaggio e autoriciclaggio

<u>Ricettazione</u>
L'art. 648 c.p. incrimina chi "fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare".
Per acquisto dovrebbe intendersi l'effetto di un attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.
Il termine ricevere starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.
Per occultamento dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.
La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico (come precisato dalla giurisprudenza), tra l'autore del reato principale e il terzo acquirente.
L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".
Lo scopo dell'incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell'evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

Riciclaggio
Tale reato consiste nel fatto di chiunque "fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa". Il delitto in esame sussiste anche quando l'autore del delitto da cui il denaro o le cose provengono, sia non imputabile o non punibile, o quando manchi una condizione di procedibilità riferita a tale delitto. È necessario che antecedentemente ad esso sia stato commesso un delitto non colposo al quale, però, il riciclatore non abbia partecipato a titolo di concorso.
La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale ed è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.
La disposizione è applicabile anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto. E' rilevante il fatto di chi ponga ostacoli alla identificazione dei beni suddetti dopo che essi sono stati sostituiti o trasferiti.

Autoriciclaggio
Nell'ambito della famiglia di cui all'art. 25 *octies*, Decreto 231, assume particolare rilevanza il reato di autoriciclaggio (art. 648 ter.1, c.p.). È una fattispecie di recente introduzione, che pone diverse problematiche a ragione della tecnica legislativa impiegata e delle oscillazioni ravvisabili nelle prime pronunce giurisprudenziali, peraltro ancora limitate.

Il reato è commesso da chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
Le pene sono aumentate nel caso in cui il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni.
Non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.
Sono previste pene maggiori nei casi in cui i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

In base ad una valutazione prognostica realizzata alla luce delle peculiarità del contesto analizzato e della natura dell'attività svolta da Comodepur scpa, i reati base che, oltre quelli già presenti nel catalogo dei reati presupposto, potrebbero essere ipoteticamente commessi sono:

- ✓ Reati tributari.
- ✓ Truffa (residuale).

Ragionevolmente, ed in base ad una valutazione prognostica, devono ritenersi prevalentemente esposte al rischio di commissione dei suddetti reati base le aree qui di seguito indicate:

- Acquisti di beni e servizi, per il rischio di acquisti in tutto o in parte inesistenti, sì da costituire una riserva da utilizzare successivamente o nasconderne l'origine utilizzando fondi illeciti.
- Amministrazione Finanza e Controllo:
  - Per il rischio di registrare fatture fittizie o di emettere fittizie note di credito al fine di ridurre il reddito imponibile o fornire una veste lecita a proventi di origine illecita
  - Per il rischio di impiego di proventi illeciti per effettuate pagamenti a clienti per servizi effettivamente prestati
  - Per il rischio di omettere in tutto o in parte il versamento dei tributi, in maniera tale da costituire una riserva da utilizzare successivamente.
  - Gestione Risorse Umane, per il rischio di erogazione al personale di retribuzioni mediante proventi illeciti, nonché quello di pagamento di retribuzioni e bonus fittizi

4.8 Attività sensibili al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Trattasi di rischi ritenuti in Comodepur molto bassi.
Ragionevolmente d in base ad una valutazione prognostica devono ritenersi prevalentemente a rischio le seguenti aree:

- Acquisto di beni e servizi, attraverso il conferimento di incarichi di consulenza e forniture o mediante dazioni o promesse di utilità strumentali a condizionare il soggetto chiamato a deporre.
- Gestione Risorse Umane, relativamente all'instaurazione di rapporti di lavoro o al riconoscimento di benefits di qualsiasi natura o alla mancata comunicazione di sanzioni disciplinari dovute, strumentali al condizionamento del soggetto che deve testimoniare. Tale ultima casistica presenta un rischio basso.
- Amministrazione e Finanza, relativamente all'erogazione di somme strumentali al condizionamento del soggetto chiamato a testimoniare.
- Ispezioni ed autorizzazioni, attraverso dazioni o promesse di utilità, dirette a condizionare il soggetto chiamato a deporre.

4.9 Attività sensibili ai delitti contro l'industria e il commercio, abusi di mercato, violazioni del diritto di autore

Alla luce dell'attività svolta da Comodepur scpa il rischio connesso alle anzidette famiglie in oggetto è molto basso.

4.10 Attività sensibili ai delitti contro la personalità individuale

Alla luce dell'attività svolta da Comodepur scpa il rischio connesso alla famiglia in oggetto è molto basso ed è legato al potenziale impiego di personale in condizioni di sfruttamento.

4.11 Attività sensibili ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Alla luce dell'attività svolta da Comodepur scpa il rischio connesso alla famiglia in epigrafe è molto basso.

4.12 Attività sensibili al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Nella Gestione delle Risorse Umane il rischio legato all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare risulta molto basso.

5. Presidi di prevenzione

Al fine di prevenire i rischi connessi ai reati in commento, sono presenti principalmente i seguenti presidi:

- Modello 231 e, in particolare, Protocolli 231 e Codice Etico.
- Statuto di Comodepur scpa
- Organigramma con corrispondenti funzioni.
- Documento di Valutazione dei Rischi (DVR).
- Manuale integrato qualità, ambiente, sicurezza, energia.
- Circolari interne