

# **ANTIRICICLAGGIO E CONTRASTO FINANZIAMENTI AL TERRORISMO (D. LGS. 231/2007, COME MODIFICATO DAL D. LGS. 90/2017)**

**INDICE**

1. Premessa .....	3
2. Termini e definizioni. ....	3
3. Scopo e campo di applicazione.....	3
4. Il quadro normativo.....	4
5. Ruolo e compiti degli organi aziendali in consac.....	11
5.1. Le attività di supervisione strategica.....	11
5.2. Le operazioni di natura gestionale.....	12
5.3. Formazione, misure organizzative e operative.....	12
6. La segnalazione di operazioni sospette.....	13
7. L'archiviazione delle informazioni.....	14
8. Le funzioni di controllo.....	14

**Lista di Distribuzione**

- DIGE, DILE, DISI, DT, ROSA, RPC

**Redazione****Data**

- OPC

30/10/2017

**Verifica Operativa****Data**

- DIGE

**Approvazione****Data**

- CdA

## 1. Premessa

Il riciclaggio di denaro proveniente da azioni illegali rappresenta uno dei più gravi fenomeni criminali. Il reinvestimento dei proventi illeciti in attività legali e la presenza di operatori e di organismi economici collusi con la criminalità alterano infatti profondamente i meccanismi di mercato, inficiando l'efficienza e la correttezza di ogni transazione finanziaria e indebolendo il sistema economico nel suo complesso.

Con la globalizzazione dell'attività finanziaria e il rapido sviluppo delle tecnologie dell'informazione, che aprono a nuove opportunità operative, aumentano i rischi connessi con il riciclaggio di capitali illeciti. Per tali ragioni, ai consueti strumenti repressivi, comuni all'azione di contrasto di ogni altra attività criminosa, occorre affiancare un sistema di strumenti a carattere preventivo. La medesima tipologia di strumenti va estesa anche sul versante del contrasto del finanziamento al terrorismo, che, sebbene in modo speculare rispetto a quanto avvenga per il riciclaggio, si caratterizza per un collegamento con il sistema finanziario.

## 2. Termini e definizioni

CdA	consiglio di amministrazione
CED	centro elaborazione dati consac
consac	consac gestioni idriche spa
CS	collegio sindacale
DIGE	direttore generale
DILE	direttore legale
DISI	direttore servizi idropotabili
DT	direttore tecnico
OPC	organizzazione, pianificazione, controllo
ROSA	responsabile operativo servizi ambientali
RPC	responsabile prevenzione e corruzione
TA	team di auditing aziendale
UC	ufficio contratti servizio idrico integrato consac
UCP	ufficio contabilità e pagamenti
UGA	ufficio gare e appalti consac
UIF	unità di informazione finanziaria per l'Italia

- Tab.1 -

## 3. Scopo e campo di applicazione

Il presente documento definisce gli obblighi del personale aziendale e descrive gli assetti organizzativi a salvaguardia dei rischi di riciclaggio e finanziamento al terrorismo, col

presupposto che efficaci misure adottate, su più livelli, costituiscono condizione essenziale per prevenire e mitigare fattori di rischio in tema.

Nello specifico delinea:

- i ruoli, i compiti e le responsabilità del personale dipendente nella valutazione del rischio e nella segnalazione di operazioni sospette;
- le linee guida per la conservazione della documentazione e delle evidenze dei rapporti e delle operazioni;
- l'attività di controllo e di coordinamento, anche attraverso idonei flussi informativi attivati a cadenza periodica, attribuita in modo specifico al RPC, il cui fine è anche quello di stimolare una collaborazione attiva e continuativa fra tutti i soggetti coinvolti.

#### **4. Il quadro normativo**

Il decreto legislativo n. 90 del 25 maggio 2017 riscrive integralmente, fra gli altri, il decreto legislativo n. 231/2007 in tema di contrasto al riciclaggio e al finanziamento al terrorismo, in attuazione della direttiva (UE) 2015/849 (c.d. IV Direttiva Antiriciclaggio).

Le principali novità del provvedimento sono sinteticamente di seguito riportate.

#### ***Definizione di riciclaggio***

Nella nozione di "riciclaggio" rientrano le seguenti tipologie di operazioni:

- la conversione o il trasferimento di beni, effettuati essendo a conoscenza della provenienza da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;
- l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- la partecipazione ad uno degli atti di cui ai punti precedenti e l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione.

Il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali.

#### ***Finanziamento del terrorismo***

L'espressione indica qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo

quanto previsto dalle leggi penali, indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte suindicate.

### **Soggetti obbligati**

La normativa antiriciclaggio interessa una vasta platea di soggetti, persone fisiche e giuridiche, nonché categorie professionali, fra i quali:

- intermediari bancari e finanziari (il decreto elenca le tipologie di società rientranti in questa categoria; fra le tante, le banche, Poste Italiane, le Sim e le Sgr);
- altri operatori finanziari (fra questi le società fiduciarie e i mediatori creditizi);
- professionisti (in forma individuale, associata o societaria): vi rientrano:
- dottori commercialisti, esperti contabili, consulenti del lavoro;
- ogni altro soggetto che rende i servizi forniti da periti, consulenti e altri soggetti che svolgono in maniera professionale, anche nei confronti dei propri associati o iscritti, attività in materia di contabilità e tributi (compresi associazioni di categoria di imprenditori e commercianti, CAF e patronati);
- una disciplina peculiare è quella riservata a notai e avvocati: essi sono soggetti obbligati quando, in nome o per conto dei propri clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i propri clienti nella predisposizione o nella realizzazione di operazioni riguardanti le seguenti attività:
- trasferimento a qualsiasi titolo di diritti reali su beni immobili o attività economiche;
- gestione di denaro, strumenti finanziari o altri beni;
- apertura o gestione di conti bancari, libretti di deposito e conti di titoli;
- organizzazione degli apporti necessari alla costituzione, alla gestione o all'amministrazione di società;
- costituzione, gestione o amministrazione di società, enti, trust o soggetti giuridici analoghi;
- revisori legali e società di revisione legale
- altri operatori non finanziari; tra questi, i soggetti che esercitano le seguenti attività:
- commercio di cose antiche, case d'asta, gallerie di arte;
- operatori professionali in oro;
- agenti immobiliari;
- mediatori civili,
- esercenti di attività di recupero stragiudiziale dei crediti per conto di terzi;
- custodia e trasporto di denaro contante, titoli o valori a mezzo di guardie giurate, ecc.;
- prestatori di servizi di gioco

Il riferimento specifico alle società partecipate è all'art. 10 del d. lgs. 231/2007:

“1. Le disposizioni di cui al presente articolo si applicano agli uffici delle Pubbliche amministrazioni competenti allo svolgimento di compiti di amministrazione attiva o di controllo, nell'ambito dei seguenti procedimenti o procedure:

- a) procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione;
- b) procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al codice dei contratti pubblici;

c) procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati.

2. In funzione del rischio di riciclaggio o di finanziamento del terrorismo, il Comitato di sicurezza finanziaria, anche sulla base dell'analisi nazionale del rischio di cui all'articolo 14, individua categorie di attività amministrative, svolte dalle Pubbliche amministrazioni responsabili dei procedimenti di cui al comma 1, rispetto a cui non trovano applicazione gli obblighi di cui al presente articolo. Con le medesime modalità e secondo i medesimi criteri, il Comitato di sicurezza finanziaria può individuare procedimenti, ulteriori rispetto a quelli di cui al comma 1, per i quali trovano applicazione gli obblighi di cui al presente articolo.

3. Il Comitato di sicurezza finanziaria elabora linee guida per la mappatura e la valutazione dei rischi di riciclaggio e finanziamento del terrorismo cui gli uffici delle Pubbliche amministrazioni, responsabili dei procedimenti di cui al comma 1, sono esposti nell'esercizio della propria attività istituzionale. Sulla base delle predette linee guida, le medesime Pubbliche amministrazioni adottano procedure interne, proporzionate alle proprie dimensioni organizzative e operative, idonee a valutare il livello di esposizione dei propri uffici al rischio e indicano le misure necessarie a mitigarlo.

4. Al fine di consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio e di finanziamento del terrorismo, le Pubbliche amministrazioni comunicano alla UIF dati e informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell'esercizio della propria attività istituzionale. La UIF, in apposite istruzioni, adottate sentito il Comitato di sicurezza finanziaria, individua i dati e le informazioni da trasmettere, le modalità e i termini della relativa comunicazione nonché gli indicatori per agevolare la rilevazione delle operazioni sospette.

5. Le Pubbliche amministrazioni responsabili dei procedimenti di cui al comma 1, nel quadro dei programmi di formazione continua del personale realizzati in attuazione dell'articolo 3 del decreto legislativo 1° dicembre 2009, n. 178, adottano misure idonee ad assicurare il riconoscimento, da parte dei propri dipendenti delle fattispecie meritevoli di essere comunicate ai sensi del presente articolo.

6. L'inosservanza delle norme di cui alla presente disposizione assume rilievo ai fini dell'articolo 21, comma 1-bis, del decreto legislativo 30 marzo 2001, n. 165.”

All'art. 1 il decreto definisce così le pubbliche amministrazioni: “[...] le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, gli enti pubblici nazionali, le società partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'articolo 2359 del codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea nonché i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica [...]”.

### **Autorità di controllo**

Sono disciplinate in dettaglio le competenze delle varie autorità di controllo coinvolte nella prevenzione e nella repressione del riciclaggio. Fra queste: il Ministero dell'Economia e

delle Finanze, il Comitato di sicurezza finanziaria, le autorità di vigilanza di settore, l'Unità di informazione finanziaria per l'Italia (UIF), la Direzione Nazionale antimafia e antiterrorismo, il Nucleo speciale di polizia valutaria della Guardia di Finanza.

Un ruolo attivo è attribuito agli organismi di autoregolamentazione, che anche attraverso le rispettive articolazioni territoriali ed i consigli di disciplina, promuovono e controllano l'adempimento degli obblighi di antiriciclaggio da parte dei professionisti iscritti nei propri albi ed elenchi.

### **Principali obblighi**

I principali obblighi in materia di antiriciclaggio riguardano l'adeguata verifica della clientela e del titolare effettivo e la segnalazione delle operazioni sospette.

L'obbligo di adeguata verifica del cliente e del titolare effettivo scatta, fra le altre ipotesi:

- in occasione dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale;
- in occasione dell'esecuzione di un'operazione occasionale, disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con una operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata ovvero che consista in un trasferimento di fondi superiore a 1.000 euro.

In ogni caso i soggetti obbligati procedono all'adeguata verifica del cliente e del titolare effettivo:

- quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione.

Per banche, Poste Italiane S.p.A., istituti di moneta elettronica e di pagamento, gli obblighi di adeguata verifica della clientela sono comunque osservati quando agiscono da tramite o siano comunque parte nel trasferimento di denaro contante o titoli al portatore, in euro o valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, di importo complessivamente pari o superiore a 15.000 euro.

Gli obblighi di adeguata verifica della clientela non si osservano in relazione allo svolgimento dell'attività di mera redazione e trasmissione o di sola trasmissione delle dichiarazioni derivanti da obblighi fiscali e degli adempimenti in materia di amministrazione del personale.

Gli obblighi di adeguata verifica della clientela si attuano attraverso:

- l'identificazione del cliente e la verifica della sua identità attraverso riscontro di un documento d'identità o di altro documento di riconoscimento equipollente, nonché sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- l'identificazione del titolare effettivo e la verifica della sua identità;

- l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale;
- il controllo costante del rapporto con il cliente per tutta la sua durata, attraverso l'esame della complessiva operatività del cliente medesimo, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività.

In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo può essere posticipata ad un momento successivo (entro 30 giorni) all'instaurazione del rapporto o al conferimento dell'incarico per lo svolgimento di una prestazione professionale, se ciò è necessario a consentire l'ordinaria gestione dell'attività oggetto del rapporto decorso tale termine, se la verifica dell'identità si rivela impossibile, i soggetti obbligati dovranno astenersi e valutare, sussistendone i presupposti, se effettuare una segnalazione di operazione sospetta.

Per i professionisti, limitatamente ai casi in cui esaminano la posizione giuridica del cliente o svolgono compiti di difesa o rappresentanza del cliente in un procedimento giudiziario, anche tramite una convenzione di negoziazione assistita, compresa la consulenza sull'eventualità di intentarlo o evitarlo, è previsto l'esonero dall'obbligo di verifica dell'identità del cliente e del titolare effettivo fino al momento del conferimento dell'incarico.

### ***Adempimento degli obblighi di adeguata verifica***

Il decreto specifica quali sono le modalità con cui assolvere gli obblighi di adeguata verifica. Fra queste, in primo luogo:

- l'identificazione del cliente e del titolare effettivo, svolta in presenza del medesimo cliente o dell'esecutore, anche attraverso dipendenti o collaboratori del soggetto obbligato: l'identificazione consiste nell'acquisizione dei dati identificativi forniti dal cliente, previa esibizione di un documento d'identità valido o altro documento di riconoscimento equipollente, del quale viene acquisita copia in formato cartaceo o elettronico. Il cliente deve inoltre fornire sotto la propria responsabilità le informazioni necessarie a consentire l'identificazione del titolare effettivo.

Sono inoltre indicati una serie di casi nei quali l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente.

- la verifica dell'identità del cliente, del titolare effettivo e dell'esecutore richiede il riscontro della veridicità dei dati identificativi contenuti nei documenti e delle informazioni acquisiti all'atto dell'identificazione, quando sussistano dubbi, incertezze o incongruenze; il riscontro può essere effettuato, fra le altre modalità, attraverso la consultazione del sistema pubblico per la prevenzione del furto di identità di cui al d.lgs. n. 64/2011;
- l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale;
- il controllo costante nel corso del rapporto continuativo o della prestazione professionale si attua attraverso l'analisi delle operazioni effettuate e delle attività svolte o individuate durante tutta la durata del rapporto, in modo da verificare che esse siano coerenti con la conoscenza che il soggetto obbligato ha del cliente e del suo profilo di rischio, anche riguardo, se necessario, all'origine dei fondi.



Il decreto individua una serie di fattori di rischio da tenere in adeguata considerazione, riferiti ai seguenti elementi:

- clienti: rapporti continuativi o prestazioni professionali instaurati o eseguiti in circostanze anomale, clienti residenti o aventi sede in aree geografiche ad alto rischio, strutture qualificabili come veicoli di interposizione patrimoniale, attività economiche caratterizzate da elevato utilizzo di contante;
- prodotti, servizi, operazioni o canali di distribuzione: servizi offerti a clientela dotata di patrimoni ingenti, prodotti o operazioni che potrebbero favorire l'anonimato, pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività ecc;
- aree geografiche: paesi terzi privi di efficaci presidi di prevenzione del riciclaggio e del finanziamento del terrorismo secondo le raccomandazioni del GAFI, paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da elevato livello di corruzione o permeabilità ad altre attività criminose, paesi soggetti a sanzioni emanate da organismi nazionali e internazionali o che finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche.

Le autorità di vigilanza di settore e gli organismi di autoregolamentazione possono individuare ulteriori fattori di rischio da prendere in considerazione e stabilire misure rafforzate di adeguata verifica della clientela, ulteriori rispetto a quelle indicate al decreto.

L'adeguata verifica rafforzata è comunque sempre necessaria in caso di: clienti residenti in paesi terzi ad alto rischio individuati dalla Commissione Europea; rapporti di corrispondenza transfrontalieri con un ente creditizio o istituto finanziario corrispondente di un paese terzo; rapporti continuativi, prestazioni professionali o operazioni con clienti e relativi titolari effettivi che siano persone politicamente esposte.

### ***Obbligo di segnalazione delle operazioni sospette***

I soggetti obbligati, prima di compiere l'operazione, devono inviare senza ritardo alla UIF una segnalazione di operazione sospetta "quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa". Il decreto poi specifica quali sono gli indici dai quali desumere il "sospetto", anche in base agli indicatori di anomalia elaborati e periodicamente aggiornati dalla UIF. Salvo casi specificamente indicati, l'operazione può essere compiuta solo dopo che è stata effettuata la segnalazione. La segnalazione contiene i dati, le informazioni, la descrizione delle operazioni ed i motivi del sospetto.

Sono esonerati dall'obbligo di segnalazione delle operazioni sospette i professionisti per le informazioni che ricevono da un loro cliente o ottengono riguardo allo stesso nel corso dell'esame della posizione giuridica o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso.

Per i professionisti, la segnalazione di operazione sospetta deve essere inviata direttamente alla UIF ovvero agli organismi di autoregolamentazione (in questo caso un apposito decreto ministeriale stabilirà le specifiche e le modalità e garanzie di tutela della riservatezza dell'identità del segnalante).

### ***Misure per tutelare l'identità della persona del segnalante***

Per non vanificare gli obblighi di segnalazione e non esporre a rischi la persona del segnalante sono previste una serie di misure volte a tutelarne l'identità:

- i soggetti obbligati e gli organismi di autoregolamentazione devono adottare tutte le misure idonee ad assicurare la riservatezza dell'identità dei segnalanti;
- l'autorità giudiziaria adotta le misure necessarie ad assicurare che l'identità del segnalante sia mantenuta riservata; il nominativo del segnalante non può essere inserito nel fascicolo del Pubblico Ministero né in quello per il dibattimento, e la sua identità non può essere rivelata, salvo che l'Autorità giudiziaria non disponga altrimenti, con provvedimento motivato ed assicurando l'adozione di ogni accorgimento idoneo a tutelare il segnalante se indispensabile ai fini dell'accertamento dei reati per i quali si procede;
- in caso di denuncia o comunicazione di notizia di reato non è fatta menzione dell'identità del segnalante, anche se conosciuta.

### ***Sanzioni penali e amministrative***

L'art. 55 del nuovo testo del d.lgs. n. 231/2007 prevede le sanzioni penali: queste le principali fattispecie, tutte punite con la reclusione da 6 mesi a 3 anni e la multa da 10.000 a 30.000 euro:

- soggetto tenuto agli obblighi di adeguata verifica che falsifica dati e informazioni ovvero utilizza dati e informazioni falsi relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione;
- soggetto tenuto all'osservanza degli obblighi di conservazione che acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei predetti dati e informazioni;
- soggetto obbligato a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, che fornisce dati falsi o informazioni non veritiere.

Il decreto interviene anche sull'apparato sanzionatorio amministrativo: queste le principali fattispecie:

- l'inosservanza degli obblighi di adeguata verifica e dell'obbligo di astensione è punita con la sanzione amministrativa pecuniaria di 2.000 euro; nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, la sanzione va da 2.500 a 50.000 euro;
- è prevista una sanzione amministrativa pecuniaria di 2.000 euro per l'inosservanza degli obblighi di conservazione; anche qui in caso di violazioni gravi, ripetute o sistematiche ovvero plurime, la sanzione va da 2.500 a 50.000 euro;

- per l'inosservanza delle norme relative all'obbligo di segnalazione delle operazioni sospette si applica una sanzione amministrativa pecuniaria di 3.000 euro; in caso di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione da 30.000 a 300.000 euro.

E' introdotta inoltre una nuova fattispecie di illecito amministrativo degli enti (art. 25-octies, d.lgs. n.231/2001). In caso di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nei confronti dell'ente si applicano la sanzione pecuniaria da 200 a 800 quote e le sanzioni interdittive di cui all'art. 9, comma 2, per una durata fino a 2 anni, quali sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la P.A., esclusione da agevolazioni, finanziamenti, contributi o sussidi, divieto di pubblicizzare beni o servizi.

## **5. Ruolo e compiti degli organi aziendali in consac**

Ai fini della mitigazione del rischio assumono rilievo prioritario il coinvolgimento degli organi societari e il corretto adempimento degli obblighi che su questi ricadono.

In particolare, gli organi aziendali, ciascuno secondo le proprie competenze e responsabilità, sono tenuti a:

- definire politiche aziendali coerenti con i principi e le regole antiriciclaggio;
- adottare linee di policy idonee a preservare l'integrità aziendale;
- porre in atto misure organizzative e operative atte a evitare il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento al terrorismo;
- svolgere controlli sul rispetto della normativa e sull'adeguato presidio dei rischi.

Più nello specifico, spettano al RCP:

- le attività di supervisione strategica sulla base degli orientamenti strategici delineati dal CdA;
- l'esecuzione di operazioni di natura gestionale, anche sulla scorta di indicazioni fornite periodicamente dal DIGE, dal DISI, dal DT e dal ROSA circa i processi da loro presidiati;
- la formazione delle unità aziendali operativamente coinvolte in processi di cui al c. 1 dell'art. 10 del D. Lgs. 231/2007 prima citato.

### **5.1. Le attività di supervisione strategica**

Il RCP, nell'ambito della funzione di supervisione strategica, ha il compito di:

- riesaminare periodicamente gli orientamenti strategici definiti dal CdA al fine di adeguare opportunamente le politiche di governo dei rischi connessi con il riciclaggio e il finanziamento al terrorismo. In ogni caso le politiche devono risultare adeguate all'entità e alla tipologia dei rischi cui l'attività di consac è concretamente esposta;
- assicurare nel continuo che i compiti e le responsabilità in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo siano allocate in modo chiaro e appropriato,

garantendo che le funzioni operative e quelle di controllo siano distinte e che le funzioni medesime siano fornite di risorse qualitativamente e quantitativamente adeguate;

- assicurare che venga approntato un sistema di flussi informativi adeguato, completo e tempestivo, garantendo al contempo la tutela della riservatezza dei soggetti che hanno partecipato alla procedura di segnalazione di operazione sospetta;
- delineare un sistema di controlli interni organico e coordinato, funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio, assicurandone l'efficacia nel tempo.

## **5.2. Le operazioni di natura gestionale**

Il RCP riunisce in sé, oltre alla funzione di supervisione strategica, anche quella di gestione, intesa come attuazione degli indirizzi deliberati dal CdA. Tale funzione **viene** esercitata col supporto del DIGE, del DISI, del DT e del ROSA, ciascuno per le aree di propria competenza. In tale ambito il RCP ha il compito di:

- verificare la stesura e l'aggiornamento delle procedure interne e le responsabilità delle strutture e delle funzioni aziendali al fine di individuare aree aziendali in cui sono allocati processi o fasi di essi che, in qualunque modo, possano far sorgere la necessità di monitorare eventuali rischi di riciclaggio e finanziamento al terrorismo;
- evitare al contempo il coinvolgimento inconsapevole di personale aziendale in fatti di riciclaggio e di finanziamento del terrorismo;
- in caso di segnalazione di operazioni sospette garantire certezza di riferimento e omogeneità nei comportamenti a tutte le strutture coinvolte;
- adottare misure volte ad assicurare la massima riservatezza sull'identità delle persone che hanno partecipato alla procedura di segnalazione di operazione sospetta
- assicurare il tempestivo assolvimento degli obblighi di comunicazione alle autorità preposte, così come previsto dalla normativa vigente;
- definire i flussi informativi finalizzati ad assicurare la conoscenza dei fattori di rischio a tutte le strutture aziendali coinvolte e agli organi incaricati di funzioni di controllo promuovendo e organizzando programmi di addestramento e formazione del personale dipendente - e di eventuali collaboratori - sugli obblighi derivanti dalla disciplina in materia di antiriciclaggio e di finanziamento al terrorismo internazionale; tale attività di qualificazione deve rivestire carattere di continuità e di sistematicità e tenere conto dell'evoluzione della normativa e delle procedure predisposte dalla banca
- adottare strumenti idonei a consentire la costante verifica dell'attività svolta dai dipendenti - e da eventuali collaboratori - al fine di rilevare eventuali anomalie che emergano nei comportamenti e nelle comunicazioni indirizzate ai propri referenti.

## **5.3. Formazione, misure organizzative e operative**

Il RCP è responsabile anche di un'attenta opera di addestramento e di formazione del proprio personale sugli obblighi previsti dalla normativa antiriciclaggio. Tale opera riveste carattere di continuità e sistematicità nell'ambito di programmi organici che tengono conto dell'evoluzione della normativa e delle procedure. Un'efficace applicazione della normativa antiriciclaggio presuppone infatti la piena consapevolezza delle finalità e dei principi che

ne sorreggono l'impianto e deve permettere al personale di acquisire piena conoscenza degli obblighi e delle responsabilità aziendali che possono derivare dal mancato adempimento dei medesimi. Conformemente alle disposizioni normative, i programmi interni di formazione del personale riservano particolare cura allo sviluppo di un'elevata preparazione dei dipendenti coinvolti direttamente nei processi di cui al c. 1 dell'art. 10 del D. Lgs. 231/2007 - UC, CED, UGA, UCP, per ogni rapporto afferente sia al ciclo acquisti che al ciclo vendite - nonché ai responsabili e agli altri collaboratori, di volta in volta indicati dal RCP dal DIGE, dal DISI, dal DT e dal ROSA, in quanto implicati in procedure particolarmente sensibili in un'ottica di politiche di antiriciclaggio e di lotta al terrorismo. Il rischio di imbattersi in operazioni di tale natura va specificamente valutato, per ogni attività eseguita, in riferimento sia al soggetto col quale consac instaura rapporti sia agli elementi caratterizzanti i rapporti medesimi.

A titolo esemplificativo e non esaustivo, in riferimento al soggetto:

- natura giuridica;
- complessità e articolazione della struttura organizzativa e identificazione del titolare effettivo;
- partecipazione di persone politicamente esposte;
- incarichi in società, associazioni, fondazioni soprattutto se aventi sede in paesi ad alto rischio a causa dell'utilizzo eccessivo di contante o non collaborativi - stati extra UE con regime antiriciclaggio non equivalente - ;
- processi penali o indagini in corso;
- comportamenti non trasparenti e non collaborativi;
- residenza in luoghi lontano dal domicilio.

Con riferimento all'operazione:

- occasionalità dell'operazione;
- operazione straordinaria rispetto alla natura del soggetto;
- operazione complessa che può agevolare l'opacità delle relazioni intercorrenti con altri soggetti coinvolti;
- richiesta di utilizzo di mezzi di pagamento non tracciati per importi elevati;
- ragionevolezza dell'operazione sotto il profilo economico – finanziario;
- coerenza dell'ammontare dell'operazione rispetto al profilo economico e finanziario del soggetto.

## **6. La segnalazione di operazioni sospette**

Ciascun dipendente che rilevi, nell'esercizio delle attività aziendali, il configurarsi del rischio di operazioni di riciclaggio di denaro o forme di finanziamento al terrorismo ne dà immediata comunicazione al RCP. Compiute le dovute valutazioni, questi ne informa il rappresentante legale di consac che, in quanto in possesso dei necessari requisiti di indipendenza, autorevolezza e professionalità, provvede a trasmettere all'UIF le segnalazioni ritenute fondate.

## **7. L'archiviazione delle informazioni**

Al RCP spetta, fra le altre, la gestione documentale delle attività di formazione eseguite. Le azioni di aggiornamento periodico sono opportunamente verbalizzate, con evidenza dei dati dei partecipanti. I verbali sono conservati, in formato cartaceo e/o elettronico, in ordine cronologico. Nella prima fase di introduzione in organico di nuovo personale, all'atto dell'assunzione può essere prevista anche un'azione formativa da attuarsi col metodo dell'affiancamento. Il RCP ha inoltre l'obbligo di conservare ciascun documento, in forma cartacea e/o elettronica, acquisito per l'assolvimento agli obblighi di valutazione del rischio. L'archiviazione è eseguita in maniera tale da consentire la ricerca e l'utilizzo delle informazioni in caso di indagini su casi di riciclaggio o finanziamento al terrorismo o per ogni attività di analisi condotta dall'UIF o da altre autorità competenti.

## **8. Le funzioni di controllo**

Le funzioni di controllo sono demandate al CS e al TA. Il CS vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei controlli antiriciclaggio. Nell'esercizio delle proprie attribuzioni, il CS si avvale, se necessario, di personale aziendale per lo svolgimento delle verifiche e degli accertamenti necessari.

In tale ambito il CS:

- valuta con particolare attenzione l'idoneità delle procedure in essere per l'adeguata verifica del rischio, la registrazione e la conservazione delle informazioni e per la segnalazione delle operazioni sospette;
- stimola l'azione di approfondimento dei motivi di eventuali carenze, anomalie e irregolarità riscontrate e promuove l'adozione delle opportune misure correttive.  
Tale organo viene sentito anche in merito alla definizione degli elementi dell'architettura complessiva del sistema di gestione e controllo del rischio di riciclaggio e di finanziamento del terrorismo.

Il TA verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.

Attraverso verifiche sistematiche, anche di tipo ispettivo, verifica tra l'altro:

- il costante rispetto dell'obbligo di adeguata verifica, sia nella fase di instaurazione del rapporto con soggetti sospetti, che nello svilupparsi nel tempo della relazione;
- l'effettiva acquisizione e l'ordinata conservazione dei dati e documenti;
- l'effettivo grado di coinvolgimento del personale dipendente nonché dei responsabili in un'ottica di collaborazione attiva.

Gli interventi sono oggetto di pianificazione per consentire che tutte le strutture operative siano sottoposte a verifica in un congruo arco di tempo e che le iniziative siano più frequenti nei confronti delle strutture maggiormente esposte ai rischi di riciclaggio e di finanziamento del terrorismo.