



BANCA PASSADORE & C.

MODELLO ORGANIZZATIVO

ai sensi del Decreto Legislativo 231/2001

Edizione Maggio 2010

PREMESSA

Il presente documento descrive il modello di organizzazione e gestione adottato dalla Banca Passadore & C. S.p.A. ai sensi dell'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231 ed è redatto in coerenza con le “Linee guida dell’Associazione Bancaria Italiana”.

Il Modello è inteso come l’insieme delle regole operative e delle norme deontologiche adottate dalla Banca in funzione delle specifiche attività svolte al fine di prevenire la commissione di reati previsti dal D. Lgs 231/2001.



1. IL DECRETO LEGISLATIVO 231/2001 E LA NORMATIVA RILEVANTE.....	1
1.1 PRINCIPI	1
1.2 LA NATURA DELLA RESPONSABILITA'	1
1.3 I SOGGETTI IN POSIZIONE APICALE ED I SOTTOPOSTI.....	1
1.4 I REATI.....	1
1.5 PRESUPPOSTI DI ESCLUSIONE DALLA RESPONSABILITA' DELL'ENTE.....	4
2. ATTIVITA' SVOLTE DALLA BANCA FINALIZZATE AL RECEPIMENTO DEL D.LGS. 231/2001	6
3. L'ORGANISMO DI VIGILANZA.....	7
3.1 NOMINA E COMPOSIZIONE DELL'ORGANISMO DI VIGILANZA.....	7
3.2 FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA AI SENSI DELL'ART. 6 D.LGS. 231/2001	7
3.3 REQUISITI DI INDIPENDENZA, PROFESSIONALITA' E RISERVATEZZA DELL'ORGANISMO DI VIGILANZA.....	8
3.4 MODALITÀ DI FUNZIONAMENTO DELL'ORGANISMO DI VIGILANZA	8
3.5 MODALITÀ DI SVOLGIMENTO DELL'INCARICO DELL'ORGANISMO DI VIGILANZA.....	9
3.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA	9
3.7 RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI.....	10
3.8 REPORTING DELL'ORGANISMO DI VIGILANZA VERSO IL CONSIGLIO DI AMMINISTRAZIONE ED IL COLLEGIO SINDACALE.....	10
4. PRINCIPI ED ELEMENTI ISPIRATORI DEL MODELLO	11
5. LA FORMAZIONE E L'AGGIORNAMENTO DELLE RISORSE UMANE E LA DIFFUSIONE DEL MODELLO	12
6. INDIVIDUAZIONE DELLE PRINCIPALI ATTIVITA' NEL CUI AMBITO POSSONO ESSERE COMMESSI REATI	13
7. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE.....	14
7.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	14
8. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.....	16
9. REATI DI CRIMINALITA' ORGANIZZATA.....	17
9.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	17
10. REATI CONTRO LA FEDE PUBBLICA.....	18
10.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	18
11. REATI SOCIETARI.....	19
11.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	19
12. REATI CON FINALITA' EVERSIVE E DI TERRORISMO	21
12.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	21
13. REATI DI ABUSO DI INFORMAZIONI PRIVILEGIATE E DI MANIPOLAZIONE DEL MERCATO	22
13.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	22
14. REATI CONNESSI CON LA VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO	23
15. REATI CONNESSI ALLA RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA E REATI TRANSNAZIONALI	24
16. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE	25
16.1 PRINCIPI GENERALI DI COMPORTAMENTO.....	25
17. ALTRI REATI	26
18. SISTEMA SANZIONATORIO	27
18.1 PRINCIPI GENERALI.....	27
18.2 MISURE NEI CONFRONTI DEI LAVORATORI SUBORDINATI CUI SI APPLICA IL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO (CCNL) PER IL SETTORE CREDITO	27
18.3 MISURE NEI CONFRONTI DEI DIRIGENTI	27
18.4 MISURE NEI CONFRONTI DI AMMINISTRATORI, SINDACI ED ALTA DIREZIONE	27
18.5 MISURE NEI CONFRONTI DI CONSULENTI E FORNITORI	27

ALLEGATO MODELLO ORGANIZZATIVO PER LA SICUREZZA E LA SALUTE DEI LAVORATORI



1. IL DECRETO LEGISLATIVO 231/2001 E LA NORMATIVA RILEVANTE

1.1 PRINCIPI

Il D.Lgs. 231/2001, recante la “disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell’articolo 11 della Legge 29 Settembre 2000, n° 300”, recepisce provvedimenti, anche comunitari, volti a sollecitare una crescente responsabilizzazione della persona giuridica, al fine di contrastare, con maggiore efficacia, la criminalità economica.

1.2 LA NATURA DELLA RESPONSABILITÀ

Il D.Lgs. 231/2001 prevede una “responsabilità amministrativa”, che mostra una palese analogia con la responsabilità penale. Infatti, il suo accertamento avviene nell’ambito del processo penale ed è autonoma rispetto alla responsabilità della persona fisica che ha commesso il reato: secondo il disposto dell’art. 8 l’ente potrà essere dichiarato responsabile, anche se la persona fisica che ha commesso il reato non sia imputabile ovvero non sia stata individuata.

Presupposti perchè un ente possa incorrere in tale responsabilità – e che di conseguenza siano ad esso imputabili le sanzioni pecuniarie o interdittive dallo stesso decreto previste – sono:

- a) che un soggetto che riveste posizione apicale all’interno della sua struttura, ovvero un sottoposto, abbia commesso uno dei reati previsti dalla parte speciale del Decreto;
- b) che il reato sia stato commesso nell’interesse o a vantaggio dell’ente;
- c) che il reato commesso dalle persone fisiche (soggetti in posizione apicale o sottoposti) derivi da una “colpa di organizzazione”.

Da ciò consegue che **non è prefigurabile** una responsabilità dell’ente ove la persona fisica che abbia commesso il reato abbia agito **nell’interesse esclusivo proprio o di terzi** ovvero nell’ipotesi in cui all’ente non sia imputabile alcuna “colpa organizzativa”, intesa come lo stato soggettivo imputabile all’ente consistente nel non avere istituito un efficiente ed efficace sistema di prevenzione dei reati.

Mentre per i reati societari il legislatore circoscrive la responsabilità della persona giuridica qualora il soggetto abbia agito perseguendo l’interesse della società, con riferimento alle altre fattispecie di reato l’ente risulta invece punibile anche nell’ipotesi in cui l’autore materiale del reato, pur non agendo volutamente nell’interesse dell’ente, rechi a quest’ultimo un vantaggio.

1.3 I SOGGETTI IN POSIZIONE APICALE ED I SOTTOPOSTI

L’art. 5 del D.Lgs. 231/2001 stabilisce che l’ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- 1) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (cosiddetti soggetti “in posizione apicale”);
- 2) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al punto precedente. Tutti i soggetti di cui ai punti 1) e 2) che precedono saranno indicati nel seguito del documento come “Soggetti”.

1.4 I REATI

Fattispecie di reato previste dal D.Lgs. 231/2001 (Capo I, sezione III: *Responsabilità amministrativa da reato*)

▪ Reati commessi nei rapporti con la Pubblica Amministrazione

Art. 24, D.Lgs. 231/2001, 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:

- Malversazione a danno dello Stato o di altro ente pubblico o dell’Unione Europea (art. 316-bis, c.p.);
- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altri enti pubblici o dell’Unione Europea (art. 316-ter, c.p.);
- Truffa a danno dello Stato o di altro ente pubblico (art. 640, c.2, n.1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche a danno dello Stato, di altri enti pubblici, dell’Unione Europea (art. 640-bis, c.p.);
- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640-ter, c.p.).



Art. 25, D.Lgs. 231/2001, concussione e corruzione:

- Concussione (art. 317, c.p.);
- Corruzione per un atto d'ufficio (art. 318, c.p.);
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319, c.p.);
- Circostanze aggravanti (art. 319-bis, c.p.);
- Corruzione in atti giudiziari (art. 319-ter, c.p.);
- Pene per il corruttore (art. 321, c.p.);
- Istigazione alla corruzione (art. 322, c.p.).

▪ **Reati informatici e trattamento illecito di dati**

Art. 24-bis, D.Lgs. 231/2001, (introdotto dalla l. 48/2008, art. 7), *delitti informatici e trattamento illecito di dati:*

- Documenti informatici (art. 491-bis, c.p.: falsità in un documento pubblico o privato avente efficacia probatoria);
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter, c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater, c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies, c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater, c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies, c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis, c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter, c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater, c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies, c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

▪ **Reati di criminalità organizzata**

Art. 24-ter, D.Lgs. 231/2001, (introdotto dalla l. 94/2009, art. 2), *delitti di criminalità organizzata:*

- Associazione per delinquere (art. 416, c.p., ad eccezione del comma 6);
- Associazione per delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 D.Lgs. 286/1998 (art. 416, comma 6, c.p.);
- Associazione di tipo mafioso (art. 416-bis, c.p.);
- Scambio elettorale politico-mafioso (art. 416-ter, c.p.);
- Sequestro di persona a scopo di rapina o di estorsione (art. 630, c.p.);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (*escluse quelle denominate "da bersaglio da sala", o ad emissione di gas, nonché le armi ad aria compressa o gas compressi e gli strumenti lanciarazzi -art. 2, c. 3, l. 110/1975*) (art. 407, comma 2, lettera a), numero 5, c.p.p.).

▪ **Reati contro la fede pubblica**

Art. 25-bis, D.Lgs. 231/2001, (introdotto dall'art. 6 del D.L. 350/2001, convertito con l. 409/2001 e modificato con l. 99/2009), *falsità in monete, in carte di pubblico credito e in valori di bollo e in strumenti o segni di riconoscimento:*

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453, c.p.);
- Alterazione di monete (art. 454, c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455, c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457, c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459, c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460, c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461, c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464, c.p.);
- Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473, c.p.);



- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474, c.p.).

Art. 25-bis-1, D.Lgs. 231/2001, (introdotto dalla l. 99/2009, art. 15), *delitti contro l'industria e il commercio*:

- Turbata libertà dell'industria o del commercio (art. 513, c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis, c.p.);
- Frodi contro le industrie nazionali (art. 514, c.p.);
- Frode nell'esercizio del commercio (art. 515, c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516, c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517, c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter, c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater, c.p.).

▪ **Reati societari**

Art. 25-ter, D.Lgs. 231/2001, (introdotto dal D.Lgs. 61/2002, art. 3; modificato dalla l. 262/2005, artt. 31 e 39):

- False comunicazioni sociali (art. 2621, c.c.);
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622, c. 1 e 3, c.c.);
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624, c. 1 e 2, c.c.);
- Impedito controllo (art. 2625, c. 2, c.c.);
- Formazione fittizia del capitale (art. 2632, c.c.);
- Indebita restituzione dei conferimenti (art. 2626, c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627, c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628, c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629, c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633, c.c.);
- Illecita influenza sull'assemblea (art. 2636, c.c.);
- Aggiotaggio (art. 2637, c.c.);
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis, c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, c. 1 e 2, c.c.).

▪ **Reati con finalità di terrorismo o di eversione dell'ordine democratico**

Art. 25-quater, D.Lgs. 231/2001, (introdotto dalla l. 7/2003, art. 3):

- Reati previsti dal codice penale e dalle leggi speciali.

▪ **Abusi di mercato**

Art. 25-sexies, D.Lgs. 231/2001, (introdotto dalla l. 62/2005, art. 9):

- Parte V, titolo I-bis, capo II, TUF (D.Lgs. 58/1998):
 - o Abuso di informazioni privilegiate (art. 184, TUF e, come illecito amministrativo, art. 187 bis, TUF);
 - o Manipolazione del mercato (art. 185, TUF e, come illecito amministrativo, art. 187 ter, TUF).

▪ **Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (D.Lgs. 81/2008, TUSSL)**

Art. 25-septies, D.Lgs. 231/2001, (introdotto dalla l. 123/2007, art. 9; sostituito dal D.Lgs. 81/2008, art. 300):

- Omicidio colposo (art. 589, c.p.);
- Lesioni personali colpose (art. 590, c. 3, c.p.).

▪ **Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita**

Art. 25-octies, D.Lgs. 231/2001, (introdotto dal D.Lgs. 231/2007, art. 63):

- Ricettazione (art. 648, c.p.);
- Riciclaggio (art. 648-bis, c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter, c.p.).

▪ **Delitti in materia di violazione del diritto d'autore**

Art. 25-novies, D.Lgs. 231/2001, (introdotto dalla l. 99/2009, art. 15):

- Immissione su sistemi di reti telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o parte di esse (art. 171, c.1, lett. a-bis, l. 633/1941);



- Reati di cui al punto precedente commessi su opere altrui non destinati alla pubblicazione qualora ne risulti offeso l'onore o la reputazione dell'autore (art. 171, c. 3, l. 633/1941);
 - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di un programma per elaboratore (art. 171-bis, c. 1, l. 633/1941);
 - Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati; estrazione o reimpiego della banca di dati; distribuzione, vendita o concessione in locazione della banca di dati (art. 171-bis, c. 2, l. 633/1941);
 - Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicale o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati (art. 171-ter, c. 1, l. 633/1941);
 - Riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita, cessione o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessione di qualsiasi genere, di opere dell'ingegno protette (art. 171-ter, c. 2, l. 633/1941); - Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies, l. 633/1941);
 - Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, l. 633/1941).
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Art. 25-decies, D.Lgs. 231/2001, (introdotto dalla l. 116/2009, art. 4)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

- **La responsabilità amministrativa di un ente sorge anche in relazione ai seguenti reati:**

Reati transnazionali (l. 146/2006, artt. 3 e 10)

L'art. 3 della legge definisce reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) cfr. art. 25-decies;
- Favoreggiamento personale (art. 378 c.p.).

Delitti contro la personalità individuale e pratiche di mutilazione (artt. 25 quinquies e 25 quater-1, D.Lgs. 231/2001)

Trattasi di una serie di delitti, previsti dagli artt. 600 – 602 e dall'art. 583-bis c.p. in tema di schiavitù, prostituzione e pornografia minorile, pornografia virtuale e pratiche di mutilazione degli organi genitali.

1.5 PRESUPPOSTI DI ESCLUSIONE DALLA RESPONSABILITÀ DELL'ENTE

Nell'ipotesi in cui l'ente risulti responsabile per i reati commessi nel suo interesse o a suo vantaggio da soggetti apicali ovvero da persone sottoposte alla direzione o alla vigilanza di questi ultimi, l'articolo 6 del D.Lgs. 231/2001 prevede



l'esonero da detta responsabilità, se l'ente dimostra che:

- a) ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento, è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

I reati commessi da soggetti sottoposti all'altrui direzione possono pertanto essere imputati all'ente solo se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, obblighi che si presuppongono osservati se l'ente, prima della commissione del reato, ha adottato, ed efficacemente attuato, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Si osserva peraltro che, in sede di procedimento penale, il giudice sarà libero di valutare l'effettiva idoneità del modello organizzativo adottato dall'ente a prevenire i reati.

Relativamente alla particolare categoria dei reati societari (art. 25-ter), inoltre, la responsabilità dell'ente è configurabile nell'ipotesi in cui il reato non sarebbe potuto essere perpetrato se gli amministratori o i direttori generali *“avessero vigilato in conformità degli obblighi inerenti alla loro carica”*.

2. ATTIVITA' SVOLTE DALLA BANCA FINALIZZATE AL RECEPIMENTO DEL D.LGS. 231/2001

La Banca si è dotata di un **CODICE ETICO** nel quale vengono formalizzati i principi verso i quali la Banca orienta la propria attività, che consistono nella rigorosa osservanza della legge, nella concorrenza leale, nella trasparenza, nel rispetto degli interessi legittimi dei Clienti, dei fornitori, dei dipendenti, degli azionisti, delle istituzioni e della collettività.

Tali valori vengono posti a fondamento di ogni comportamento e di ogni attività aziendale, a qualsiasi livello adottati dalla struttura organizzativa della Banca.

In nessun modo la convinzione di agire nell'interesse o a vantaggio della Banca può giustificare l'adozione di comportamenti in contrasto con i principi indicati nel Codice.

Il Codice è portato a conoscenza di tutti coloro ai quali si applica tramite opportune modalità di diffusione.

La Banca adotta tutti gli strumenti di controllo interni ed esterni previsti dalla legislazione vigente e dalle disposizioni degli Organi di Vigilanza e si è dotata di un sistema di regole interne costituite da:

- Regolamento interno
- Comunicazioni di Servizio e Istruzioni operative, che, in dettaglio, disciplinano:

- Anagrafe
- Antiriciclaggio
- Assegni
- Banche corrispondenti
- Bonifici e pagamenti
- Carte di credito e Bancomat
- Certificati di Deposito
- Conti correnti
- Estero merci
- Fidi
- Imposte e Contributi-Riscossioni
- Mutui e finanziamenti
- Organizzazione dei Servizi e Sportelli
- Personale
- Portafoglio
- Privacy
- Servizi diversi per la Clientela
- Sistema Informativo
- Titoli borsa e tesoreria

- Documento Programmatico per la Sicurezza

• Codice di Autodisciplina che assolvono alla funzione di organizzare il sistema dei poteri e delle deleghe, di regolamentare e proceduralizzare le attività svolte e di stabilire norme comportamentali specifiche volte a prevenire deviazioni dai principi ispiratori del Codice Etico. In particolare, il sistema delle deleghe, oggetto di continue revisioni, è basato su poteri a firma sociale doppia e/o singola di soggetti nominativamente identificati, consentendo, quindi, un efficace controllo dell'operatività.

Il complesso delle regole sopra citate incorpora un articolato sistema di controlli interni, coerente con le caratteristiche dimensionali e operative della Banca, ed è ritenuto funzionale anche alla prevenzione dei reati oggetto del D.Lgs. 231/2001. Peraltro, l'evoluzione normativa che contraddistingue il perimetro di riferimento di detto decreto ha reso opportuno una miglior specificazione del modello organizzativo della Banca mediante la redazione del presente documento volto ad enfatizzare l'attenzione della Banca alla tematica in oggetto.

Il compito di monitorare l'adeguatezza e la funzionalità del modello organizzativo e l'intero sistema dei controlli interni, in ottemperanza alle istruzioni degli Organi di Vigilanza, è affidato all'Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo.



3. L'ORGANISMO DI VIGILANZA

Ai sensi di quanto disposto dall'art. 6 del D.Lgs. 231/2001 è istituito in Banca un organo collegiale ("Organismo di Vigilanza") con il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo e di curarne l'aggiornamento.

L'Organismo di Vigilanza deve improntarsi a principi di autonomia ed indipendenza, quindi, per garantirne la terzietà, riporta e risponde direttamente al Consiglio di Amministrazione della Banca.

3.1 NOMINA E COMPOSIZIONE DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza è un organo collegiale composto dal Responsabile del Servizio Ispettorato e da altri due membri dotati di idonei requisiti di professionalità ed indipendenza nominati dal Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, preferibilmente scelti tra i Consiglieri indipendenti.

I componenti dell'Organismo di Vigilanza rimangono in carica fino alla scadenza del mandato del Consiglio di Amministrazione che li ha nominati.

Il Consiglio di Amministrazione della Banca, con il parere del Collegio Sindacale, può revocare in ogni momento il mandato ai componenti dell'Organismo di Vigilanza per inadempimento degli obblighi di riservatezza e diligenza.

In caso di rinuncia o decadenza di un membro dell'Organismo di Vigilanza il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, procede alla nomina di un sostituto che rimarrà in carica fino alla scadenza naturale del mandato.

Non possono essere designati membri dell'Organismo di Vigilanza, ed eventualmente decadono dal mandato, coloro i quali abbiano subito sentenze di condanna per i reati previsti dal D.Lgs. 231/2001 o che comportino l'interdizione, anche temporanea, dai pubblici uffici o che, comunque, si trovino in condizioni ostative previste dal Codice Etico della Banca.

L'Organismo di Vigilanza è presieduto dal Presidente, nominato dal Consiglio di Amministrazione fra i due membri non di diritto, dotato dei seguenti poteri:

- curare le formalità relative alla convocazione, fissazione dell'ordine del giorno, svolgimento delle riunioni dell'Organismo di Vigilanza;
- coordinare i lavori dell'Organismo di Vigilanza;
- dare esecuzione alle determinazioni dell'Organismo di Vigilanza.

La nomina deliberata dal Consiglio di Amministrazione richiede la formale accettazione da parte di ciascun membro designato.

La mancata partecipazione a più di due riunioni consecutive senza giustificato motivo comporta la decadenza del membro effettivo dell'Organismo di Vigilanza dal suo mandato.

3.2 FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA AI SENSI DELL'ART. 6 D.LGS. 231/2001

All'Organismo di Vigilanza sono attribuiti compiti di vigilanza sul funzionamento e l'osservanza del Modello Organizzativo, nonché di verifica sulla coerenza e validità nel tempo.

All'Organismo di Vigilanza sono demandati i seguenti compiti:

- vigilare sul funzionamento e sull'osservanza del Modello Organizzativo, tramite verifica della coerenza tra comportamenti concreti ed il Modello;
- valutare l'adeguatezza del Modello, ossia della sua reale capacità di prevenire, in linea di massima, i comportamenti voluti contrari alle disposizioni di Legge;
- monitorare il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del Modello in modo particolare con riferimento all'adeguamento a nuove normative ed alla gestione di nuove attività; provvedere, avvalendosi della collaborazione della Direzione Operativa e del Servizio Controllo Rischi e Conformità, all'aggiornamento del Modello, nell'ipotesi in cui si renda necessario effettuare correzioni ed adeguamenti;
- costituire un riferimento per i dipendenti della Banca che ad esso devono rivolgersi per segnalare condotte illecite;
- monitorare l'adeguato livello di diffusione, conoscenza e comprensione dei principi del Modello da parte del Personale della Banca, nonché della corretta attuazione degli appositi programmi di informazione/formazione e comunicazione interna;



- valutare le eventuali segnalazioni;
- accertare e segnalare al Consiglio di Amministrazione, per gli opportuni provvedimenti, le eventuali violazioni del Modello che possano comportare l'insorgere di responsabilità.

Le condizioni operative garantite per conseguire la massima efficacia di azione dell'Organismo di Vigilanza riguardano:

- l'accesso, senza limitazioni, alle informazioni aziendali rilevanti, senza vincoli di subordinazione gerarchica che possano condizionarne l'autonomia di giudizio, anche verso i vertici della Banca;
- l'obbligo di fornire informazione da parte di qualunque funzione aziendale, al verificarsi di eventi o circostanze che possano assumere rilievo al fine del presidio.

Per perseguire gli obiettivi descritti, l'Organismo di Vigilanza si avvale delle risorse professionali del Servizio Ispettorato e del Servizio Controllo Rischi e Conformità e può, inoltre, servirsi, nell'esercizio della sua attività, della collaborazione di soggetti esterni alla Banca (es. consulenti), disponendo in autonomia di adeguate risorse finanziarie. I consulenti esterni ed il personale della Banca che collaborassero con l'Organismo di Vigilanza sono anch'essi vincolati all'impegno di riservatezza.

3.3 REQUISITI DI INDIPENDENZA, PROFESSIONALITÀ E RISERVATEZZA DELL'ORGANISMO DI VIGILANZA

I membri indipendenti dell'Organismo di Vigilanza non devono essere legati alla Banca da rapporti di natura patrimoniale che ne compromettano l'indipendenza.

Non possono quindi:

- intrattenere, direttamente o indirettamente, relazioni economiche con la Banca tali da pregiudicarne l'indipendenza;
- essere titolari, direttamente o indirettamente, di partecipazioni azionarie di entità tale da permettergli di esercitare il controllo o un'influenza notevole sulla Banca;
- essere stretti familiari di amministratori esecutivi della Banca o di soggetti che si trovino nelle situazioni indicate nei punti precedenti.

Per quanto riguarda, invece, i membri dell'Organismo di Vigilanza dipendenti della Banca, l'autonomia va affermata attraverso la loro professionalità.

I membri dell'Organismo di Vigilanza:

- devono collocarsi in posizione di terzietà rispetto a coloro che rivestono funzioni di rappresentanza, amministrazione, direzione della Banca e sui quali sono chiamati ad esercitare la vigilanza;
- non devono avere ruoli operativi all'interno della Banca, che ne pregiudicherebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

I membri dell'Organismo di Vigilanza devono essere dotati di requisiti di professionalità idonei a garantire la loro imparzialità di giudizio ed autorevolezza, pertanto devono essere dotati delle seguenti competenze:

- conoscenza dell'organizzazione e dei principali processi aziendali;
- conoscenze giuridiche tali da consentire l'identificazione delle fattispecie suscettibili di configurare ipotesi di reato;
- capacità di individuazione e di valutazione degli impatti derivanti dalla normativa sui processi aziendali.

I membri dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso - con particolare riferimento alle segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello e si astengono dal ricercare ed utilizzare informazioni riservate per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza. In ogni caso, ogni informazione in possesso dei membri dell'Organismo di Vigilanza viene trattata in conformità con la legislazione vigente in materia ed, in particolare, con il D.Lgs. 196/2003 (codice in materia di protezione dei dati personali).

3.4 MODALITÀ DI FUNZIONAMENTO DELL'ORGANISMO DI VIGILANZA

Date le finalità perseguite dall'Organismo, sono necessarie una snellezza operativa e una persistenza di controllo conseguibili solo con un continuo interscambio di informazioni fra i membri dell'Organismo stesso. In tale ottica l'attività routinaria non è necessariamente legata alle formali riunioni ma si sviluppa mediante le varie forme di comunicazione disponibili. Tale attività è comunque oggetto di verbalizzazione nell'ambito delle riunioni formali previste. L'Organismo di Vigilanza si riunisce, su convocazione del Presidente, con cadenza almeno semestrale e, comunque, ogniqualvolta ne sia fatta richiesta da un membro o se ne presenti la necessità.

Si intende in ogni caso convocata validamente la riunione alla quale, pure in assenza di formale convocazione ai sensi di



quanto precedentemente indicato, partecipino tutti i membri dell'Organismo di Vigilanza.

Le riunioni dell'Organismo di Vigilanza sono valide con la presenza della maggioranza dei suoi membri e sono presiedute dal Presidente o, in sua assenza, dall'altro membro non di diritto .

Le delibere dell'Organismo di Vigilanza sono prese a maggioranza assoluta dei membri presenti.

Le delibere sono assunte con voto palese.

Di ogni riunione deve redigersi un verbale, sottoscritto dagli intervenuti, da conservarsi in apposita raccolta a cura del Responsabile del Servizio Ispettorato della Banca.

Ciascun membro dell'Organismo di Vigilanza ha diritto di far annotare nel verbale i motivi del suo dissenso.

E' fatto obbligo a ciascun membro dell'Organismo di Vigilanza di dare comunicazione agli altri membri e di astenersi dalla votazione nei casi in cui lo stesso si trovi in situazioni di conflitto di interessi, anche potenziale, in relazione all'oggetto della delibera. L'esistenza della situazione di conflitto e della conseguente astensione deve essere fatta constatare dal verbale della seduta.

3.5 MODALITÀ DI SVOLGIMENTO DELL'INCARICO DELL'ORGANISMO DI VIGILANZA

L'attività dell'Organismo di Vigilanza deve avere carattere di continuità tramite la verifica della costante adeguatezza del Modello e dell'operatività a quanto disposto dalla vigente normativa.

Nel vigilare sul funzionamento e sull'osservanza del Modello, l'Organismo di Vigilanza ha come base le informazioni e le risultanze del Servizio Ispettorato oltre alle eventuali segnalazioni pervenute all'Organismo stesso. I controlli vengono effettuati con la frequenza considerata più opportuna in base ad un giudizio sulla criticità ed importanza dei processi monitorati e sui livelli di rischio in loro insiti.

La verifica della coerenza dei comportamenti tenuti con il Modello è anche svolta tramite appositi controlli dell'Organismo che, all'uopo, si avvale delle risorse del Servizio Ispettorato ed eventualmente di altri Servizi.

Relativamente al monitoraggio nel tempo dei requisiti di solidità e funzionalità del Modello, l'Organismo di Vigilanza si avvale della funzione di Conformità, specie per quanto riguarda gli adeguamenti alla normativa, e si coordina con la Direzione Operativa per ciò che concerne l'adeguamento e l'implementazione del Modello per le nuove attività intraprese dalla Banca.

3.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i destinatari del Modello (componenti degli Organi Sociali, Dipendenti, Dirigenti, Collaboratori, ecc.) hanno l'obbligo di collaborare per una piena ed efficace attuazione del Modello.

Qualora i "Soggetti", i collaboratori ed i consulenti esterni vengano a conoscenza di situazioni, reali o potenziali, illegali o eticamente scorrette che, direttamente o indirettamente, procurano vantaggio per la Banca, devono immediatamente informare l'Organismo di Vigilanza e, ove applicabile, i propri superiori gerarchici, dandone comunicazione scritta.

Nel caso in cui i "Soggetti" di cui sopra ricevano richieste esplicite o implicite di benefici di qualsiasi natura da parte della Pubblica Amministrazione ovvero da parte di persone fisiche o giuridiche che agiscano alle dipendenze o per conto della P.A. devono informare immediatamente, per iscritto, l'Organismo di Vigilanza e, ove applicabile, i propri responsabili.

I "Soggetti" sono inoltre tenuti a segnalare, obbligatoriamente e tempestivamente, all'Organismo di Vigilanza provvedimenti e/o notizie provenienti da organi di Polizia Giudiziaria, o da qualsiasi altra autorità, nonchè richieste di assistenza legale in caso di avvio di procedimento giudiziario a carico dei Dipendenti o notizie in merito a procedimenti disciplinari in corso ed alle eventuali sanzioni irrogate.

I responsabili operativi sono tenuti a vigilare sull'attività dei propri collaboratori, al fine di prevenire qualsiasi violazione di norme. I responsabili operativi devono conoscere i processi e le attività svolte nelle proprie aree e strutture in cui possono essere commessi atti illeciti; inoltre, essi devono cooperare con l'Organismo di Vigilanza e la Direzione per l'istituzione, l'aggiornamento e la divulgazione di regole idonee a prevenirne la commissione.

L'Organismo di Vigilanza si rende garante della riservatezza dell'identità dei soggetti segnalanti, allo scopo di tutelare gli stessi da eventuali ritorsioni o discriminazioni di qualsiasi genere o natura.

L'Organismo di Vigilanza è tenuto a prendere in considerazione tutte le segnalazioni ricevute.



Le segnalazioni possono essere effettuate a mezzo: posta elettronica, telefax, posta ordinaria e/o interna.

3.7 RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI

I documenti di compendio dei controlli svolti, corredati degli eventuali rilievi e delle risposte dei Responsabili dell'attività, vengono conservati, sia in formato elettronico in un'apposita directory sia su supporto cartaceo quando recanti appunti manoscritti, a cura del Responsabile del Servizio Ispettorato e a disposizione dell'Organismo di Vigilanza.

L'archiviazione avviene per periodo di competenza e per argomento, per una durata di almeno 10 anni.

3.8 REPORTING DELL'ORGANISMO DI VIGILANZA VERSO IL CONSIGLIO DI AMMINISTRAZIONE ED IL COLLEGIO SINDACALE

L'Organismo di Vigilanza, in attuazione dei poteri e dei compiti attribuiti dal Consiglio di Amministrazione, relaziona semestralmente il Consiglio di Amministrazione e il Collegio Sindacale in merito alle verifiche effettuate ai fini della prevenzione dei reati di cui al presente Modello.

Nel caso rilevi comportamenti illeciti e/o difformi da quanto stabilito nel Modello, l'Organismo di Vigilanza informa senza indugio il Consiglio di Amministrazione, il Collegio Sindacale e il Direttore Generale.

4. PRINCIPI ED ELEMENTI ISPIRATORI DEL MODELLO

Il Modello è costituito dall'insieme delle regole interne di cui la Banca è dotata in funzione delle specifiche attività svolte e dei relativi rischi connessi.

Il Modello individua le attività nel cui ambito possono essere commessi reati e definisce i principi comportamentali necessari per evitare che siano commessi.

Il Modello considera quali propri principi fondamentali:

- **trasparenza** dei comportamenti sia all'interno della Banca che nei rapporti con controparti esterne;
- **correttezza** da parte di tutti i soggetti facenti capo alla Banca, garantita dal rispetto delle disposizioni di legge, di regolamento e delle procedure organizzative interne;
- **tracciabilità** delle operazioni relative alle aree sensibili, finalizzata a garantire la verificabilità della coerenza e congruenza delle stesse, anche tramite un appropriato supporto documentale.

I principi operativi cui il Modello si ispira sono:

- i requisiti indicati dal D.Lgs. 231/2001 ed in particolare:
 - l'attribuzione ad un Organismo di Vigilanza del compito di promuovere l'attuazione efficace e corretta del Modello;
 - la messa a disposizione dell'Organismo di Vigilanza di risorse adeguate a supportarlo nei compiti affidatigli;
 - l'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico;
 - l'attività di sensibilizzazione e diffusione, a tutti i livelli aziendali, delle regole comportamentali e delle procedure istituite.
- la normativa vigente cui devono sottostare gli Intermediari Finanziari (es. Testo Unico Bancario, Testo Unico della Finanza, Istruzioni di Vigilanza di Banca d'Italia, Regolamenti CONSOB, ecc.).
- i precedenti giurisprudenziali relativi al tema specifico della responsabilità amministrativa delle società ed in generale della tipologia di reati ai quali il Modello si riferisce.
- le linee guida pubblicate da ABI.

Costituiscono parte integrante del Modello sia le procedure finora adottate dalla Banca, sia le nuove procedure che verranno predisposte ed introdotte, secondo l'assetto normativo interno riportato al capitolo 2.

Il Modello viene aggiornato in caso di variazioni legislative oppure quando si ritenga necessario modificare le regole e le norme comportamentali; l'aggiornamento del Modello è curato dalla Direzione Operativa di concerto con l'Organismo di Vigilanza della Banca.

5. LA FORMAZIONE E L'AGGIORNAMENTO DELLE RISORSE UMANE E LA DIFFUSIONE DEL MODELLO

Il Modello organizzativo è distribuito a tutti i dipendenti mediante pubblicazione in Intranet.

Ai fini dell'efficacia del presente Modello è obiettivo della Banca assicurare, sia alle risorse già presenti in azienda sia a quelle che saranno inserite, una corretta conoscenza delle regole di condotta ivi contenute.

Il mancato rispetto delle regole ivi previste dà luogo all'applicazione delle sanzioni specificate nel successivo capitolo 15.

La Banca ottempera all'obbligo di formazione del proprio personale attraverso la realizzazione di specifici interventi, rivolti ai neoassunti e di uno specifico intervento annuale rivolto a tutti i dipendenti a cura del Servizio Personale.

Il sistema di informazione e formazione è realizzato dal Servizio Personale in collaborazione con i Responsabili delle Funzioni di volta in volta coinvolte nell'applicazione del Modello.

6. INDIVIDUAZIONE DELLE PRINCIPALI ATTIVITA' NEL CUI AMBITO POSSONO ESSERE COMMESSI REATI

Erogazione del credito.

Intermediazione e consulenza su strumenti finanziari.

Operatività “di sportello” connessa alla messa in circolazione dei valori.

Gestione dei finanziamenti pubblici.

Redazione e pubblicazione di documenti societari.

Rapporti con la società di revisione.

Gestione dei rapporti con autorità regolamentari e con il mercato (es. Banca d'Italia, UIC, CONSOB).

Gestione dei rapporti con soggetti istituzionali (es. ASL, Agenzia delle Entrate, Guardia di Finanza, Enti Locali, Ufficio del Catasto, Camera di Commercio).

Affari legali e contenzioso.

Gestione e manutenzione dei sistemi informatici.

7. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Le principali aree sensibili nei rapporti con la Pubblica Amministrazione, in considerazione dell'attuale operatività della Banca, sono le seguenti:

Gestione dei rapporti con soggetti istituzionali: con riferimento agli artt. 318 ss. c.p. (corruzione) nei rapporti di natura autorizzativa con la Pubblica Amministrazione;

Affari legali e contenzioso: con riferimento ai reati di cui agli artt. 318 ss. c.p. (corruzione) per il contenzioso ed i rapporti con pubblici ufficiali;

Rapporti con la Pubblica Amministrazione di natura commerciale (es. fornitore di beni o servizi con riferimento alla possibile commissione dei reati di cui agli artt. 318 ss. c.p. e 640 ss. c.p. (corruzione e truffa ai danni dello Stato));

Gestione Fondi / Contributi erogati dalla Pubblica Amministrazione (es. Artigiancassa, Fondi BEI, ecc.): con riferimento alla possibile commissione dei reati di cui agli artt. 316-bis, 316-ter, 318 ss. c.p. e 640 ss. c.p. (malversazione, indebita percezione di erogazioni, corruzione e truffa ai danni dello Stato);

Controlli esterni: i rapporti con le autorità pubbliche in caso di ispezioni costituiscono un'area sensibile con riferimento ai reati di cui agli artt. 318 ss. c.p. (corruzione). Inoltre, durante tali ispezioni potrebbe anche consumarsi il reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

7.1 PRINCIPI GENERALI DI COMPORTAMENTO

Nei rapporti con la Pubblica Amministrazione i "Soggetti" devono operare in modo conforme alla legge e all'etica secondo principi di correttezza, lealtà, trasparenza.

Sono tassativamente vietati pagamenti o compensi, sotto qualsiasi forma, offerti, promessi od effettuati direttamente o per il tramite di una persona fisica o giuridica per indurre, facilitare o remunerare una decisione, il compimento di un atto d'ufficio o contrario ai doveri d'ufficio della Pubblica Amministrazione.

Le disposizioni sopra indicate non si applicano a spese di rappresentanza ordinarie e ragionevoli o ad omaggi e atti di cortesia di modico valore e comunque tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere interpretati come finalizzati all'acquisizione impropria di vantaggi, sempre che non violino le disposizioni di legge.

Ai "Soggetti" è fatto tassativo divieto di utilizzare o presentare dichiarazioni o documenti falsi o attestanti cose non vere, ovvero omettere informazioni dovute, per conseguire contributi, finanziamenti, o altre erogazioni comunque denominate concesse dallo Stato, da un Ente pubblico o dall'Unione Europea. Ai "Soggetti" è fatto tassativo divieto di non destinare contributi, finanziamenti o altre erogazioni comunque denominate, concesse dallo Stato, da un Ente pubblico o dall'Unione Europea, alle specifiche iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse per le quali sono stati concessi.

In caso di ottenimento di erogazioni, contributi o finanziamenti da parte della Pubblica Amministrazione, deve essere predisposto un apposito rendiconto sulle modalità di effettiva utilizzazione dei fondi ottenuti.

Ai "Soggetti" è vietato tassativamente alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire illegalmente con qualsiasi modalità, anche indirettamente per il tramite di terzi, su dati, informazioni o programmi contenuti in un sistema informatico o telematico, o ad esso pertinente, a danno dello Stato o di un Ente Pubblico, per procurare direttamente o indirettamente un vantaggio o un'utilità alla Società.

Sono tassativamente vietati pagamenti o compensi, sotto qualsiasi forma, offerti, promessi od effettuati direttamente o per il tramite di una persona fisica o giuridica per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Qualora i "Soggetti" ricevano richieste esplicite o implicite di benefici di qualsiasi natura da parte della Pubblica Amministrazione devono immediatamente sospendere ogni rapporto e informare per iscritto l'Organismo di Vigilanza ed, eventualmente, le autorità competenti.

Nel caso in cui la Pubblica Amministrazione sia fornitore, direttamente od indirettamente, di beni o servizi alla Banca le forniture, gli appalti e i subappalti devono essere motivati da effettive esigenze aziendali e la scelta del fornitore deve, in ogni caso, essere effettuata tenendo esclusivamente conto di parametri tecnici ed economici e nel



rispetto delle vigenti prassi e procedure aziendali. I contratti devono essere stipulati per iscritto. L'importo della fornitura non deve essere superiore all'effettivo valore dei beni o delle prestazioni dedotte nel contratto di fornitura.

In nessun caso, nella trattativa commerciale o nella gestione del successivo rapporto contrattuale devono essere concesse condizioni di favore alla Pubblica Amministrazione, salvo che le migliori condizioni non risultino espressamente previste da provvedimenti della Pubblica Amministrazione stessa (bandi di gara).

8. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Le principali aree sensibili nell'ambito dei reati informatici sono rappresentate dal trattamento e dalla conservazione dei dati, nonché dalla continuità e dalla correttezza dei processi. In particolare, vengono in rilievo le alterazioni, interruzioni di servizio, manomissioni, diffusioni indebite di dati e documenti.

Per prevenire ed impedire la falsificazione di documenti aventi efficacia probatoria, la Banca ha adottato idonei ed appropriati sistemi in materia di conservazione della documentazione contrattuale e di rendicontazione.

Per tutelarsi dall'accesso abusivo al sistema, la Banca si è dotata di opportuni strumenti informatici. Inoltre, sono state predisposte credenziali di accesso differenziato per Dipendenti e Clienti con password crittografate, pertanto non visibili.

Per prevenire l'indebita installazione, anche involontaria, di impianti che possano danneggiare o interrompere il sistema informatico, la gestione di apparecchiature informatiche (macchine, apparati o programmi) è stata centralizzata presso il Servizio Informatica Individuale e Networking.

Per i reati previsti dall'art. 635-bis (danneggiamento di informazioni, dati e programmi informatici) e dall'art. 635quater (danneggiamento di sistemi informatici o telematici), la Banca si è dotata di strumenti volti al controllo e alla limitazione degli accessi a dati e programmi in ambiente di produzione quali, ad esempio, la separazione dell'ambiente di produzione da quello di sviluppo e la generazione di utenze personalizzate che consentano accessi diversificati in funzione delle mansioni dei Dipendenti.

La Banca ha adottato, ai sensi del D.Lgs. 196/2003 ("Codice in materia di protezione dei dati personali"), il "Documento Programmatico Sicurezza", al quale si rimanda per una dettagliata ed unitaria descrizione degli strumenti e dei processi sopra descritti in tema di sicurezza informatica aziendale, nonché il "Regolamento interno per l'utilizzo della posta elettronica e della rete internet". Tali documenti stabiliscono, tra l'altro, i comportamenti ai quali si devono attenere i Dipendenti (i documenti sono entrambi pubblicati nella sezione "Sicurezza" della Intranet Aziendale).

9. REATI DI CRIMINALITA' ORGANIZZATA

La configurazione e la natura delle fattispecie criminose di cui all'art. 24-ter (reati di criminalità organizzata) abbracciano un ampio ventaglio di situazioni trasversali alle varie attività della Banca che trovano però un comune denominatore nella rilevanza delle relazioni personali. La prevenzione di detti reati è presidiata dalla prassi e dagli obblighi di *adeguata verifica della Clientela*.

9.1 PRINCIPI GENERALI DI COMPORTAMENTO

La Banca ha adottato le procedure richieste dalle “Istruzioni operative per l’individuazione di operazioni sospette” emanate dalla Banca d’Italia.

La Banca inoltre adotta i seguenti principi:

- qualunque erogazione di fondi presuppone un’istruttoria cui partecipano e deliberano soggetti e funzioni diverse all’interno della Banca al fine di minimizzare il rischio di una manipolazione illecita di dati ed aumentare la condivisione delle conoscenze e delle decisioni all’interno della Banca stessa;
- qualunque afflusso significativo di fondi sui conti o depositi della Clientela presuppone un’attenta valutazione della coerenza e della compatibilità dell’operazione con il profilo del Cliente;
- nel caso in cui il Cliente effettui con frequenza operazioni in nome o a favore di terzi che non appaiono giustificate da legami familiari o da rapporti idonei a giustificarle o, nell’ipotesi contraria, in cui vi siano frequenti operazioni effettuate da terzi in nome o a favore di un Cliente, senza plausibili giustificazioni, l’anomalia deve essere evidenziata e sottoposta all’Organismo di Vigilanza della Banca.

10. REATI CONTRO LA FEDE PUBBLICA

La principale area sensibile nell'ambito dei reati contro la fede pubblica è rappresentata dall'operatività di sportello nell'attività di movimentazione del contante, con riferimento ai reati di falsità in monete, in carte di pubblico credito e in valori di bollo, e specificatamente:

Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453, c.p.);

Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455, c.p.);

Spendita di monete falsificate ricevute in buona fede (art. 457, c.p.).

10.1 PRINCIPI GENERALI DI COMPORTAMENTO

Tutti coloro che operano nell'interesse, a vantaggio o comunque per conto della Banca, senza alcuna distinzione o eccezione, sono tenuti, nel trattamento di valori di qualsiasi natura (in particolare, banconote, monete e valori di bollo aventi corso legale nello Stato e all'estero o materiali utilizzati per la fabbricazione di questi) ad operare nel rispetto della legge, dei regolamenti e delle discipline interne, con onestà, integrità, correttezza e buona fede.

I Dipendenti della Banca in particolare devono strettamente attenersi alle procedure riportate nelle specifiche normative di legge, istruzioni di Banca d'Italia e normativa interna emanate in materia di controllo dei valori trattati, di immediato ritiro dei biglietti di accertata o sospetta falsità e di qualità di banconote rimesse in circolazione anche attraverso apparecchiature per i prelievi automatici.

Particolare attenzione dovrà essere inoltre prestata nella negoziazione con Clientela non sufficientemente conosciuta ovvero avente ad oggetto importi di rilevante entità (comportamento peraltro già richiesto anche per altre finalità).

Inoltre, nello svolgimento delle attività nei confronti di terzi, in particolare con le società di trattamento e trasporto valori, i Dipendenti osservano i principi comportamentali di cui sopra anche al fine di evitare qualsiasi concorso in reati che detti terzi, eventualmente, commettessero all'interno della propria sfera operativa.

11. REATI SOCIETARI

Le aree sensibili nell'ambito dei reati societari, in considerazione dell'attuale operatività della Banca, sono le seguenti:

Redazione e pubblicazione di documenti societari (es. bilanci) con riferimento ai reati di cui agli artt. 2621, 2622 c.c. (false comunicazioni sociali e false comunicazioni sociali in danno dei soci o dei creditori);

Rapporti con la società di revisione con riferimento al reato di impedito controllo di cui all'art. 2625 c.c.;

Gestione dei rapporti con autorità regolamentari (es. UIC, Banca d'Italia, CONSOB) con riferimento ai reati di falso di cui agli artt. 2621 e 2622 c.c., ma anche ai reati di agiotaggio (art. 2637 c.c.) e di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.). Nei rapporti con le autorità regolamentari potrebbero avvenire anche episodi di corruzione rilevanti ai sensi dell'art. 318 c.p. (corruzione);

Conflitti di interesse degli amministratori con riferimento al reato di omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.).

11.1 PRINCIPI GENERALI DI COMPORTAMENTO

Principi generali

Gli Organi Sociali della Banca e tutti gli altri "Soggetti", ciascuno nella misura e con le modalità richieste dalle proprie funzioni, non possono porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente, integrino, direttamente o indirettamente, fattispecie di reato rientranti tra quelle di cui all'art. 25 ter del D.Lgs. 231/2001, ed in particolare violino principi e procedure riportati nel presente capitolo.

Conseguentemente, si prevede l'esplicito obbligo a carico dei soggetti sopra indicati di:

- mantenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Società e dei relativi Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà dell'Organo Sociale competente.

Inoltre, nello svolgimento delle attività nei confronti di terzi i "Soggetti" osservano i principi comportamentali di cui sopra anche al fine di evitare qualsiasi concorso in reati che detti terzi, eventualmente, commetteressero all'interno della propria sfera operativa.

Correttezza contabile

Il bilancio d'esercizio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale ed il risultato economico dell'esercizio della Banca.

I sistemi interni, i risultati finanziari e le registrazioni contabili della Banca devono rispecchiare, fedelmente e con ragionevole dettaglio, le operazioni. La contabilità dovrà rispettare i principi contabili previsti dalle norme primarie e secondarie. Tutte le poste all'attivo e al passivo della Banca devono essere correttamente riportate nei libri contabili dell'azienda così come devono essere riportati tutti gli impegni assunti dalla Banca (cosiddette poste "sotto la linea" e/o "fuori bilancio").

Per ogni operazione è conservata agli atti degli uffici coinvolti un'adeguata documentazione di supporto, volta a consentire la ricostruzione dell'operazione sia contrattuale che contabile.

Ogni dipendente è tenuto a segnalare, con tempestività e riservatezza, per iscritto, all'Organismo di Vigilanza ed al proprio diretto superiore ogni omissione, imprecisione o falsificazione delle scritture contabili o dei documenti di supporto di cui sia, in qualsiasi modo, venuto a conoscenza.

I dipendenti coinvolti nelle revisioni o ispezioni delle Autorità di Vigilanza devono adottare un comportamento veritiero e fornire ai rappresentanti incaricati dalla Banca informazioni corrette ed accurate.



Comunicazioni esterne

Tutte le comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico devono contenere informazioni chiare, precise, veritiere e complete.

I “Soggetti” devono astenersi dal diffondere notizie false e tali da poter ingannare il pubblico in ordine alla reale situazione della Banca, così da incidere – nell’interesse o a vantaggio della Società – sull’affidamento che i terzi rivestono nella stabilità della stessa.

Inoltre, sono vietati i comportamenti fraudolenti diretti a danneggiare l’immagine presso il pubblico di una concorrente o ad attuare una ritorsione nei confronti di altro Ente, minandone la credibilità.

E’ politica della Banca diffondere i dati sulla situazione aziendale tramite canali istituzionali con la massima tempestività, avuto riguardo alle esigenze di riservatezza ed evitando divulgazioni di informazioni utili alla concorrenza.

Il rilascio di interviste agli Organi di stampa/mass media è effettuato previa autorizzazione del Presidente del Consiglio di Amministrazione.

Ulteriori condotte vietate

Ai “Soggetti”, in particolare agli Amministratori, è vietato:

- impedire o ostacolare, attraverso occultamenti o altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, alla società di revisione o alle Autorità di Vigilanza;
- diffondere notizie false ovvero porre in essere operazioni simulate o altri artifici tali da provocare una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati;
- determinare o influenzare l’assunzione delle deliberazioni dell’Assemblea dei Soci, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

12. REATI CON FINALITA' EVERSIVE E DI TERRORISMO

La configurazione e la natura delle fattispecie criminose di cui all'art. 25-quater (reati con finalità di terrorismo o di eversione dell'ordine democratico) è tale per cui, ove un reato di quelli previsti sia stato commesso, è probabile che l'operatore abbia agito nell'interesse esclusivo proprio o di terzi; in concreto si può ritenere difficile prefigurare un interesse o anche solo un vantaggio della Banca a seguito della concessione di un finanziamento destinato ad agevolare una attività terroristica o eversiva.

12.1 PRINCIPI GENERALI DI COMPORTAMENTO

La Banca ha adottato le procedure richieste dalle "Istruzioni operative per l'individuazione di operazioni sospette" emanate dalla Banca d'Italia.

La Banca inoltre adotta i seguenti principi:

- qualunque erogazione di fondi presuppone una istruttoria cui partecipano e deliberano soggetti e funzioni diverse all'interno della Banca al fine di minimizzare il rischio di una manipolazione illecita di dati ed aumentare la condivisione delle conoscenze e delle decisioni all'interno della Banca stessa;
- qualunque erogazione di fondi presuppone una approfondita conoscenza della Clientela, ciò consente di valutare la coerenza e la compatibilità dell'operazione con il profilo del Cliente;
- nel caso in cui il Cliente effettui con frequenza operazioni in nome o a favore di terzi che non appaiono giustificate da legami familiari o da rapporti idonei a giustificarle o, nell'ipotesi contraria, in cui vi siano frequenti operazioni effettuate da terzi in nome o a favore di un Cliente, senza plausibili giustificazioni, l'anomalia deve essere evidenziata e sottoposta all'Organismo di Vigilanza della Banca;
- tutte le persone che svolgono attività di istruttoria ed erogazione del credito, a prescindere dal titolo giuridico in base al quale prestano la loro attività lavorativa, sono adeguatamente informate degli obblighi, delle responsabilità personali ed aziendali che possono derivare dal mancato adempimento delle regole e dei presidi posti a prevenzione dei reati di cui all'art. 25-quater del D. Lgs. 231/2001;
- tutte le persone che svolgono attività di istruttoria ed erogazione del credito, a prescindere dal titolo giuridico in base al quale prestano la loro attività lavorativa, ove rilevino, in buona fede, anomalie in operazioni da altri poste in essere, devono immediatamente informare l'Organismo di Vigilanza della Banca.

13. REATI DI ABUSO DI INFORMAZIONI PRIVILEGIATE E DI MANIPOLAZIONE DEL MERCATO

Nel corso del rapporto di collaborazione con la Banca, potrebbe capitare che un “Soggetto” abbia accesso ad informazioni non di dominio pubblico, di carattere confidenziale e/o riservato, aventi ad oggetto le attività della Banca o con questa comunque connesse.

Tutte le informazioni che non sono di dominio pubblico e delle quali si viene in possesso nel contesto di una relazione di affari nella quale la Banca è coinvolta a qualsiasi titolo devono essere ritenute di carattere riservato.

Le informazioni di carattere riservato includono, naturalmente, le informazioni privilegiate, ossia le informazioni specifiche suscettibili, se divulgate, di influenzare sensibilmente il prezzo di mercato di uno strumento finanziario.

In generale vanno considerate riservate le informazioni apprese attraverso fonti alle quali il pubblico non ha accesso.

13.1 PRINCIPI GENERALI DI COMPORTAMENTO

La Banca si è dotata una procedura informatica per facilitare la selezione degli ordini inseriti sia relativamente ai singoli titoli sia relativamente al loro cumularsi nel tempo, enfatizzando l'importanza dell'attività di monitoraggio del market abuse svolta dagli operatori a contatto con la Clientela e/o con le controparti e consentendo un attento e documentato approfondimento di eventuali operazioni suscettibili di diventare oggetto di segnalazione alla CONSOB (“test del ragionevole sospetto”).

La Banca inoltre adotta i seguenti principi:

- non è ammesso l'utilizzo di informazioni riservate in violazione di eventuali obblighi fiduciari, al fine di realizzare un profitto personale (es. tramite negoziazione di strumenti finanziari) o per la Banca.
- non è consentita la divulgazione di informazioni riservate a persone che non siano vincolate da rapporti di collaborazione con la Banca, fatta eccezione per i casi in cui le suddette informazioni siano indispensabili allo svolgimento delle attività per conto della Banca stessa e comunque dopo preventiva autorizzazione del terzo dante causa.
- qualsiasi analisi, studio, relazione ed altro materiale non pubblico realizzato o utilizzato per conto della Banca è, e resta, di proprietà della Banca stessa ; anche dopo la cessazione del rapporto di collaborazione, detto materiale non può essere divulgato o comunicato a terzi senza il consenso della Banca.

14. REATI CONNESSI CON LA VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

La Banca ha adottato tutti gli strumenti e le procedure previste dal D.Lgs. 81/2008 e dalla normativa correlata, sulla base di un'attenta valutazione dei rischi.

La Banca, tramite i propri organi allo scopo identificati, provvede

- al monitoraggio continuo dei rischi;
- all'adeguamento dei presidi posti a tutela dei Dipendenti;
- all'informazione e formazione sia dei propri Dipendenti sia di tutti i soggetti terzi che si trovano ad operare negli ambienti di lavoro della Banca.

Le principali procedure, manuali, specifiche disposizioni interne e informazioni poste a tutela dei Dipendenti sono disponibili nella Intranet Aziendale (sezione "Sicurezza"). Istruzioni circostanziate sono fornite ai Dipendenti tramite corsi di formazione tenuti da personale specializzato esterno.

In particolare, la Banca si è dotata di un "Modello Organizzativo per la sicurezza e la salute dei lavoratori" che definisce la politica per la sicurezza e la salute sul lavoro e descrive dettagliatamente il sistema di gestione della stessa. Tale documento, che nello specifico riporta, tra l'altro, competenze, responsabilità ed iter procedurale:

* è volto ad assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;

* prevede idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al punto precedente;

* prevede, per quanto richiesto dalla natura e dimensioni della Banca e dal tipo di attività svolta, un'articolazione di funzioni che assicura le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il "Modello Organizzativo per la sicurezza e la salute dei lavoratori" è allegato, in quanto ne fa parte integrante, al presente Modello Organizzativo ai sensi del D.Lgs. 231/2001.

15. REATI CONNESSI ALLA RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA E REATI TRANSNAZIONALI

La Banca ha adottato idonei ed appropriati sistemi e procedure in materia di obblighi di adeguata verifica della Clientela, di segnalazione delle operazioni sospette, di conservazione dei documenti, di controllo interno, di valutazione e di gestione del rischio, di garanzia dell'osservanza delle disposizioni pertinenti e di comunicazione per prevenire e impedire la realizzazione di operazioni di riciclaggio o di finanziamento del terrorismo. Particolare attenzione è data alla formazione del personale sia mediante corsi di autoformazione disponibili sulla Intranet Aziendale sia nell'ambito dei corsi in aula.

La Banca adempie a tutti gli obblighi previsti avendo riguardo alle informazioni possedute o acquisite nell'ambito della propria attività istituzionale o professionale. Particolare attenzione viene riservata alle operazioni classificate per contanti, che vengono periodicamente riproposte all'esame dei responsabili delle dipendenze interessate.

La Banca si avvale, ad integrazione dell'attività routinaria di monitoraggio delle operazioni, di una procedura informatica, "Gianos", che rileva ed evidenzia mensilmente eventuali operazioni che risultino, secondo criteri oggettivi, anomale e quindi suscettibili di diventare oggetto di segnalazione come "operazioni sospette".

Inoltre, mediante un apposito pacchetto applicativo "COMMA 3D", la Banca verifica l'identità di coloro i quali si presentano alla sportello per svolgere operazioni comparando il nominativo di tali soggetti con data base aggiornati da fonti di principali enti (Gazzetta ufficiale dell'Unione Europea, OFAC, ABI e liste prodotte da Banca d'Italia, UIF, Ministero dell'Economia e delle Finanze) contenenti un elenco dei terroristi.

Per l'identificazione dei soggetti citati, l'analisi dell'operatività e i principi di comportamento si fa riferimento alle "Istruzioni operative per l'individuazione di operazioni sospette" emanate dalla Banca d'Italia (disponibili sulla Intranet Aziendale).

16. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

Nei reati di violazione del diritto d'autore si configurano tutte le azioni perpetrate con strumenti informatici e non, relative all'acquisizione, alla divulgazione, alla duplicazione e all'utilizzo in genere di "opere dell'ingegno protette" quali, ad esempio, programmi per elaboratore, banche dati, opere, libri e/o dispense.

Vista la tipologia dell'attività svolta dalla Banca, le fattispecie direttamente riferibili alle attività svolte dalla Banca sono la duplicazione, l'utilizzo e la divulgazione di opere su supporto informatico.

16.1 PRINCIPI GENERALI DI COMPORTAMENTO

Il "Documento Programmatico Sicurezza", nonché il "Regolamento interno per l'utilizzo della posta elettronica e della rete internet", adottati dalla Banca ai sensi del D.Lgs. 196/2003 ("Codice in materia di protezione dei dati personali"), disciplinano, tra l'altro, i comportamenti ai quali tutti i Dipendenti della Banca sono tenuti al fine di prevenire i reati della fattispecie, ed i relativi controlli effettuati.

Pur rimandando ai suddetti documenti (pubblicati nella sezione "Sicurezza" della Intranet Aziendale) per una più completa descrizione delle disposizioni emanate, si richiamano i principali adempimenti a titolo di esempio non esaustivo:

- l'installazione di programmi deve essere autorizzata dalla Direzione e deve essere effettuata unicamente dal personale tecnico della Banca;
- non è consentito lo scarico di programmi prelevati da internet, nemmeno qualora trattasi di software gratuiti (freeware) o shareware se non espressamente autorizzati dalla Direzione;
- sui PC della Banca non è consentita l'installazione di apparati di comunicazione propri (ad esempio modem); sui PC della Banca non è consentito l'ascolto di files audio o musicali nonché la visione di video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi;
- tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) devono essere preventivamente opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti;
- le comunicazioni inviate a mezzo posta elettronica verso l'esterno non devono contenere dati riservati o protetti;
- le reti di trasmissione, tra le Dipendenze della Banca o con l'esterno, devono essere dotate delle adeguate protezioni onde evitare la non corretta divulgazione.

17 ALTRI REATI

Gli ulteriori reati previsti dal D. Lgs. 231/2001 e successive modifiche ed integrazioni (reati contro la personalità individuale, pedopornografia, pornografia virtuale, ecc.) non sono trattati nel dettaglio in quanto non riferibili direttamente alle attività caratteristiche svolte dalla Banca.

Ciò nonostante, il processo di erogazione del credito, in considerazione delle modalità operative adottate dai soggetti finanziati e/o dei fornitori nello svolgimento delle loro attività, potrebbe essere potenzialmente collegabile alle fattispecie di reato indicate. In particolare, rilevano le regole comportamentali sul corretto utilizzo degli strumenti informatici messi dalla Banca a disposizione del personale esplicitate in dettaglio nel “Documento Programmatico per la Sicurezza” ed il “Regolamento interno per l’utilizzo della posta elettronica e della rete internet” pubblicati sulla Intranet aziendale; gli strumenti informatici devono essere utilizzati esclusivamente per il miglior svolgimento dell’attività lavorativa e con modalità tali da non arrecare pregiudizio alla Banca ed al suo sistema informatico.

Con riferimento a tali reati trovano in ogni caso applicazione i presidi indicati al capitolo 2 del presente Modello Organizzativo.

18 SISTEMA SANZIONATORIO

18.1 PRINCIPI GENERALI

L'efficacia del Modello è legata anche all'adeguatezza del sistema sanzionatorio previsto in caso di violazione delle regole di condotta e, in generale, delle procedure e dei regolamenti interni.

Le sanzioni saranno commisurate alla gravità dell'infrazione ed all'eventuale reiterazione della stessa; della recidività si terrà conto anche ai fini della comminazione di un'eventuale sanzione espulsiva.

Una inesatta interpretazione dei principi e delle regole stabiliti dal Modello potrà costituire esimente dall'applicazione delle sanzioni in oggetto soltanto nei casi di comportamenti in buona fede.

18.2 MISURE NEI CONFRONTI DEI LAVORATORI SUBORDINATI CUI SI APPLICA IL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO (CCNL) PER IL SETTORE CREDITO

Ai lavoratori subordinati appartenenti alle aree professionali dalla 1^a alla 3^a e ai quadri direttivi si applicano le sanzioni disciplinari previste dal CCNL, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori.

La contestazione delle infrazioni è effettuata, di norma, su segnalazione dell'Organismo di Vigilanza, dopo avere sentito il parere del Responsabile del soggetto che ha commesso il reato; i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano, nei limiti della competenza, nelle attribuzioni dei soggetti ai quali vengono conferiti i relativi poteri dal Consiglio di Amministrazione.

18.3 MISURE NEI CONFRONTI DEI DIRIGENTI

In caso di violazione, da parte di dirigenti, delle procedure previste dal Modello o di tenuta, nello svolgimento di attività sensibili, di una condotta non conforme alle prescrizioni del Modello stesso, la Banca provvede ad applicare nei confronti dei responsabili le misure ritenute più idonee in conformità a quanto previsto dal CCNL, ovvero il licenziamento, con o senza preavviso.

La contestazione delle infrazioni è effettuata, di norma, su segnalazione / proposta dell'Organismo di Vigilanza; i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano, nei limiti della competenza, nelle attribuzioni dei soggetti ai quali vengono dal Consiglio di Amministrazione conferiti i relativi poteri.

18.4 MISURE NEI CONFRONTI DI AMMINISTRATORI, SINDACI ED ALTA DIREZIONE

In caso di violazione delle procedure previste dal Modello o di tenuta, nello svolgimento di attività sensibili, di una condotta non conforme alle prescrizioni del Modello, è prevista una formale informativa da parte dell'Organismo di Vigilanza al Consiglio di Amministrazione e al Collegio Sindacale per l'opportuna valutazione, sulle cui risultanze verrà data informativa allo stesso Organismo di Vigilanza. In caso di inattività del Consiglio di Amministrazione e del Collegio Sindacale, l'Organismo avrà la facoltà di relazionare direttamente l'Assemblea dei Soci.

Per Amministratori e Sindaci, il Consiglio di Amministrazione potrà proporre alla successiva Assemblea dei Soci la revoca per giusta causa.

18.5 MISURE NEI CONFRONTI DI CONSULENTI E FORNITORI

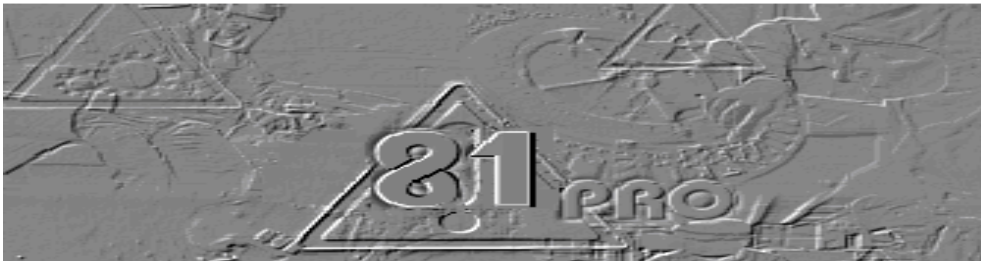
La commissione dei reati di cui al D.Lgs. 231/2001 da parte di Consulenti o di Fornitori, così come ogni violazione da parte degli stessi delle regole di cui al Modello, comporterà, per le funzioni aziendali che con gli stessi intrattengono rapporti, l'obbligo di informare l'Organismo di Vigilanza, che attiverà il Direttore Generale al fine di azionare tutti gli strumenti contrattuali e di legge a disposizione per la tutela dei diritti della Banca, ivi compresi, ove del caso, la risoluzione dei rapporti contrattuali e la richiesta di risarcimento dei danni.





**BANCA PASSADORE & C.
VIA E. VERNAZZA 27
GENOVA**

**MODELLO ORGANIZZATIVO
PER LA SICUREZZA E LA SALUTE
DEI LAVORATORI**



Adempimenti degli obblighi previsti dal D.Lgs. 09 APRILE 2008, N. 81

INDICE

PREMESSA	1
ARTICOLAZIONE DEL TESTO	1
IL RESPONSABILE DEL SISTEMA	1
1. SCOPO E CAMPO DI APPLICAZIONE DEL MODELLO ORGANIZZATIVO PER LA SICUREZZA NEI LUOGHI DI LAVORO	2
1.1 Scopo del Modello Organizzativo per la Sicurezza nei luoghi di lavoro	2
1.2 Campo di applicazione del SGSL	2
2. RIFERIMENTI NORMATIVI	3
3. TERMINI E DEFINIZIONI	4
4. LA POLITICA PER LA SICUREZZA E SALUTE SUL LAVORO	7
4.1 Scopo	7
4.2 Applicabilità	7
4.3 Responsabilità	7
4.4 Azioni e metodi	7
4.4.1 <i>Analisi e avvio</i>	7
4.4.2 <i>Emanazione della politica di SSL</i>	7
4.4.3 <i>Contenuti</i>	7
4.4.4 <i>Riesame della politica di SSL</i>	8
4.4.5 <i>Documentazione, diffusione e disponibilità</i>	8
4.5 Documentazione e registrazioni	8
LA POLITICA PER LA SICUREZZA E SALUTE SUL LAVORO IN BANCA PASSADORE & C.	9
5. PIANIFICAZIONE	10
5.1 Scopo	10
5.2 Applicabilità	10
5.3 Responsabilità	10
5.4 Azioni e metodi	10
5.4.1 <i>Individuazione dei requisiti legali</i>	10
5.4.2 <i>Individuazione dei pericoli per la SSL, valutazione del rischio e controllo del rischio</i>	10
5.4.3 <i>Obiettivi di SSL</i>	11
5.4.4 <i>Documento di Valutazione dei Rischi</i>	12
5.5 Documentazione e registrazioni	15
6. ORGANIZZAZIONE DEL SISTEMA: COMPITI E RESPONSABILITA'	16
6.1 Scopo	16
6.2 Applicabilità	16
6.3 Responsabilità	16
6.4 Azioni e metodi	16
6.5 Documentazione e registrazioni	17
7. GESTIONE DELLE RISORSE STRUMENTALI	18
7.1 Scopo	18
7.2 Applicabilità	18
7.3 Responsabilità	18
7.4 Azioni e metodi	18
7.4.1 <i>Impianti generali a servizio dei luoghi di lavoro</i>	18
7.4.2 <i>Manutenzione e verifiche periodiche</i>	18
7.4.3 <i>Impianti, macchine e attrezzature</i>	19
7.4.4 <i>Impianti e presidi antincendio</i>	22
7.5 Documentazione e registrazioni	22
8. ADOZIONE E GESTIONE DEI DISPOSITIVI DI PROTEZIONE INDIVIDUALE	23
8.1 Scopo	23
8.2 Applicabilità	23
8.3 Responsabilità	23
8.4 Azioni e metodi	23
8.4.1 <i>Scelta dei DPI</i>	23
8.4.2 <i>Acquisto, consegna e gestione dei DPI</i>	24
8.4.3 <i>Uso e conservazione dei DPI</i>	24
8.5 Documentazione e registrazioni	25
9. ORGANIZZAZIONE DEL SISTEMA: COINVOLGIMENTO DEL PERSONALE	26
9.1 Scopo	26
9.2 Applicabilità	26
9.3 Responsabilità	26
9.4 Azioni e metodi	26
9.5 Documentazione e registrazioni	27

10	ORGANIZZAZIONE DEL SISTEMA: INFORMAZIONE, FORMAZIONE, ADDESTRAMENTO, CONSAPEVOLEZZA, SANZIONI	28
	10.1 Scopo	28
	10.2 Applicabilità	28
	10.3 Responsabilità	28
	10.4 Azioni e metodi	28
	10.5 Documentazione e registrazioni	30
11	ORGANIZZAZIONE DEL SISTEMA: COMUNICAZIONE, FLUSSO INFORMATIVO E COOPERAZIONE	31
	11.1 Scopo	31
	11.2 Applicabilità	31
	11.3 Responsabilità	31
	11.4 Azioni e metodi	31
	11.5 Documentazione e registrazioni	32
12	ORGANIZZAZIONE DEL SISTEMA: DOCUMENTAZIONE	33
	12.1 Scopo	33
	12.2 Applicabilità	33
	12.3 Responsabilità	33
	12.4 Azioni e metodi	33
	12.4.1 Documentazione del SGSL	33
	12.4.2 Documentazione di SSL	34
	12.5 Documentazione e registrazioni	34
13	ORGANIZZAZIONE DEL SISTEMA: INTEGRAZIONE NEI PROCESSI AZIENDALI E GESTIONE OPERATIVA	35
	13.1 Scopo	35
	13.2 Applicabilità	35
	13.3 Responsabilità	35
	13.4 Azioni e metodi	35
	13.5 Documentazione e registrazioni	36
14	MONITORAGGIO	37
	14.1 Scopo	37
	14.2 Applicabilità	37
	14.3 Responsabilità	37
	14.4 Azioni e metodi	37
	14.4.1 Monitoraggio di 1° livello	37
	14.4.2 Monitoraggio di 2° livello	37
	14.4.3 Trattamento delle non conformità	37
	14.4.4 Relazione e monitoraggio	38
	14.4.5 Caratteristiche e responsabilità dei verificatori	38
	14.5 Documentazione e registrazioni	38
15	RIESAME DEL SISTEMA	39
	15.1 Scopo	39
	15.2 Applicabilità	39
	15.3 Responsabilità	39
	15.4 Azioni e metodi	39
	15.5 Documentazione e registrazioni	40

PREMESSA

Il D.Lgs. 81/2008 (Testo Unico Sicurezza) ha rivisto l'intero corpus della normativa in materia di Salute e Sicurezza nei luoghi di lavoro, riorganizzando le disposizioni di Legge precedentemente vigenti frammentate in più Decreti o Leggi ed ha, inoltre, rivisto l'art. 25-septies del D.Lgs. 231/2001 sulla "Responsabilità amministrativa degli enti per omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro".

Il presente "**Modello Organizzativo per la Sicurezza dei Lavoratori**" viene redatto al fine di esplicitare la politica della **Banca Passadore & C.** in materia di Salute e Sicurezza dei Lavoratori e la gestione della stessa.

L'art. 30 del D.Lgs. 81/2008 fa riferimento alle "*Linee Guida UNI-INAIL*" quali valido strumento di aiuto nella definizione di un sistema di gestione della sicurezza nei luoghi di lavoro idoneo ad avere efficacia esimente della "Responsabilità amministrativa degli enti" di cui al citato D.Lgs. 231/2001. Dette "*Linee guida UNI-INAIL*" sono state utilizzate come riferimento nella predisposizione del modello organizzativo della Banca.

Il grado di articolazione e complessità di un modello organizzativo, infine, non può prescindere dalla dimensione e dal tipo di azienda che lo adotta. Per questo motivo il modello organizzativo della Banca deriva dalla rielaborazione delle "*Linee guida UNI-INAIL*" adattate alle caratteristiche dimensionali e operative della **Banca Passadore & C.**

ARTICOLAZIONE DEL TESTO

Il "Modello Organizzativo per la Sicurezza dei Lavoratori" presenta 15 capitoli tutti strutturati, ad eccezione dei primi 3, in modo analogo: Scopo, Applicabilità, Responsabilità, Azioni e metodi, Documentazione e registrazioni.

Nel paragrafo "Scopo" viene data un'indicazione di massima della funzione rivestita dal capitolo, ovvero dal suo oggetto, nell'ambito del sistema di gestione della sicurezza nei luoghi di lavoro. In parte vengono ripresi gli argomenti presenti nelle Linee Guida UNI-INAIL, rendendo più "operativa" la formulazione dei principi in queste contenuti.

Nel paragrafo "Applicabilità" sono di volta in volta indicati gli ambiti di applicazione dell'argomento trattato.

Nel paragrafo "Responsabilità" sono indicati i soggetti chiamati in causa nel seguito del capitolo in quanto destinatari di precisi obblighi all'interno del sistema.

Di norma, i soggetti citati in questo paragrafo hanno precisi compiti e responsabilità nel realizzare ed applicare il sistema indipendentemente da responsabilità in materia di sicurezza che le norme vigenti attribuiscono loro.

Nel paragrafo "Azioni e metodi" vengono descritte, in modo esauriente, le attività che i soggetti individuati devono svolgere per dare attuazione concreta a quanto disposto. A seconda della complessità dell'argomento i paragrafi possono essere più o meno esauritivi e, in alcuni casi, gli aspetti esecutivi specifici sono demandati a istruzioni operative non presenti nel modello organizzativo.

Nel paragrafo "Documentazione e registrazioni" sono identificati i documenti che originano dalla applicazione di quanto contenuto nel capitolo o le documentazioni previste dalle norme vigenti.

Per alcuni documenti sono previsti aggiornamenti periodici; sarà cura del "Responsabile del sistema" gestirne l'archiviazione.

Occorre precisare che, tranne per alcuni limitati casi, nelle norme vigenti in materia di sicurezza sul lavoro non sono reperibili indicazioni sulla durata di conservazione della documentazione. È quindi una scelta del realizzatore del sistema la definizione del periodo di conservazione della documentazione, fatta salva la necessità di poter dimostrare in ogni momento l'avvenuto rispetto degli obblighi di legge.

IL RESPONSABILE DEL SISTEMA

La realizzazione del sistema di gestione richiede che il datore di lavoro individui un soggetto cui affidare il compito di assicurare che il sistema di gestione sia realizzato e mantenuto in funzione efficacemente.

Il "Responsabile del sistema" (RSGSL) per la **Banca Passadore & C.** viene identificato nel RSPP.

1. SCOPO E CAMPO DI APPLICAZIONE DEL MODELLO ORGANIZZATIVO PER LA SICUREZZA NEI LUOGHI DI LAVORO

1.1 *Scopo del Modello Organizzativo per la Sicurezza nei luoghi di lavoro*

La gestione della salute e della sicurezza sul lavoro costituisce parte integrante della gestione generale della Banca. La **Banca Passadore & C.** intende volontariamente adottare un sistema di gestione della salute e sicurezza sul lavoro (in seguito denominato SGSL) che integri obiettivi e politiche per la salute e sicurezza nella progettazione e gestione di sistemi di lavoro e di produzione.

Adottando questo SGSL la Banca si propone di:

- ridurre progressivamente i costi complessivi della SSL compresi quelli derivanti da incidenti, infortuni e malattie correlate al lavoro minimizzando i rischi cui possono essere esposti i dipendenti o i terzi (clienti, fornitori, visitatori, ecc.);
- aumentare la propria efficienza e le proprie prestazioni;
- contribuire a migliorare i livelli di salute e sicurezza sul lavoro;
- migliorare la propria immagine interna ed esterna.

Il SGSL definisce le modalità per individuare, all'interno della struttura organizzativa aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme di salute e sicurezza vigenti.

Fermo restando il rispetto delle norme di legge, il SGSL che la Banca adotta:

- prevede il monitoraggio effettuato prevalentemente con personale interno;
- non è soggetto a certificazione da parte terza;
- consente l'adattamento all'evoluzione di leggi, regolamenti e norme di buona tecnica;
- coinvolge i lavoratori e i loro rappresentanti.

1.2 *Campo di applicazione del SGSL*

Il SGSL si applica alle attività svolte dalla Banca presso tutte le proprie Dipendenze.

E' disegnato secondo le peculiarità della Banca, comprendenti la sua articolazione organizzativa e funzionale nonché la distribuzione o dislocazione sul territorio.

2. RIFERIMENTI NORMATIVI

La predisposizione del sistema di gestione salute e sicurezza (SGSL) è stata attuata secondo le indicazioni riportate nelle *“Linee Guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL)”* UNI-INAIL.

3. TERMINI E DEFINIZIONI

Nell'ambito del presente modello organizzativo vengono utilizzati i termini e le definizioni contenuti nella normativa di legge o tecnica in vigore, che si riportano per agevolare la consultazione del documento:

- **Addestramento:** complesso delle attività dirette a fare apprendere ai lavoratori l'uso corretto di attrezzature, macchine, impianti, sostanze, dispositivi, anche di protezione individuale, e le procedure di lavoro. (D.Lgs. 81/2008, art. 2, comma 1, lettera cc)
- **Addetto al Servizio di Prevenzione e Protezione (ASPP):** persona facente parte del Servizio di Prevenzione e Protezione in possesso delle opportune capacità e requisiti professionali. (D.Lgs. 81/2008, art. 2, comma 1, lettera g)
- **Appaltatore:** è il soggetto che si obbliga nei confronti del committente a fornire un'opera e/o una prestazione con mezzi propri.
- **Attrezzatura di lavoro:** qualsiasi macchina, apparecchio, utensile od impianto destinato ad essere usato durante il lavoro. (D.Lgs. 81/2008, art. 69)
- **Datore di lavoro (DdL):** il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa. Nelle pubbliche amministrazioni di cui all'articolo 1, comma 2, del D.Lgs. 165/2001, per datore di lavoro si intende il dirigente al quale spettano i poteri di gestione, ovvero il funzionario non avente qualifica dirigenziale, nei soli casi in cui quest'ultimo sia preposto ad un ufficio avente autonomia gestionale, individuato dall'organo di vertice delle singole amministrazioni tenendo conto dell'ubicazione e dell'ambito funzionale degli uffici nei quali viene svolta l'attività, e dotato di autonomi poteri decisionali e di spesa. In caso di omessa individuazione, o di individuazione non conforme ai criteri sopra indicati, il datore di lavoro coincide con l'organo di vertice medesimo. (D.Lgs. 81/2008, art. 2, comma 1, lettera b)
- **Dirigente:** persona che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa. (D.Lgs. 81/2008, art. 2, comma 1, lettera d)
- **Dispositivi di Protezione Individuale (DPI):** attrezzatura destinata ad essere indossata e tenuta dal lavoratore allo scopo di proteggerlo contro uno o più rischi suscettibili di minacciarne la sicurezza o la salute durante il lavoro, nonché ogni complemento o accessorio destinato a tale scopo. (D.Lgs. 81/2008, art. 74, comma 1)
- **Fabbricante:** soggetto che produce e immette sul mercato o in servizio macchine, apparecchiature, impianti, dispositivi. (D.P.R. 459/1996) Il fabbricante può essere sia interno che esterno all'organizzazione.
- **Formazione:** processo educativo attraverso il quale trasferire ai lavoratori ed agli altri soggetti del sistema di prevenzione e protezione aziendale conoscenze e procedure utili all'acquisizione di competenze per lo svolgimento in sicurezza dei rispettivi compiti in azienda e all'identificazione, alla riduzione e alla gestione dei rischi. (D.Lgs. 81/2008, art. 2, comma 1, lettera aa)
- **Incidente:** evento dovuto a causa fortuita che ha la potenzialità di condurre ad un infortunio o di provocare danni alle cose.
- **Informazione:** complesso delle attività dirette a fornire conoscenze utili all'identificazione, alla riduzione e alla gestione dei rischi in ambiente di lavoro. (D.Lgs. 81/2008, art. 2, comma 1, lettera bb)
- **Infortunio:** evento dovuto a causa fortuita che produca lesioni corporali obiettivamente riscontrabili, in occasione di lavoro.
- **Lavoratore:** persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore così definito è equiparato: il socio lavoratore di cooperativa o di società, anche di fatto, che presta la sua attività per conto delle società e dell'ente stesso; l'associato

in partecipazione di cui all'articolo 2549, e seguenti del Codice Civile; il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento di cui all'articolo 18 della Legge 196/1997, e di cui a specifiche disposizioni delle leggi regionali promosse al fine di realizzare momenti di alternanza tra studio e lavoro o di agevolare le scelte professionali mediante la conoscenza diretta del mondo del lavoro; l'allievo degli istituti di istruzione ed universitari e il partecipante ai corsi di formazione professionale nei quali si faccia uso di laboratori, attrezzature di lavoro in genere, agenti chimici, fisici e biologici, ivi comprese le apparecchiature fornite di videoterminali limitatamente ai periodi in cui l'allievo sia effettivamente applicato alla strumentazioni o ai laboratori in questione; il volontario, come definito dalla Legge 266/1991; i volontari del Corpo Nazionale dei Vigili del Fuoco e della Protezione Civile; il volontario che effettua il servizio civile; il lavoratore di cui al D.Lgs. 468/1997, e successive modificazioni. (D.Lgs. 81/2008, art. 2, comma 1, lettera a)

- **Linee guida:** atti di indirizzo e coordinamento per l'applicazione della normativa in materia di salute e sicurezza predisposti dai Ministeri, dalle regioni, dall'ISPESL e dall'INAIL e approvati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. (D.Lgs. 81/2008, art. 2, comma 1, lettera z)
- **Luogo di lavoro:** i luoghi destinati a contenere posti di lavoro, ubicati all'interno dell'azienda ovvero dell'unità produttiva, nonché ogni altro luogo nell'area della medesima azienda ovvero unità produttiva comunque accessibile per il lavoro.
- **Malattia professionale:** evento morboso contratto a causa e nell'esercizio delle lavorazioni svolte.
- **Medico competente (MC):** medico in possesso di uno dei seguenti titoli:
 1. specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica o in tossicologia industriale o in igiene industriale o in fisiologia ed igiene del lavoro o in clinica del lavoro o in igiene e medicina preventiva o in medicina legale e delle assicurazioni ed altre specializzazioni individuate, ove necessario, con decreto del Ministro della sanità di concerto con il Ministro dell'università e della ricerca scientifica e tecnologica;
 2. docenza o libera docenza in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica o in tossicologia industriale o in igiene industriale o in fisiologia ed igiene del lavoro;
 3. autorizzazione di cui all'art. 55 del decreto legislativo 15 agosto 1991, n. 277. (D.Lgs. 81/2008, art. 2, comma 1, lettera h)
- **Modello di organizzazione e di gestione:** modello organizzativo e gestionale per la definizione e l'attuazione di una politica aziendale per la salute e sicurezza, ai sensi dell'articolo 6, comma 1, lettera a), del D.Lgs. 231/2001, idoneo a prevenire i reati di cui agli articoli 589 e 590, terzo comma, del Codice Penale, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro. (D.Lgs. 81/2008, art. 2, comma 1, lettera dd)
- **Non conformità (n.c.):** difformità dagli standard adottati o mancato rispetto dei requisiti legali, dei regolamenti, delle pratiche, delle procedure, delle istruzioni operative, dello schema di sistema di gestione adottato.
- **Norma tecnica:** specifica tecnica, approvata e pubblicata da un'organizzazione internazionale, da un organismo europeo o da un organismo nazionale di normalizzazione, la cui osservanza non sia obbligatoria. (D.Lgs. 81/2008, art. 2, comma 1, lettera u)
- **Obiettivi:** risultati, in termini di prestazioni di SSL, che una organizzazione stabilisce di raggiungere.
- **Pericolo:** proprietà o qualità intrinseca di un determinato fattore avente il potenziale di causare danni. (D.Lgs. 81/2008, art. 2, comma 1, lettera r)
- **Posto di lavoro:** postazioni, fisse o variabili, in cui il lavoratore espleta la sua mansione.
- **Preposto:** persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa. (D.Lgs. 81/2008, art. 2, comma 1, lettera e)

- **Prevenzione:** il complesso delle disposizioni o misure necessarie anche secondo la particolarità del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno. (D.Lgs. 81/2008, art. 2, comma 1, lettera n)
- **Rappresentante dei lavoratori per la sicurezza (RLS):** persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro. (D.Lgs. 81/2008, art. 2, comma 1, lettera i)
- **Requisiti legali:** norme di legge e/o regolamenti di livello comunitario, statale, locale, ed ogni impegno assunto volontariamente applicabile all'organizzazione in materia di SSL.
- **Responsabile del servizio di prevenzione e protezione (RSPP):** persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del D.Lgs. 81/2008 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi. (D.Lgs. 81/2008, art. 2, comma 1, lettera f)
- **Responsabile del SGSL (RSGSL):** soggetto incaricato dal DdL, dotato di adeguata capacità ed autorità all'interno dell'azienda, a cui è affidato in tutto o in parte il compito, indipendentemente da ulteriori responsabilità aziendali, di coordinare e verificare che il SGSL sia realizzato in conformità alle Linee Guida UNI-INAIL.
- **Rischio:** probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione. (D.Lgs. 81/2008, art. 2, comma 1, lettera s)
- **Salute:** stato di completo benessere fisico, mentale e sociale, non consistente solo in un'assenza di malattia o d'infermità. (D.Lgs. 81/2008, art. 2, comma 1, lettera o)
- **Servizio di prevenzione e protezione dai rischi (SPP):** insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali nell'azienda, ovvero unità produttiva. (D.Lgs. 81/2008, art. 2, comma 1, lettera l)
- **SGSL:** Sistema di Gestione della Salute e Sicurezza sul Lavoro.
- **Sistema di promozione della salute e sicurezza:** complesso dei soggetti istituzionali che concorrono, con la partecipazione delle parti sociali, alla realizzazione dei programmi di intervento finalizzati a migliorare le condizioni di salute e sicurezza dei lavoratori. (D.Lgs. 81/2008, art. 2, comma 1, lettera p)
- **Sorveglianza sanitaria:** insieme degli atti medici, finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori, in relazione all'ambiente di lavoro, ai fattori di rischio professionali e alle modalità di svolgimento dell'attività lavorativa. (D.Lgs. 81/2008, art. 2, comma 1, lettera m)
- **SSL:** Sicurezza e Salute dei Lavoratori.
- **Terzi:** soggetti diversi dal datore di lavoro, dai Dirigenti, dai Preposti e dai lavoratori, che possono, a qualsiasi titolo, trovarsi all'interno dei luoghi di lavoro o che possono essere influenzati o influenzare le attività lavorative e/o le condizioni di prevenzione.
- **Unità produttiva:** stabilimento o struttura finalizzati alla produzione di beni o all'erogazione di servizi, dotati di autonomia finanziaria e tecnico funzionale. (D.Lgs. 81/2008, art. 2, comma 1, lettera t)
- **Valutazione del rischio (VDR):** valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione in cui essi prestano la propria attività, finalizzata ad individuare le adeguate misure di prevenzione e di protezione e ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza. (D.Lgs. 81/2008, art. 2, comma 1, lettera q)

Termini di uso specialistico possono essere utilizzati e definiti in singole parti del SGSL.

4. LA POLITICA PER LA SICUREZZA E SALUTE SUL LAVORO

4.1 Scopo

La politica di SSL costituisce un riferimento fondamentale ed essenziale per tutti i partecipanti alla vita aziendale e per tutti coloro che, esterni alla Banca, hanno con essa rapporti. Essa deve far comprendere, declinando anche gli obiettivi strategici, i principi cui si ispira ogni azione aziendale, nell'ottica della salute e sicurezza e benessere di tutti i partecipanti alla vita aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte presso la Banca. Il documento di politica indica in sostanza quale "missione" si è data la Banca in tema di SSL, esprimendo le motivazioni che stanno alla base, la ferma volontà della Direzione della Banca a perseguire gli obiettivi posti, la consapevolezza dei risultati auspicati cui tendere, le responsabilità da assumere. La politica è la "carta" fondamentale della Banca in tema di SSL.

4.2 Applicabilità

La politica di SSL si applica a tutte le attività svolte dall'azienda e descritte nei capitoli "Scopo e campo di applicazione del SGSL".

4.3 Responsabilità

Il DdL è responsabile dei contenuti della politica di SSL, della sua emanazione, attuazione e aggiornamento.

4.4 Azioni e metodi

4.4.1 Analisi e avvio

Per consentire una prima definizione della politica, il DdL o una figura da questi incaricata, dopo aver coinvolto le parti interessate e i RRLLS, effettua una analisi di SSL preliminare per evidenziare i punti focali dell'organizzazione in relazione alla sicurezza e salute sul lavoro.

L'analisi è effettuata mediante colloqui/interviste con le funzioni aziendali interessate, mediante ispezioni, misurazioni, ecc., e prende in considerazione:

- la storia dell'insediamento;
- l'organizzazione aziendale;
- gli aspetti di SSL che possono avere impatti significativi;
- le prescrizioni legislative e regolamentari applicabili;
- le prestazioni di SSL in relazione a tali prescrizioni;
- gli incidenti e le malattie professionali verificatesi in precedenza.

L'analisi di avvio tiene conto dei risultati della valutazione del rischio.

4.4.2 Emanazione della politica di SSL

Il DdL, tenendo conto:

- della natura e del livello dei rischi presenti,
 - della tipologia dei contratti di lavoro,
 - dei risultati dell'analisi iniziale o del monitoraggio successivo,
- elabora la politica di SSL della Banca.

4.4.3 Contenuti

La politica di SSL comprende:

- l'impegno al rispetto della legislazione e degli accordi applicabili alla SSL (in quanto presupposto fondamentale alla applicabilità di un sistema di gestione);
- l'affermazione che la responsabilità nella gestione della SSL riguarda l'intera organizzazione aziendale, dal datore di lavoro sino ad ogni lavoratore, ciascuno secondo le proprie attribuzioni e competenze (per evitare che la prevenzione sia considerata competenza esclusiva di alcuni soggetti con conseguente deresponsabilizzazione degli altri e mancanza di partecipazione attiva);

- l'impegno a considerare la SSL ed i relativi risultati come parte integrante della gestione aziendale (considerando quindi un risultato di SSL gratificante ed importante quanto un risultato di produzione o di qualità);
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a far sì che i lavoratori siano sensibilizzati e formati per svolgere i loro compiti in sicurezza e per assumere le loro responsabilità in materia di SSL;
- l'impegno al coinvolgimento ed alla consultazione dei lavoratori, anche attraverso i loro rappresentanti per la sicurezza;
- l'impegno a riesaminare periodicamente la politica stessa ed il sistema di gestione attuato;
- l'impegno a definire e diffondere all'interno dell'azienda gli obiettivi di SSL e i relativi programmi di attuazione.

I punti sopraindicati costituiscono anche il quadro di riferimento per stabilire e riesaminare obiettivi e traguardi di SSL.

4.4.4 Riesame della politica di SSL

La politica di SSL è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame può inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.

Il riesame non comporta necessariamente la modifica della politica.

4.4.5 Documentazione, diffusione e disponibilità

La politica di SSL emessa dal DdL viene illustrata e diffusa a tutto il personale.

Ogni qualvolta avviene una modifica della politica di SSL, si provvede all'aggiornamento e alla divulgazione del presente documento.

4.5 Documentazione e registrazioni

I documenti sono conservati dal RSGSL.

**LA POLITICA PER LA SICUREZZA E SALUTE SUL LAVORO
IN
BANCA PASSADORE & C.**

La Direzione della **Banca Passadore & C.** si impegna, mettendo a disposizione risorse umane, strumentali, ed economiche, a perseguire gli obiettivi di miglioramento della sicurezza e salute dei lavoratori, come parte integrante della propria attività e come impegno strategico rispetto alle finalità più generali della Banca.

Rende noto questo documento e lo diffonde a tutti i soggetti della Banca stessa e si impegna affinché:

1. fin dalla fase di definizione di nuove attività, o nella revisione di quelle esistenti, gli aspetti della sicurezza siano considerati contenuti essenziali;
2. tutti i lavoratori siano formati, informati e sensibilizzati per svolgere i loro compiti in sicurezza e per assumere le loro responsabilità in materia di SSL;
3. tutta la struttura aziendale (Dirigenti, Preposti, Lavoratori, ecc.) partecipi, secondo le proprie attribuzioni e competenze, al raggiungimento degli obiettivi di sicurezza assegnati affinché:
 - la progettazione dei luoghi di lavoro, gli impianti e le attrezzature, le macchine, i metodi operativi e gli aspetti organizzativi siano realizzati in modo da salvaguardare la salute dei lavoratori, i beni aziendali, i terzi e la comunità in cui la Banca opera;
 - l'informazione sui rischi aziendali sia diffusa a tutti i lavoratori; la formazione degli stessi sia effettuata ed aggiornata con specifico riferimento alla mansione svolta;
 - si faccia fronte con rapidità, efficacia e diligenza a necessità emergenti nel corso delle attività lavorative;
 - siano promosse la cooperazione fra le varie risorse aziendali, la collaborazione con le organizzazioni imprenditoriali e con enti esterni preposti;
 - siano rispettate tutte le leggi e regolamenti vigenti, formulate procedure e ci si attenga agli standard aziendali individuati;
 - siano gestite le proprie attività anche con l'obiettivo di prevenire incidenti, infortuni e malattie professionali. Siano indirizzate a tale scopo la progettazione, la conduzione e la manutenzione, ivi comprese le operazioni di pulizia dei luoghi di lavoro, macchine e impianti.

5. PIANIFICAZIONE

5.1 Scopo

Al fine di dare concreta attuazione alla politica di SSL ogni attività aziendale è analizzata, tenendo conto di tutte le possibili condizioni, e vengono definiti degli obiettivi coerenti con la politica di SSL, all'interno di uno specifico piano nell'ambito del SGSL. Per ogni obiettivo sono definite le azioni necessarie al raggiungimento, le responsabilità, le risorse ed i metodi per misurarne il raggiungimento.

La pianificazione costituisce uno dei cardini fondamentali del sistema. Essa consente inoltre di avere esatta conoscenza dei compiti che sono affidati a ciascuno e delle relative responsabilità.

Primi elementi considerati nella pianificazione delle attività per la SSL sono l'individuazione dei requisiti legali cui la Banca deve attenersi e l'individuazione dei pericoli per la SSL, la valutazione del rischio ed il controllo del rischio.

5.2 Applicabilità

Si applica a tutte le attività svolte dalla Banca e descritte nel capitolo "Scopo e campo di applicazione del SGSL".

5.3 Responsabilità

DdL, RSPP, RSGSL, MC, Responsabili dei Servizi.

5.4 Azioni e metodi

5.4.1 Individuazione dei requisiti legali

Preliminarmente alla definizione degli obiettivi specifici di SSL occorre identificare i requisiti in materia di SSL derivanti da leggi e regolamenti comunitari, nazionali, regionali e locali e da ogni altro eventuale accordo, prescrizione, o simile sottoscritto dalla Banca applicabili alle attività e ai prodotti/servizi svolti.

Allo scopo il RSPP:

- analizza tutti gli argomenti normati in materia di sicurezza e salute, utilizzando anche dati esistenti, documenti di associazioni imprenditoriali, sindacali, bibliografie, testi, ecc.;
- sulla base della conoscenza degli elementi delle attività/servizi dell'organizzazione, individua le leggi/norme che interessano la Banca;
- reperisce i testi di tali norme;
- per identificare eventuali altre prescrizioni o accordi volontari sottoscritti dalla Banca, effettua interviste con il DdL;
- per garantire gli aggiornamenti normativi, si mantiene aggiornato ed esamina le informazioni pervenute da associazioni imprenditoriali, sindacali e dalla stampa specializzata;
- procede quindi all'individuazione dei requisiti e degli adempimenti derivanti dal rispetto di tali norme legali e accordi volontari specificamente applicabili all'attività svolta dall'organizzazione, nonché alla relativa valutazione di conformità.

La modifica normativa comporta il riesame e, se necessario, la modifica dei requisiti applicabili.

La modifica di prodotto e/o di processo comporta l'esame di conformità rispetto ai requisiti applicabili nonché l'individuazione/ricerca di altre eventuali norme che diventano applicabili, con la conseguente definizione di requisiti ulteriori.

5.4.2 Individuazione dei pericoli per la SSL, valutazione del rischio e controllo del rischio

Tutte le attività svolte all'interno dei locali della Banca, nonché le attività svolte da terzi all'interno dei locali stessi e che possono interferire con le proprie attività (appaltatori)

sono analizzate per individuare i pericoli presenti nonché gli aspetti organizzativi ed operativi che possono influire significativamente sulla SSL (in modo reale o potenziale).

L'analisi è coordinata dal RSPP, in collaborazione con tutta la struttura aziendale (Dirigenti, Preposti, lavoratori), con il MC e con le imprese esterne operanti all'interno dei locali della Banca.

La valutazione del rischio è preceduta dalla consultazione, da parte del DdL o di soggetto da questi delegato, dei RRLLS, come previsto dal D.Lgs. 81/2008.

I processi lavorativi vengono scomposti in fasi elementari, vengono individuate le fonti e le situazioni pericolose e valutati i rischi.

Si considerano anche le attività saltuarie svolte presso la Banca.

Nella analisi e valutazione si tiene conto anche delle materie utilizzate, delle risorse energetiche, dei tipi di imballo, dei rifiuti prodotti.

Stima del rischio

L'individuazione e quantificazione dei pericoli e valutazione dei rischi sul lavoro per stimare i rischi viene effettuata tenendo in conto:

- la gravità del danno potenziale;
- la frequenza di manifestazione del pericolo, ovvero la durata della esposizione;
- la presenza ed efficacia delle misure di prevenzione (collettive e individuali, di tipo tecnico, organizzativo, procedurale);
- l'addestramento lavorativo impartito (considerando anche i lavoratori interinali, le attività temporanee o in appalto, ecc.);
- la formazione alla sicurezza impartita;
- l'esperienza aziendale sulla manifestazione del singolo rischio;
- la novità della attività in esame (ogni volta che si introduce o si modifica un rischio viene valutata l'interazione con l'ambiente di lavoro);
- l'individuazione, se pertinente, delle quantità/concentrazioni degli inquinanti;
- la coerenza delle procedure lavorative con gli obiettivi di prevenzione.

Aggiornamenti/modifiche

Il riesame e l'eventuale aggiornamento della valutazione dei rischi viene effettuato annualmente e a seguito di possibili eventi o situazioni che lo rendano necessario.

In particolare la valutazione è aggiornata in conseguenza a:

- modifica legislativa o regolamentare o di accordi volontari;
- modifica degli elementi dell'attività svolta e/o dei prodotti/servizi;
- risultati degli audit ed, eventualmente, modifica della politica.

L'aggiornamento della valutazione dei rischi comporta la consultazione preventiva degli RRLLS.

Per l'aggiornamento o modifica della valutazione del rischio si applica la presente sezione del modello organizzativo.

I pericoli significativi e i valori attribuiti ai rischi rilevati compongono, insieme ai criteri adottati ed al programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, il "Documento di Valutazione dei Rischi" previsto all'art. 17, comma 1, lettera a) del D.Lgs. 81/2008.

La valutazione del rischio costituisce uno degli elementi fondamentali da prendere in considerazione per determinare gli obiettivi di SSL.

5.4.3 Obiettivi di SSL

Gli obiettivi di SSL relativi alle attività/servizi della Banca costituiscono i traguardi che la Banca si pone, in coerenza con la politica di SSL emanata.

Gli obiettivi di SSL sono stabiliti dal DdL su proposta del RSPP, e sono sottoposti a monitoraggio ed a riesame periodico.

Definizione degli obiettivi

Il RSPP individua gli aspetti significativi dal punto di vista del rischio per la SSL, quantifica i dati misurabili, valuta la conformità nei confronti delle norme di legge e di eventuali accordi volontari, evidenzia quegli aspetti che, pur non producendo rischi non tollerabili, possono comportare responsabilità di tipo penale o amministrativo.

Sulla base di queste analisi, il RSPP propone obiettivi di SSL coerenti con la politica aziendale e finalizzati a prevenire, ridurre o eliminare i rischi significativi.

Per ciascun obiettivo proposto è presentato un piano per il raggiungimento dello stesso contenente:

- eventuali mete intermedie,
- individuazione delle figure/strutture coinvolte nella realizzazione del piano stesso,
- attribuzione dei compiti e delle responsabilità relative,
- definizione delle risorse necessarie, comprese quelle economiche,
- modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi,

affinché ciascuno, in base alle proprie competenze, li analizzi dal punto di vista economico/finanziario, commerciale, produttivo/tecnologico (come impiantistica e come effetti sulle attività/servizi).

Il DdL, dopo aver consultato i RRLS, stabilisce infine gli obiettivi e i traguardi da raggiungere.

Per ogni obiettivo o traguardo stabilito, sono individuati uno o più indicatori di prestazione di SSL, ad esempio:

- numero di infortuni,
- numero di incidenti,
- livelli di rischio residuo,
- livelli di esposizione degli addetti,
- percentuale di riscontri positivi ai controlli,
- ecc.

Tali indicatori sono, se possibile, rapportati ai livelli di attività.

Il raggiungimento degli obiettivi è tenuto sotto controllo attraverso il monitoraggio del programma SSL conseguente e degli indicatori di prestazione e tramite il riesame annuale della direzione.

Riesame

Il riesame e la definizione di nuovi obiettivi o la loro modifica avviene annualmente preferibilmente in occasione della verifica gestionale o della formulazione del bilancio aziendale, nonché a seguito di possibili eventi o situazioni che lo rendano necessario, ed in particolare a seguito di:

- controllo di avanzamento dei programmi di SSL;
- attività di sorveglianza e misurazione degli indicatori di prestazione;
- variazioni dell'organizzazione e delle attività lavorative;
- cause esterne non prevedibili (cambiamento della legislazione, richieste commerciali, richieste di parti interessate, ecc.).

In tutti i casi sopraindicati il RSGSL segue l'iter previsto dalla sezione specifica e dalla presente sezione del modello organizzativo.

5.4.4 Documento di Valutazione dei Rischi

A seguito della valutazione dei rischi viene redatto il "Documento di Valutazione dei Rischi", sottoscritto da DdL, RSPP e, per presa visione, da MC e RRLS, che contiene in dettaglio il metodo per mezzo del quale è stata effettuata la valutazione stessa nonché i valori di rischio e gli eventuali interventi da mettere in atto per la mitigazione del rischio stesso.

Tale documento è oggetto di aggiornamento e revisione secondo le modalità indicate nel precedente paragrafo.

Valutazioni specifiche

A integrazione del "Documento di Valutazione dei Rischi", in ottemperanza a quanto disposto dalla normativa vigente, sono previste le seguenti valutazioni su rischi specifici

per i quali può essere prevista la redazione di specifici documenti che costituiscono, pertanto, parte integrante del "Documento di Valutazione dei Rischi" principale:

5.4.4.1 Valutazione del rischio chimico

Nella valutazione dei rischi, la Banca effettua la valutazione dei rischi per la sicurezza e la salute dei lavoratori derivanti dalla presenza di agenti chimici. La valutazione del rischio è relativa ai prodotti e/o sostanze ed alle attività che ne presuppongono l'impiego da parte del personale addetto.

5.4.4.2 Valutazione del rischio rumore

La Banca, nell'ambito della valutazione dei rischi per la salute legati alle attività svolte dal proprio personale, valuta l'esposizione degli stessi al rumore generato dall'uso delle macchine/attrezzature e dall'effettuazione delle attività previste dalla mansione in generale, nel rispetto della normativa specifica vigente e secondo le indicazioni delle linee guida disponibili.

La valutazione deve essere realizzata da personale competente, sotto la responsabilità del DdL.

Le modalità di effettuazione della valutazione del rischio, le caratteristiche della strumentazione impiegata, il suo esito, l'indicazione degli obblighi a carico del DdL, le misure da attuare sono riportati all'interno di uno specifico "Rapporto di valutazione del rischio rumore".

Tale rapporto sarà oggetto ad aggiornamenti ogniqualvolta si verificano cambiamenti in merito a:

- tipologia di attività svolte,
- macchine/attrezzature in uso da parte degli operatori,
- tempi di utilizzo macchine/attrezzature o comunque di esposizione alle fonti di rumore e, comunque, secondo quanto previsto da norme e linee guida vigenti.

5.4.4.3 Valutazione del rischio incendio

La valutazione del rischio incendio degli ambienti di lavoro è prevista come parte integrante del "Documento di Valutazione dei Rischi" ed è oggetto di aggiornamento ogniqualvolta risulti necessario a fronte di significative variazioni in particolare di: quantità e tipologia di materiale combustibile presente e depositato, rilevanti modifiche dell'attività e dell'assetto e/o dell'organizzazione aziendale.

La valutazione del rischio incendio è effettuata come indicato di seguito.

Metodologia per la valutazione

La metodologia per la valutazione del rischio incendio, sulla base di quanto indicato dalla normativa vigente è basata sulle seguenti fasi:

- fase preliminare: raccolta dati ed informazioni in particolare sulle caratteristiche dell'attività svolta e degli ambienti lavorativi (caratteristiche struttura, impianti, materiali combustibili, verifica iter autorizzativi, raccolta documentazione, ecc.);
- individuazione di ogni pericolo di incendio (presenza materiali combustibili, infiammabili, sorgenti di innesco, ecc.);
- individuazione dell'eventuale presenza di persone soggette a particolari rischi (persone disabili, visitatori, clienti, terzi, ecc.);
- modalità di eliminazione o riduzione di tali pericoli (rimozione/separazione materiali e prodotti combustibili e/o infiammabili rispetto a possibili sorgenti di innesco, verifica idoneità attrezzature antincendio, adozione di procedure di sicurezza, adozione di procedure di coordinamento con ditte esterne, ecc.);
- valutazione e classificazione del rischio residuo, secondo le modalità definite dalla normativa vigente;
- verifica dell'adeguatezza delle misure di sicurezza esistenti e dell'eventuale necessità di integrazione delle stesse. Le misure possono essere di tipo tecnico, legate alle caratteristiche ed all'idoneità degli impianti installati, o legate ad aspetti quali le vie di esodo (verifica dell'adeguatezza e della sicura percorribilità in condizioni di emergenze), i mezzi e le dotazioni

antincendio a disposizione (estintori, impianti di rilevazione fumo, pulsanti di allarme, ecc.) e l'organizzazione interna.

Per quanto riguarda:

- le dotazioni di sicurezza presenti negli ambienti di lavoro atte a fronteggiare un incendio,
- le modalità di verifica periodica e dei controlli dei presidi antincendio,
- la descrizione delle vie di esodo a disposizione del personale e di quanti si trovano negli ambienti di lavoro,
- l'organizzazione aziendale atta a fronteggiare l'insorgenza di incendi e, in generale, situazioni di emergenza,
- le procedure predisposte dalla Banca per fronteggiare situazioni di emergenza,
- le attività di informazione, formazione e addestramento previste per i componenti della squadra di emergenza e di tutto il personale;

fare riferimento a:

- "Documento di Valutazione dei Rischi",
- "Piano di emergenza ed evacuazione".

5.4.4.4 Valutazione del rischio vibrazioni

Il DdL deve effettuare un'identificazione preliminare del livello di esposizione dei propri lavoratori alle vibrazioni e, in funzione di questo, valutare se necessario effettuare specifiche misurazioni in conformità agli standard tecnici riportati nella normativa vigente.

In particolare le vibrazioni meccaniche cui possono essere esposti i lavoratori nel corso dello svolgimento della propria mansione, sono suddivise in due categorie:

- vibrazioni trasmesse al sistema mano-braccio (in grado di determinare disturbi vascolari, osteoarticolari, neurologici o muscolari);
- vibrazioni trasmesse al corpo intero (in grado di determinare in particolare lombalgie e traumi del rachide).

Ove i risultati della valutazione lo richiedano, il DdL dovrà disporre, per la riduzione del rischio, le misure minime di carattere tecnico-organizzativo, tra cui la sorveglianza sanitaria dei lavoratori potenzialmente esposti a vibrazioni meccaniche ritenute nocive per la salute.

Il DdL dovrà fornire eventualmente una giustificazione del fatto di non ritenere necessario approfondire la valutazione, sulla base dei seguenti criteri:

- livello, tipo e durata dell'esposizione;
- valori limite di esposizione e valori di esposizione che fanno scattare l'azione;
- eventuali effetti diretti ed indiretti sulla salute e sicurezza dei lavoratori;
- informazioni fornite dal costruttore dell'attrezzatura di lavoro;
- esistenza di attrezzature alternative progettate per ridurre l'esposizione;
- eventuale prolungamento del periodo di esposizione sotto la responsabilità del DdL;
- condizioni di lavoro gravose, quali le basse temperature;
- informazioni derivanti dalla sorveglianza sanitaria svolta o da ricerche bibliografiche.

La valutazione del rischio viene aggiornata in funzione di modifiche sostanziali o qualora le risultanze e la sorveglianza sanitaria lo richiedano.

La metodologia applicata per la valutazione del rischio è riportata all'interno dello specifico "Documento di Valutazione dei Rischi".

5.4.4.5 Altre valutazioni

Altre valutazioni potranno essere redatte in base all'evoluzione della normativa, quali, ad esempio:

- valutazione del rischio amianto;

- valutazione del rischio da eventi criminosi;
- valutazione del rischio esplosione;
- valutazione del rischio per la presenza di campi elettromagnetici;
- valutazione del rischio per le lavoratrici gestanti.

5.5 Documentazione e registrazioni

- "Documenti di Valutazione dei Rischi"
- Testi delle norme

I documenti e i testi delle norme sono gestiti dal RSGSL e da questi conservati.

6 ORGANIZZAZIONE DEL SISTEMA: COMPITI E RESPONSABILITA'

6.1 Scopo

In una corretta organizzazione aziendale tutti i partecipanti all'attività produttiva hanno un ruolo definito ed a tutti noto, così come i relativi compiti e responsabilità.

L'esatta definizione dei compiti consente di evitare sprechi, sovrapposizioni, malintesi, carenze e conflitti che nuocciono all'economia aziendale.

Tali ruoli, compiti e responsabilità, particolarmente in tema di SSL, sono diffusi tra tutti i partecipanti all'attività produttiva oltre che tra coloro che assumono precisi incarichi previsti dalle norme di legge (DdL, RSPP, MC, RRLS, ASPP).

6.2 Applicabilità

L'attribuzione dei compiti e responsabilità in materia di SSL ed in materia di SGSL si applica a tutte le attività svolte ed a tutta la struttura organizzativa della Banca come descritte nei capitoli "Scopo e campo di applicazione del SGSL"

6.3 Responsabilità

L'attribuzione di compiti e responsabilità compete esclusivamente al DdL, fatti salvi i limiti previsti dalle norme di legge.

6.4 Azioni e metodi

L'organigramma della Banca stabilisce:

- la denominazione delle Unità Organizzative e i nomi dei rispettivi Responsabili;
- i rapporti gerarchici e funzionali.

Il DdL definisce le attribuzioni di responsabilità per le attività inerenti il SGSL, per le funzioni riportate in organigramma.

Il DdL nomina un suo rappresentante (RSGSL), in posizione di staff al DdL a cui affida ruolo, responsabilità e autorità per:

- assicurare che il SGSL sia definito, applicato e mantenuto in conformità al riferimento adottato;
- riferire al DdL sulle prestazioni del sistema.

Il DdL definisce le responsabilità in materia di SSL, accompagnando l'attribuzione dall'indicazione dei compiti e delle autonomie operative, con l'indicazione delle risorse di cui il soggetto può disporre in quanto necessarie e ponendo particolare attenzione alla definizione dei compiti di ispezione, verifica e sorveglianza in materia di SSL. Nell'ambito delle attribuzioni di specifici incarichi rientra la designazione delle figure previste dalla normativa vigente: RSPP, ASPP, addetti alle emergenze, MC.

In relazione alla designazione del RSPP prevista dall'art. 17, comma 1, lettera b), del D.Lgs. 81/2008, il DdL provvede alla consultazione preventiva degli RRLS. Quindi, il DdL procede alla designazione formale degli eventuali ASPP e del RSPP ed alla comunicazione del nominativo di quest'ultimo agli organi di vigilanza competenti per territorio.

Il DdL provvede alla comunicazione annuale dei nominativi degli RRLS agli organi di vigilanza competenti per territorio, come indicato all'art. 18, comma 1, lettera aa), del D.Lgs. 81/2008.

Il DdL provvede alla designazione degli addetti alla gestione delle emergenze (addetti alla prevenzione incendi, lotta antincendio, evacuazione dei lavoratori, pronto soccorso), cui affida i compiti di intervento indicati all'art. 17, comma 1, lettera b), del D.Lgs. 81/2008.

Una volta individuati i potenziali addetti, sulla base delle indicazioni ricavate dall'attività di valutazione dei rischi e tenendo conto del parere del MC, il DdL provvede alla consultazione preventiva dei RRLS.

Successivamente il DdL procede alla designazione formale; i lavoratori non possono, se non per giustificato motivo, rifiutare la designazione.

Il DdL provvede alla designazione del MC cui affida i compiti previsti dagli artt. 25, 39, 40 e 41 del D.Lgs. 81/2008.

Il soggetto che si intende designare come MC deve possedere le caratteristiche definite all'art. 2, comma 1, lettera h), del D.Lgs. 81/2008.

E' facoltà del DdL provvedere all'eventuale attribuzione dell'incarico a un Consulente esterno per la Sicurezza.

Riesame e modifiche

Il riesame della struttura e delle responsabilità attribuite alle varie figure avviene annualmente in occasione del riesame da parte della Direzione, tenendo conto delle osservazioni raccolte all'interno della Banca. Altre modifiche possono inoltre avvenire a seguito di eventi o situazioni che lo rendano necessario ed in particolare qualora emergano nuove esigenze aziendali (ad esempio turn-over di personale). Le modalità sono le stesse sopra descritte.

6.5 Documentazione e registrazioni

- Organigramma
- Designazione del RSPP
- Comunicazione nominativo del RSPP a ASL
- Comunicazione nominativi dei RRLLS a INAIL
- Designazione degli addetti emergenze
- Designazione del MC
- Designazione del Consulente esterno per la Sicurezza
- Lettere di attribuzione compiti e responsabilità

I documenti sopraindicati sono conservati dal RSGSL.

7 GESTIONE DELLE RISORSE STRUMENTALI

7.1 Scopo

La gestione dei beni strumentali può avere impatti anche significativi sulla SSL, pertanto un'ottimale gestione della SSL non può prescindere da una corretta gestione dei beni strumentali stessi.

Il D.Lgs. 37/2008, inoltre, dispone una serie di incombenze tecnico-amministrative da espletare in occasione di installazione di nuovi impianti o di interventi di modifica o manutenzione straordinaria a quelli esistenti. Tra queste sono comprese la verifica dell'adeguatezza degli impianti esistenti, la predisposizione di opportune fasi di progettazione e l'intervento di tecnici abilitati per l'effettuazione degli interventi.

7.2 Applicabilità

E' relativa a tutte le risorse strumentali della Banca quali:

- impianti generali a servizio dei luoghi di lavoro;
- impianti, macchine e attrezzature di lavoro;
- impianti e presidi antincendio;

e si applica per le attività di:

- scelta ed acquisto;
- utilizzo di sicurezza;
- mantenimento in efficienza.

7.3 Responsabilità

Il DdL, il RSPP e i Responsabili dei Servizi (con particolare rilevanza per coloro che hanno potere di acquisto - Servizio Tecnico, Ufficio Economato, Servizio Informatica Individuale e Networking) sono responsabili dell'attuazione di quanto disposto.

Il RSPP è responsabile della verifica del rispetto delle norme di sicurezza.

Il Responsabile del Servizio Tecnico è responsabile delle verifiche tecniche, dell'adeguatezza degli impianti e del rispetto di quanto disposto dalla normativa vigente.

7.4 Azioni e metodi

7.4.1 Impianti generali a servizio dei luoghi di lavoro

Gli impianti generali a servizio dei luoghi di lavoro sono definiti e progettati da parte di tecnici abilitati, in funzione delle esigenze aziendali ed in conformità alle norme vigenti e tecniche di riferimento.

7.4.2 Manutenzione e verifiche periodiche

Per quanto riguarda la manutenzione sugli impianti (termoidraulico, aeraulico, elettrico, messa a terra, ecc.) la Banca si avvale di specifici contratti di manutenzione con ditte specializzate.

All'interno dei contratti sono specificate le modalità di realizzazione degli interventi, comprendendo sia la manutenzione di tipo ordinario sia quella straordinaria a seguito del verificarsi di guasti o anomalie di funzionamento.

Le modalità di intervento previste rispondono ai requisiti previsti dalla normativa tecnica e ordinaria di riferimento.

La registrazione degli interventi effettuati sugli impianti (controlli, manutenzione programmata o straordinaria) da personale interno qualificato o da ditte esterne specializzate viene gestita dal Servizio Tecnico della Banca.

In particolare per gli impianti termoidraulici, la registrazione degli interventi avviene mediante compilazione, da parte della ditta incaricata della manutenzione, del Libretto di centrale/impianto, secondo le modalità previste dalla normativa vigente.

Per gli impianti soggetti a verifiche periodiche obbligatorie previste dalla normativa vigente (impianti termici, impianti di messa a terra) la scadenza e la successiva vidimazione dell'effettuazione degli interventi, effettuati a cura di ditta esterna autorizzata e/o di ente di vigilanza preposto, è gestita a cura del Servizio Tecnico della Banca.

7.4.3 Impianti, macchine e attrezzature

7.4.3.1 Scelta e acquisto di nuova risorsa

La scelta di nuove risorse strumentali ai fini dell'acquisto (o noleggio) viene effettuata dal DdL in collaborazione con i Responsabili dei Servizi interessati (ivi compreso il Servizio Tecnico) e con il RSPP.

La scelta dovrà essere preceduta sia da una valutazione delle caratteristiche tecniche della nuova risorsa, in relazione alle esigenze della Banca, che da una valutazione dei requisiti di sicurezza della stessa (con riferimento al "Documento di Valutazione dei Rischi", alla normativa vigente e tecnica applicabile).

Per la scelta può essere interpellato un possibile fornitore o consulenti specializzati.

All'esito della suddetta verifica si dovrà dare la preferenza, a parità di prestazioni, all'attrezzatura di lavoro che garantisce il maggior livello di sicurezza.

7.4.3.2 Fornitura e messa in servizio

Il Servizio Tecnico, sentiti il RSPP e il DdL si occuperà di definire l'acquisto (o il noleggio) e definirà col fornitore le modalità di consegna e/o installazione della nuova risorsa completa di "Manuale di uso e manutenzione" e di "Dichiarazione di Conformità" ove previsti.

Prima della messa in servizio della macchina o attrezzatura il Servizio Tecnico con il RSPP verifica la presenza della documentazione necessaria e controlla l'efficienza e la sicurezza della nuova risorsa.

Il Servizio Tecnico provvederà ad archiviare la documentazione acquisita e registrerà la nuova risorsa modificando il lay-out che riporta il posizionamento della stessa nei locali della Banca.

La messa in servizio di un nuovo impianto o macchina può avvenire solamente dopo l'effettuazione, da parte dell'installatore e/o del progettista, delle prove di collaudo previste dalle norme tecniche applicabili.

Per gli impianti e presidi soggetti a specifiche norme di legge il DdL, con il supporto del RSPP, e con l'eventuale collaborazione di consulente tecnico appositamente incaricato, procederà all'adempimento dei relativi obblighi autorizzativi, di collaudo e di verifica periodica presso gli enti preposti (Amministrazione Provinciale, ISPEL, Vigili del Fuoco, A.U.S.L. - U.O. Impiantistica Antinfortunistica).

Il DdL e il RSPP, previa consultazione dei RRLLS, dovranno valutare la necessità di procedere all'aggiornamento del "Documento di valutazione dei Rischi" ed alla fornitura ai lavoratori interessati di eventuali nuovi DPI.

Valuteranno, inoltre, la necessità di aggiornare la segnaletica di sicurezza presente in Banca.

7.4.3.3 Utilizzo di impianti, macchine e attrezzature

L'utilizzo in sicurezza degli impianti, macchine e attrezzature viene assicurato mediante l'impiego di personale debitamente formato.

Per le operazioni e/o attrezzature giudicate più pericolose, tenendo conto delle risultanze della valutazione dei rischi, è prevista l'elaborazione di specifiche istruzioni operative da parte del RSPP in collaborazione con il Responsabile del Servizio interessato (è prevista, se del caso, la collaborazione diretta con gli operatori).

La formazione e l'addestramento saranno completati dalla messa a disposizione ed illustrazione del "Manuale di istruzioni per l'uso" della macchina

o attrezzatura in questione e dalla consegna delle istruzioni scritte, quando previste.

Il controllo per il corretto uso di macchine ed attrezzature è sotto la responsabilità del Responsabile del Servizio interessato e comprende:

- il rispetto delle istruzioni operative;
- l'utilizzo dei dispositivi e sistemi di sicurezza di macchine ed attrezzature come da "Libretto di uso e manutenzione";
- l'utilizzo dei DPI previsti per l'uso di macchine e attrezzature.

Nel caso detti Responsabili rilevino situazioni o comportamenti pericolosi, incidenti o infortuni durante l'utilizzo delle macchine e delle attrezzature sono tenuti a seguire quanto previsto dalla gestione delle non conformità, delle azioni correttive e preventive.

7.4.3.4 Controlli periodici e manutenzione a impianti, macchine e attrezzature

Contestualmente alla messa in opera di nuovi impianti e presidi, l'installatore dovrà fornire tutta la documentazione prevista dalle relative norme tecniche e di legge.

Il Responsabile del Servizio Tecnico procederà ad archiviare la documentazione acquisita e registrerà la nuova risorsa.

Il DdL e il RSPP valuteranno inoltre la necessità di aggiornare la segnaletica di sicurezza presente in Banca.

7.4.3.5 Utilizzo impianti e presidi antincendio

L'utilizzo degli impianti e dei presidi antincendio è regolato mediante la definizione di specifiche procedure e istruzioni di emergenza ed è subordinato ad apposita formazione ed addestramento specifico per gli addetti alle emergenze.

7.4.3.6 Controlli periodici e manutenzione a impianti e presidi antincendio

I presidi antincendio e le dotazioni di sicurezza in uso devono essere sottoposti a controlli e verifiche periodiche al fine di accertarne ed assicurarne la disponibilità, l'efficienza e l'efficacia in caso di emergenza.

In particolare le misure di protezione antincendio, in ottemperanza della normativa vigente devono essere oggetto di:

Tipo di verifica	Responsabile della verifica	Frequenza	Oggetto della verifica
Sorveglianza	Personale della Banca appositamente istruito	Mensile	Verificare che l'impianto e l'attrezzatura antincendio, nelle normali condizioni operative, siano facilmente accessibili e non presentino danni materiali accertabili tramite esame visivo
Controllo	Ditta di manutenzione incaricata	Semestrale	Verificare la completa e corretta funzionalità dell'impianto e dell'attrezzatura antincendio
Revisione	Ditta di manutenzione incaricata	Determinata da norme specifiche per singoli impianti e attrezzature	Verificare e rendere perfettamente efficiente l'impianto e l'attrezzatura antincendio tramite opportuni accertamenti
Manutenzione	Ditta di manutenzione incaricata	All'occorrenza	Finalizzata a mantenere in efficienza ed in buono stato l'impianto e l'attrezzatura antincendio. Ordinaria: effettuata sul posto con strumenti ed attrezzi di uso corrente Straordinaria: che richiede mezzi di particolare importanza o comporti sostituzione di intere parti di impianto o la completa revisione o sostituzione di parti

Per la registrazione delle attività di sorveglianza, controllo, revisione e manutenzione delle dotazioni antincendio vengono utilizzate delle apposite schede (compilate a cura del personale che effettua l'intervento) archiviate a cura del Servizio Tecnico.

Il "Registro Antincendio", compilato a cura del SPP, viene aggiornato periodicamente sulla base delle suddette schede.

Sulla base delle indicazioni fornite dai manuali di uso e manutenzione e della normativa vigente e tecnica applicabile sono individuate le tipologie di controllo periodico volto a garantire e mantenere la sicurezza e la salute dei lavoratori che le utilizzano.

Quindi, il Responsabile del Servizio Tecnico definisce, per ogni impianto, macchina e attrezzatura un programma di controllo e manutenzione, in collaborazione con il RSPP.

Detto programma determina la tipologia e la tempistica degli interventi di controllo periodico e di manutenzione programmata ai quali assoggettare le macchine, apparecchiature, attrezzature e a chi questi interventi sono stati affidati.

I controlli sono mirati alla verifica dell'efficienza dei dispositivi di sicurezza ed alla presenza ed integrità dei ripari di protezione, mentre gli interventi di manutenzione ordinaria di macchine e attrezzature sono necessari per mantenere efficienti nel tempo le attrezzature di lavoro. Queste attività sono demandate a personale appositamente formato ed istruito, e sono svolte in conformità alle leggi vigenti ed alle indicazioni fornite dal manuale di uso e manutenzione dell'attrezzatura.

Gli altri interventi più complessi, quali: controlli tecnici particolari, manutenzioni straordinarie, modifica o adeguamento di un'attrezzatura, che richiedono competenze particolari, sono affidati a personale esterno qualificato.

Tutti gli interventi effettuati andranno registrati a cura del manutentore. Il Responsabile del Servizio Tecnico dovrà garantire il rispetto delle periodicità degli interventi e la corretta registrazione degli stessi.

Per attrezzature di lavoro soggette a normativa di sicurezza specifica, ad esempio gli apparecchi di sollevamento, dovranno essere adottati i programmi di manutenzione ed i registri di controllo obbligatori predisposti dal costruttore dell'attrezzatura.

Particolare attenzione sarà posta nella programmazione e nella registrazione dei controlli previsti dalla normativa vigente.

Sono oggetto di verifica e controllo tutti i presidi antincendio quali:

- Estintori portatili a polvere.
- Estintori portatili a CO₂.
- Pulsanti di allarmi e suonerie.
- Impianti automatici di rilevazione incendio.
- Impianti di rilevazione fumi.
- Impianti automatici di estinzione incendio.
- Impianti idrici antincendio: idranti, naspi, cassette porta lancia, manichette.
- Vie di esodo: segnaletica, illuminazione di emergenza.
- Porte REI.

7.4.3.7 Vendita/rottamazione di risorse strumentali

La vendita di risorse strumentali deve essere eseguita dopo averne accertato la conformità alla normativa vigente ed aver eventualmente provveduto alla messa in sicurezza delle stesse. All'acquirente deve essere fornita la documentazione prescritta dalla normativa vigente.

In caso di rottamazione dovrà essere richiesta alla ditta incaricata documentazione comprovante l'avvenuta demolizione.

L'attività descritta nel presente paragrafo è a cura del Servizio Tecnico della Banca.

7.4.4 Impianti e presidi antincendio

La gestione delle attività di acquisto, messa in servizio, utilizzo e manutenzione di impianti e presidi antincendio non differisce sostanzialmente da quanto indicato per le altre risorse strumentali, ma richiede alcune specifiche individuate dalla normativa vigente e dalle norme tecniche di riferimento.

7.4.4.1 Scelta e acquisto di nuova risorsa antincendio

Per l'acquisizione di un nuovo impianto o presidio antincendio valgono le medesime indicazioni fornite nei precedenti paragrafi relativi a scelta e acquisto delle altre risorse strumentali.

In particolare tali fasi saranno precedute da un'attenta valutazione sulla necessità di richiesta di Certificato di Prevenzione Incendi e dalla eventuale conseguente fase progettuale.

7.5 Documentazione e registrazioni

- Schede di manutenzione
 - Libretto di uso e manutenzione
 - Schemi degli impianti
 - Lay-out dei locali della Banca e disposizione di macchine e attrezzature di lavoro
 - Progetti relativi alle modifiche agli impianti esistenti
 - Documentazione richiesta dalla normativa vigente
 - "Certificato di Prevenzione Incendi"
- conservati dal Servizio Tecnico
- "Registro Antincendio"
- conservati dal RSGSL.

8 ADOZIONE E GESTIONE DEI DISPOSITIVI DI PROTEZIONE INDIVIDUALE

8.1 Scopo

I DPI rivestono un'importanza rilevante per la riduzione del rischio a carico dei lavoratori, pertanto l'adozione e la gestione dei DPI stessi necessita di particolare cura.

8.2 Applicabilità

Si applica a tutte le fasi di gestione dei DPI messe in atto dalla Banca: individuazione caratteristiche, scelta, consegna, uso e conservazione, sostituzione.

8.3 Responsabilità

Il DdL è responsabile dell'adozione dei DPI necessari (la cui scelta avviene con il coinvolgimento di RSPP, MC, RRLS e Responsabile del Servizio Tecnico) e della consegna dei DPI stessi agli operatori che ne necessitano.

Il DdL, il RSPP e il personale operativo interessato sono responsabili dell'attuazione di quanto disposto.

Il RSPP è responsabile della verifica del rispetto delle norme di sicurezza.

8.4 Azioni e metodi

Nell'ambito della valutazione dei rischi si identificano le situazioni per le quali i rischi non possono essere evitati o significativamente ridotti da misure tecniche concretamente attuabili e che quindi risulta necessario fronteggiare mediante l'uso dei Dispositivi di Protezione Individuale.

La scelta e la gestione dei DPI presso la Banca Passadore & C. avviene secondo le modalità descritte nei paragrafi successivi che indicano i compiti e le responsabilità specifiche per dette attività.

8.4.1 Scelta dei DPI

In seguito all'individuazione delle necessità di utilizzare dei DPI con la valutazione dei rischi in base al programma delle misure di prevenzione e di protezione, il DdL in collaborazione con il RSPP e il Responsabile del Servizio Tecnico e consultando il MC e gli RRLS, procede alla scelta di detti dispositivi con:

- l'individuazione delle tipologie di DPI da adottare;
- la valutazione delle caratteristiche dei DPI disponibili sul mercato, scegliendo quelli che soddisfano sia le specifiche esigenze di natura protettiva, sia gli aspetti ergonomici e di accessibilità;
- la definizione delle condizioni in cui i DPI devono essere utilizzati, particolarmente per quanto riguarda la durata dell'uso.

Ogniquale volta intervengono variazioni significative degli elementi di valutazione viene aggiornata la dotazione di DPI con lo stesso iter di valutazione e scelta utilizzato per la prima scelta.

Per la scelta dei DPI la Banca tiene in considerazione che:

- al crescere della potenziale gravità delle conseguenze lesive derivanti dai rischi individuati bisogna ricorrere a DPI di maggiore efficacia ed affidabilità;
- i DPI devono essere adeguati ai rischi, alle lavorazioni ed alla persona che li indossa;
- i DPI devono rispondere ai requisiti essenziali di sicurezza, la cui conformità è attestata dal fabbricante, mediante marcatura CE;
- i DPI devono rispondere alle caratteristiche delle norme tecniche di riferimento.

Al fine di valutare l'efficienza e l'efficacia i DPI adottati, nell'ottica del miglioramento delle condizioni di sicurezza e salute dei lavoratori, la Banca prevede di effettuare dopo un certo tempo dall'adozione e consegna dei diversi DPI una verifica dell'idoneità e dell'adeguatezza del dispositivo mediante interviste agli operatori ed attraverso relazioni dei MC sui risultati della sorveglianza sanitaria.

8.4.2 *Acquisto, consegna e gestione dei DPI*

Nella gestione dei DPI la Banca garantisce:

- l'acquisto di DPI corrispondenti alla scelta effettuata nel corso della valutazione,
- la consegna e l'utilizzo dei DPI soltanto per usi previsti fornendo istruzioni comprensibili ai lavoratori su:
 - i rischi dai quali il DPI lo proteggono;
 - l'uso corretto e l'utilizzo pratico dei DPI;
- il mantenimento in efficienza dei DPI mediante la manutenzione, le sostituzioni necessarie e la conservazione.

Per garantire corrette istruzioni la Banca provvede alla formazione e alla formazione dei lavoratori interessati.

L'acquisto dei DPI da adottare o da approvvigionare può essere effettuato dal RSPP o dal Responsabile del Servizio Tecnico facendo riferimento a quanto indicato precedentemente, in base alla situazione delle scorte ed a quanto previsto nel "Documento di Valutazione dei Rischi".

Il controllo periodico dell'attività di consegna e l'effettiva attività di formazione ed informazione sui DPI sono affidate al RSPP.

I DPI previsti vengono consegnati ai singoli operatori all'assunzione, o all'atto della destinazione alla mansione che ne richieda la dotazione, a cura del Responsabile del Servizio Tecnico e vengono sostituiti in caso di usura o rottura.

E' prevista la compilazione di una ricevuta per formalizzare l'avvenuta consegna dei DPI. L'avvenuta consegna viene quindi verificata durante le attività di verifica del sistema.

Le informazioni sull'utilizzo dei DPI sono contenute nelle istruzioni operative specifiche e nel paragrafo "Uso e conservazione dei DPI", che riporta anche le indicazioni sulle modalità di richiesta di sostituzione di quelli usurati. La formazione in merito viene trattata nei corsi e nell'addestramento previsti dall'apposito programma di formazione per le mansioni interessate.

Il controllo sull'uso corretto dei DPI da parte degli operatori interessati è demandata ai Responsabili dei relativi Servizi ed i comportamenti anomali vengono dagli stessi segnalati secondo quanto stabilito in merito all'osservazione dei comportamenti pericolosi.

8.4.3 *Uso e conservazione dei DPI*

Gli addetti che hanno in dotazione DPI e indumenti di lavoro per l'uso, la conservazione e la sostituzione degli stessi devono attenersi alle disposizioni di seguito indicate.

I DPI:

devono essere:

- usati sul posto di lavoro secondo le istruzioni verbali ricevute, secondo quanto indicato nelle istruzioni operative impartite e secondo le presenti istruzioni;
- usati con cura e tenuti puliti (secondo possibilità di lavoro);
- indossati correttamente;
- usati in tutte le operazioni per le quali sono previsti;
- messi nell'armadietto alla fine dell'attività che ne richiede l'utilizzo;
- sostituiti se rotti o molto rovinati facendone richiesta al Responsabile del Servizio Tecnico;
- sostituiti se sono mascherine o tappi anche se sono sporchi;

non devono essere:

- usati per operazioni per le quali non sono previsti;
- portati all'esterno della Banca (con esclusione per gli indumenti di lavoro) se non previa autorizzazione;
- lasciati all'esterno degli armadietti quando non utilizzati;

sono consegnati:

- al momento dell'assunzione, o all'atto della destinazione alla mansione che ne richieda la dotazione, da parte del Responsabile del Servizio Tecnico;

sono cambiati:

- una volta all'anno gli indumenti di lavoro;
- in qualsiasi momento se sono rotti o deteriorati (previa restituzione di quelli non più idonei).

8.5 Documentazione e registrazioni

- Caratteristiche dei DPI adottati
- Assegnazione dei DPI

I documenti sono conservati dal Responsabile del Servizio Tecnico.

9 ORGANIZZAZIONE DEL SISTEMA: COINVOLGIMENTO DEL PERSONALE

9.1 Scopo

La concezione secondo la quale un SGSL è efficace quando ottiene il sostegno e l'impegno di tutti i dipendenti della Banca deriva dalla consapevolezza che ognuno deve dare, per la parte di propria competenza e nell'ambito del proprio ruolo aziendale, il suo contributo per la propria ed altrui sicurezza.

Ma ciò si può ottenere solo se ognuno ne ha un'intima convinzione e se ognuno si sente direttamente coinvolto.

Senza questa risorsa culturale non si può dare un contributo attivo alla sicurezza comune, ma si subiscono passivamente disposizioni ed ordini che ne svuotano l'impegno e, conseguentemente, l'efficacia dei risultati ottenibili.

Il coinvolgimento del personale raggiunge un suo primo obiettivo quando tutti danno un contributo costruttivo all'applicazione del sistema ed al suo miglioramento con suggerimenti ed osservazioni.

9.2 Applicabilità

Si applica a tutte le attività svolte dalla Banca e descritte nei capitoli "Scopo e campo di applicazione del SGSL".

9.3 Responsabilità

Il DdL è responsabile della scelta delle forme di coinvolgimento del personale.

Il RSGSL è responsabile dell'individuazione delle forme di coinvolgimento del personale per la partecipazione attiva al SGSL.

Il DdL è responsabile della consultazione dei RRLLS nei casi previsti dalla normativa vigente.

Il DdL è responsabile della convocazione della riunione periodica di prevenzione e può delegare il RSPP ad assolvere a tale obbligo.

9.4 Azioni e metodi

Il RSGSL esamina l'elenco dei requisiti legali e verifica che ciascuno degli obblighi di consultazione possa essere rispettato attraverso:

- l'inserimento della fase di consultazione all'interno di altra procedura o istruzione operativa;
- la procedura o l'istruzione operativa specifica.

La riunione periodica di prevenzione prevista dall'art. 35 del D.Lgs. 81/2008 viene convocata annualmente, con convocazione scritta su cui è riportato l'ordine del giorno ovvero l'elenco degli argomenti che saranno trattati.

Saranno sempre trattati:

- l'esame del documento di valutazione dei rischi;
- l'idoneità dei DPI;
- i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e protezione della loro salute.

I soggetti convocati sono:

- il DdL;
- il RSPP;
- il MC;
- i RRLLS.

La riunione è indetta anche in occasione di variazioni significative delle condizioni di esposizione al rischio per i lavoratori, compresi i casi di introduzione di nuove tecnologie che hanno riflessi sulle condizioni di sicurezza e salute.

Il RSPP funge da segretario della riunione e redige il verbale che tiene a disposizione dei partecipanti.

Il RSGSL individua, sentiti gli RRLLS, le possibili forme di coinvolgimento del personale della Banca nell'applicazione del SGSL e le sottopone all'esame del DdL per l'approvazione.

Il coinvolgimento si realizza, ad esempio, in occasione di:

- procedure di raccolta delle osservazioni in materia di SSL, presentate anche nel capitolo "Comunicazione, flusso informativo e cooperazione";
- inserimento della SSL in occasione di riunioni aziendali;
- altro.

Il RSGSL elabora specifiche modalità e/o procedure per dare attuazione alle forme di coinvolgimento approvate dal DdL anche inserendo, quando pertinente, uno specifico richiamo al coinvolgimento dei lavoratori all'interno di procedure o istruzioni operative destinate ad altro fine.

Il RSGSL individua gli indicatori di prestazione più adatti al monitoraggio di ciascuna forma di coinvolgimento.

9.5 Documentazione e registrazioni

- Convocazione della riunione periodica
- Verbale della riunione periodica

I documenti sono conservati dal RSGSL.

10 ORGANIZZAZIONE DEL SISTEMA: INFORMAZIONE, FORMAZIONE, ADDESTRAMENTO, CONSAPEVOLEZZA, SANZIONI

10.1 Scopo

Ogni sistema organizzativo può raggiungere i suoi obiettivi se ha una natura dinamica, evolvendosi conseguentemente agli input che gli pervengono.

Le informazioni specifiche che arricchiscono la conoscenza, la formazione che educa ad utilizzare dette informazioni e l'addestramento allo svolgimento delle proprie mansioni, mettono in condizione tutto il personale della Banca di essere pienamente cosciente del proprio ruolo, delle proprie responsabilità, delle possibilità di sviluppo e crescita.

Sinteticamente, l'informazione, la formazione e l'addestramento danno coscienza dell'importanza della SSL nel contesto produttivo aziendale.

Il SGSL deve definire e mantenere attive le modalità per assicurare che il personale sia ad ogni livello consapevole:

- dell'importanza della conformità delle proprie azioni rispetto alla politica ed ai requisiti del SGSL;
- delle conseguenze che la propria attività ha nei confronti della SSL;
- delle possibili conseguenze dovute ad uno scostamento da quanto fissato in materia di SSL.

Deve inoltre garantire il rispetto degli obblighi di legge in materia di informazione, formazione e addestramento dei lavoratori, nonché di informazione del personale esterno presente nell'insediamento.

10.2 Applicabilità

Si applica a tutte le attività svolte dalla Banca e descritte nei capitoli "Scopo e campo di applicazione del SGSL".

10.3 Responsabilità

Il DdL è responsabile dell'informazione, formazione ed addestramento dei lavoratori e dell'informazione delle persone presenti od operanti nei locali della Banca.

Il DdL può delegare altra persona ad assolvere a tali obblighi.

Il RSPD è responsabile di proporre i programmi di informazione e formazione dei lavoratori.

Il RSGSL è responsabile della definizione e dell'applicazione delle modalità per mantenere un'elevata consapevolezza dell'importanza delle proprie azioni ai fini del raggiungimento degli obiettivi di SSL stabiliti dall'azienda.

Il MC partecipa attivamente alle attività di informazione e formazione.

10.4 Azioni e metodi

I criteri secondo i quali avvengono la pianificazione e lo svolgimento delle attività di informazione, formazione, addestramento e consapevolezza del personale sono i seguenti.

Sensibilizzazione e consapevolezza

L'attività di sensibilizzazione è estesa a tutto il personale della Banca e viene attuata con continuità e periodicamente con le seguenti modalità:

- riunioni periodiche (almeno annuali) in cui il DdL esprime direttamente a tutti i lavoratori l'impegno di SSL della Banca, la politica, gli obiettivi, i traguardi e i programmi di SSL, nonché la necessità e l'importanza che tutti attuino il SGSL;
- riunioni periodiche, a gruppi omogenei, in cui i rispettivi Responsabili sensibilizzano il personale sui ruoli, responsabilità, effetti sulla SSL delle attività svolte, comportamenti da tenere in ogni circostanza, potenziali conseguenze derivanti dalla mancata attuazione del SGSL.

Questa attività si svolge in base ad un programma annuale che può ripetersi o essere modificato in base al riesame annuale.

In seguito a introduzione di prodotti, tecnologie, legislazioni nuove/modificate o in seguito ad avvenimenti imprevisti può essere programmata una specifica campagna di sensibilizzazione.

Informazione

L'informazione è fornita a tutti i lavoratori della Banca sia al momento dell'assunzione sia in occasione di ogni variazione di mansione o delle condizioni di esposizione a rischio.

Gli argomenti della informazione sono definiti dal RSPP ed approvati dal DdL, anche in base alle risultanze della valutazione dei rischi, e riguardano almeno:

- i rischi per la sicurezza e la salute connessi all'attività della Banca in generale;
- le misure e le attività di protezione e prevenzione adottate;
- i rischi specifici cui è esposto in relazione all'attività svolta, le normative di sicurezza e le disposizioni aziendali in materia;
- le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori;
- il RSPP ed il MC;
- i nominativi dei lavoratori incaricati di applicare le misure di lotta all'incendio, evacuazione dei lavoratori e pronto soccorso.

A ciascun lavoratore è inoltre fornita, per quanto di competenza, informazione specifica su:

- uso delle attrezzature di lavoro;
- uso dei dispositivi di protezione individuale;
- movimentazione manuale dei carichi;
- utilizzo di VDT;
- segnaletica di sicurezza visuale, gestuale, vocale, luminosa e sonora;
- ogni altro fattore di rischio e argomento rilevante ai fini della SSL individuato e definito nel programma di informazione.

L'informazione può essere fornita, e ripetuta periodicamente, da figure interne o esterne alla Banca.

Il programma della informazione per i lavoratori è oggetto di trattazione nel corso della riunione periodica di prevenzione.

Alcune figure aziendali (RSPP, MC, RRLS) sono oggetto di una informazione specifica.

Competenze e formazione

Per ogni attività/compito che può avere impatti significativi sulla SSL, come individuate anche nella valutazione dei rischi, viene identificato il personale interessato.

Per questo personale, i relativi Responsabili di Servizio, coinvolgendo il RSPP, identificano le competenze necessarie in termini di conoscenze e capacità:

- la conoscenza deriva da adeguata istruzione e cultura di base, oppure da formazione di aula;
- la capacità deriva da adeguato addestramento (teorico e sul campo) e/o da esperienza acquisita.

Per tutto il personale i Responsabili dei relativi Servizi valutano le competenze disponibili (in termini di conoscenza e capacità).

La differenza fra competenze necessarie (obiettivo) e competenze disponibili (stato di fatto) consente di determinare le necessità di formazione (per adeguare le conoscenze) e di addestramento (per adeguare le capacità).

Da queste analisi scaturiscono i programmi di formazione e addestramento.

Gli argomenti oggetto di formazione proposti dal RSPP comprendono, tra gli altri, i contenuti del modello organizzativo, delle procedure, delle istruzioni operative, gli aspetti di SSL significativi, i programmi di SSL, le prestazioni di SSL e ogni altro aspetto del SGSL.

Il programma di formazione e addestramento per i lavoratori è oggetto di trattazione nel corso della riunione periodica di prevenzione.

Le modifiche di legislazione, processo, tecnologia oppure avvenimenti imprevisti possono far emergere la necessità di modificare le capacità del personale e quindi dar luogo ad una modifica del programma di formazione e addestramento.

Ad ogni nuova assunzione o cambio di mansione deve essere effettuata la verifica di cui sopra ed attuato il conseguente programma che ne deriva.

Le attività di formazione e addestramento effettuate sono opportunamente registrate.

Individuazione dei docenti

I corsi di formazione e/o di informazione possono essere tenuti indifferentemente sia da personale interno sia da personale esterno alla Banca, i docenti potranno quindi essere, a seconda della tipologia di intervento:

- RSPP,
- MC,
- Preposti,
- RRLS,
- esperti in materia (ad esempio per i corsi antincendio).

Scelta della metodologia didattica e individuazione degli strumenti

L'efficacia della formazione è molto legata alle metodologie didattiche individuate. Il coinvolgimento dei partecipanti, la loro partecipazione e l'induzione di motivazioni a comportamenti corretti passa per l'attività formativa e le modalità di svolgimento della stessa.

Per il perseguimento di questo obiettivo sono privilegiate tutte le metodologie didattiche "attive" che prevedono il coinvolgimento diretto dei partecipanti.

Di conseguenza anche gli strumenti utilizzati per la formazione devono rendere la partecipazione ai corsi "attiva" evitando che il partecipante subisca passivamente il trasferimento di conoscenze/nozioni.

Modalità di valutazione

Per conseguire un adeguato livello di conoscenza in materia di SSL da parte dei lavoratori, la valutazione della formazione degli stessi deve avvenire con costanza, pertanto:

- sarà cura dei propositi osservare il comportamento dei propri collaboratori (avendo cura di correggere i comportamenti scorretti e rinforzando quelli corretti);
- sarà cura dei Responsabili dei Servizi valutare la competenza dei nuovi assunti (soprattutto per coloro i quali siano adibiti ad attività che comportino un maggior livello di rischio);
- sarà cura del RSPP controllare lo stato e l'andamento degli incidenti e dei comportamenti pericolosi;
- sarà cura dei docenti verificare il livello di apprendimento alla fine dei singoli corsi.

Sanzioni

Tutti i dipendenti della Banca Passadore & C. sono tenuti ad osservare le disposizioni contenute nel presente modello organizzativo avendo cura di tenere un comportamento corretto nella gestione della SSL.

Non dovranno, pertanto, essere poste in essere situazioni che possano essere causa di danno per sé o per altri e dovranno essere segnalate prontamente al SPP tutte le anomalie rilevate.

Il mancato rispetto o la violazione delle regole sopra ricordate determina l'applicazione dei provvedimenti disciplinari previsti dal C.C.N.L. per i dipendenti delle aziende di credito, finanziarie e strumentali, nonché delle azioni civili e penali stabilite dalla legge.

Riesame e modifiche

In aggiunta a quanto sopra riportato, il riesame dei programmi di sensibilizzazione, di informazione, di formazione e addestramento viene effettuato a seguito di altri possibili eventi o situazioni che lo rendano necessario.

10.5 Documentazione e registrazioni

- Registrazioni delle attività di informazione
- Registrazioni delle verifiche di formazione e addestramento

I documenti sono conservati dal RSGSL.

11 ORGANIZZAZIONE DEL SISTEMA: COMUNICAZIONE, FLUSSO INFORMATIVO E COOPERAZIONE

11.1 Scopo

Scopo di una corretta forma di comunicazione è quello di far pervenire a tutti i soggetti della Banca tutte quelle informazioni necessarie per consentire a ciascuno di esercitare appieno ed in sintonia con gli altri il proprio ruolo.

Si tratta dell'organizzazione razionalizzata del flusso informativo tale da consentire il trasferimento delle informazioni utili attraverso comunicazioni pluridirezionali, mirate e sintetiche, in grado di rendere partecipe tutto il personale della Banca, per la parte di interesse, ai fini della SSL.

Il flusso è quindi biunivoco:

- verticale: dall'alta dirigenza verso la base e viceversa;
- orizzontale: tra Responsabili dei Servizi, da lavoratore a lavoratore.

La cooperazione nasce dalla conoscenza delle altrui esigenze e dalla necessità di trovare le sinergie necessarie alla crescita comune.

Non va poi trascurata la comunicazione da e verso l'esterno, nella consapevolezza che la Banca vive ed opera in un contesto sociale.

11.2 Applicabilità

Si applica a tutte le attività svolte dalla Banca e descritte nei capitoli "Scopo e campo di applicazione del SGSL".

11.3 Responsabilità

RSGSL, DdL, Responsabili dei Servizi/Uffici/Dipendenze.

11.4 Azioni e metodi

Le attività di gestione della comunicazione di SSL interna ed esterna seguono i seguenti criteri.

Comunicazione interna: suddivisa in comunicazione top-down, bottom-up e tra funzioni.

La comunicazione bottom-up comprende la segnalazione e la gestione di rilievi, osservazioni, proposte, provenienti da personale della Banca.

La ricezione è effettuata dal responsabile gerarchico, qualunque sia il livello del proponente.

Il responsabile gerarchico è tenuto a ricevere qualunque tipo di comunicazione e a trasmetterla al RSGSL.

Il RSGSL riceve ogni segnalazione e le trasmette alle funzioni interessate; inoltre, se necessario, elabora e consegna al responsabile gerarchico risposta scritta in tempi congrui, per il successivo inoltro al richiedente.

La comunicazione top-down ha la funzione fondamentale di aumentare la conoscenza del sistema, informando il personale della Banca su:

- politica, obiettivi, traguardi, programma di SSL, prestazioni di SSL, struttura organizzativa, ecc.;
- contenuti del manuale, delle procedure, delle istruzioni operative;
- ogni altro aspetto del SGSL.

La comunicazione dall'alto può avvenire per mezzo di:

- comunicati interni diffusi a tutti gli interessati;
- riunioni a gruppi omogenei o allargati a tutto il personale, secondo l'argomento, condotte dall'ente di competenza;
- incontri singoli su particolari argomenti (quali ad esempio risultati di audit, esiti di riesami, prestazioni ambientali, ecc.).

Comunicazione esterna: suddivisa in passiva e attiva.

Passiva - Ogni rilievo, osservazione, richiesta, ecc. proveniente dall'esterno e relativa a temi di SSL deve essere convogliata al RSGSL. Se si tratta di richiesta verbale deve essere tradotta in forma scritta dal ricevente.

Ogni richiesta deve essere archiviata.

Il RSGSL deve sempre rispondere entro un termine prefissato.

L'invio della risposta è sempre subordinato a verifica ed approvazione del DdL.

Attiva - È responsabilità del DdL e riguarda essenzialmente:

- la politica e l'impegno della Banca verso la SSL;
- i risultati e i miglioramenti conseguiti;
- specifiche iniziative.

I mezzi utilizzati possono comprendere:

- la diffusione di comunicati;
- la distribuzione di materiale informativo, ecc.

Tra i soggetti destinatari si possono individuare almeno:

- il personale esterno (committenti, fornitori, collaboratori esterni);
- il pubblico (clienti, visitatori, soggetti interessati).

Iter amministrativo infortuni

In caso di infortunio, secondo quanto previsto dalla normativa vigente:

- Nell'eventualità di un infortunio con prognosi di almeno un giorno, un addetto al Servizio Personale:
 - compila il Registro Infortuni;
 - invia la segnalazione statistica all'INAIL.
- Nell'eventualità di un infortunio con prognosi superiore ai tre giorni, un addetto al Servizio Personale:
 - compila il Registro Infortuni;
 - invia entro due giorni da quello in cui il DdL ne ha avuto notizia tramite il certificato medico (i due giorni si contano a partire dal quarto giorno di infortunio qualora, inizialmente, l'inabilità sia stata guaribile entro tre giorni) una denuncia dell'accaduto all'INAIL;
 - invia entro due giorni una denuncia dell'accaduto all'Autorità di Pubblica Sicurezza del Comune nel quale è avvenuto l'infortunio. (Se l'infortunio ha avuto luogo in viaggio e in territorio straniero, l'Autorità di Pubblica Sicurezza è quella nella cui circoscrizione è compreso il primo luogo di fermata in territorio italiano. Nei Comuni ove manchi l'ufficio di Pubblica Sicurezza la denuncia deve essere inoltrata al Sindaco).
- Nell'eventualità di un infortunio mortale o per il quale si tema la morte, un addetto al Servizio Personale:
 - compila il Registro Infortuni;
 - invia entro ventiquattro ore una denuncia dell'accaduto all'INAIL;
 - invia entro due giorni una denuncia dell'accaduto all'Autorità di Pubblica Sicurezza del Comune nel quale è avvenuto l'infortunio. (Se l'infortunio ha avuto luogo in viaggio e in territorio straniero, l'Autorità di Pubblica Sicurezza è quella nella cui circoscrizione è compreso il primo luogo di fermata in territorio italiano. Nei Comuni ove manchi l'ufficio di Pubblica Sicurezza la denuncia deve essere inoltrata al Sindaco).

Riesame

Il riesame delle attività di comunicazione viene effettuato annualmente e a seguito di possibili eventi o situazioni che lo rendano necessario.

11.5 Documentazione e registrazioni

- Documentazione delle comunicazioni attive
- Documentazione delle risposte alle osservazioni di SSL

La documentazione relativa alle comunicazioni è gestita dal RSGSL.

12 ORGANIZZAZIONE DEL SISTEMA: DOCUMENTAZIONE

12.1 Scopo

La conoscenza delle normative che interessano, la conoscenza delle scelte aziendali e di tutti i riferimenti e metodi cui si ispira l'azione aziendale, in modo chiaro, inequivocabile ed incontrovertibile costituisce un punto fermo di riferimento su cui si basano la consapevolezza, la cooperazione e la partecipazione.

Appare quindi indispensabile che esista un governo della documentazione, gestito in modo dinamico ed efficace ai fini del miglioramento continuo delle condizioni di SSL.

Ciò è tanto più importante in tema di SSL per la presenza di una normativa vigente di particolare rilievo. Lo scopo del capitolo è descrivere come vengono documentati gli elementi fondamentali del SGSL al fine di consentire alla Banca la gestione nel tempo delle conoscenze pertinenti la SSL, l'implementazione ed il monitoraggio del SGSL.

12.2 Applicabilità

Si applica a tutte le documentazioni contemplate nel SGSL e descritte nel presente modello organizzativo.

12.3 Responsabilità

RSGSL, DdL.

12.4 Azioni e metodi

Per documentazione si intende sia la documentazione del SGSL che la documentazione di SSL. Nella documentazione del SGSL sono compresi tutti i documenti citati nel presente modello organizzativo, nelle procedure operative e nelle istruzioni operative.

La documentazione di SSL comprende:

- leggi, regolamenti, norme antinfortunistiche attinenti l'attività della Banca;
- regolamenti e accordi aziendali;
- quella richiesta dalla normativa vigente in materia di SSL (ad esempio: "Documento di Valutazione dei Rischi", elenco delle sostanze pericolose, CPI, rapporto di analisi delle esposizioni al rumore, ecc.);
- manuali, istruzioni per l'uso di macchine, attrezzature, DPI, forniti dai costruttori.

12.4.1 Documentazione del SGSL

È organizzata su 3 livelli:

- Modello organizzativo: descrive le modalità e i criteri di funzionamento del SGSL.
- Procedure, istruzioni operative: descrivono le attività necessarie per dare attuazione a specifici elementi del SGSL.
- Piani, programmi, disposizioni, modulistica, ecc.: definiscono come applicare i criteri alle specifiche situazioni.

Modello Organizzativo

Il modello organizzativo descrive il SGSL e le modalità e i criteri con cui il sistema è realizzato, gestito e revisionato; descrive la politica, l'organizzazione, le responsabilità e le modalità con cui vengono prese le decisioni; permette di identificare, definire, realizzare e controllare tutte le attività che hanno influenza sulla SSL in conformità con le Linee Guida UNI-INAIL.

Il modello organizzativo è redatto dal RSGSL ed approvato dal DdL, così come le successive revisioni.

Procedure

Le procedure sviluppate in dettaglio nelle relative sezioni del modello organizzativo riportano i riferimenti alle procedure attinenti, definendo per ogni attività (cosa) le responsabilità (chi) e le relative modalità di attuazione (come, dove, e quando).

Dall'applicazione delle singole procedure (definite nelle singole sezioni del modello organizzativo) scaturiscono le documentazioni e le registrazioni che dimostrano l'attuazione del SGSL.

Un elenco completo e aggiornato è conservato dal RSGSL.

Istruzioni operative

Descrivono in dettaglio le modalità di corretta attuazione di attività o processi della Banca.

Un elenco completo e aggiornato è conservato dal RSGSL.

Piani

Definiscono le modalità di attuazione di specifiche attività che si svolgono ripetutamente e periodicamente (la cui frequenza è definita dal modello organizzativo). Essi riportano le azioni pianificate, le responsabilità, le risorse e le tempistiche.

Un elenco completo e aggiornato è conservato dal RSGSL.

Programmi

Identificano le modalità di attuazione di azioni specifiche, da svolgersi in un arco di tempo ben definito (ad esempio programma di informazione, programma di formazione, ecc.). Essi riportano le azioni programmate, le responsabilità, le risorse e le tempistiche.

Un elenco completo e aggiornato è conservato dal RSGSL.

Disposizioni

Sono documenti emessi dal DdL per dare attuazione a specifici requisiti citati dal modello organizzativo (ad esempio politica, organigramma, lettere di incarico, ecc.).

Un elenco completo e aggiornato è conservato dal RSGSL.

Modulistica

Sono documenti di registrazione richiamati dal modello organizzativo, con cui si dà evidenza dell'applicazione del SGSL (ad esempio verbali di riunione, informazione e formazione del personale, ecc.).

Un elenco completo e aggiornato è conservato dal RSGSL.

12.4.2 Documentazione di SSL

È raccolta, gestita e conservata a cura del RSGSL. Nel modello organizzativo sono definite le modalità riguardanti la gestione della documentazione di SSL, con indicazione:

- della figura incaricata della gestione;
- della ubicazione dei documenti.

12.5 Documentazione e registrazioni

- Procedure
- Istruzioni operative
- Piani di SSL
- Programmi di SSL
- Disposizioni di SSL
- Documenti previsti dalla normativa vigente

La documentazione del SGSL è gestita dal RSGSL.

13 ORGANIZZAZIONE DEL SISTEMA: INTEGRAZIONE NEI PROCESSI AZIENDALI E GESTIONE OPERATIVA

13.1 Scopo

Il successo di un SGSL sta nella sua piena integrazione nel seno della pianificazione, azione e controllo più generale della Banca, nel senso che ogni processo, ogni procedura deve contemplare gli aspetti di SSL.

Ciò in linea con la politica generale della Banca di cui la "politica" per la SSL è parte integrante e determinante e con gli obiettivi strategici verso cui è proiettata.

Questa impostazione porta ad una continua revisione ed aggiornamento, in tal senso, delle analisi dei processi e procedure, della definizione dei compiti e responsabilità e dei rilevamenti connessi al controllo operativo.

13.2 Applicabilità

Si applica a tutte le attività svolte dalla Banca e descritte nei capitoli "Scopo e campo di applicazione del SGSL".

13.3 Responsabilità

Il RSGSL, in collaborazione con il RSPP e con i Responsabili dei Servizi, individua le attività, i comportamenti, le funzioni della Banca che presentano aspetti rilevanti ai fini della SSL e predispone specifiche procedure, istruzioni operative o disposizioni.

Il DdL è responsabile dell'approvazione finale.

13.4 Azioni e metodi

L'identificazione dei requisiti legali e di altro tipo, la valutazione di conformità e la valutazione dei rischi sul lavoro forniscono indicazioni sugli elementi dell'attività della Banca che necessitano di regolamentazione.

Il RSGSL, in collaborazione con il RSPP, definisce il sistema di regolamentazione necessario per ciascuno di questi elementi e predispone specifiche procedure, istruzioni operative, disposizioni, corredandole della documentazione necessaria.

Procedure e istruzioni operative sono predisposte coinvolgendo i Responsabili dei Servizi e sono poi sottoposte al DdL per l'approvazione e successivamente emanate.

Tra gli elementi da sottoporre a regolamentazione saranno comunque compresi almeno:

- gestione delle emergenze;
- selezione e gestione dei dispositivi di protezione individuale;
- gestione degli incidenti;
- appalti imprese esterne;
- progettazione e realizzazione di processi, attrezzature, impianti;
- acquisti di servizi, materiali, macchinari e impianti;
- assunzione e qualificazione, inserimento, spostamento, cambio di mansioni dei lavoratori;
- sorveglianza sanitaria;
- organizzazione e funzionamento del SPP.

Potranno essere compresi inoltre i seguenti aspetti:

- esposizione ad agenti cancerogeni;
- esposizione ad agenti biologici;
- qualificazione e scelta dei fornitori e degli appaltatori;
- prevenzione incendi;
- manutenzione normale e straordinaria;
- pulizia;
- ecc.

I provvedimenti di regolamentazione adottati (procedure, istruzioni operative, ecc.):

- stabiliscono le corrette modalità operative da applicare nello svolgimento dell'attività lavorativa;
- contengono i divieti specifici e le specifiche di ciò che non deve assolutamente essere fatto;
- indicano le responsabilità dell'attività di gestione;

- indicano, se necessario, le modalità di registrazione delle attività e di eventi che sono o possono essere determinanti al fine di prevenire o ridurre gli impatti sulla SSL.

Le procedure, le istruzioni operative, le disposizioni sono riesaminate e revisionate in base all'esperienza acquisita, in particolare dopo che si è verificata un'emergenza o un incidente, tenendo conto, inoltre, delle segnalazioni ricevute dai lavoratori o dai RRLLS.

13.5 Documentazione e registrazioni

- Istruzioni operative
- Disposizioni
- Documentazioni previste dalla normativa vigente

La documentazione del SGSL è gestita dal RSGSL, che provvede alla distribuzione della documentazione aggiornata.

14 MONITORAGGIO

14.1 Scopo

Il monitoraggio costituisce una fase fondamentale del sistema perché consente ad ogni lavoratore, prima di ogni altro, di tenere sotto controllo la propria attività, riscontrando eventuali anomalie, non solo in termini di SSL ma anche in termini produttivi e qualitativi. La conoscenza degli eventuali scostamenti dagli obiettivi pianificati può evidenziare le eventuali carenze e far comprendere dove e come intervenire per assicurare il raggiungimento degli obiettivi preposti. Ciò è, a maggior ragione, valevole per il controllo sulla funzionalità del SGSL.

14.2 Applicabilità

Il monitoraggio si applica a tutti gli obiettivi pianificati ed a tutto il SGSL, come definito nel presente modello organizzativo.

14.3 Responsabilità

RSGSL, DdL, Responsabili dei Servizi, Preposti.

14.4 Azioni e metodi

Il monitoraggio vuole misurare in modo affidabile e ripetibile il funzionamento del SGSL, in tutte le sue parti componenti, nonché il miglioramento o il mantenimento delle condizioni di SSL.

Il RSGSL deve individuare per ciascun elemento il miglior modo di monitoraggio e deve elaborare un piano in cui siano chiaramente definiti i modi, i tempi e le responsabilità per il monitoraggio. Il RSGSL sottopone il piano dei monitoraggi al DdL che, dopo aver consultato i RRLLS, lo approva.

14.4.1 Monitoraggio di 1° livello

Il monitoraggio di 1° livello ha lo scopo di tenere sotto controllo le misure preventive e protettive predisposte dalla Banca in materia di SSL.

Il monitoraggio di 1° livello è svolto principalmente da parte del lavoratore e del Preposto. Le modalità di monitoraggio sono contenute nelle istruzioni operative, nelle quali sono riportate in modo chiaro quali siano le operazioni o prescrizioni da sorvegliare, quali metodi si debbano adottare per la sorveglianza, chi abbia la responsabilità del controllo e la frequenza di effettuazione del controllo. Se il monitoraggio comporta, per aspetti specialistici (ad esempio per verifiche strumentali), il ricorso ad altre risorse interne o esterne alla Banca questo è segnalato nelle istruzioni operative.

14.4.2 Monitoraggio di 2° livello

Il monitoraggio di 2° livello ha lo scopo di stabilire se il sistema è conforme a quanto pianificato e consente di raggiungere gli obiettivi, e se è correttamente applicato e mantenuto attivo.

Il monitoraggio di 2° livello viene effettuato a cura del RSGSL e del RSPD tramite verifiche ed ispezioni con frequenza almeno annuale e produce la segnalazione delle eventuali situazioni di non conformità.

Il monitoraggio della funzionalità del sistema deve consentire al DdL l'adozione delle decisioni strategiche di propria competenza, quali ad esempio l'adeguamento della politica di SSL o la redistribuzione dei compiti e responsabilità.

14.4.3 Trattamento delle non conformità

Il corretto trattamento delle non conformità costituisce l'indispensabile presupposto al funzionamento nel tempo del SGSL.

Le non conformità riscontrate nel corso del monitoraggio possono presentarsi ai diversi livelli su cui questo è articolato e richiedere diverse modalità di trattamento.

Le non conformità riscontrate nel monitoraggio di 1° livello richiedono un intervento immediato per il ripristino delle condizioni corrette, sia da parte del lavoratore, se questo rientra nelle sue competenze e capacità, sia da parte del superiore gerarchico. Le non conformità riscontrate nel monitoraggio previsto dalle istruzioni di SSL richiedono l'immediata segnalazione al superiore gerarchico, al RSPP ed al RSGSL per l'opportuno intervento per la rimozione del problema tecnico o organizzativo riscontrato.

Le non conformità riscontrate nel monitoraggio di 2° livello richiedono un riesame della correttezza delle istruzioni di SSL, della loro effettiva applicazione e delle azioni di informazione, formazione e sensibilizzazione attuate, anche per l'applicazione dei provvedimenti correttivi previsti.

Il RSGSL analizza le non conformità segnalate o riscontrate e stabilisce se siano riconducibili a problemi tecnici, comportamentali, o organizzativi; sulla base di questa analisi elabora e propone le variazioni alle procedure e istruzioni di SSL ed al programma di sensibilizzazione, informazione, formazione e addestramento.

Al verificarsi di un incidente, il Responsabile del Servizio presso il quale ha avuto luogo l'incidente avvia immediatamente le azioni correttive necessarie e segnala l'accaduto e l'intervento attuato al RSPP ed al RSGSL.

14.4.4 Relazione e monitoraggio

Il RSGSL raccoglie i risultati del monitoraggio di 1° e di 2° livello, le segnalazioni di non conformità integrate con l'indicazione delle azioni di trattamento attuate, le segnalazioni del RRLLS, ed elabora una relazione che sottopone al DdL prima della revisione annuale del sistema ed in ogni caso qualora si renda necessaria una revisione anticipata.

14.4.5 Caratteristiche e responsabilità dei verificatori

Nell'attribuire le responsabilità per l'effettuazione del monitoraggio debbono essere tenute in conto:

- la disponibilità in termini di tempo dei verificatori;
- il livello di esperienza richiesto nelle verifiche;
- la necessità di conoscenze specialistiche o esperienza tecnica;
- il livello di formazione.

In particolare, il monitoraggio di 2° livello è affidato a personale competente, obiettivo e imparziale, indipendente dal settore di lavoro ove effettua la verifica ispettiva.

In base alle responsabilità attribuite ed alle modalità di misurazione definite, il RSGSL deve far sì che i soggetti individuati siano in grado, per quanto di loro pertinenza, di:

- agire in conformità ai requisiti stabiliti per il monitoraggio e mantenersi entro l'ambito del monitoraggio stesso;
- approntare e adempiere con obiettività ed efficienza agli incarichi assegnati;
- seguire le procedure definite;
- raccogliere ed analizzare elementi, in particolare osservazioni e suggerimenti dei lavoratori e dei loro rappresentanti, che consentano di giungere a conclusioni relative all'efficacia del SGSL sottoposto al monitoraggio;
- prestare attenzione agli elementi che possono influenzarne gli esiti;
- documentare ed esporre i risultati del monitoraggio.

Il DdL può decidere autonomamente se avvalersi della collaborazione di personale esterno alla Banca per l'effettuazione di tutta o parte della verifica ispettiva del monitoraggio di 2° livello. In questo ultimo caso i soggetti incaricati dovranno prendere visione del presente modello organizzativo e della documentazione in esso prevista e presentare una relazione finale dell'attività di monitoraggio.

14.5 Documentazione e registrazioni

- Obiettivi di SSL
- Relazione finale di monitoraggio

I documenti sono conservati dal RSGSL.

15 RIESAME DEL SISTEMA

15.1 Scopo

Il riesame del sistema consente alla Direzione della Banca di ottenere gli elementi quantitativi e qualitativi atti a consentire una corretta e documentata valutazione sul funzionamento del sistema e sul raggiungimento degli obiettivi generali della Banca e sull'adeguatezza degli obiettivi stessi.

Questo esame sta alla base di uno sviluppo nel raggiungimento degli obiettivi di SSL nell'ottica del miglioramento continuo.

15.2 Applicabilità

Tutto il sistema di gestione SGSL, come descritto nel presente manuale.

15.3 Responsabilità

Il DdL ha la responsabilità del riesame del sistema.

Il RSGSL predispone la documentazione necessaria.

15.4 Azioni e metodi

Il riesame del DdL consiste nell'analisi del funzionamento del sistema nel suo complesso, sia dal punto di vista dell'adeguatezza dei requisiti di SSL stabiliti in funzione della realtà aziendale (politica di SSL), sia dal punto di vista dell'efficacia delle prestazioni di SSL del sistema (risultati).

Il risultato del riesame è l'individuazione delle opportunità e delle necessità di miglioramento del sistema e/o delle prestazioni di SSL.

Il DdL valuta se il sistema è correttamente strutturato rispetto alla realtà della Banca e ai suoi aspetti di SSL significativi, ed in particolare:

- se la politica, gli obiettivi e i traguardi stabiliti sono commisurati ai rischi effettivi;
- se il sistema è in grado di reagire ed adattarsi prontamente ai cambiamenti del contesto interno/esterno (nuove leggi, nuovi impianti, ecc.);
- se i risultati delle prestazioni di SSL corrispondono a quanto pianificato e se tali risultati sono mantenuti nel tempo in modo sistematico ed affidabile.

Il riesame è basato sull'analisi dei seguenti documenti del SGSL:

- risultati dei monitoraggi interni;
- segnalazioni delle non conformità e delle relative azioni correttive;
- segnalazioni degli incidenti;
- statistiche infortuni;
- azioni preventive proposte;
- rapporti sulle emergenze (reali o simulate);
- verbali delle riunioni periodiche;
- risultanze delle azioni di coinvolgimento del personale;
- risultanze delle consultazioni dei RRLS;
- grado di raggiungimento degli obiettivi di SSL.

Può venire utilizzato ogni altro documento utile del SGSL, oppure documenti specificamente richiesti al RSGSL, che ha la responsabilità di preparare preventivamente tutta la documentazione sopraelencata.

Vengono inoltre presi in considerazione altri aspetti quali:

- variazioni della legislazione;
- rilevanti modifiche a prodotti/processi/tecnologie;
- cambiamenti organizzativi;
- progetti di ampliamenti o rilocalizzazione;
- miglioramenti significativi di tecnologie di SSL o collegate;
- notizie di cronaca relative a incidenti/emergenze in situazioni analoghe.

Il DdL effettua il riesame almeno annualmente.

Se lo ritiene opportuno, il DdL può effettuare riesami anche ad intervalli più brevi ed anche limitati a specifici aspetti. Il riesame può inoltre avvenire a seguito di possibili eventi o situazioni particolarmente significativi che lo rendano necessario, segnalati dal RSGSL.

Da questo esame e tenendo sempre ben presente l'impegno al miglioramento e alla prevenzione, il DdL determina l'eventuale necessità di apportare variazioni alla politica, agli obiettivi o ai diversi elementi del SGSL.

Il riesame si conclude con l'eventuale revisione del modello organizzativo riportante i miglioramenti e le modifiche ritenute opportune; tali aggiornamenti, modifiche o integrazioni sono comunicati a tutte le funzioni aziendali ed a tutto il personale, nei modi previsti ai capitoli 9 e 10.

15.5 Documentazione e registrazioni

- Verbale della riunione periodica
- Relazione finale di monitoraggio
- Verbale di sintesi del riesame
- Segnalazioni incidenti
- Comunicazioni interne ed esterne

I documenti sono conservati dal RSGSL.

