LA GESTIONE DEL RISCHIO INDUSTRIALE

Concetto Aprile, Paola De Nictolis, Michele Messina, Eugenio Tagliani

1. Premessa

Le direttive dell'Unione Europea, sia per quanto riguarda la sicurezza nei luoghi di lavoro che per quanto attiene al controllo dei pericoli di incidenti rilevanti connessi con la produzione, impiego e trasporto di sostanze pericolose, prevedono, per gli stabilimenti industriali, l'adozione di misure di sicurezza nell'ambito di una organica politica di prevenzione degli incidenti e gestione del rischio.

In Italia, i gestori delle attività soggette alla normativa Seveso hanno presentato i rapporti di sicurezza che sono stati già valutati dall'Autorità Competente (Comitati Tecnici Regionali di Prevenzione Incendi integrati ai sensi dell'art.19 del decreto legislativo 334/99).

Sulla base delle conclusioni delle istruttorie dei rapporti di sicurezza, l'Autorità Pubblica dovrà procedere alla **pianificazione di emergenza esterna** agli stabilimenti ed all'attuazione del decreto 9 Maggio 2001 relativo ai **requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale** per le zone interessate da stabilimenti a rischio di incidente rilevante.

L' Autorità Pubblica, inoltre, dovrà fornire, in modo puntuale, le informazioni (riguardanti le misure di sicurezza da adottare e le norme di comportamento da osservare in caso di incidente) ad ogni persona e ad ogni struttura frequentata dal pubblico che possono essere colpite da un incidente industriale.

Per la gestione del rischio industriale, oltre le "**linee guida per l'attuazione del sistema di gestione della sicurezza"** (cfr. decreto Ministero Ambiente del 9 Agosto 2000), l'Autorità Pubblica dovrà individuare le aree ad elevata concentrazione di stabilimenti industriali e definire i criteri di valutazione dell' **"effetto domino".**

I gestori, a loro volta, dovranno rielaborare, in applicazione della direttiva comunitaria 2003/105/CE del 16 dicembre 2003 e della emananda legge di recepimento italiana, il **piano di emergenza interno** consultando il personale che lavora nello stabilimento, ivi compreso il personale delle imprese subappaltatrici a lungo termine.

Sarà loro compito, inoltre, promuovere e realizzare sistematici interventi di formazione del personale addetto alla gestione dei rischi di incidente, ad ogni livello di organizzazione dell'azienda, coinvolgendo il personale delle imprese subappaltatrici che lavorano nello stabilimento.

In definitiva, la normativa europea prevede compiti differenziati per il gestore e per la Pubblica Amministrazione:

- per il gestore: l'obbligo di effettuare la valutazione dei rischi connessi alla propria attività, di definire la politica di prevenzione degli incidenti e di attuare il sistema di gestione della sicurezza;
- per la Pubblica Amministrazione: validazione delle analisi di rischio effettuate dal gestore, controlli e verifiche delle misure di sicurezza adottate, prescrizione di eventuali interventi migliorativi, informazione della popolazione, pianificazione dell'emergenza esterna e controllo dell'urbanizzazione.

Inoltre, si dovrà affrontare la questione della tollerabilità del rischio associato alle attività umane, tenuto conto degli aspetti sociale ed economico, per valutare la sua accettabilità e compatibilità con la qualità della vita.

Tutto ciò premesso, anche in relazione alle **attuali emergenze planetarie** (**rischi di attentati terroristici**), è necessario approfondire le tematiche inerenti i **fattori incontrollabili di incidente** al fine di fornire indicazioni ai gestori per una migliore gestione del rischio industriale.

2. La gestione del rischio industriale

Le maggiori difficoltà si incontrano nel controllo di alcuni pericoli, dalle caratteristiche non facilmente definibili, per i quali i classici metodi di analisi del rischio devono essere criticamente valutati, modificati e testati, per una loro efficace applicazione.

Vi sono fattori cioè che sfuggono alle analisi deterministiche perché presentano aspetti sociali e politici che richiedono un approccio più variegato, anche comunque sistematico. Tra questi fattori: instabilità sociale e politica, nazionale ed internazionale; condizioni di stress ed insoddisfazione personale tra gli addetti.

Altre attività hanno un elevato margine di incertezza; tra queste:

- attività a prevalente controllo umano;
- attività quasi integralmente automatizzate/computerizzate, per le quali un eventuale attacco di pirateria informatica potrebbe avere conseguenze molto gravi e comunque non facilmente prevedibili.

Oltre a ciò, i rischi intrinseci delle attività industriali a rischio di incidente rilevante, spesso ben individuati e governabili con strumenti consolidati di analisi e gestione, a tutt'oggi non sono affrontati in modo del tutto sistematico.

Quello che sembra mancare, complessivamente, è una incisiva azione di Risk Management, svolta con adeguate risorse economiche ed umane.

Nella sua più ampia e corretta accezione infatti, con il termine Risk Management si identifica la gestione di tutte le problematiche di rischio dell'azienda: economiche, finanziarie, ambientali, di processo, di *safety* e *security*, informatiche, ecc.

Raramente è presente una figura di coordinatore per tutti gli aspetti coinvolti, col ruolo di armonizzare i progetti di difesa, prevenzione e protezione, per produrre un sistema integrato che offra le migliori garanzie di successo e ottimizzazione delle risorse.
Deve quindi nascere una filosofia progettuale e gestionale/organizzativa capace di analizzare le singole problematiche e di sintetizzale in un progetto integrato di sicurezza.

3. La sicurezza integrata

I vari aspetti della sicurezza vengono analizzati sia separatamente che in relazione reciproca, in modo da adattare le valutazioni e le scelte alle esigenze complessive di protezione.
Alla base di questa impostazione ci sono l'esperienza e le diverse professionalità dei tecnici, meglio se in un gruppo di lavoro, che intervengono sia a livello progettuale che ispettivo, consentendo un approccio semplice ed efficace.
D'altra parte il D. Lgs. 334/99 richiede implicitamente un'analisi di sicurezza integrata sulle attività soggette, con l'adozione di specifiche misure di difesa anticrimine che si aggiungano a quelle di prevenzione e protezione nei riguardi di incendi, esplosioni, emissioni, ecc.: tale estensione dell'analisi dei rischi diventa ancora più necessaria dopo i recenti atti di terrorismo internazionale.
Su un altro fronte, recenti statistiche indicano l'aumento degli incendio dolosi o presunti tale, sia in Italia che negli altri paesi occidentali, con conseguente lievitazione degli oneri sociali che gravano direttamente sulle proprietà ed attività danneggiate e indirettamente sull'intera collettività, secondo il principio di mutualità che sta alla base dell'attività assicurativa.
Questo, oltre a rappresentare un ulteriore elemento di spinta alla formazione di specialisti nell'investigazione incendi e allo sviluppo di un approccio sistematico per l'individuazione delle cause d'incendio, dovrebbe far riflettere sull'esigenza di elevare il livello di protezione contro il dolo. Ecco che le due discipline - Prevenzione Incendi e sicurezza anticrimine - devono integrarsi, per offrire concrete possibilità di successo.
Tale approccio si traduce:

- da un lato nell'utilizzo sistematico di strumenti ingegneristici di studio, analisi e progettazione che utilizzano i più recenti risultati della ricerca scientifica e tecnologica;
- dall'altro nell'applicazione concreta del Risk Management e della Risk Analysis alle realtà produttive interessate, coinvolgendo anche aspetti economici e di mercato, oltre che squisitamente tecnici.

L'analisi del rischio è peraltro il fondamento di ogni indagine finalizzata sia alla progettazione che alla verifica dei sistema di sicurezza.

Nei paesi anglosassoni o scandinavi, così come in Belgio o in Francia, le compagnie di assicurazione richiedono specifiche misure di prevenzione e protezione quale condizione necessaria per concedere la copertura assicurativa; tali misure, a seconda della loro estensione e tipologia, consentiranno all'assicurato di ottenere condizioni di polizza più vantaggiose, e contemporaneamente di ridurre i costi sociali grazie alla probabile diminuzione dei sinistri, frutto di un più elevato livello di sicurezza.

Da questo punto di vista le compagnie di assicurazione sono particolarmente attive nei confronti della prevenzione da fare attuare alle aziende.

Ma il discorso va anche oltre, non limitandosi ad una richiesta generica né alla mera constatazione dell'esistenza delle misure di sicurezza, ma dedicando attenzione e spazio anche alla verifica di rispondenza degli impianti alle norme di buona tecnica di riferimento.

Secondo questa logica, quindi, l'assicuratore europeo tende a promuovere la prevenzione, attività questa che dovrebbe svolgersi nel nostro Paese in sinergia tra le aziende, le compagnie di assicurazione/riassicurazione e gli organismi di controllo.

Il ruolo dell'assicuratore è particolarmente importante e dovrebbe essere caratterizzato da una maggiore intransigenza di fronte ad eventuali carenze riscontrate in fase di sopralluogo. Il rilascio della "copertura assicurativa" dovrebbe allora essere subordinato all'adozione, da parte dell'azienda, delle necessarie misure di prevenzione e protezione che consentano di riportare il rischio nel campo dell'assicurabilità.

Quindi occorrerebbe anche la valutazione rigorosa delle misure anticrimine, integrate con quelle antincendio ed antinquinamento.

Purtroppo la competizione commerciale produce alcune distorsioni in questo meccanismo, che inevitabilmente portano ad uno scollamento tra l'attuazione di una corretta prevenzione incendi e l'attività assicurativa, con il risultato che, in molte aziende, il livello di rischio rimane ancora troppo elevato.

L'assicurato, da parte sua, ritiene più vantaggioso trasferire interamente il proprio rischio alla compagnia di assicurazione che gli concede una polizza con elevati massimali, così da garantirsi anche contro incendi di grave entità, magari accettando elevati scoperti e franchigie. Appare evidente come, nel campo dei rischi rilevanti, le ripercussioni di un approccio carente possano essere pesantissime.

4. La *Security*

Le aziende soggette alla normativa "Seveso" finora non hanno affrontato gli aspetti di security in modo organico. Alla luce degli attuali fattori di instabilità e di rischio a livello internazionale, si impone invece un cambio di strategia.

La security deve quindi essere gestita al pari della safety, cioè della sicurezza dei processi e contro gli incendi, esplosioni, rilasci.

Perché si sviluppi un modello efficace occorrono:

- Leadership della Direzione, attraverso le procedure, il coinvolgimento, le comunicazioni, le risorse umane;
- Chiara responsabilità, definita attraverso l'organizzazione interna;
- Verifica dell'efficienza delle misure di sicurezza, ispezioni, implementazione continua;
- Richiesta di informazioni agli Enti preposti alla sicurezza pubblica circa potenziali minacce, per identificare i punti deboli del sistema;
- Stesura di rapporti a seguito di sinistro o mancato incidente, completo di indicazioni sulle vulnerabilità emerse;
- Condivisione delle esperienze negative con altre aziende (intrusioni, furti, sabotaggi, manomissioni – avvenuti o tentati).

Di seguito analizziamo i singoli aspetti.

<u>Analisi del rischio – vulnerabilità</u>

Vengono esaminati i siti, installazioni, attrezzature e risorse vulnerabili rispetto ai pericoli identificati e si determinano le idonee contromisure, proporzionate al livello di rischio.

I punti critici vengono periodicamente riesaminati e, se necessario, le misure di prevenzione e protezione vengono adeguate. Qualsiasi modifica di strutture, lay-out, organizzazione, deve passare al vaglio dei responsabili della sicurezza-security, che valuteranno le ripercussioni sul sistema.

Procedure di sicurezza

Vengono innanzitutto esaminate l'organizzazione interna aziendale e le attività dei singoli reparti e persone, individuando operazioni, percorsi, attività, accessi e responsabilità significative ai fini della sicurezza fisica.
Sono poi adottate le congrue misure di sicurezza, sul piano procedurale, secondo una logica gerarchica di autorizzazioni, permessi e responsabilità.
Tali misure procedurali devono essere estese a tutto il personale, in modo diversificato, compresi dirigenti, fornitori, personale di sorveglianza, dipendenti di ditte terze.

Report di incidenti (o quasi incidenti) ed indagini

Ogni fatto che abbia pertinenza con la violazione delle misure di sicurezza, fisiche o procedurali, deve essere esaurientemente investigato, per individuare eventuali carenze o necessità di rafforzare le misure in essere o estendere la prevenzione in altra direzione.
Esempi, non esaustivi, di situazioni di interesse:

- segnali di tentativi di intrusione;
- presenza o passaggio di persone o mezzi non autorizzati in aree ad accesso limitato oppure lungo percorsi interdetti, quali recinzioni, condotte, sottostazioni elettriche o cabine gas;
- richiesta di informazioni tecniche specifiche e delicate da parte di persone estranee o senza ruoli adeguati in azienda;
- anomalie di processo non spiegabili in modo tecnico o non riconducibili a cause plausibili;
- assenza o diminuzione non spiegabile di materiali/sostanze pericolose.

Protezione delle informazioni

Le informazioni sensibili devono essere identificate e quindi protette.
Esse possono riguardare:

- il lay–out interno con le apparecchiature, serbatoi, reattori, depositi, maggiormente vulnerabili;
- i sistemi operativi che controllano le apparecchiature di processo;
- i sistemi operativi di gestione dell'intera attività.

E' ormai reale e temibile il rischio di un attacco terroristico condotto attraverso le reti informatiche, capace di interagire con i suddetti sistemi operativi, se non adeguatamente protetti.

Gestione dei processi

Occorre sviluppare la capacità di interrompere rapidamente ed in sicurezza i processi pericolosi/critici, ricorrendo sia a sistemi tecnici che alla formazione e addestramento dei lavoratori.

Specifiche misure anticrimine

Quando si teme un'azione criminosa su obiettivi sensibili quali le industrie ad alto rischio, bisogna mettere in campo tutte le misure anticrimine, integrate in un più ampio sistema che comprende le misure di sicurezza antincendio e di processo.

Saranno utilizzati:

- barriere antintrusione;
- rivelatori di tipo perimetrale quali contatti magnetici, microfoni selettivi, rivelatori di vibrazione, ecc.;
- rivelatori volumetrici;
- sistemi a cavo sensibile, interrato o meno;
- sistemi di videosorveglianza;
- sistemi di controllo accessi.

Problematiche ambientali – inquinamento

Se da un lato il progresso scientifico contribuisce notevolmente a raffinare l'analisi dei rischi, dall'altro l'avanzamento tecnologico (per la costante innovazione di processi e prodotti e la crescente concentrazione di risorse) introduce nuove tipologie di rischio e aumenta il livello di vulnerabilità dei sistemi.

I costi di un evento incidentale sono funzione, in generale, di:

- caratteristiche del processo;
- modalità di accadimento;
- sensibilità dell'area;
- entità economica del danno da risarcire.

Elenchiamo di seguito le principali tipicità del rischio di inquinamento.

- Carattere improvviso oppure graduale del rilascio. E' evidente che il primo può configurare situazioni molto più temibili, per via delle quantità di prodotto rilasciate e dell'esposizione immediata delle persone;
- Variabilità dei fattori di rischio. Esistono attualmente circa 10 milioni di composti chimici conosciuti ed ogni anno se ne aggiungono altri nuovi 4.000 circa. Ne consegue un aumento del grado di incertezza, in particolare nella valutazione preventiva delle possibili conseguenze sull'uomo e sull'ambiente del generico composto. Anche in campo tecnologico l'evoluzione ed il progresso delle tecniche produttive ed impiantistiche fanno aumentare la complessità e quindi la vulnerabilità dei sistemi.
- Specificità nell'analisi dei rischi: eventi con bassa probabilità di accadimento e alta magnitudo delle conseguenze. Tra i metodi utilizzati nell'analisi dei rischi, quello dell'analisi storica degli eventi incidentali riveste un ruolo particolarmente importante. E' evidente che se una banca dati contiene pochi eventi, la significatività dell'analisi e dei risultati può essere fortemente compromessa. Inoltre, per gli eventi mai occorsi il margine di aleatorietà degli effetti rimane molto elevato, pur utilizzando adeguate tecniche di analisi e proiezione.
- Rapporto causale. E' molto difficile individuare con certezza i responsabili di un danno di tipo graduale (rilascio ridotto ma continuato nel tempo) in aree a forte concentrazione industriale e per prodotti a largo impiego o diffusione.
- Differimento temporale tra accadimento dell'evento e manifestazione del danno. In particolare, non sono noti gli effetti secondari e ritardati di molte sostanza chimiche sull'uomo.

Per far fronte a queste problematiche, oltre a disporre di figure di Risk Manager ad alta specializzazione, occorre prevedere una gestione assicurativa adeguata al livello dei danni potenziali in caso di incidente e alll'aleatorietà dei fattori di rischio.

A tale scopo opera, già dal 1980, il *Pool Inquinamento per l'assicurazione e la riassicurazione della responsabilità civile per danni a terzi da inquinamento*, istituito per innalzare il livello professionale degli assicuratori e per offrire copertura completa (rilasci continui o conseguenti a un incidente rilevante).

5. La misurazione del rischio

Per ogni unità di rischio occorre individuare le caratteristiche di:

- Frequenza: numero di sinistri, riconducibili al rischio in esame, che l'azienda potrebbe subire nell'arco di tempo considerato;
- Gravità: entità dei danni prodotti dal singolo sinistro:
- Perdite potenziali: perdite dovute ai sinistri previsti nell'arco di tempo considerato.

I suddetti parametri possono essere indagati trmite diverse tecniche, riconducibili a due macro-categorie:

- tecniche statistiche
- tecniche discrezionali.

Le tecniche statistiche utilizzano la statistica inferenziale e sono idonee se le informazioni storiche sul rischio sono numerose e significative.

Tale tipo di statistica analizza un campione di eventi occorsi, per ottenere *proiezioni* degli andamenti futuri.

La raccolta delle informazioni (il più possibile complete ed omogenee) rappresenta la fase più delicata.

Le tecniche discrezionali implicano una valutazione discrezionale dell'analista e sono preferibili se le informazioni storiche sui sinistri sono nulle o molto carenti.

Queste tecniche si basano essenzialmente sull'esperienza e conoscenza dello specifico rischio da parte del valutatore. In questo caso occorrono delle linee guida per *oggettivizzare* l'analisi.

Per esempio, si possono stabilire le seguenti scale:

<u>Frequenza</u>

- *pressoché nulla*
- *lieve*
- *moderata*
- *definita*

<u>Gravità</u>

Quella conseguente a:

NLE - *Normal Loss Expectancy – tutti i mezzi di protezione disponibili, interni ed esterni.*

PML – *Probable Maximum Loss – disponibili solo alcuni mezzi interni e tutti gli esterni*

MFL – *Maximum Foreseeable Loss – nessun mezzo interno disponibile ma tutti gli esterni*

MPL – *Maximum Possible Loss – nessun mezzo disponibile, né interno né esterno*

Viene, in conclusione, determinato l'ammontare massimo di perdite annue raggiungibile, che può essere puro oppure corretto, nel caso in cui le perdite ipotizzate siano ridotte con azioni di prevenzione e di trasferimento del rischio.

6. Conclusioni

Per una svolta nella politica di sicurezza globale occorre in sintesi:

- introdurre una o più figure di Risk Manager in azienda, debitamente formati e qualificati;
- piena attuazione dei Sistemi di Gestione della Sicurezza;
- coinvolgimento dei lavoratori, a tutti i livelli, nell'attività di pianificazione e gestione della sicurezza;
- formazione specifica e frequenti esercitazioni di emergenza;
- corretta analisi e gestione dei mediante strumenti tecnici ed organizzativi di prevenzione e protezione, da un lato, ed un adeguato trasferimento del rischio, dall'altro.
- riqualificazione e responsabilizzazione delle compagnie di assicurazione nell'assunzione del rischio;
- potenziamento della rete ispettiva degli Enti preposti, con finalità "formative" nei confronti delle aziende più che repressiva;
- confronto sistematico tra le parti interessate.