



DERRIS

Il clima cambia. Riduciamo i rischi.

LA GESTIONE DEI RISCHI E DELLE EMERGENZE

Ing. Marco Santinato
Azione E2 - Piattaforma web DERRIS

Settembre 2017



Marco Santinato, docente Cineas.

Laurea in Ingegneria Chimica presso il Politecnico di Milano. Dopo esperienze nel Gruppo ENI e nella Consulenza d'Impresa nel campo delle valutazioni patrimoniali di aziende per fusioni e transazioni (M&A), ha operato all'interno di un grande Gruppo Assicurativo Internazionale ricoprendo nel tempo la responsabilità di diverse strutture organizzative: Risk Engineering e Risk Management, Direzione Assuntiva del Settore Aziende, Direzione Motor Fleet e infine Canale Partnership nell'ambito della Direzione Reti di Vendita.

Ha ricoperto anche il ruolo di Head of the Automotive Center of Competence, Italy. Dal 2011 è amministratore delegato di Per Consulting srl, la Società di Consulenza nel campo del Risk Management del Gruppo Per. Dal 1998 è docente di Risk Management presso il CINEAS al Politecnico di Milano. È stato Coordinatore del Master in Risk Engineering dal 2003 al 2007 e Membro del Consiglio di Amministrazione di CINEAS dal 2000 al 2010. È relatore in seminari di settore e in Università, ed è autore di numerosi articoli e pubblicazioni in materia di Risk Management e di Business Continuity.



INDICE

1.

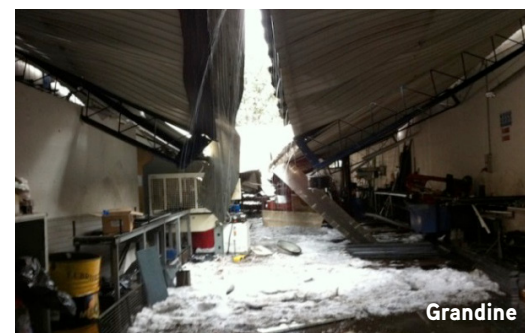
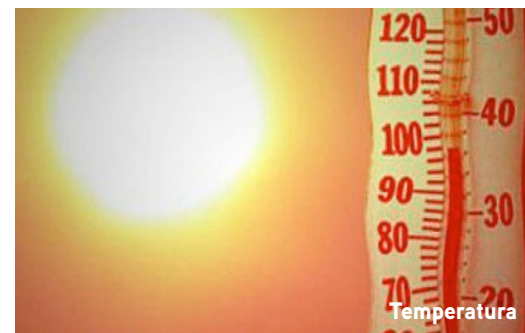
LA GESTIONE DEL RISCHIO E LA RESILIENZA

Il rischio è insito in tutte le attività e saperlo gestire in modo corretto può diventare un importante fattore di successo per qualsiasi organizzazione. Ogni evento inatteso rischia infatti di avere ripercussioni critiche, tali a volte da mettere in gioco la sopravvivenza stessa delle attività svolte.

Questo è ancora più vero nella situazione attuale, dove la vulnerabilità delle imprese (di ogni settore e dimensione) e delle strutture e infrastrutture della Pubblica Amministrazione è aumentata notevolmente per effetto del **cambiamento climatico**, della crisi finanziaria e delle perturbazioni di un mercato sempre più globalizzato.

Negli ultimi 50 anni, in particolare, gli eventi catastrofici legati al cambiamento climatico nel mondo si sono quintuplicati in numero e sono aumentati di 15 volte in termini di costi e l'Italia, con una lunga tradizione di dissesto idrogeologico (CAT/NAT) non fa eccezione.

Molto spesso i budget limitati inducono le Piccole e Medie Imprese (PMI) e le Microimprese, così come la Pubblica Amministrazione (PA), a sottovalutare le conseguenze di un mancato controllo dei rischi, perdendo così di vista anche un altro punto chiave: ogni **rischio**, se conosciuto, gestito e controllato può diventare una importante **opportunità per riconfigurare le attività e i processi, creando valore aggiunto e importanti vantaggi competitivi**.





A questo proposito è interessante osservare i risultati del recente studio dell'**Osservatorio CINEAS**, realizzato in collaborazione con **Medio-banca** e **focalizzato sulle PMI italiane**:

- > le imprese che gestiscono correttamente i rischi (**Risk Management**) hanno risultati economici e finanziari **migliori mediamente del 31% rispetto alle altre**
- > le imprese che gestiscono il rischio hanno potenzialmente un più facile accesso al credito
- > rispetto alle precedenti edizioni dello studio, il rischio finanziario, che era il più percepito, viene sostituito dai rischi informatici, legali e operativi (fra i quali quelli legati al **cambiamento climatico**).

In generale, la normale routine di qualsiasi attività può essere scossa da eventi inattesi che possono dare luogo a situazioni di **emergenza**.

Questi eventi possono innescare situazioni di vera **crisi**, ovvero di grave difficoltà, con risvolti sulla capacità produttività / di erogazione di servizi (tipicamente nel caso della PA), sulla competitività sul mercato e sull'immagine e reputazione.

Quando si verificano situazioni di crisi, i processi operativi vengono compromessi più o meno pesantemente. In caso di crisi, la sopravvivenza dell'attività dipende dalla sua capacità e rapidità di reazione, ovvero dalla sua «**resilienza**».

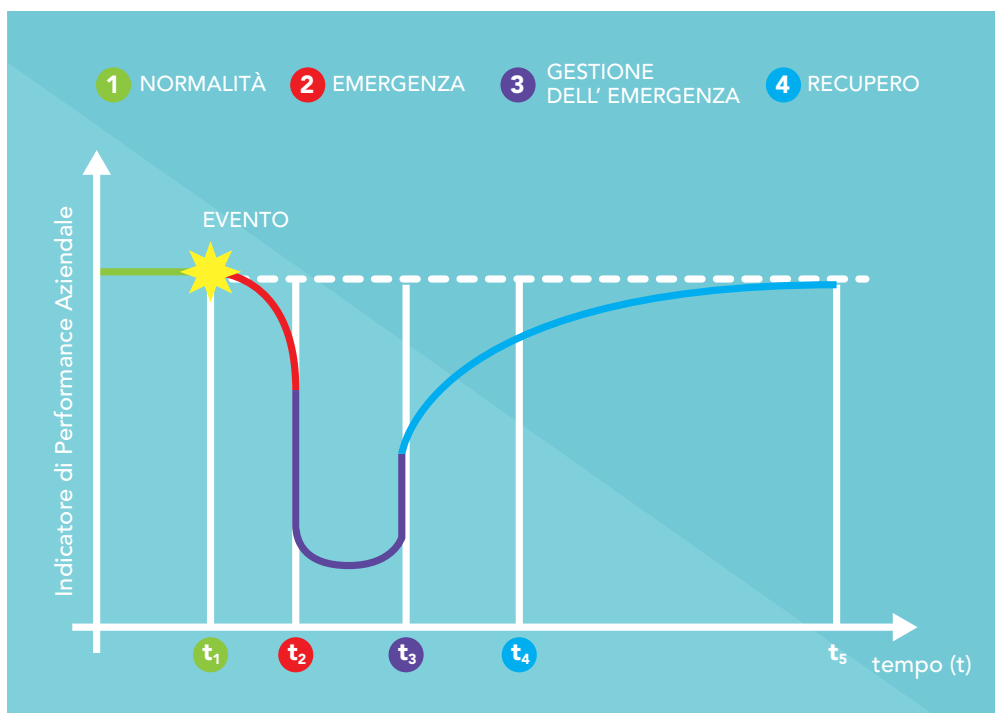


Fig. 1: Rappresentazione di una crisi con recupero delle condizioni iniziali.

La Resilienza è la capacità di un materiale di resistere ad urti improvvisi senza spezzarsi, ma nell'ambito della strategia aziendale, per **resilienza** s'intende la **capacità e rapidità di un'organizzazione a ritornare nelle condizioni precedenti dopo un evento dirompente**. In queste situazioni, il tempo di reazione diventa un fattore di successo determinante. L'obiettivo fondamentale (v. Fig. 1) è quindi quello di ritornare alla situazione preesistente l'evento, evitando le evoluzioni negative descritte nella Fig. 2.

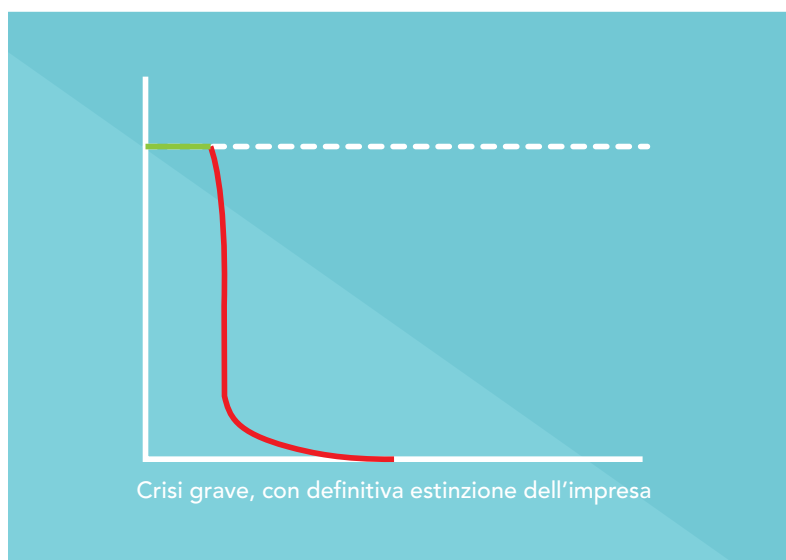
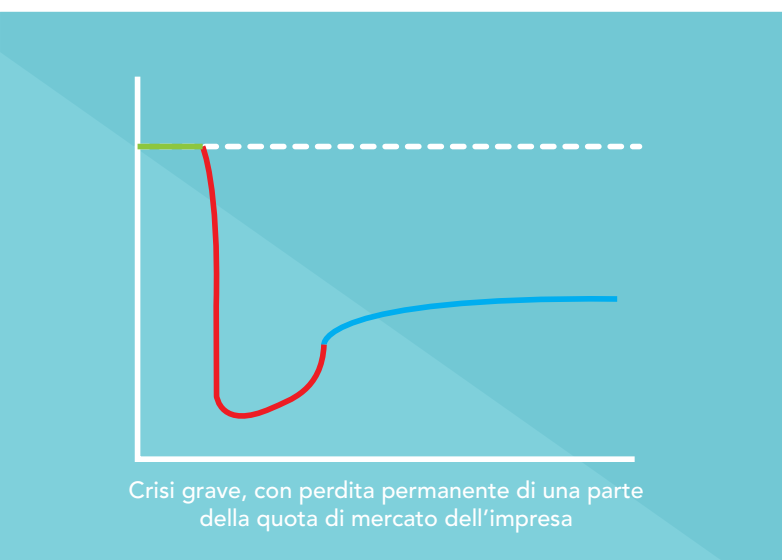


Fig. 2: Evoluzione negativa di una crisi.

Con queste premesse, ogni soggetto (impresa e area della PA) dovrebbe proteggere i fattori produttivi (materiali e immateriali) che ha a disposizione, ovvero **salvaguardare gli elementi fondamentali che sono alla base dei propri processi**, e in particolare:

- › **i propri beni (il patrimonio aziendale)**
- › **la Continuità Operativa (la capacità di continuare la produzione/l'erogazione di servizi nel tempo).**

Salvaguardare le attività (cioè “proteggerle efficacemente”) comporta il passaggio a un nuovo modo di operare denominato **“Gestione dei Rischi”**.

Con il termine **Gestione dei Rischi** (o Risk Management) si intende la **Gestione integrata dei rischi in una organizzazione (Azienda/PA), mediante la conoscenza, l'eliminazione, la riduzione, il trasferimento e il controllo dei rischi stessi.**

Lo Standard di riferimento in questo ambito è oggi definito dalla norma **UNI ISO 31000:2010 (“Gestione del rischio - Principi e linee guida”)**. Anche la nuova edizione della Norma **UNI ISO 9000:2015** fa riferimento esplicito alla necessità di adottare in azienda un approccio di questo tipo.

Gestire i Rischi in modo integrato comporta numerosi benefici. Fra questi:

- › una **migliore protezione dei fattori produttivi** (materiali e immateriali), a cui fa seguito una possibile riduzione, in caso di sinistro, dei danni materiali subiti dai beni stessi (**Danni Diretti**)
- › una **migliore protezione della continuità operativa** dei processi/delle attività aziendali, a cui fa seguito una possibile riduzione, in caso di sinistro, della perdita di fatturato conseguente alla indisponibilità dei beni aziendali danneggiati (i cosiddetti **Danni Indiretti**)
- › una maggiore **stabilizzazione dei flussi di cassa**, anche in presenza di un evento incidentale
- › un **miglioramento del profilo dell'azienda/PA presso il mercato bancario e finanziario**, che si traduce in un più facile accesso al credito e in generale ai servizi bancari
- › un **miglioramento del “profilo di rischio” verso il mercato assicurativo**, che si può tradurre nell'ottenimento di condizioni assicurative più favorevoli da parte delle Compagnie di Assicurazione
- › un **miglioramento della propria Reputazione e immagine** nei confronti del mercato e dell'opinione pubblica in generale.

La Gestione dei Rischi (Fig.3) si sviluppa secondo un processo che comprende 4 fasi:

- > L'individuazione e la quantificazione dei rischi (**ANALISI E VALUTAZIONE DEI RISCHI**)
- > Lo studio degli interventi possibili di **RIDUZIONE DEI RISCHI**
- > Il **TRASFERIMENTO** (ad esempio assicurativo) dei rischi ritenuti non accettabili
- > La verifica dell'accettabilità dei rischi ritenuti (**RITENZIONE**)



Fig. 3: Il processo di "Gestione dei Rischi".

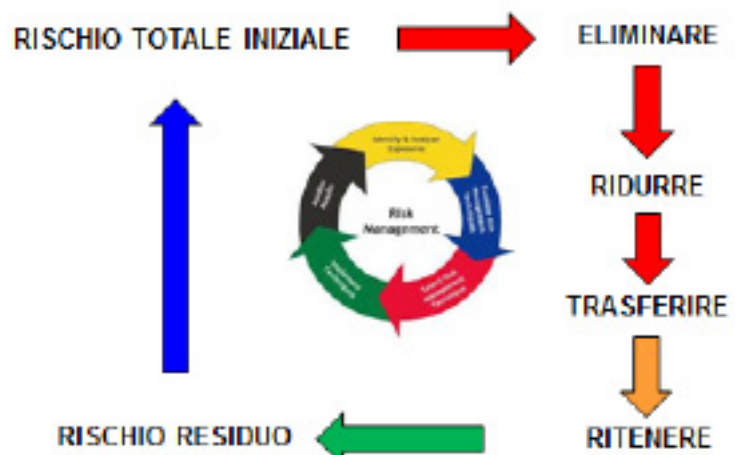
Il primo passo del processo (**Analisi e Valutazione dei Rischi**) ha per scopo:

- > L'**Identificazione** dei principali scenari di rischio che possono interessare l'organizzazione (azienda, PA) causando un'interruzione significativa dei suoi processi
- > La **Quantificazione** degli scenari di rischio di cui sopra in termini di **probabilità di accadimento (P)** e di **severità dell'evento (S)**

I passi successivi sono:

- > La **Definizione** e la **proposta delle opportune misure correttive** (eliminazione, riduzione)
- > Il **Trasferimento** dei rischi non accettabili
- > La Verifica dell'accettabilità dei Rischi Ritenuti.

È molto importante re-iterare periodicamente le attività di cui sopra (Fig. 4), poiché nel tempo l'organizzazione può mutare / evolvere, così come le condizioni al contorno (il clima, il mercato di riferimento, ecc...).



2.

GLI SCENARI DI RISCHIO

Il Rischio (o Scenario di Rischio) può essere espresso come segue:

$$R = H \times V \times E$$

dove:

- › **H (Pericolosità - H, Hazard)**: è la probabilità di accadimento di un evento
- › **V (Vulnerabilità) - V, Vulnerability**: è la propensione di un bene a subire un danno
- › **E (Elementi a rischio o Esposizione -E, Exposure)**: è il valore economico del bene

Il rischio può anche essere definito come il prodotto della Probabilità (P) di accadimento di un evento per la Severità (S) degli effetti dannosi conseguenti:

$$R = P \times S$$

Con riferimento al **cambiamento climatico**, gli **scenari di rischio** considerati sono i seguenti:
alluvione, pioggia, vento, fulminazione, grandine, temperatura e franamento.

Gli Effetti associati agli scenari di cui sopra possono essere espressi in termini di:

- › **Effetti patrimoniali**: che incidono sul valore dei beni materiali e immateriali dell'organizzazione
- › **Effetti reddituali**: che incidono sulla capacità da parte dell'organizzazione di generare reddito (valore) nel tempo
- › **Effetti sulle persone**: che si riferiscono ai danni alle risorse umane dell'organizzazione e/o a terze persone.

Secondo il linguaggio assicurativo, gli effetti possono essere espressi in termini di:

- > **Danni Diretti** (**Property Damage – PD**): danni ai fattori produttivi materiali (risorse umane, macchinari, attrezzature, edifici, merci, ecc...)
- > **Danni Indiretti** (**Business Interruption – BI**): perdita di produzione / profitto lordo, margine di contribuzione
- > **Danni Conseguenziali** (**Consequential Damages**): ripercussioni sull'immagine dell'organizzazione presso il mercato, le autorità, il mondo finanziario; perdita di quote di mercato; deterioramento delle relazioni con clienti e partner strategici; ripercussioni sul valore finanziario dell'impresa; difficoltà di accesso a crediti erogati dal sistema bancario; perdita di documentazione / informazioni chiave/sensibili, ecc.)

3.

L'ANALISI E LA VALUTAZIONE DEL RISCHIO

L'Analisi e la Valutazione del Rischio è il processo logico che porta all'individuazione dei possibili eventi anomali/ incidentali che si possono verificare e alla valutazione delle loro conseguenze. Poiché ogni organizzazione (impresa / PA) è un sistema articolato e complesso, l'identificazione degli scenari di rischio deve procedere attraverso un percorso strutturato, rigoroso e chiaro: è quindi necessario seguire un **approccio sistemico**.

Le domande chiave che ci si deve porre in questa fase sono le seguenti:

- › **Quali sono i punti deboli** (o di vulnerabilità) dell'organizzazione verso i rischi derivanti dal cambiamento climatico nel contesto nel quale opera?
- › Cosa viene fatto per **ridurre la probabilità** che si verifichino eventi dannosi?
- › Cosa viene fatto per **ridurre la severità** di tali eventi?

Il primo passo nella Analisi e Valutazione dei Rischi è costituito dalla raccolta e dalla elaborazione di tutte le informazioni disponibili. Queste sono, **con particolare riferimento agli scenari legati al cambiamento climatico**:

3.1. INFORMAZIONI SUL CONTESTO GEOGRAFICO OVE SORGE L'ATTIVITÀ (IMPRESA/PA)

- Mappe relative alla pericolosità idrogeologica (Fig.5)
- Altre Mappe di pericolosità

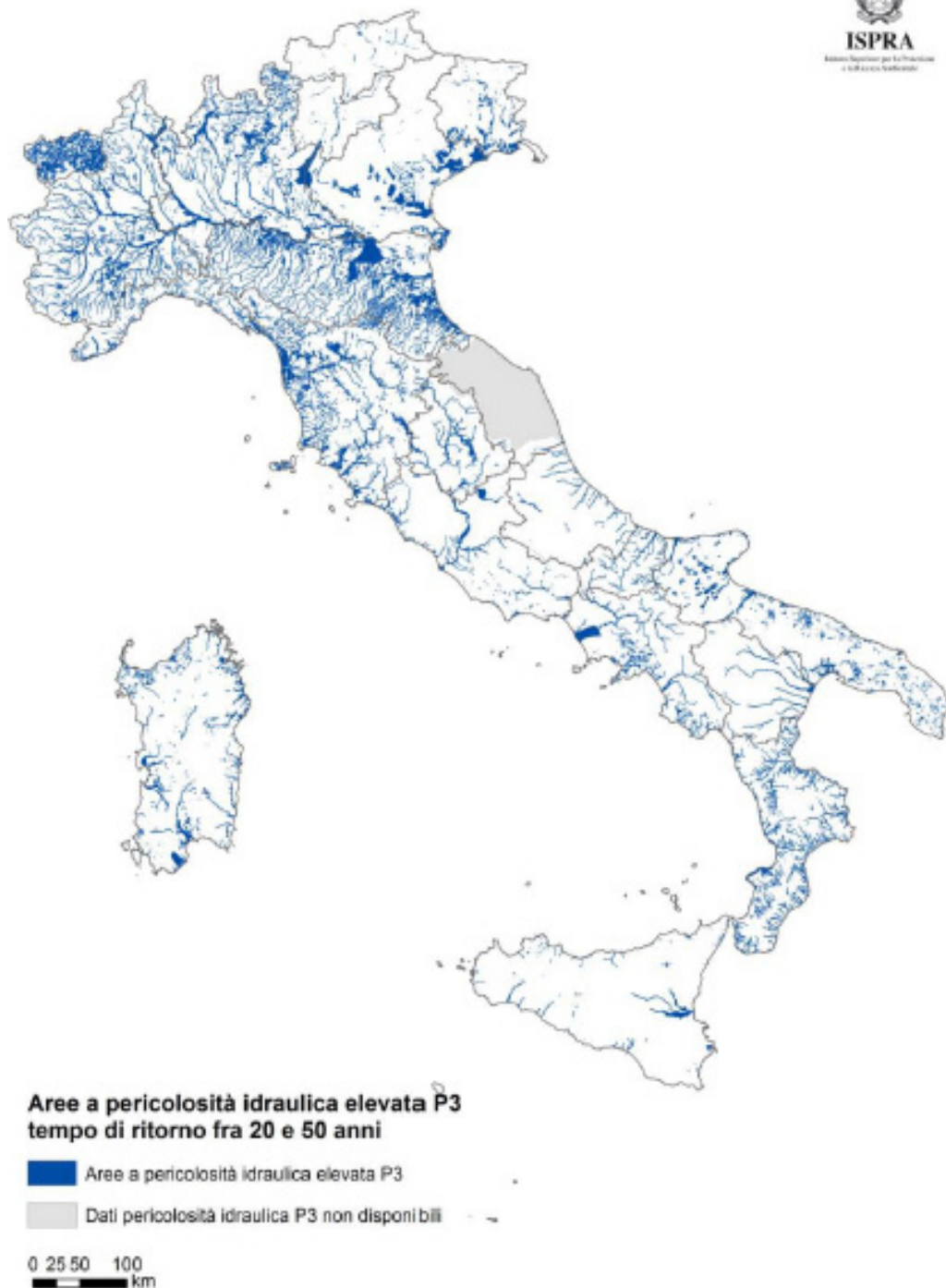


Fig. 5: Mappa relativa alla pericolosità idrogeologica (Fonte: ISPRA).

3.2. DESCRIZIONE DEL SITO OVE SI TROVA L'ATTIVITÀ (IMPRESA / PA)

3.2.1. Caratteristiche idrometeorologiche con particolare riferimento a:

- › Alluvioni
- › Bombe d'acqua
- › Forti piogge
- › Trombe d'aria
- › Grandine
- › Forti venti
- › Fulmini
- › Ondate di caldo
- ›

3.2.2. Caratteristiche geologiche con particolare riferimento a:

- › Frane
- › Smottamenti

3.3. DESCRIZIONE DEL PROCESSO OPERATIVO

- › Schema a blocchi delle fasi del processo
- › Fasi pericolose della produzione/lavorazione
- › Stoccaggio di prodotti infiammabili, combustibili, tossici, etc..
- › Movimentazione dei prodotti infiammabili, combustibili, tossici, etc..
- › Presenza di materiali / prodotti combustibili
- › Presenza di materiali / prodotti potenzialmente inquinanti
- › ...

3.4. DESCRIZIONE DEI SERVIZI GENERALI (IMPRESA / PA)

- › Ricevimento, trasformazione e distribuzione dell'energia elettrica
- › Impianti di climatizzazione/raffrescamento
- › Impianti di riscaldamento
- › Impianti di produzione del vapore
- › Impianti di cogenerazione
- › Impianti per aria compressa
- › Impianti di trattamento reflui
- › ...

3.5. CARATTERISTICHE COSTRUTTIVE DEI FABBRICATI

- › Vulnerabilità a inondazione e/o allagamento
- › Vulnerabilità a grandine e pioggia
- › Compartimentazione interna
- › Resistenza al vento di tetti ed elementi strutturali «deboli» (Es. lucernari)
- › Resistenza antisismica delle strutture
- › ...

3.6. MAGAZZINI / STOCCAGGI / DEPOSITI

- › Modalità di stoccaggio
- › Modalità di movimentazione delle merci
- › ...

3.7. CENTRO ELABORAZIONE DATI

- › Tipologia di elaboratori / server / apparecchiature HD / SW
- › Sistemi e procedure di back-up
- › Presenza di sistemi U.P.S
- › ...

3.8. PROTEZIONI

- › Passive
- › Attive
- › Automatiche
- › Manuali

3.9. PROCEDURE

- › Presenza di piani di emergenza / piani di gestione delle crisi
- › Organizzazione ed intervento delle squadre di emergenza
- › Attivazione dei piani di recupero
- › ...

3.10. INTERRUZIONE DELLE ATTIVITÀ OPERATIVE (BUSINESS INTERRUPTION)

- › Fornitura di materie prime e semilavorati e di servizi
- › Presenza di colli di bottiglia nei cicli di produzione
- › Interrelazione con altre aziende/organizzazioni
- › ...

Una volta identificata la pericolosità dell'area nella quale sorge l'Impresa / PA rispetto agli scenari considerati (alluvione, pioggia, vento, fulminazione, grandine, temperatura e franamento) e acquisite le informazioni chiave, occorre valutare (stimare) il potenziale impatto sui processi aziendali in termini di probabilità di accadimento (P) e di severità degli Effetti.

Nel caso del progetto DERRIS, per agevolare le PMI, lo strumento di autovalutazione del rischio consente la geolocalizzazione dell'impresa e le permette di avere un'indicazione qualitativa del livello di pericolosità dell'area in cui è collocata (in termini di probabilità che accada un evento e/o di intensità che potrebbe avere), sulla base di 7 mappe di pericolo corrispondenti ai 7 principali eventi naturali considerati (alluvione, pioggia, vento, fulminazione, grandine, temperatura, frana).

La **Probabilità di accadimento (P) dello scenario di rischio considerato** può essere stimata sulla base delle statistiche degli eventi incidentali disponibili (esperienza diretta dell'organizzazione & Database reperibili in

letteratura) oppure sulla base di una valutazione qualitativa (Fig. 6). La **Severità (S)** degli Effetti può essere valutata relativamente ad ogni scenario esaminato sulla base di una **scala relativa di severità** definita preventivamente dall'organizzazione e specifica della stessa (è opportuno associare ad ogni grado di severità una valorizzazione economica dello scenario di rischio (€) (Fig. 6).

Probabilità di accadimento e Severità degli effetti associati allo specifico scenario di rischio sono le coordinate che definiscono il posizionamento dello scenario nella **Matrice di Rischio** o **Mapa di Rischio** (Figg. 6 e 7).

Secondo l'approccio di Gestione del Rischio, la severità (S) del rischio è l'indicatore più importante della significatività del rischio e quindi della necessità di interventi / azioni correttive.

VALUTAZIONE DEL RISCHIO (RISK EVALUATION) Probabilità di accadimento e Severità dell'evento

LIVELLI DI FREQUENZA

- A → frequente
- B → moderato
- C → occasionale
- D → remoto
- E → inverosimile
- F → quasi impossibile

CATEGORIE DI SVERITÀ

I	CATASTROFICO
II	CRITICO
III	MARGINALE
IV	TRASCURABILE

Profilo di Rischio (Risk Map o Matrice dei Rischi)

		IV	III	II	I
Livello di frequenza del rischio ↑	A				
	B		Sc.6	Sc.3, Sc.9	
	C		Sc.7, Sc.8		Sc.1, Sc.4
	D			Sc.5	
	E				
	F				
		→ Categoria degli effetti del rischio			

↑ incremento del rischio

Fig. 6: Matrice dei Rischi o Mapa di Rischio.

Profilo di Rischio (Risk Map o Matrice dei Rischi)

	IV	III	II	I
A	Massima	Massima	Massima	Massima
B	Media	Massima	Massima	Massima
C	Media	Media	Massima	Massima
D	Minima	Media	Media	Massima
E	Minima	Minima	Media	Media
F	Minima	Minima	Minima	Media

Livello di frequenza del rischio ↑
 ↓
 Categoria degli effetti del rischio →

Fig. 7: Matrice dei Rischi o Mappa di Rischio

4.

ESEMPI DI MAPPATURA DEL RISCHIO

4.1. ESEMPIO 1: AZIENDA MANIFATTURIERA, UBIcata IN ADIACENZA AD UN CORSO D'ACQUA

4.1.1. Scenario considerato: Alluvione



Fig.8: Vista dall'alto dell'Azienda (Fonte: Google Maps)

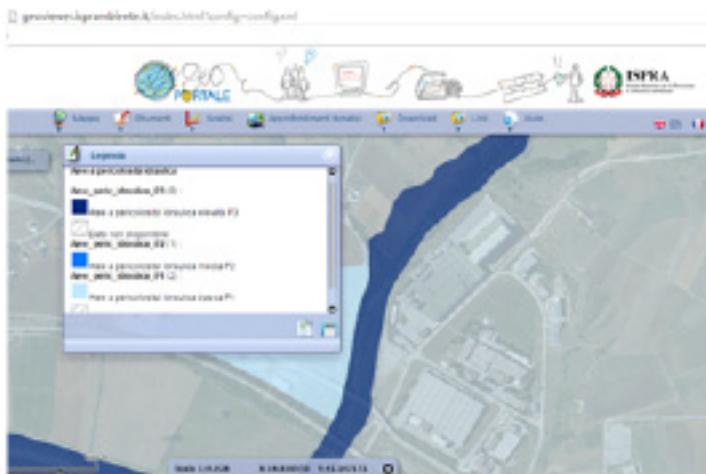


Fig.9: Vista dall'alto dell'Azienda con indicazione delle zone pericolose dal punto di vista idraulico (Fonte: ISPRA)

4.1.2. Scenario considerato: Franamento

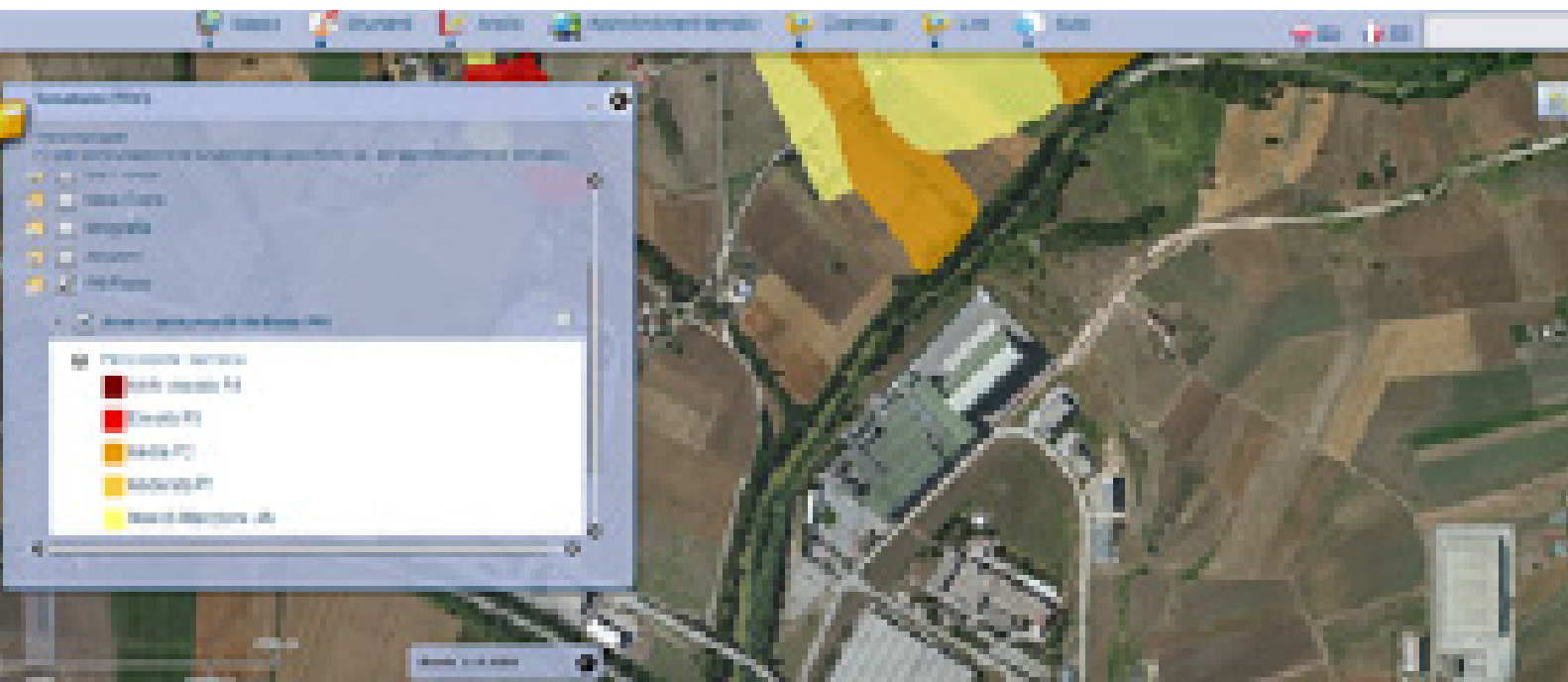


Fig.10: Vista dall'alto dell'Azienda con indicazione delle zone pericolose dal punto di vista statico (Fonte: ISPRA)

Il posizionamento sulla Matrice dei Rischi dei 2 scenari considerati (Alluvione/allagamento e Franamento) per l'Azienda in oggetto è il seguente:

	IV	III	II	I
A				
B				Alluvione / Allagamento
C				
D				
E				
F			Franamento	

CATEGORIA DEGLI EFFETTI DEL RISCHIO

Fig.11: Matrice dei Rischi

L'impresa considerata presenta quindi la **massima esposizione al rischio alluvione/allagamento**, come risultato di una **probabilità di accadimento elevata (B)** e di una **severità degli effetti molto elevata (I)**.

E infatti, ecco cosa si è verificato nella realtà. In concomitanza di forti piogge...



Il corso d'acqua adiacente è esondato...
E questi sono stati gli effetti!!



Fonte: PER S.p.A.

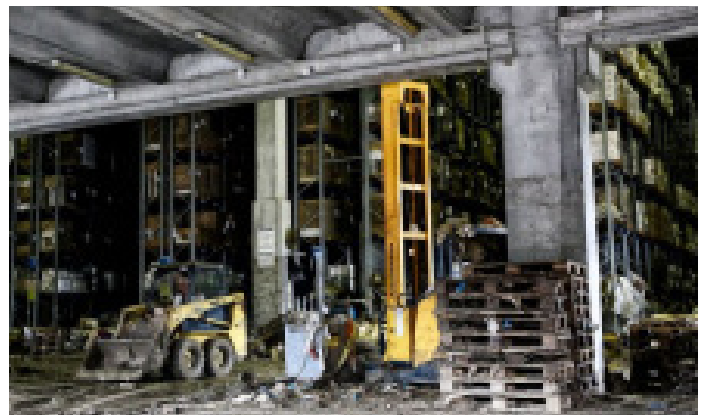


Fig.12: gli effetti della alluvione sull'azienda considerata (Fonte: Panorama – Credits: Olycom/Cesare Purini)

4.2.2. Scenario considerato: Franamento

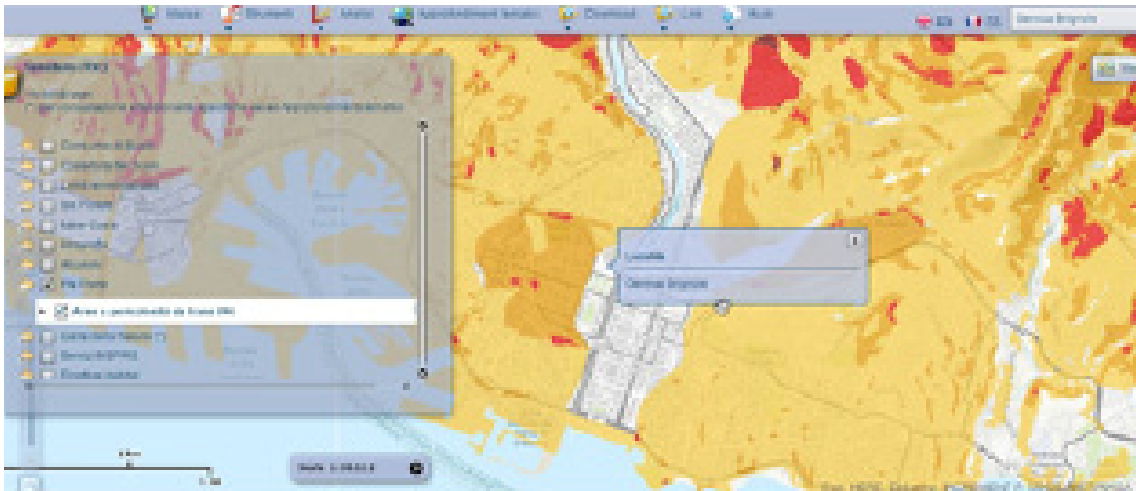


Fig.15: Vista dall'alto della Città di Genova con indicazione delle zone pericolose dal punto di vista statico (Fonte: ISPRA)

Il posizionamento sulla Matrice dei Rischi dei 2 scenari considerati (Alluvione/allagamento e Franamento) per la zona oggetto di valutazione è il seguente:

	IV	III	II	I
A				
B				Alluvione / Allagamento
C				
D			Franamento	
E				
F				

LIVELLO DI FREQUENZA DEL RISCHIO

CATEGORIA DEGLI EFFETTI DEL RISCHIO

Fig.16: Matrice dei Rischi

La stazione di Genova Brignole considerata presenta quindi la **massima esposizione al rischio alluvione/allagamento**, risultato di una **probabilità di accadimento elevata (B)** e di una **severità degli effetti molto elevata (I)**.

Non trascurabile risulta anche l'esposizione a fenomeni di dissesto statico.

Infatti, ecco cosa si è verificato nella realtà.



<http://zenastormchaser.it>

In concomitanza di forti piogge... Questi sono stati gli Effetti... ALLUVIONE!



Fig.17: Gli Effetti dell'Alluvione

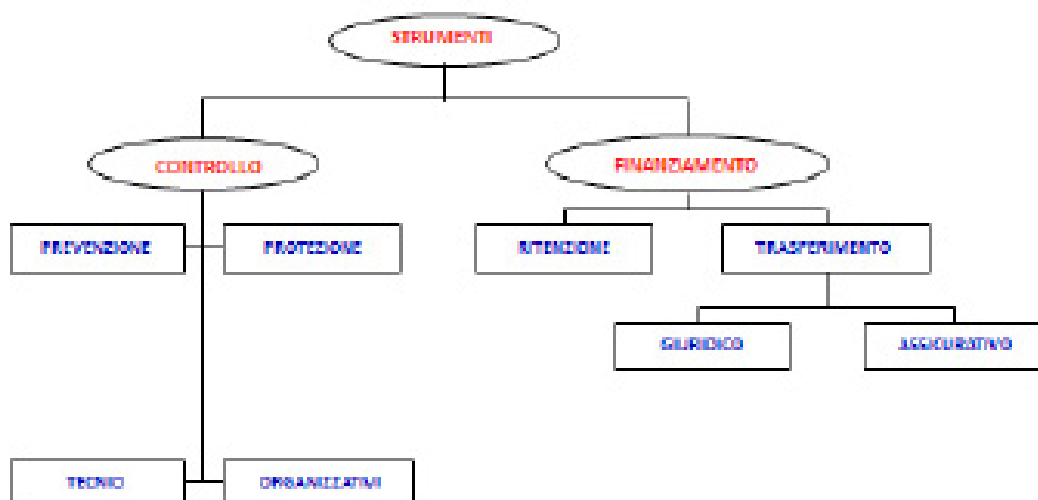


5.

CONTROLLO E LA GESTIONE DEL RISCHIO

Gli strumenti a disposizione delle organizzazioni (imprese e PA) per gestire in modo ottimale i rischi evidenziati nel processo di analisi e valutazione sono di due tipi:

- > strumenti di **controllo**
- > strumenti di **finanziamento**



Fra gli strumenti di controllo, **l'elusione (o eliminazione) e la prevenzione** mirano a impedire il verificarsi dell'evento, mentre gli **strumenti di protezione** (dato per scontato che l'evento dannoso si verifichi) consentono di minimizzarne gli effetti sulle strutture e sulle operazioni aziendali.

Fra gli strumenti di finanziamento, **l'assicurazione, il trasferimento non assicurativo e la ritenzione** consentono di sottrarre l'organizzazione alle conseguenze finanziarie derivanti dal verificarsi dell'evento e del danno conseguente.

Una modalità molto efficace per rappresentare l'impatto degli strumenti di gestione e controllo dei rischi è quella di utilizzare la rappresentazione tipica della Matrice o Mappa del rischio, nella quale ogni punto di una curva rappresenta uno specifico scenario, caratterizzato da una certa Probabilità di accadimento e una certa Severità degli effetti.

Vediamo nel seguito come agiscono i vari strumenti.

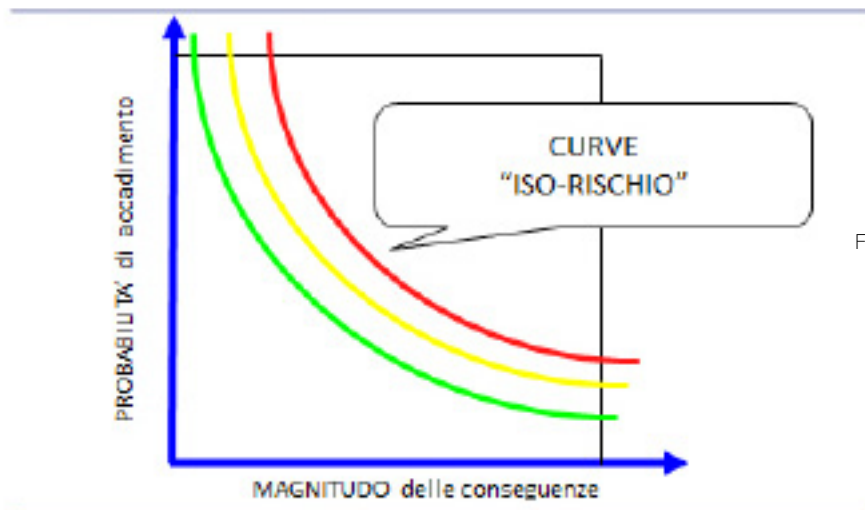
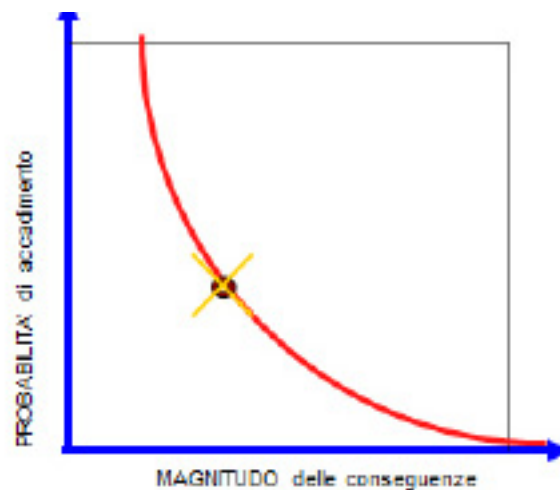


Fig.19: le curve ISO-RISCHIO

ELUSIONE DEL RISCHIO (ELIMINAZIONE)

L'**Elusione** è l'**eliminazione del rischio** per mezzo dell'abbandono dell'attività o delle operazioni che lo determinano.

L'Elusione può avvenire mediante:



): l'elusione del rischio

- > la rinuncia ad uno dei business aziendali
- > la chiusura di reparti/aree
- > l'abbandono di tecnologie
- > la sostituzione di materiali o componenti.

DIMINUZIONE DEL RISCHIO

La diminuzione del rischio può avvenire mediante misure di **Prevenzione** e/o **Protezione**.

- › La **prevenzione** è l'insieme delle misure di sicurezza finalizzate a impedire il prodursi di eventi dannosi.
- › La **prevenzione** è un'azione che consente di ridurre la probabilità di accadimento di un evento, a parità di grado di severità (magnitudo).

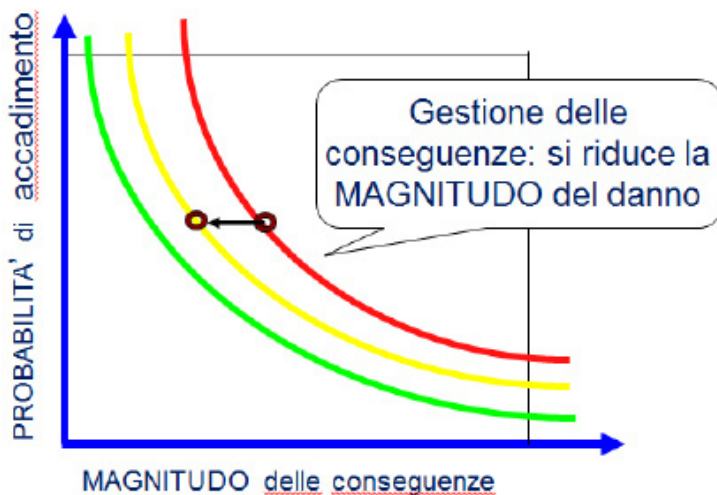
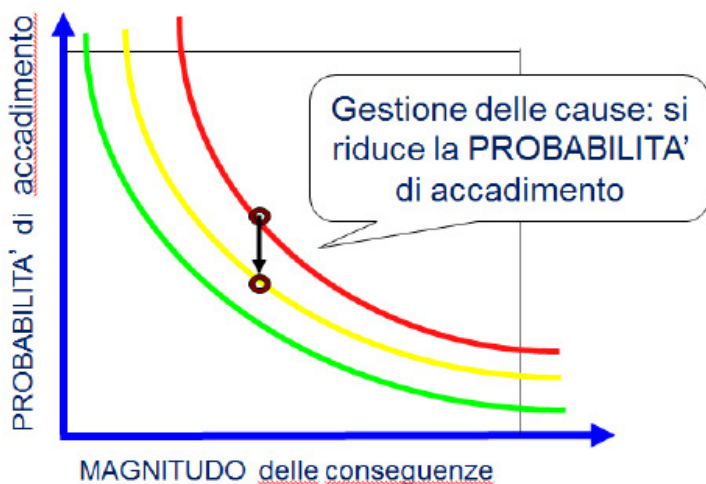


Fig. 21: i concetti di prevenzione e protezione

Prevenzione e Protezione del rischio vengono spesso riunite nell'unica denominazione di **"Loss control"**.

Le tecniche e gli interventi di loss control possono essere ricondotti a tre categorie generali:

- › attrezzature e impianti di sicurezza
- › procedure operative
- › formazione degli operatori.

TRASFERIMENTO DEL RISCHIO

Trasferimento Assicurativo (Assicurazione)

- › L'Assicurazione è un contratto che garantisce una copertura finanziaria al verificarsi di un evento dannoso o sinistro (assicurazione danni) oppure in relazione ad eventi della vita di una persona (assicurazione vita).
- › L'impresa trasferisce alla compagnia assicurativa le (o parte delle) conseguenze monetarie dell'evento dannoso.

Trasferimento non Assicurativo

- › Il trasferimento non assicurativo è lo spostamento del rischio su soggetti diversi da una compagnia di assicurazione, trasferendo le conseguenze e / o la gestione delle attività da cui l'evento dannoso può trarre origine a terzi.

RITENZIONE DEL RISCHIO

- › La ritenzione è l'assunzione da parte dell'organizzazione di una quota del rischio: i danni eventuali relativi a tale quota sono quindi sostenuti con mezzi finanziari interni. La ritenzione può essere di due tipi: consapevole oppure inconsapevole.

La **Ritenzione consapevole** si verifica quando l'organizzazione ha la piena consapevolezza dell'esistenza del rischio, della sua entità e dell'ammontare delle perdite che dovranno essere sostenute in proprio al verificarsi dell'evento sfavorevole.

La **Ritenzione inconsapevole**: si verifica quando l'organizzazione, per effetto di una condizione di ignoranza, assume una quota di rischio superiore a quella desiderata. Può essere originata da una mancata identificazione del rischio, da una sottovalutazione dell'entità del rischio oppure dalla sopravvalutazione dell'efficacia degli interventi intrapresi.

È estremamente importante che ogni organizzazione (impresa/PA) abbia la piena consapevolezza della propria situazione, ovvero conosca il proprio livello di ritenzione del rischio e quindi il rischio residuo (ciò che rimane dopo aver seguito i vari passi del processo di gestione dei rischi). Infatti, quanto più elevato sarà il livello di ritenzione (e quindi il rischio residuo), tanto maggiore sarà la quota di rischio di cui l'azienda dovrà farsi carico: nel caso si verifichi un evento negativo, gli eventuali danni relativi a tale quota dovranno essere sostenuti con mezzi finanziari interni all'impresa.

In pratica, le misure da adottare per un **efficace Controllo e Gestione dei rischi correlati ai cambiamenti climatici** dovranno rispondere alle seguenti esigenze:

- › proteggere il patrimonio aziendale
- › garantire la continuità operativa nel tempo (**continuità dei processi operativi/di erogazione di servizi**).

Alcune misure saranno specifiche per lo Scenario di Rischio considerato (alluvione, allagamento,...); altre manifesteranno la loro efficacia rispetto a più scenari.

Tipiche **Misure Tecnico-Impiantistiche generali suggerite** sono le seguenti:

- › Verificare l'adeguatezza delle coperture e dei tamponamenti degli edifici a resistere a fenomeni atmosferici di particolare intensità; in caso di (parziale / totale) inadeguatezza, procedere con gli interventi del caso.
- › Verificare l'adeguatezza (efficacia ed efficienza) dei sistemi di raccolta e di scarico delle acque pluviali e della rete fognaria dell'azienda/dell'ubicazione: se inadeguati, implementare le opportune azioni correttive.
- › Verificare l'adeguatezza (efficacia ed efficienza) dei sistemi di protezione dalle scariche elettriche atmosferiche: se necessario implementare tali sistemi per incrementare il livello di protezione complessivo.
- › Realizzare (se possibile) opere di contenimento (argini, separazioni, muri di protezione) atti a proteggere una o più aree dell'area considerata da fenomeni di alluvione / inondazione.
- › Proteggere le apparecchiature critiche (macchinari, attrezzature, apparecchiature elettroniche...) oppure rilocarle in aree meno vulnerabili agli effetti delle calamità naturali.
- › Proteggere le merci (materie prime, semilavorati, prodotti finiti, materiale per imballaggio, ...) oppure rilocarle in aree meno vulnerabili agli effetti delle calamità naturali.
- › Proteggere la documentazione critica dell'organizzazione (dati tecnici - archivio tecnico, Q&A, dati di produzione - dati amministrativi e contabili, dati sensibili relativi ai clienti, documentazione legale dell'impresa, ecc.), oppure rilocarla in aree meno vulnerabili agli effetti delle calamità naturali.

Nel caso dei principali Scenari di rischio considerati relativi ai cambiamenti climatici:

1. Alluvione
2. Pioggia
3. Vento
4. Fulminazione
5. Grandine
6. Temperatura
7. Frana

I possibili interventi specifici di prevenzione e protezione dei beni / del patrimonio aziendale possono essere sintetizzati come segue:

1) **Alluvione**

- › Scegliere una collocazione non esposta a livello generale
- › Sopraelevare il livello base del proprio stabilimento al di sopra del livello di alluvione con periodo di ritorno di almeno 500 anni
- › Sopraelevare il pavimento del piano terra dei fabbricati al di sopra del livello di alluvione con periodo di ritorno di almeno 500 anni
- › Non installare impianti e servizi al di sotto di questo livello, oppure renderli invulnerabili all'acqua
- › Ancorare opportunamente al suolo serbatoi e contenitori che potrebbero galleggiare
- › Tenere in posizione sicura le sostanze pericolose dilavabili
- › Predisporre un piano di Preparazione all'Emergenza Alluvione, da implementarsi in caso di segnali premonitori o da comunicazioni ufficiali da parte delle autorità

2) **Pioggia**

Poiché non è possibile ridurre la quantità di pioggia e neppure controllare che questa cada trasversalmente a causa delle raffiche di vento, la strategia è quella di prevenire la penetrazione di acqua e, se questo avvenisse, impedire che questa bagni impianti e materiali.

Per prevenire l'**ingresso** dell'acqua:

- › Valutare la posizione altimetrica e sopraelevare il pavimento
- › Progettare e realizzare coperture e pluviali in modo che restino integri anche nel caso di piogge eccessive
- › Manutenerne e pulire regolarmente tetti, grondaie, pluviali e fognature
- › Installare dispositivi di allarme e chiusura automatica di lucernari e finestre

Per impedire il **bagnamento** di impianti e materiali:

- › Installare impianti ed apparecchiature elettriche con grado di protezione resistente al bagnamento
- › Posizionare tutte le merci e i materiali in posizione rialzata da terra
- › Individuare tipologie di confezionamento e coperture dei contenitori che siano adatte a sopportare un certo bagnamento senza danno per il prodotto

3) **Vento e trombe d'aria**

- › Ancorare le tegole al tetto con appositi ganci di fissaggio
- › Provvedere all'ancoraggio di impianti e insegne posti sul tetto o comunque all'esterno
- › Evitare il deposito di macchinari e merci vulnerabili e di particolare valore all'aperto o sotto tettoie e tensostrutture

- › Utilizzare infissi e finestre con caratteristiche di elevata resistenza al vento
- › Verificare periodicamente le condizioni di manutenzione dei tetti e delle coperture con particolare attenzione all'integrità degli ancoraggi
- › Verificare la chiusura di lucernari e finestre
- › Verificare periodicamente il buono stato di salute di piante ad alto fusto presenti nelle vicinanze e rimuovere rami ed alberi fragili

4) **Fulminazione**

Non sono noti ad oggi dispositivi o sistemi atti a prevenire la formazione di fulmini: ciò significa che l'unica strategia difensiva è quella della protezione. La **protezione esterna** è realizzata in modo da:

- › intercettare le fulminazioni dirette con un sistema di captatori;
- › condurre la corrente da fulmine in modo sicuro verso terra con un sistema di calate;
- › distribuire la corrente di fulmine nella terra.

La **protezione interna** è realizzata in modo da:

- › mantenere una distanza minima di sicurezza tra gli elementi del sistema di protezione esterna e altri elementi conduttori all'interno della struttura;
- › creare un collegamento equipotenziale tra installazioni metalliche e linee all'interno dell'impianto mediante il collegamento diretto di tutte le parti conduttrici separate dell'impianto oppure mediante scaricatori di sovratensioni (SPD).

5) **Grandine**

È ritenuto possibile prevenire la caduta di grandine sparando particolari razzi nelle nuvole che presentano le condizioni premonitrici di grandinate. Questa metodologia è ampiamente utilizzata in agricoltura (es. vigneti) in quanto è certo che se grandinerà una parte delle coltivazioni sarà certamente colpita.

Per quanto riguarda le attività industriali la strategia è quella di prevenire l'intasamento di pluviali e fognature e di impedire che i chicchi colpiscano coperture, impianti e materiali.

Per prevenire l'intasamento delle condutture:

- › Sovradimensionamento dei pluviali e delle ghiotte
- › Manutenzione e pulizia regolare di tetti, grondaie, pluviali e fognature

Per mitigare l'effetto dell'impatto dei chicchi:

- › Installare reti di protezione di adeguata resistenza su quanto deve stare necessariamente all'aperto
- › Utilizzare coperture e finestre che abbiano adeguata resistenza all'urto di chicchi di grande dimensione
- › Evitare di stoccare all'aperto materiali e merci fragili

6) **Temperatura (Ondate di calore)**

Ridurre la produzione di calore:

- › usare dispositivi a basso consumo energetico;
- › usare lampadine fluorescenti e soprattutto a LED;
- › incrementare la luce naturale nei nuovi edifici per ridurre l'uso di illuminazione artificiale;
- › regolare in automatico l'uso dell'illuminazione artificiale;
- › in giornate calde, minimizzare l'uso di apparecchiature energivore;
- › spegnere e scollegare computer e macchine elettriche quando non utilizzati.

Aumentare il raffrescamento naturale:

- › dotare le finestre di dispositivi di ombreggiamento esterni per proteggere i locali da radiazione solare;
- › collocare la vegetazione in modo da bloccare i raggi del sole, minimizzare il trasferimento di calore all'interno degli edifici e quindi ridurre la necessità di aria condizionata;
- › realizzare "camini termici" che impiegano correnti convettive per estrarre l'aria calda dall'edificio;
- › predisporre elementi d'acqua quali fontane e laghetti.

Modificare albedo ed emissività:

- › uso di asfalto o cemento colorato;
- › uso di pavimentazioni erbacee e tetti verdi;
- › uso di tetti freddi: sono realizzati con materiali altamente riflettenti ed emissivi e durante i picchi estivi possono rimanere di circa 30°C più freddi rispetto ai tetti realizzati con materiali tradizionali.

7) **Frana**

Poiché non è possibile sapere quando avverrà una frana e non è generalmente possibile costruire edifici e in grado di resistere all'impatto delle rocce e dei detriti, occorre:

- › Scegliere una collocazione non esposta a livello generale
- › Monitorare costantemente i segnali premonitori, ad esempio:
 - › emergenze idriche di rilevante portata con aumento di torbidità
 - › modificazioni della geometria dell'alveo
 - › fratture di trazione alla sommità del versante
 - › ceppaie fortemente inclinate lungo il versante
- › Attuare il Piano di Emergenza (evacuazione) sulla base dei dati derivanti dal monitoraggio e delle soglie di allarme prefissate
- › Realizzazione di interventi strutturali di messa in sicurezza della zona:
 - › valli paramassi
 - › cunei deviatori
 - › briglie

6.

COME GESTIRE LE EMERGENZE

Abbiamo visto che quando si verifica una situazione di crisi, la preparazione preventiva e il tempo di reazione sono fattori di successo (o di insuccesso) determinanti. E' quindi importante per tutte le organizzazioni (Imprese / PA) prepararsi in modo adeguato al fine di gestire in modo efficace ogni situazione negativa e ritornare il più rapidamente possibile alle condizioni preesistenti.

Per poter reagire efficacemente, però, ogni organizzazione dovrebbe definire (e poi implementare) uno specifico **Programma di Gestione della Continuità Operativa** (o **Business Continuity Management -BCM**).

Gli obiettivi di questo programma saranno quelli di assicurare la continuità operativa e la sopravvivenza dell'organizzazione in ogni circostanza, e quindi di aumentarne la «Resilienza». In particolare:

- › Garantire la migliore protezione possibile dei beni aziendali
- › Mitigare i rischi e le esposizioni
- › Identificare e implementare le opportune misure di prevenzione e protezione
- › Assumere il controllo di ogni interruzione delle attività operative / del business aziendale.

La costruzione del Piano di Continuità per una organizzazione si sviluppa dal processo di Analisi e Valutazione dei rischi precedentemente descritto, integrato con una "valutazione dell'impatto sulle attività operative" (Analisi di Impatto sul Business o BIA). Quest'ultima consente di identificare le principali vulnerabilità d'impresa e di quantificarne i relativi scenari di potenziale impatto sia da un punto di vista economico-finanziario che di mercato.

Gli **obiettivi** di queste attività sono, in sintesi:

- › L'identificazione dei processi più critici dell'organizzazione, ovvero dei processi che richiedono il più alto livello di attenzione/protezione da parte del Management e dell'intera struttura
- › L'identificazione delle interdipendenze esistenti, che possono costituire eventuali punti di vulnerabilità (es. catena di fornitura o Supply Chain)
- › La valutazione degli impatti operativi, economici, finanziari, legali e di immagine conseguenti all'accadimento degli scenari di rischio considerati
- › La valutazione degli **Obiettivi di Tempo di Recupero (RTO, RPO) dei processi aziendali**, ovvero dei periodi di tempo entro i quali i sistemi, le applicazioni, i processi e le funzioni aziendali devono essere «recuperate» dopo una interruzione/indisponibilità.

- › Sulla base degli RTO di cui sopra, l'identificazione delle priorità di intervento e lo sviluppo delle strategie più efficaci per fronteggiare un qualsiasi evento ("Interruzione" oppure "Disastro")
- › L'identificazione del personale critico per il ripristino delle attività
- › L'identificazione dei fornitori critici
- › L'identificazione di ogni altro elemento utile per lo sviluppo di un sistema di Continuità Operativa (BCM).

Il **Piano di Continuità Operativa (Piano di Continuità del Business -BCP)** è un piano organico che assembla i diversi piani operativi presenti in azienda (es. il Piano di Emergenza, il Piano di Recupero dopo un Disastro e il Piano di Comunicazione in caso di Crisi). Scopo del Piano è quello di limitare ad un livello accettabile per l'impresa i tempi di interruzione della continuità operativa, evitando/riducendo fra l'altro il rischio di perdita di quote di mercato dopo una discontinuità del business aziendale.

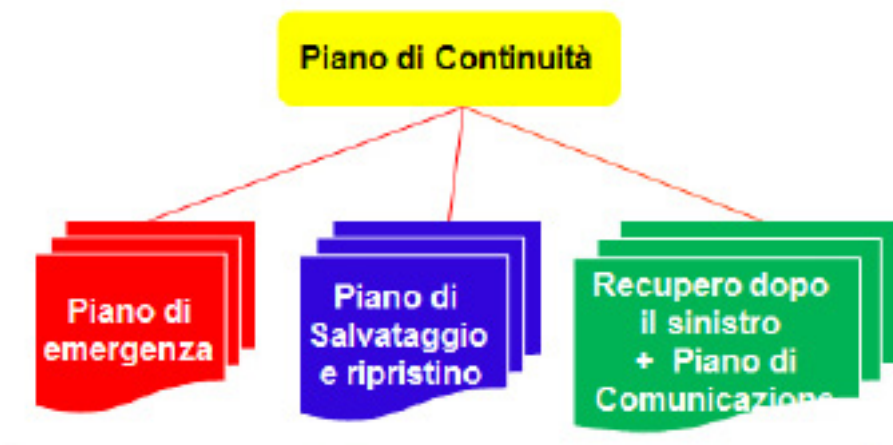


Fig.22: Il Piano di Continuità Operativa (BCP)

All'interno del Piano di Continuità, dovranno essere inclusi:

- › Il **Piano di Emergenza**, che comprende le modalità di reazione immediata ad un evento al fine di proteggere le persone, i beni, l'ambiente e minimizzare i "danni diretti".
- › Il **Piano di Salvataggio e Ripristino (DRP)**, che deve essere attivato immediatamente dopo che gli effetti dell'evento sono stati posti sotto controllo, e stabilisce le modalità di azione per minimizzare i danni. E' un documento nel quale sono descritte in modo dettagliato le azioni da intraprendere in una situazione di emergenza, con l'obiettivo di riprendere le attività strategiche aziendali entro un tempo massimo definito a priori con l'impresa.

- › **Le Attività di Recupero dopo un sinistro e il Piano di Comunicazione**, che stabiliscono rispettivamente le azioni per consentire la ripresa delle normali operazioni aziendali, riducendo l'impatto sul cash flow e sul mercato, e le modalità di gestione immediata della crisi in termini di comunicazione, minimizzando l'impatto sulla reputazione e sul business.

Per gestire nel modo più efficace lo strumento rappresentato dal Piano di Continuità, è molto importante distinguere fra "Interruzione" e "Disastro". Per fare questo è necessario introdurre i due parametri precedentemente citati: il **Recovery Time Objective (RTO)** e il **Recovery Point Objective (RPO)**, quest'ultimo usato diffusamente in ambito IT (Information Technology).

- › Si definisce **RTO – Recovery Time Objective** il periodo definito entro il quale attività e processi critici (ai fini operativi) devono essere ripristinati (ad esempio, RTO = 1g significa che entro un giorno dal disastro è necessario garantire il ripristino di un livello minimo di servizio per l'attività impattata).
- › Si definisce invece **RPO – Recovery Point Objective (ambito IT)** un valore definito pari alla perdita massima di dati sostenibile in caso di crisi (ad esempio RPO = 1g significa che è possibile sopportare la perdita di dati relativi alle 24h di lavoro precedenti al disastro).

Con queste premesse, si parla di "**Interruzione**" quando si verifica un evento tale per cui:

- › I tempi di fermata / di interruzione sono inferiori al valore stimato di RTO
- › Gli impatti (le conseguenze dell'evento) sono limitati e controllati
- › La valorizzazione delle conseguenze (espressa in €) è inferiore ad un livello prestabilito.

Parliamo invece di "**Disastro**" quando si verifica un evento tale per cui:

- › I tempi di fermata / di interruzione sono superiori al valore stimato di RTO
- › Gli impatti (le conseguenze dell'evento) sono estesi e fuori controllo
- › La valorizzazione delle conseguenze (espressa in €) è superiore ad un livello prestabilito.

Le **Strategie di Continuità operativa**, sviluppate nell'ambito del Piano, rappresentano le linee guida di una organizzazione su come gestire i processi aziendali interessati da un evento disastroso, con l'obiettivo di ritornare il più rapidamente possibile alle condizioni di normalità.

L'organizzazione dovrà decidere, per ogni processo, la strategia da intraprendere secondo la **regola delle 4T (Trasferire, Tollerare, Trattare o Terminare)**, a propria volta basata su una corretta e completa analisi costi / benefici delle alternative disponibili. Le opzioni possibili da esaminare sono quindi:

- › **Trasferire** (ad esempio mediante stipula di uno o più contratti assicurativi e/o trasferimento giuridico / contrattuale del rischio a terzi)
- › **Tollerare** (accettazione del rischio, es. in caso di costi di intervento correttivo maggiori dei benefici attesi)
- › **Trattare** (adozione di contromisure o piani di ripristino specifici in tempi accettabili)
- › **Terminare** (adozione di contromisure radicali, ad esempio la rinuncia a ripristinare poiché non conveniente per l'azienda).

In funzione dello scenario esaminato (Interruzione delle attività / Indisponibilità dei beni oppure Disastro, secondo le definizioni riportate in precedenza) dovranno essere sviluppate le Strategie di Continuità operativa più opportune. Ad esempio:

- › In caso di **Interruzione/Indisponibilità**, le Strategie di Continuità devono consentire all'organizzazione di reagire nel modo più efficace ed efficiente a tutte le situazioni (non catastrofiche / disastrose) che comportino una interruzione del business, con l'obiettivo di ritornare rapidamente alla situazione preesistente (tipico esempio è la predisposizione di un server IT «off site» da attivare immediatamente nel caso in cui il server interno non sia operativo).
- › In caso di **Disastro**, le Strategie di Recupero devono consentire all'organizzazione di reagire nel modo più efficace ed efficiente a tutte le situazioni catastrofiche / di crisi dichiarata che comportino estesi impatti sul business aziendale (tipico esempio è la presenza di un centro elaborazione dati in modalità di «mirroring», ubicato in un sito adeguatamente distante da quello gravemente danneggiato).

Nell'ambito dello sviluppo di un sistema di Continuità Operativa, la definizione delle Strategie di Continuità è fra le fasi più delicate e impegnative.

Dal punto di vista procedurale, infine, il Processo di Gestione della Crisi dovrà comprendere le seguenti fasi:

- 1) La ricezione della notifica di un potenziale evento catastrofale
- 2) La prima valutazione del potenziale evento catastrofale da parte di uno specifico "Comitato di Crisi" (verifica se si tratta di "interruzione" oppure di "disastro")
- 3) Se "disastro", la dichiarazione dell'apertura dello «Stato di Crisi» da parte del Comitato di Crisi
- 4) L'attivazione di tutti i componenti del Comitato di Crisi e dei vari responsabili tecnici
- 5) L'eventuale trasferimento delle risorse chiave necessarie presso un sito temporaneo
- 6) L'avvio delle attività di salvataggio, bonifica e ripristino (civile, elettrico/elettronico) dei fabbricati, dei macchinari e delle merci e gestione del personale coinvolto
- 7) La dichiarazione di "conclusione dello Stato di Crisi" da parte del Comitato di Crisi.

7.

LA GESTIONE DEL POST-SINISTRO

Gestire il post-sinistro negli scenari di alluvione, forti piogge, grandine, vento e trombe d'aria, fulmini, forti nevicate, ... significa mettere in atto, direttamente o con il supporto professionale di tecnici specializzati, interventi di:

- > Salvataggio
- > Bonifica superficiale
- > Risanamento
- > Ripristino Funzionale.

Nel dettaglio:

- > **Attività' di salvataggio**: si intende l'insieme degli interventi volti ad evitare l'aggravamento del danno (mediante attività di "protezione temporanea dei beni danneggiati" / "stop dei fenomeni di degrado - "stop corrosion")
- > **Attività' di bonifica superficiale**: consiste nell'asportazione da ambienti, materiali e impianti di quegli elementi che provocano degrado o corrosione, senza eseguire smontaggi
- > **Attività' di risanamento**: è l'insieme degli interventi volti a restituire ai beni coinvolti indirettamente nel sinistro quel grado di pulizia chimica globale che ne garantisca il funzionamento affidabile nel tempo, inclusi i necessari smontaggi e rimontaggi
- > **Attività' di ripristino funzionale**: è l'insieme degli interventi, normalmente comprensivi e integrativi di quelli di risanamento, volti a restituire ai macchinari e alle apparecchiature la funzionalità che avevano prima del sinistro.



Fig.23: La gestione del post-sinistro

L'intervento di Società professionali in questo ambito (Disaster Recovery) consente quasi sempre di ridurre l'entità dei Danni Diretti, dei Danni Indiretti legati alla mancata operatività dell'organizzazione (Impresa / PA) e degli eventuali Danni Conseguenziali.

Anche l'(eventuale) intervento di esperti nella gestione professionale del post-sinistro può essere pianificato e inserito (sotto forma di procedura specifica) nel Piano di Continuità Operativa dell'organizzazione.

8.

CONCLUSIONI

Per gestire nel modo più efficace una crisi da evento climatico **occorre prepararsi «prima»** che l'evento si manifesti, dotandosi degli strumenti più opportuni per **migliorare in modo significativo la resilienza del sistema (Impresa / PA).**

Perché è importante essere preparati?

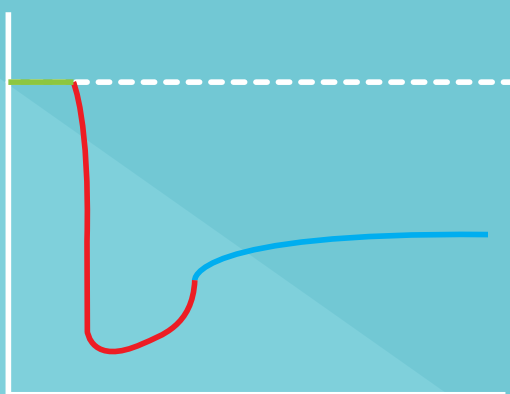
1) Perché le crisi correlate ai cambiamenti climatici non sono pianificabili...



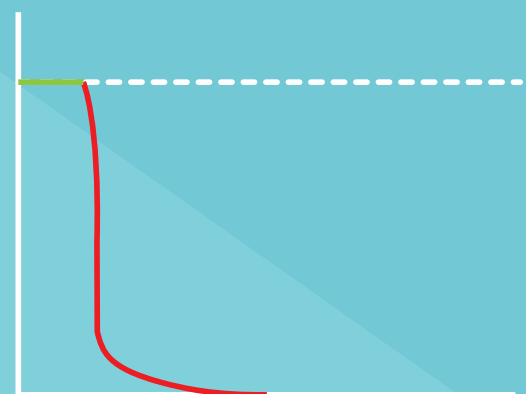
...ma **possiamo certamente prepararci ad affrontarle nel modo più efficace!**



2) Perché i **costi di una crisi** potrebbero essere drammaticamente elevati per l'organizzazione (Imprese / PA), e occorre evitare che la crisi abbia un'evoluzione NEGATIVA, portandoci fuori mercato!



Crisi grave, con perdita permanente di una parte della quota di mercato dell'impresa



Crisi grave, con definitiva estinzione dell'impresa

3) Perché i clienti, gli utenti e il Mercato in generale si aspettano **continuità nelle forniture/nell'erogazione dei servizi, sempre**

4) Perché i titolari e gli eventuali azionisti si aspettano che il management abbia il **controllo della situazione, sempre**

5) Perché i fornitori e i dipendenti si aspettano che la loro «relazione» e il loro **“sostentamento” siano garantite nel tempo**

6) Perché essere preparati è un **indicatore di grande consapevolezza e di una gestione manageriale responsabile e lungimirante**

7) Perché gli **investimenti nel campo della Gestione dei Rischi aumentano sempre il valore dell'organizzazione, preservano / migliorano la reputazione e l'immagine aziendale, migliorano la valutazione dei rischi da parte del Mercato Assicurativo, migliorano il profilo dell'Impresa presso il mercato creditizio e finanziario.**

Allegato A.

IL TOOL DERRIS, UNO STRUMENTO DI AUTOVALUTAZIONE DEL RISCHIO CLIMATICO

Per aiutare le Aziende a sviluppare il proprio **Processo di Gestione dei Rischi**, sono disponibili diversi strumenti. Uno di questi è lo **strumento di autovalutazione del rischio climatico sviluppato nell'ambito del progetto DERRIS**. Il tool DERRIS consente la geolocalizzazione dell'impresa e le permette di avere un'indicazione qualitativa del livello di pericolosità dell'area in cui è collocata, sulla base di 7 mappe di pericolo corrispondenti ai 7 principali eventi naturali considerati (alluvione, pioggia, vento, fulminazione, grandine, temperatura, frana). L'insieme delle informazioni specifiche dell'Azienda in esame (acquisite compilando una serie di semplici questionari), permette di **valutare la vulnerabilità dell'azienda e di darle un'indicazione del suo livello di rischio rispetto ai 7 eventi climatici considerati**.

Sulla base delle informazioni acquisite, poi, lo strumento fornirà automaticamente i **suggerimenti per la mitigazione del rischio relativi alla tipologia di evento**.

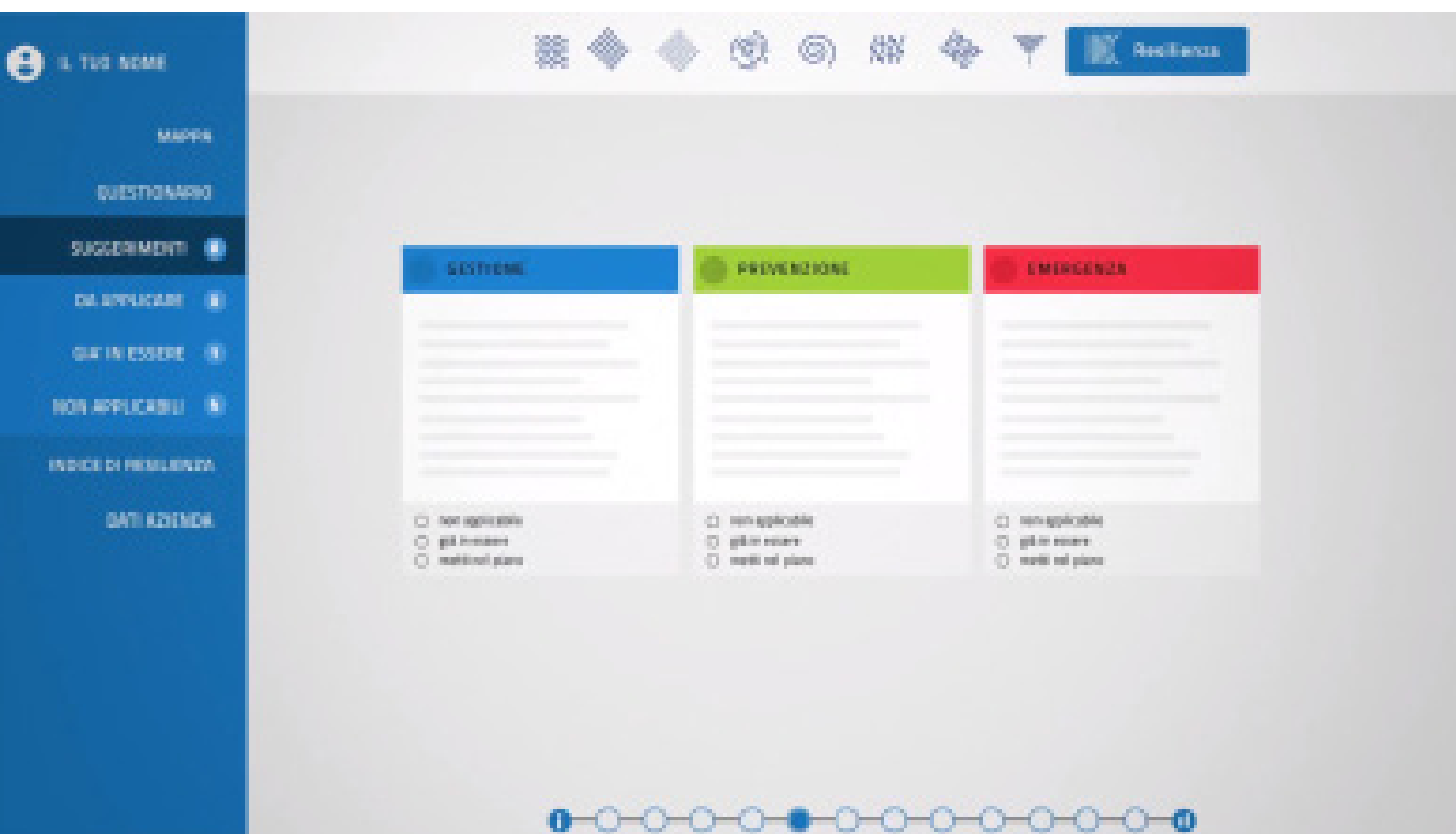



















Fig. 24: tipologie di suggerimenti previsti

INDICE DI RESILIENZA

Aspetti gestiti dall'Azienda

Attuale	Dopo gli interventi	
		Identificare i rischi climatici e possibili impatti
		Identificare le azioni per mettere in sicurezza beni, strutture ed impianti
		Definire procedure interne di prevenzione e gestione dei rischi climatici
		Formare i lavoratori e garantirne la sicurezza
		Valutare le implicazioni finanziarie
		Aumentare la resilienza del territorio collaborando con le altre aziende e la pubblica amministrazione
		Garantire la business continuity in caso di emergenza

 Aspetto gestito dall'azienda	 Aspetto parzialmente gestito dall'azienda	 Aspetto attualmente non gestito dall'azienda
--	---	--

In funzione delle risposte fornite dall'Azienda e dei suggerimenti che la stessa deciderà di inserire nel proprio **Piano d'Azione per l'adattamento ai cambiamenti climatici** (il tool calcolerà l'**Indice di resilienza dell'Azienda** (il quale fornisce un'indicazione della situazione attuale rispetto alla situazione dopo l'attuazione degli interventi correttivi).

Bibliografia

A. Floreani – *Introduzione al Risk Management: un approccio integrato alla gestione dei rischi aziendali* – ETAS

Claudio Cacciamani – *Il rischio da interruzione dell'attività di esercizio* – CERAP Egea

Patrick Lagadec – *Crisis Management: Come affrontare e gestire emergenze e imprevisti* – FrancoAngeli

Harvard Business Essentials – *Il management della crisi* – ETAS

A cura di A. Floreani – *Strategie e processi per salvaguardare il valore aziendale a seguito di un evento dannoso: Business Continuity* – KNOWITA'

Gilardoni – *“La Protezione Aziendale”* – Ed. EGEA

A cura di G. Forestieri – *“Risk Management: strumenti e politiche per la gestione dei rischi puri dell'impresa”* – Ed. EGEA

N. Misani – *“Introduzione al Risk Management”* – Ed. EGEA

R. Rota, G. Nano – *Introduzione alla affidabilità e sicurezza nell'industria di processo*, Pitagora Editore

ANRA (Associazione Nazionale Risk e Insurance Manager) – *Gli standard di Risk Management e l'ISO 31000*, 2011.



Cineas, Consorzio universitario non profit fondato nel 1987 dal Politecnico di Milano, si occupa di formazione manageriale sui temi della gestione dei rischi e di diffusione della cultura della prevenzione. Oggi il Consorzio annovera 58 soci di cui 5 atenei, primarie compagnie assicurative a livello nazionale e internazionale, società di brokeraggio, associazioni di categoria, aziende e studi professionali.

Attualmente, il Consorzio organizza 8 master annuali: Risk engineering e management on line, Insurance financial risk management, Environmental risk assessment and management, Loss adjustment basic on line, Loss adjustment advanced, Expert loss adjuster, Hospital risk management e Life Skills.

Dalla sua costituzione, Cineas ha formato quasi 2500 professionisti del rischio e del loss adjustment che rivestono ruoli di prestigio nelle principali aziende del mercato. La faculty del Consorzio è composta da 250 professionisti, esperti nelle singole discipline, provenienti sia dal mondo accademico che da quello aziendale e consulenziale.

www.derris.eu

With the contribution of the LIFE financial instrument of the European Community.
LIFE14 CCA/IT/000650

