

Emergenze, continuità di business e piani di contingenza

Analisi degli strumenti utili a fronteggiare rischi ed imprevisti nel mondo industriale

Alessandro Pone
(TheKom Srl)

Edoardo PONE
(Comerint Engineering Srl)

INTRODUZIONE

La recrudescenza di eventi delittuosi dovuti ad attività terroristiche deve incominciare a far riflettere su aspetti che non sono confinati esclusivamente in ambito politico. I fatti testimoniano che l'attività terroristica è stata esportata nei paesi industrializzati non solo ai fini di creare una divisione dell'opinione pubblica, e dunque di destabilizzare eventualmente gli assetti politici, ma ha iniziato a colpire anche le fonti economiche. Quanto accaduto nel luglio del 2005 in Egitto (Sharm el Sheikh) ne è una riprova. La domanda ricorrente è: i criteri e gli strumenti attualmente utilizzati sono in grado di far fronte alle nuove esigenze in materia di sicurezza degli impianti e di salvaguardia delle attività produttive? Certamente nell'ultimo decennio molto si è fatto per migliorare questi aspetti. Un particolare impulso è venuto anche dal "Problema dell'anno 2000". Ci si chiede però: il livello delle aziende sui temi in oggetto è omogeneo? La realtà odierna è che la maggior parte delle aziende è strutturata secondo catene cliente-fornitore (Supply Chain) piuttosto articolate. La vulnerabilità di siffatte strutture produttive, come si sa, è localizzata negli anelli deboli che potrebbero determinare il cosiddetto effetto "domino". Scenari di questo tipo sono stati mai presi in considerazione? Nel seguito si cerca di fornire degli spunti di riflessione su questi temi, cominciando dapprima a presentare gli strumenti attualmente disponibili in materia di gestione delle emergenze, di continuità di business e di contingenza per poi individuare eventuali punti critici ed infine suggerire delle azioni correttive.

LA GESTIONE DELLE EMERGENZE

L'emergenza è un evento calamitoso improvviso ed imprevisto che comporta un possibile rischio per i beni, per gli insediamenti, per l'ambiente e soprattutto per l'integrità della vita delle persone. Un simile evento richiede di essere fronteggiato con azioni immediate ed efficaci. Gli eventi che comportano rischi sono dovuti a fattori di tipo antropico o naturale. Tra i primi si citano gli incidenti industriali, quelli derivanti da inquinamento e quelli nucleari. Tra i secondi sono ben note le catastrofi provocate

da terremoti, inondazioni e frane. La probabilità che avvenga un evento dannoso non può essere del tutto eliminata, ciò che si deve perseguire è la riduzione di tale probabilità e l'attenuazione degli effetti dovuti ad un eventuale evento prodottosi. La riduzione della probabilità di accadimento di un evento calamitoso si attua mediante analisi di tipo tecnico valutando i potenziali rischi. L'attenuazione degli effetti è invece un aspetto che richiede un grande sforzo organizzativo (specifici piani per ogni tipologia di eventi possibili, integrazione tra le organizzazioni di pronto intervento, interventi effettuati da personale ben addestrato, adeguatezza di mezzi, informative rapide ai dipendenti ed alla popolazione, etc.). In base alla gravità ed entità degli eventi calamitosi, le emergenze si dividono in: limitate, locali, generali.

Le emergenze "*limitate*" sono caratterizzate da situazioni di moderato pericolo, circoscritto in ristrette aree, difficilmente estensibile ad aree limitrofe dell'impianto. Queste emergenze sono affrontate e risolte da personale interno dell'azienda appositamente designato ed addestrato. Esse comportano l'esistenza di piani di emergenza interni (PEI) predisposti, coordinati ed attuati dal Direttore dell'impianto in ottemperanza con il D.Lgs 626/94, il D.Lgs 334/99, il DM 978/2000 ed alle "Norme di Sicurezza" previste nel "Manuale Operativo di Impianto".

Le emergenze "*locali*" sono caratterizzate da situazioni di grave pericolo, localizzato inizialmente in aree circoscritte che però, nel tempo, possono estendersi ad aree limitrofe compromettendo l'integrità dell'intero impianto. Queste emergenze richiedono l'intervento coordinato di più enti o amministrazioni competenti in via ordinaria. Esse comportano l'esistenza di piani di emergenza esterni (PEE) predisposti e coordinati dal Prefetto (Legge 225/92 Art. 14).

Le emergenze "*generali*" sono caratterizzate da situazioni di grave pericolo che appaiono, sin dall'inizio, difficilmente contenibili nell'ambito dell'impianto e che, con grande probabilità, si possono estendere all'esterno. Queste emergenze per loro natura ed estensione debbono essere fronteggiate con mezzi e poteri straordinari e necessitano di interventi coordinati a livello nazionale. Esse

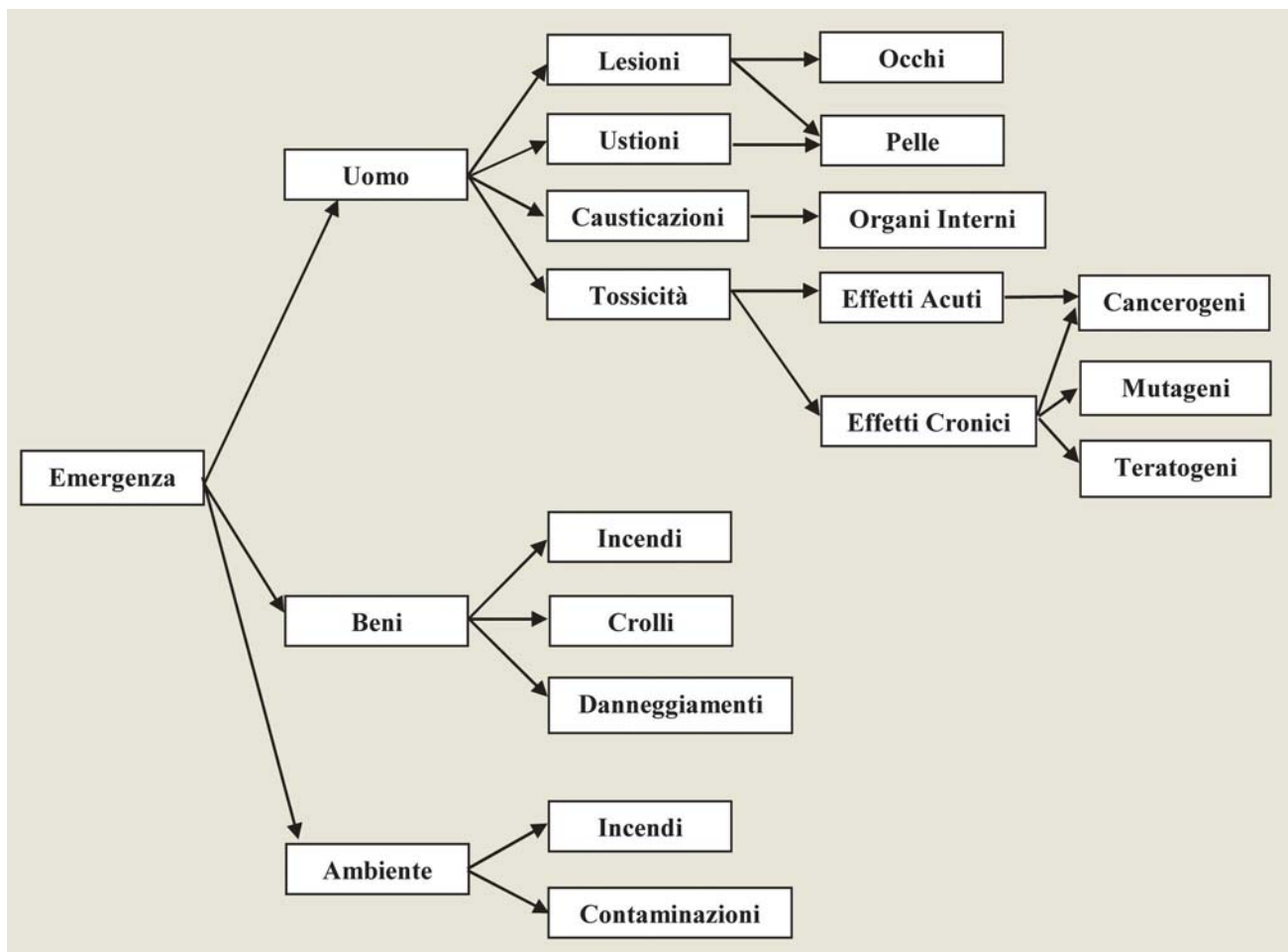


Fig. 1 Schema dei principali, potenziali danni provocati da un incidente rilevante in un impianto industriale.

Figura 2 - Impianti soggetti agli obblighi degli artt. 6-7-8 del D.Lgs 334/99 (Fonte M.A.T.T.; Elaborazione APA al 31/12/2002)

Tipologia di attività	Impianti	
	N°	%
Stabilimento chimico o petrolchimico	288	25,6
Deposito di gas liquefatti	247	22,0
Raffinazione petrolio	17	1,5
Deposito di oli minerali	298	26,5
Deposito di fitofarmaci	27	2,4
Deposito di tossici	40	3,6
Distillazione	21	1,9
Produzione e/o deposito di esplosivi	52	4,6
Centrale termoelettrica	15	1,3
Galvanotecnica	21	1,9
Produzione e/o deposito di gas tecnici	43	3,8
Acciaierie e impianti metallurgici	14	1,3
Altro	40	3,6
Totale	1.123	100,0

Figura 3 - Distribuzione sul territorio del rischio industriale - Impianti rientranti nel D.Lgs 334/99 (vedi fig. 2) (Fonte M.A.T.T.; Elaborazione APAT al 31/12/2002)

Tipologia di attività	%
Lombardia	23
Piemonte	10
Emilia	10
Veneto	8
Lazio	7
Campania	6
Sicilia	6
Puglia	4
Sardegna	4
Altre	22
Totale	100

comportano l'esistenza di un piano di emergenza nazionale (PEN) predisposto, coordinato ed attuato dal Dipartimento della Protezione Civile della Presidenza del Consiglio dei Ministri (Legge 225/92 Art. 9).

Si definisce "procedura" un documento che precisa la sequenza di azioni, le particolari modalità operative, le risorse, i mezzi ed i tempi necessari per effettuare una specifica attività (cosa fare, come farlo, con quali risorse ed in quali tempi). Si definisce "piano" l'insieme di attività necessarie a fronteggiare un ben definito problema. Esiste per ogni piano una sequenza vincolata di attività (percorso critico) che deve risultare idonea a fronteggiare ogni specifica emergenza. Un piano di emergenza è il risultato di un complesso processo che inizia con l'analisi di tutte le ipotesi di rischio, prosegue con la selezione delle ipotesi di rischio più probabili, poi con lo studio dei possibili scenari di ciascun evento considerato (previsione di ciò che può accadere), ed arriva, infine, a definire come gestire la situazione di emergenza al fine di attenuare i possibili danni dell'evento in esame. I piani di emergenza sono utilizzati da lungo tempo ed esistono per essi metodologie di realizzazione consolidate.

Le emergenze "locali" o "generali" sono attivate a seguito di un "incidente rilevante" che è definito come evento provocato da "una emissione, un incendio o un'esplosione di grande entità, dovuto a sviluppi incontrollati che si verificano durante l'attività di uno stabilimento industriale e che dia luogo ad un pericolo grave, immediato o differito, per la salute umana o per l'ambiente, all'interno o all'esterno dello stabilimento, e in cui intervengano una o più sostanze pericolose". Tali incidenti possono provocare rilasci di energia (incendi, esplosioni) o tossici (nube tossica dovuta ad emissioni di gas, vapori e fumi). Si osserva che gli effetti di un incidente rilevante comportano quasi sempre danni alle persone, ai beni ed all'ambiente (vedi figura 1). Esso può anche causare la parziale o totale perdita di un impianto. Il danno economico che si concretizza in simili circostanze è rilevante e condiziona tutto il ciclo di vita dei costi dell'impianto (LCC - Life Cycle Costing). È importante rilevare che gli eventi calamitosi sono amplificati dalla tipologia delle attività produttive e dalla natura e quantità dei beni prodotti, utilizzati ed immagazzinati. In tal caso potremmo parlare di potenziali rischi "intrinseci" agli impianti stessi. In base a questi concetti il legislatore ha emanato una legge (D.Lgs 334/99) che definisce le attività e le sostanze pericolose per le quali esistono degli obblighi speciali in tema di sicurezza. In figura 2 sono riportate le tipologie di attività classificate come pericolose ed il relativo numero di impianti censiti al 2002. In figura 3 è presentata la distribuzione sul territorio del rischio dovuto a tali impianti. I dati in oggetto sono forniti dal Ministero dell'Ambiente e della Tutela del Territorio (Elaborazione APAT al 31/12/2002) e riguardano esclusivamente le industrie rientranti nel D.Lgs 334/99. Nelle figure 4a, 4b e 4c so-

no riportate, per vari argomenti, le principali norme di riferimento.

LA CONTINUITA' DI BUSINESS

Con il termine "continuità di business", nelle aziende di produzione, si identifica l'insieme delle azioni idonee a garantire la continuità della produzione ritenuta strategica (Mission Critical) in situazioni critiche che possono pregiudicare il regolare svolgimento della normale operatività. Queste azioni sono dirette ad assicurare sia la disponibilità delle materie prime e dei materiali di consumo, sia la disponibilità e la funzionalità delle apparecchiature necessarie a supportare il livello di produzione predefinito. Il piano di continuità di business ha la funzione di ipotizzare una serie di possibili e plausibili scenari socio-economici e di definire, per ciascuno di essi, i livelli di produzione che si intendono raggiungere e le azioni da intraprendere a tale scopo. L'ottica di questi piani è quella di considerare l'azienda come un sistema chiuso ed autonomo in grado di fornire prodotti "Mission Critical" per un arco di tempo ritenuto idoneo al ripristino delle condizioni di normalità. La durata di questa autonomia è definita in base alla missione (mission) dell'azienda ed è spesso vincolata a fattori economici, legali od istituzionali.

La metodologia necessaria per sviluppare i piani di continuità di business è riassumibile nei seguenti passi principali:

- identificazione dei processi di business aziendali fondamentali (*Main Business Processes Identification*);
- analisi delle potenziali cause di rischio per i processi aziendali fondamentali (*Business Risk Analysis*). L'analisi del rischio include fattori quali le perdite di competitività, di quote di mercato, di capacità a fare business per problemi interni o per cause esterne dovute a fornitori, clienti o interruzioni di pubblici servizi. Quote di mercato od il buon nome di una azienda si possono perdere anche se altri ritengono che non si sta facendo i necessari sforzi di adeguamento alle esigenze emergenti. Da non trascurare, infine, anche fattori legati alla sicurezza e segretezza. Queste analisi, integrate in un quadro organico composto da elementi oggettivi, danno origine ad una serie di scenari di riferimento.
- stima delle eventuali perdite economiche e dei danni provocati da ciascuna delle potenziali cause di rischio (*Business Impact Analysis*). La valutazione dell'impatto sul business relativo a ciascuno degli scenari di riferimento deve essere quantificata in termini economici per avere una "misura" del potenziale danno provocato.
- individuazione dei processi di business critici (PBC) in base ad una analisi delle perdite economiche sostenibili (*Business Critical Processes Identification*).
- stesura dei piani di continuità di business per i processi di business critici (*Business Continuity and Recovery Plans issuing*).

I processi di business critici (PBC) sono individuati in base alla probabilità di accadimento delle potenziali cau-

se di rischio (scenario ipotizzato) ed al calcolo delle potenziali perdite economiche da esse causate. In funzione della tipologia di ciascun PBC (aree B-C-D di figura 5), si utilizzano differenti politiche di gestione (mitigazione, risoluzione o condivisione del rischio) nella stesura del relativo piano di continuità di business. Se non vi sono vincoli particolari (sicurezza, penali contrattuali, perdite di quote di mercato, immagine, etc.), l'equa determinazione dei costi sostenibili per affrontare gli effetti indesiderati di uno scenario ipotizzato è calcolata in base al concetto di "speranza matematica". In altri termini, la cifra da stanziare per mitigare l'evento indesiderato è data dal prodotto della probabilità di accadimento dello scenario ipotizzato moltiplicato il valore delle potenziali perdite economiche. Poiché uno scenario è costituito da diversi fattori di rischio, la formula che viene in genere applicata è:

$$CMS = p_1F_1 + p_2F_2 + \dots + p_kF_k = \sum_{j=1}^k p_jF_j = \Sigma pF$$

dove:

CMS sono i costi di mitigazione sostenibili;

p₁ è la probabilità di accadimento del fattore di rischio 1;

F₁ è la potenziale perdita economica da attribuirsi al fattore di rischio 1.

Alla base dei possibili scenari socio-economici considerati sta comunque l'assunto che, per i fornitori delle materie prime o dei semilavorati, si adotta la strategia della loro diversificazione massima compatibile con il mix più economico della fornitura necessaria. Per ciascun fornitore, con quota ben definita, si individuano anche i possibili fornitori alternativi e quindi si attua la politica di rotazione dei contratti. Per i servizi quali luce, gas, acqua (utilities), oltre ad avere fornitori esterni, si predispongono impianti ausiliari interni che garantiscano l'autonomia necessaria. Per altri tipi di servizi e per i materiali di supporto si individuano alternative praticabili o si definiscono opportuni livelli di scorta in funzione del livello di produzione e di autonomia prescelto. Le strategie di fornitura dei prodotti finiti ai clienti dipendono molto dalla natura dei prodotti e dalla tipologia di distribuzione. Certamente è necessario avere magazzini di stoccaggio per la produzione sia nell'impianto che nei nodi della catena di distribuzione ed è indispensabile prevedere alternative anche per i vettori di distribuzione.

L'enfasi che è stata sin qui data agli aspetti produttivi tiene conto del fatto che è ormai divenuta consuetudine individuare i processi di business critici quasi esclusivamente in base agli interscambi con le terze parti. Fattori tecnici quali la disponibilità e la funzionalità dell'impianto, nonostante influenzino la produzione, non sono generalmente considerati in questi piani tra le cause di rischio. Essi vengono demandati come vincoli ad altri piani, detti di contingenza, correlati con quelli di business. L'ipotesi generalmente assunta, in buona sostanza, è che l'impianto sia nelle normali condizioni di funzionamento

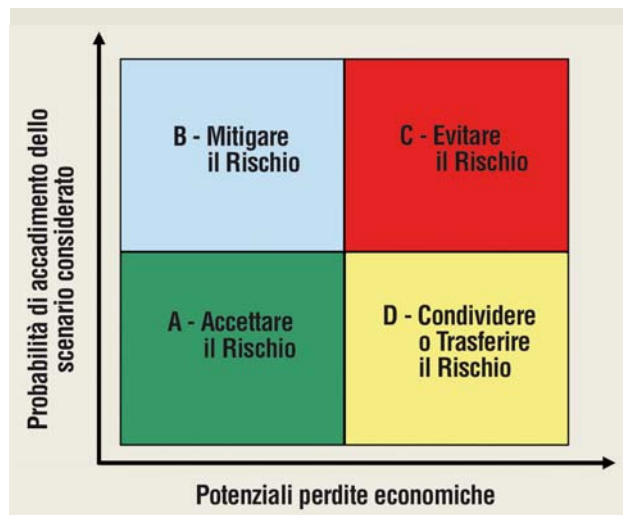


Fig. 5 Individuazione dei Processi di Business Critici (Aree B-C-D) e delle relative politiche di gestione.

e che le funzioni esercizio e manutenzione siano in grado di garantire la piena efficienza dell'impianto stesso. Ciò viene giustificato dal fatto che i piani di continuità di business hanno coperto sinora archi temporali limitati a qualche settimana. I piani di continuità di business sono nati nelle industrie americane a metà degli anni 60, si sono parzialmente diffusi solo negli anni 90 ed hanno avuto un consistente sviluppo a seguito dei piani di contingenza realizzati per il "Problema dell'Anno 2000". Nelle aziende di servizi e nella Pubblica Amministrazione il concetto di continuità di business è recepito in modo diverso ed è assimilabile a quello dei piani di contingenza.

I PIANI DI CONTINGENZA

Con il termine "contingenza" si identifica l'insieme delle azioni idonee ad eliminare o ridurre l'impatto di un rischio o di una minaccia prima, durante o dopo il verificarsi di un malfunzionamento o di un guasto degli impianti. E' bene ricordare che la disponibilità e l'efficienza degli impianti sono regolarmente assicurate dalla manutenzione con attività pianificate (manutenzione preventiva) e non (manutenzione correttiva). Gli interventi di manutenzione sono in genere effettuati in conformità con le indicazioni dei costruttori delle apparecchiature, con le "best practices" e tenendo conto dell'esperienza maturata sia in impianti simili che sull'impianto stesso. Malfunzionamenti o guasti con bassa probabilità di accadimento sono considerati anomali e non sono contemplati nelle normali procedure di manutenzione. Alcuni di essi, però, possono assumere una tale rilevanza da causare effetti potenzialmente molto pericolosi che danno origine a delle vere e proprie emergenze. L'analisi di questi malfunzionamenti o guasti "rari" o "limite" può essere affrontato mediante la ricerca di apparecchiature e componenti critici o con studi di tipo affidabilistico. Questi ultimi determinano la probabilità di guasti singoli e multipli e permettono anche di analizzare la probabilità di eventi concatenati (effetto domino). I piani di contingenza sono stati origina-

riamente sviluppati per affrontare queste problematiche ed hanno come obiettivo quello di prevenire e limitare potenziali danni rilevanti provocati da rottura o malfunzionamento di apparecchiature, in casi "rari" o "limite", e di ripristinare nel più breve tempo possibile la situazione di normale operatività. Alla base dei piani di contingenza, come si può desumere, vi sono delle problematiche tecniche di particolare complessità. Esse necessitano di essere affrontate da esperti molto qualificati che, per quanto riguarda gli impianti industriali, provengono in genere dall'ingegneria di manutenzione e dal processo. Un caso speciale di contingenza è stato il problema dell'anno 2000. Esso consisteva nella possibilità di malfunzionamento dei dispositivi elettronici che gestivano la data con otto caratteri (digit) secondo lo standard allora in uso (es.: 03/05/72). Cosa sarebbe successo il 31/12/99 alle ore 23:59? Come i dispositivi elettronici avrebbero reagito al cambio di anno (01/01/00)? I dispositivi ed i relativi software di supporto avrebbero continuato a funzionare correttamente? Sicurezza e continuità operativa sarebbero state garantite? Basti pensare a quanti dispositivi di sicurezza utilizzano questi chip e a quante funzioni di impianto sono controllate dai Distributed Control Systems (DCS) e dai Supervisory Control and Data Acquisition Systems (SCADA). Chiaramente si trattava di un problema "unico" che andava affrontato sia con la risoluzione di problemi tecnici che con definizione di procedure operative specifiche per ogni tipologia di malfunzionamento ipotizzato. Poiché il problema era comune a tutte le aziende e le pubbliche amministrazioni del mondo, oltre alla soluzione dei problemi tecnici ed infrastrutturali di ciascuna azienda, la realizzazione dei piani di contingenza venne estesa anche alle "terze parti" per evitare l'effetto "domino". La struttura dei problemi trattati dai piani di contingenza divenne pertanto la seguente:

- Analisi e soluzione di problemi tecnici relativi all'impianto (figure 6 e 7);
- Analisi e soluzione di problemi infrastrutturali dell'azienda (sistemi di automazione dell'impianto, centro EDP, rete di elaborazione dati e PC, autonomia minima per le utilities) (figure 8);
- Analisi e soluzione di problemi riguardanti le terze parti (fornitori di utilities quali acqua, luce, gas, telefonia etc.).

In tal modo si generò una certa qual sovrapposizione di contenuti tra emergenze, piani di continuità di business e di contingenza (figura 9). Furono utilizzati, infatti, differenti approcci per la realizzazione dei piani di contingenza, approcci che tuttora sono praticati e che possono essere riassunti come segue:

- quello nel quale i piani riguardano le problematiche relative al malfunzionamento di apparecchiature di impianto;
- quello nel quale i piani sono assimilati a procedure di emergenza;
- quello nel quale si dà largo spazio alle problematiche della sicurezza e dell'ambiente;

- quello nel quale l'enfasi maggiore è posta sul concetto di continuità del business.

Questo ultimo approccio, ad esempio, è quello utilizzato dalla Pubblica Amministrazione, dalla Sanità e dalle Banche. In tali contesti questi piani sono quasi esclusivamente rivolti a prevenire e mitigare gli effetti dannosi, sia per l'immagine che per l'interruzione o scadimento dei servizi, dovuti a cadute dei sistemi informativi (intrusioni esterne di hacker, virus informatici o guasti) o delle utilities. Un tipico esempio si è avuto con il black-out elettrico del 28 settembre del 2003.

E' consuetudine associare al concetto di contingenza anche qualsiasi altro evento che causi la parziale e temporanea interruzione del funzionamento degli impianti, l'interruzione di un servizio o la diminuzione degli standard di qualità (degrado) dei beni/servizi forniti.

Il tempo massimo per il ritorno alle condizioni di normalità (RTO - Recovery Time Objective) è, al massimo, dell'ordine di qualche giorno. La massima perdita economica sostenibile per ogni evento deve essere anche chiaramente definita (RPO - Recovery Point Objective). Il danno economico di queste perdite può essere rilevante.



Per visionare l'articolo completo visita il portale
www.manutenzione-online.com