Aziende resilienti

Giancarlo Butti
Europrivacy

Resilient compaines

Sommario: *La capacità di un'azienda di resistere ad eventi avversi è condizionata da molteplici fattori fra i quali la crescente dipendenza dai propri interlocutori.*

Abstract: *An organization's ability to resist to adverse events is conditioned by multiple factors including increasing reliance on its stakeholders*

1. Essere resilienti

Il termine resilienza ha fatto di recente la sua comparsa all'interno di una delle normative più invasive ed estese, in quanto perimetro di applicazione, il REGOLAMENTO (UE) 2016/679 meglio noto come GDPR (Regolamento generale sulla protezione dei dati).

Il GDPR prevede infatti, fra le misure di sicurezza (Articolo 32), che i titolari ed i responsabili, garantiscano:

a) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la* ***resilienza*** *dei sistemi e dei servizi di trattamento;*

oltreché:

b) *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*

Più in generale, per comprendere il concetto di RESILIENZA possiamo rifarci alle definizioni date dai maggiori dizionari, come il Treccani:

1. *Nella tecnologia dei materiali, la resistenza a rottura per sollecitazione dinamica, determinata con apposita prova d'urto: prova di r.; valore di r., il cui inverso è l'indice di fragilità.*
2. *Nella tecnologia dei filati e dei tessuti, l'attitudine di questi a riprendere, dopo una deformazione, l'aspetto originale.*
3. *In psicologia, la capacità di reagire di fronte a traumi, difficoltà, ecc.*

o il Garzanti:

1. *(fis.) proprietà dei materiali di resistere agli urti senza spezzarsi, rappresentata dal rapporto tra il lavoro necessario per rompere una barretta di un materiale e la sezione della barretta stessa*

2. *capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi ecc.: resilienza sociale*

Nel contesto di questo articolo consideriamo la RESILIENZA come la capacità di un'azienda di reagire di fronte ad un evento avverso.

Questo può essere causato da eventi naturali quali un terremoto, volontari quali un attacco terroristico, fortuiti quali un incidente.

In realtà un'azienda è resiliente se è in grado di affrontare qualunque tipo di evento avverso, quali il mutare della congiuntura economica, l'evoluzione del mercato, i cambiamenti tecnologici, l'interruzione della propria catena di fornitura, la crisi/perdita dei clienti strategici.

2. Il contesto

Prima di addentrarci nell'analisi dei possibili elementi da prendere in considerazione per valutare la resilienza di un'azienda, è opportuno considerare la sempre crescente interconnessione esistente fra l'azienda ed i propri interlocutori.

Questi comprendono ad esempio:

- clienti
- fornitori
- outsourcer
- utilities
- dipendenti/collaboratori
- oltreché le infrastrutture.

Eventi che interessano i propri outsourcer IT o centri esterni di lavorazione così come la perdita di figure chiave, sono elementi che possono in qualche modo influire sulla capacità di un'azienda di continuare nella propria attività; questi possono comprendere fra gli altri:

- una interruzione prolungata di fornitura di servizi essenziali al funzionamento dell'azienda, quali alimentazione elettrica, gas, combustibile, acqua, comunicazioni…
- una interruzione prolungata di fornitura di materie prime/componenti/servizi essenziali per la continuità del business
- una interruzione di commesse da parte di un cliente strategico
- l'infortunio o perdita di collaboratori essenziali
- danneggiamenti a edifici o strutture nelle vicinanze dell'azienda che impediscono o riducono in modo significativo la fruibilità o l'accesso all'area produttiva
- il danneggiamento o la chiusura prolungata a infrastrutture che garantiscono i collegamenti limitando la possibilità di movimento di personale e merci

Edifici	Distruzione fisica di edifici, impianti, infrastrutture, magazzini	• Terremoti • Tsunami ed altri eventi naturali • Incendio • Ordigno esplosivo
	Temporanea indisponibilità degli edifici	• Sostanze contaminanti • Allarme bomba • Sciopero dei trasporti • Manifestazioni • Mancanza di energia
Personale	Soggetti chiave per l'azienda • Amministratori • Detentori di know how esclusivo • Soggetti che hanno privilegi particolari (amministratori di sistema…) • Soggetti in numero rilevante	• Sequestro • Ferimento/uccisione • Ricatto (ad esempio in seguito a sequestro dei familiari o ad altri elementi) • Corruzione ad esempio ai fini di spionaggio o sabotaggio • Epidemia e simili
IT	• Distruzione di dati/informazioni e apparati • Furto di dati e informazioni con o senza perdita degli stessi • Alterazione di dati e informazioni • Interferenza nel funzionamento degli apparati e delle comunicazioni • Interferenza nel funzionamento degli impianti produttivi	• Malware • Intrusione • Sabotaggio • Attacco • Incidenti • Malfunzionamento
Interruzione di fornitura/esistenza di un fornitore essenziale	Ambiti di fornitura • Materie prime/semilavorati • Lavorazioni • Servizi essenziali • Manutenzione software personalizzato essenziale • Manutenzione impianti • …	• Attacco subito • Motivi economici • Cessata produzione • Stato di crisi • Vincoli contrattuali di esclusiva da parte di altri clienti • Contenzioso
Utilities/Telco	Interruzione fornitura di: • Elettricità • Gas • Acqua • Comunicazioni •	• Attacco/distruzione agli edifici/centrali • Attacco/guasto delle linee di distribuzione • Guasto temporaneo • Mancanza di materie prime • Contenzioso
Outsourcer	• Interruzione del servizio • Degrado del servizio a livelli inaccettabili • Interruzione delle connessioni	• Attacco/distruzione agli edifici/centrali • Attacco/guasto delle linee di connessione • Guasto temporaneo
Infrastrutture	Interruzione di: • Vie di comunicazione • Linee elettriche • Trasporto di energia • Linee di comunicazione • …	• Attentati • Crollo/distruzione • Manifestazioni • Manutenzione straordinaria • …

Tabella 1. Esempi di eventi avversi

Per ognuno di questi interlocutori l'azienda dovrebbe valutare i possibili scenari di crisi ed i possibili impatti, al fine di individuare e pianificare le possibili soluzioni.

Non necessariamente tali soluzioni devono essere fra loro omogenee e coerenti in quanto le singole macroaree ed all'interno di queste il singolo fornitore/outsourcer/cliente possono essere oggetto di specifiche soluzioni.

Ad esempio, per quanto attiene i fornitori è possibile individuare una serie di strategie preventive quali:

- la definizione di criteri di selezione del fornitore che consentano di valutare la sua resilienza
- la predisposizione di specifiche clausole contrattuali
- la verifica della priorità di fornitura nei confronti degli altri clienti
- la verifica della documentazione attestante la capacità di garantire la continuità operativa
- la verifica della documentazione dei test effettuati/della partecipazione ai test di terzi
- la verifica della documentazione in merito a precedenti incidenti e alla loro gestione
- la valutazione delle conseguenze di una interruzione di fornitura (in funzione della durata della interruzione)
- …

e risolutive, quali ad esempio:

- l'individuazione di fornitori alternativi
- lo stoccaggio di materie prime e di componenti
- l'utilizzo di materiali/processi alternativi
- l'autoproduzione (ad esempio di energia elettrica)
- …

Quello che conta è che l'azienda abbia effettuato una opportuna valutazione dei vari scenari di crisi ed individuato preventivamente le possibili soluzioni che possono comprendere, fra gli altri, il non mettere in atto alcuna azione preventiva.

L'importante è che l'azienda ne sia consapevole ed abbia valutato e continuamente monitorato l'evoluzione sia degli scenari di crisi, sia dei propri interlocutori a vario titolo.

L'insieme delle azioni che l'azienda può mettere in atto rientrano in quello che è il piano di continuità operativa, basato ad esempio su criteri suggeriti da standard e buone pratiche come quelle del BCI (Business Continuity Institute, https://www.thebci.org/).

Gli scenari e le possibili soluzioni prospettati da questi standard trovano un parziale recepimento anche in alcune normative, quali la Circolare 285 di Banca d'Italia (relativa al mondo finanziario), o nella vecchia versione del CAD (relativo alla pubblica amministrazione).

Pur essendo parziali, gli scenari e le soluzioni descritte all'interno di queste normative e le soluzioni proposte dai rispettivi organismi tecnici,[1] possono trovare una valida applicazione anche nelle organizzazioni diverse da quelle citate.

In particolare i documenti prodotti sono di norma di alta qualità e, quantomeno quelli rivolti alla P.A., liberamente e gratuitamente disponibili a tutti.

3. Valutare il rischio

Qual è la probabilità che un'azienda possa subire un evento avverso e quali sono i danni che può subire in questo caso?

Sebbene esistano numerose metodologie di analisi del rischio[2] queste si rifanno in genere a due formulazioni; la classica:

RISCHIO = PROBABILITÀ X IMPATTO

o la più generica formula che introduce nella valutazione anche altri elementi quali le vulnerabilità e le minacce.

RISCHIO = f(Probabilità, Danno, Vulnerabilità, Minacce)

È evidente che nel caso di eventi avversi naturali, quali un terremoto, questi sono legati essenzialmente alla collocazione geografica dell'azienda ed alla periodicità ed intensità nel tempo di tali eventi. Altri elementi che possono aumentare il livello di rischio legato alla posizione dell'azienda sono determinati anche da elementi non legati all'ambiente naturale, quali ad esempio la presenza di altre aziende che effettuano lavorazioni pericolose o che sono un probabile obiettivo di attacco terroristico (ad esempio le infrastrutture critiche).

Diverso è il caso di eventi che sono determinati, ad esempio, da azione volontarie di malintenzionati, siano questi esterni o interni all'azienda.

La probabilità di accadimento di tali eventi è determinata da un lato dall'appetibilità dell'azienda e dall'altro dalla facilità con cui un attaccante può portare avanti la propria azione.

Difficilmente è possibile intervenire sul livello di appetibilità di un'azienda, perchè questa è una sua caratteristica intrinseca.

È quindi necessario provvedere con delle opportune contromisure, alcuni esempi delle quali sono riportati nelle tabelle 2, 3, 5.

---

[1] Agenzia per l'Italia digitale: *Linee guida per il disaster recovery delle pubbliche amministrazioni.* ABILAB: *Metodologie varie, strumenti, gruppi di lavoro, osservatorio sulla business continuity*

[2] G. Butti, A. Piamonte: Misurare la physical cyber security - La Comunicazione N.R.&N. http://www.isticom.it/documenti/rivista/rivista2016/6_85-118_misurare_la_sicurezzaiscom.pdf

È evidente che tale riflessione dovrebbe essere estesa alla catena dei propri interlocutori; più un soggetto appare appetibile, maggiori dovrebbero essere le misure di sicurezza e prevenzione in essere.

È significativo notare che le misure di prevenzione e sicurezza sono molto specifiche e coprono cioè ambiti di rischio ben definiti.

Ad esempio l'attivazione di un sito di disaster recovery per il proprio data center non è esaustivo rispetto a tutte le possibili minacce di natura informatica; un malware potrebbe contemporaneamente diffondersi sia presso il CED principale, sia presso il CED secondario.

Di fatto una soluzione costosa, quali un sito di DR, risolve situazioni di indisponibilità di larga parte del sistema informativo presso il CED primario o la mancanza/inagibilità del CED stesso. Situazioni più limitate di crisi, quali la mancanza di singole componenti del sistema informativo sono risolte con altre tecniche come illustrato nei successivi paragrafi.

Anche eventi apparentemente più banali, quali ad esempio il malfunzionamento prolungato di un'applicazione, potrebbero tuttavia portare ad una interruzione di un servizio essenziale per l'azienda ed è per questo che è fondamentale disporre di contratti di assistenza con tempi di intervento concordati e stringenti con i propri fornitori.

In considerazione della costante automazione ed interconnessione anche dei dispositivi di produzione, gli aspetti della sicurezza IT e della capacità di garantire la continuità del servizio, non vanno più limitati alle componenti tradizionali del sistema informativo, ma vanno estesi ai reparti produttivi dell'azienda.

Per quanto attiene eventuali attacchi cyber le misure di sicurezza devono comprendere sia interventi di natura preventiva, sia un costante monitoraggio degli eventi di sicurezza, attività quest'ultima estremamente onerosa e specialistica, che sicuramente non è alla portata della maggior parte delle aziende.

Il passaggio al cloud potrebbe essere in molti casi una soluzione, in quanto il ricorso a servizi di prevenzione e monitoraggio centralizzati rendono applicabile anche alle piccole e medie aziende strumenti e misure di sicurezza altrimenti fuori portata.

Indispensabile inoltre una cultura della sicurezza, sia per indirizzare tutti gli utenti verso comportamenti virtuosi nella gestione degli strumenti aziendali, sia per consentire loro di individuare e segnalare immediatamente le varie tipologie di attacco, che in molti casi si configurano con l'inoltro di una semplice mail.

Elementi di rischio della sede in base alla collocazione	– Zona sismica – Corsi d'acqua nelle vicinanze con rischio esondazione – Aziende con lavorazioni pericolose – Installazioni pericolose (aeroporti, depositi carburanti...) – Area degradata
Elementi di mitigazione in base alla vicinanza dei servizi	– Carabinieri o altre forze di polizia e vigilanza – Ospedali o altri presidi – Vigili del fuoco
Misure di sicurezza generali della sede	Anti intrusione – Antifurto – Vigilanza – Videosorveglianza – Controllo accessi – Recinzioni – Cancelli – Grate alle finestre – Porta blindata – Serratura di sicurezza Antincendio – Estintori – Idranti – Rilevatori – Allarmi – Porte taglia fuoco Altre misure – Antisismica – Anti allagamento – Eventi atmosferici (fulmini)
Altro	Regolarità degli impianti – Elettrico – Climatizzazione Continuità elettrica – UPS – Generatori Altro – Aree separate per ricevimento clienti/fornitori
Procedure	– Procedura di gestione degli accessi (comprese autorizzazioni, revoche, smarrimento badge…) – Procedura di gestione dei visitatori/manutentori

Tabella 2. Protezione di un edificio
Fonte: Sicurezza totale 4.0 L'ABC sulla phisycal cyber security per i DPO e le PMI (e non solo), G. Butti ITER

Misure di sicurezza CED	Anti intrusione – Adeguato posizionamento all'interno dell'edificio – Pareti soffitto/pavimento – Pareti di adeguato spessore e robustezza – Misure anti effrazione – Controllo accessi – Videosorveglianza – Antincendio – Rilevatori di fumo, calore, allagamento – Misure antincendio compatibili con le apparecchiature presenti – Porte antincendio di adeguata dimensione – Interruttore generale della alimentazione elettrica – Impianto di climatizzazione – Continuità elettrica – Gruppo di continuità (per lo spegnimento corretto) – Gruppo elettrogeno (per la continuità del servizio) – Coerenza fra i dispositivi di continuità e le normative VVFF – Apparecchiature e impianti – Pavimento galleggiante per l'adeguato posizionamento dei cavi – Corretto e ordinato posizionamento dei cavi elettrici – Corretto e ordinato posizionamento dei cavi di rete – Posizionamento ordinato delle apparecchiature nei rack – Spazio intorno ai rack adeguato alla movimentazione e manutenzione delle apparecchiature – Gestione remota delle apparecchiature

Tabella 3. Protezione di un CED (Fonte: Sicurezza totale 4.0, G. Butti - ITER)

Altra fonte di rischio è rappresentata dalla mancata formalizzazione del know how aziendale e dell'eccesivo ricorso a figure chiave[3].

Tali figure possono essere esse stesse oggetto di attacchi o ricatti analogamente ad altre tipologie di figure critiche per un'azienda quali gli amministratori, o dotate di particolari privilegi che possono mettere a rischio la resilienza dell'azienda, quali gli amministratori di sistema.

Perdita assoluta	Perdita di informazione che il collaboratore non aveva condiviso ed esplicitato e che quindi non sono state acquisite nel patrimonio informativo aziendale. Danno derivante dal passaggio del collaboratore alla concorrenza alla quale potrà 'vendere' le proprie specifiche competenze e le informazioni relative all'azienda di provenienza
Perdita parziale	Perdita di competenza e conoscenza in seguito a variazione di ruolo in azienda Degrado delle prestazioni in seguito ad insoddisfazione o 'stress'

Tabella 4. Perdita di un collaboratore
Fonte:La tutela del capitale intellettuale, G. Butti – www.sicurezzainternazionale.gov.it

[3] G. BUTTI, *La tutela del capitale intellettuale,* Il Mondo dell'intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2016, http://www.sicurezzanazionale.gov.it/sisr.nsf/aziende-e-sicurezza/la-tutela-del-capitaleintellettuale.htm

4. Implementare la comunità operativa

La continuità operativa di un'azienda è sempre più spesso condizionata dal corretto funzionamento del suo sistema informativo.

Riveste quindi un ruolo particolarmente importante la continuità dei servizi IT.

Al riguardo il settore bancario ha una specifica normativa dal 2004; in seguito altri settori, come la PA, hanno emesso specifiche normative sulla continuità operativa.

Adeguato posizionamento all'interno dell'edificio Uso del locale unicamente come CED
Pareti soffitto/pavimento senza discontinuità Pareti di adeguato spessore e robustezza
Misure anti effrazione Controllo accessi Videosorveglianza
Rilevatori di fumo, di calore, di allagamento Misure antincendio idonee all'uso con le apparecchiature presenti Interruttore generale dell'alimentazione elettrica Misure per la continuità elettrica Gruppo di continuità e stabilizzatore Gruppo elettrogeno Coerenza fra i dispositivi di continuità e le normative VVFF
Impianto di climatizzazione
Porte antincendio di adeguata dimensione Pavimento galleggiante per l'adeguato posizionamento dei cavi
Corretto ed ordinato posizionamento dei cavi di alimentazione Corretto ed ordinato posizionamento dei cavi di rete Identificazione dei cavi
Posizionamento ordinato delle apparecchiature nei rack Spazio intorno ai rack adeguato per la movimentazione e manutenzione delle apparecchiature
Gestione remota delle apparecchiature

Tabella 5a. Protezione di un CED (Fonte: Sicurezza totale 4.0, G.Butti – ITER)

VIRUS e PROGRAMMI PERICOLOSI Misure tecniche ed organizzative per la protezione del sistema informativo da software malevolo	Presenza di antivirus su tutte le postazioni Processo di aggiornamento Processo di scansione
	Aspetti organizzativi e gestionali Procedura in caso di allerta Procedura per la gestione di utility che possono bypassare le normali misure di sicurezza Istruzioni che vietano l'uso di file o software non autorizzati
FIREWALL Misure tecniche ed organizzative per la protezione del sistema informativo da intrusioni principalmente dalle reti esterne (internet, outsourcer, partner….)	Presenza di firewall centralizzato e/o personale, adeguatamente configurato
	Aspetti organizzativi e gestionali Procedura di aggiornamento Procedura di monitoraggio Procedura in caso di allerta
RETE COMUNICAZIONI Misure tecniche per la realizzazione	Uso di cablaggio adeguato Segmentazione fisica Protezione fisica dei cavi lungo tutto il loro percorso e di tutti gli apparati di rete Segmentazione logica Uso di protocolli sicuri Disabilitazione protocolli non sicuri Uso VPN Crittografia nella trasmissione Uso di certificati Creazione DMZ per server esposti Firewall opportunamente configurati
	Aspetti organizzativi e gestionali Revisione periodica della configurazione Monitoraggio delle prestazioni Monitoraggio dei tentativi di accesso fraudolenti Aggiornamento periodico del software Gestione delle vulnerabilità degli apparati di rete Gestione degli accessi esterni (VPN, RAS…)
MONITORAGGIO Strumenti disponibili per l'attività di monitoraggio	IDS IPS Sniffer Network scanner Content Filtering Correlazione di eventi
	Aspetti organizzativi e gestionali Verifica degli aspetti normativi per l'uso dei dispositivi di monitoraggio Sincronizzazione dei sistemi Registrazione dei log Raccolta e gestione dei log per fini interni Raccolta e gestione dei log per opponibilità a terzi Analisi dei log

Tabella 5b. Misure di sicurezza logica

VULNERABILITA' Misure tecniche ed organizzative per gestire le vulnerabilità dei sistemi	Vulnerability assessment periodico Hardening dei sistemi Attivazione di processi automatici di aggiornamento
	Aspetti organizzativi e gestionali Mappatura dei sistemi Definizione delle modalità di gestione delle vulnerabilità (manuale o automatica) Procedura di allertamento Procedura di valutazione Procedura di installazione o modifica configurazioni
(*) HARDENING Processo per la messa in sicurezza dei sistemi	Disattivazione delle funzionalità di servizi inutili Adeguata configurazione Revisione periodica
AGGIORNAMENTO SISTEMI Misure tecniche ed organizzative per gestire gli aggiornamenti dei sistemi non legati ad aspetti di sicurezza	Gestione patch
	Aspetti organizzativi e gestionali Mappatura dei sistemi Definizione delle modalità di gestione degli aggiornamenti (manuale o automatica) Procedura di allertamento Procedura di valutazione Procedura di installazione

Tabella 5c. Misure di sicurezza logica

Va precisato che entrambe le normative, pur dando larga enfasi alla continuità del sistema informativo, hanno come punto di attenzione la continuità della azienda nel suo complesso, anche per le parti non strettamente IT.

È in tale contesto che fanno la loro comparsa termini come Alta Affidabilità (alta disponibilità), *Disaster Recovery* (nel seguito *DR*) e *Business Continuity* (nel seguito *BC*) che pur esprimendo concetti molto diversi fra loro, sono tutti orientati a garantire la continuità di un servizio. È assolutamente fondamentale che questi termini siano condivisi nel loro significato fra tutti gli attori, siano essi interni o esterni, coinvolti nella progettazione, realizzazione e gestione di una soluzione atta a garantire la resilienza di un'azienda.

Tabella 6. Impatti diretti, indiretti e consequenziali (Fonte: Sicurezza totale 4.0, G. Butti – ITER)

Descrizione del bene	Disco fisso
Impatto diretto	Rottura
Impatti indiretti	Perdita dati Interruzione del servizio
Impatti consequenziali	Perdite economiche Danno di immagine Rischio legale

5. Alta Affidabilità

Per Alta Affidabilità si intende la capacità di un sistema di resistere a situazioni locali, anche estese di guasto (perdita di un singolo componente di un server: disco, alimentatore, scheda di rete…, di un intero server, di un apparato di rete, di un intero locale CED), al fine di consentire la continuità nell'erogazione del servizio.

Le soluzioni normalmente adottate si basano sulla duplicazione degli elementi e sulla predisposizione di infrastrutture in grado di contrastare i rischi più comuni (mancanza di alimentazione, incendio, allagamento…). Si va dalla semplice ridondanza dei componenti, fino alla replica di un intero gruppo di server o alla replica di interi locali CED, collocandoli in posizioni tra loro più o meno geograficamente distanti.

La ridondanza può comprendere gli impianti di alimentazione elettrica, il cablaggio di rete, i sistemi di condizionamento e tutti gli altri apparati che servono a garantire il corretto funzionamento degli apparati IT, gli apparati di rete e la rete geografica (instradata su percorsi diversi e spesso di differenti operatori). Il tutto commisurato ovviamente al risultato che si desidera ottenere e al rapporto fra i costi e i benefici attesi.

In una piccola/media azienda è già molto se si vi è una ridondanza di server, mentre in una banca non è raro trovare duplicate intere stanze del CED, nello stesso edificio o in edifici vicini in un campus di dimensioni limitate (il confine fra Alta Affidabilità e *DR* in questi casi può essere molto labile e limitarsi alla semplice definizione). Questo consente ovviamente di mantenere con facilità un sincronismo dei dati, che sono duplicati o replicati nel continuo due o più volte sui vari dispositivi di storage.

La ridondanza dei vari apparati può essere molto costosa, ma è assolutamente indispensabile evitare che esistano componenti non ridondati il cui guasto possa compromettere tutta l'architettura.

Altro aspetto molto importante è la corretta progettazione e disposizione dei vari elementi (ad esempio è poco utile avere due router, di cui uno sia il backup dell'altro, posizionati nello stesso *rack*).

Altri errori da evitare sono ad esempio il posizionamento delle batterie tampone all'interno del CED, il posizionamento di apparecchiature elettriche sotto un condizionatore che potrebbe perdere liquidi, la mancanza di un accordo formalizzato con un fornitore per un rifornimento garantito di carburante anche nel week end, la mancata ridondanza dell'impianto di condizionamento …

Mentre una grossa azienda dispone probabilmente di una propria autonoma sede, molte realtà anche significative hanno la loro sede in edifici condivisi con altre organizzazioni, il cui livello di sicurezza non è noto a priori. In un contesto di promiscuità con altre organizzazioni vanno quindi valutati molti altri fattori; ad esempio il fatto che il proprio CED possa essere allagato da infiltrazioni d'acqua dei locali soprastanti, o che il proprio personale debba essere sgombrato a causa di un incendio al piano sottostante (esperienza questa vissuta in prima persona dall'autore).

Il CED dovrebbe essere raggiungibile e gestibile il più possibile da remoto, onde evitare un'interruzione del servizio derivante dalla irraggiungibilità o inagibilità fisica dello stesso.

Chi progetta l'Alta Affidabilità pensa solitamente che sia sufficiente garantire che gli apparati del CED possano restare operativi anche in situazioni critiche.

Raro è infatti il caso che vengano posti sotto gruppo di continuità le postazioni utente o l'illuminazione degli uffici, con la conseguenza che i servizi del CED sono attivi, senza che però nessuno li possa utilizzare.

In fase di progettazione di una soluzione in Alta Affidabilità del proprio sistema informativo sarà quindi necessario prendere in considerazione l'intera catena degli elementi che possano garantire un servizio per l'utente finale.

Alta affidabilità	La capacità di un sistema di resistere a situazioni locali, anche estese di guasto (perdita di un singolo componente di un server: disco, alimentatore, scheda di rete…, di un intero server, di un apparato di rete, di un intero locale CED), al fine di consentire la continuità nell'erogazione del servizio.
Disaster Recovery	Il DR si occupa di garantire la continuità del servizio ICT in caso di guasto esteso/distruzione del sistema informativo o infrastruttura fisica che lo ospita.
Business Continuity	La business continuity si occupa della continuità del business. Si tratta di un tema più ampio e complesso della semplice capacità di ripristinare il sistema informativo di un'organizzazione.

Tabella 7. I termini della continuità operativa

6. Le soluzioni per il DR

L'Alta Affidabilità non è un'alternativa al *DR* e non va con questo confusa. Un danneggiamento esteso, che comprometta il corretto funzionamento del sito primario (o la sua agibilità), richiederà necessariamente la disponibilità di un sito alternativo dove poter ripartire. Una copia di dati, sistemi, applicazioni, configurazioni e relativa documentazione dovrà quindi essere sempre disponibile e utilizzabile, in un luogo adeguatamente lontano dal sito principale.

Tra la situazione estrema e quella di regolare erogazione dei servizi ci sono molti stadi intermedi, che andrebbero definiti e valutati a priori, in modo da non lasciare incertezze nella corretta gestione dei casi di emergenza.

L'attivazione del piano di *DR* è infatti un'attività molto rischiosa e spesso senza ritorno, che quindi va effettuata con le dovute cautele: si attivano le azioni di *DR* proprio quando non è possibile farne a meno.

Nella pratica esistono inoltre diverse situazioni di malfunzionamento del sistema informativo per le quali né l'Alta Affidabilità, né il *DR* costituiscono un rimedio.

Oltre alle problematiche che possono derivare da un attacco cyber, si è già citato come anche un semplice malfunzionamento di un applicativo può bloccare per ore l'erogazione di un servizio IT. Questo aspetto va adeguatamente valutato al fine di distinguere la vera emergenza dalla

normale operatività. Nelle due situazioni, anche se apparentemente simili come risultato finale (una mancata erogazione del servizio) posso valere regole operative e ruoli gerarchici diversi.

Per quanto attiene alle possibili soluzioni per il *DR*, queste variano moltissimo, in funzione delle architetture, dei tempi di ripristino richiesti, dei budget allocati.

Per una piccola/media azienda il *DR* può essere costituito dalla copia di dati, applicazioni, configurazioni e da un adeguato contratto di assistenza che consenta di ripristinare nel più breve tempo possibile l'uso di server e apparecchiature, installandovi le copie dei dati e del software precedentemente salvati.

La cosa più importante in questo caso è disporre dell'opportuna documentazione di tutte le configurazioni presenti.

Per massimizzare la possibilità di ripristino della operatività è utile in questi casi concentrare in un unico repository tutti i file vitali per l'azienda, siano essi costituiti da data base o archivi destrutturati, ivi inclusi tutti quelli creati con i *tool* di produttività individuale. La *policy* dell'azienda deve vietare agli operatori di poter salvare file indispensabili per lo svolgimento del proprio lavoro sulle proprie postazioni individuali (condizione questa che si può effettivamente verificare solo in fase di test). Le organizzazioni, anche le più grandi, fanno un larghissimo uso di applicazioni realizzate direttamente dagli utenti mediante strumenti di produttività individuale, di norma non censite e della cui importanza si ha evidenza solo quando non sono più disponibili.

Per le organizzazioni di grosse dimensioni, o meglio per l'azienda che hanno *Data Center* significativi, il problema è molto più articolato; sono infatti sufficienti pochi elementi non replicati o non aggiornati (e quindi non allineati) per rischiare di vanificare tutto il lavoro svolto o quantomeno per richiedere significative attività di analisi e operativa per riattivare il corretto funzionamento del CED. È al riguardo indispensabile un consistente e aggiornato apparato documentale, che consenta di avere sotto controllo tutti i componenti che costituiscono il CED, le loro configurazioni, le loro interdipendenze. Tale documentazione deve essere sempre accessibile e quindi non deve essere conservata sugli stessi server che è necessario ripristinare.

È pertanto necessario predisporre un vero e proprio piano di *DR* nel quale occorre specificare dettagliatamente gli strumenti da adottare e le azioni da eseguire in via preventiva (in fase di progettazione e implementazione) e in caso di incidente, sia da parte degli operatori incaricati di gestire l'ordinaria amministrazione, sia da quelli responsabili della riattivazione del sito secondario (questi ultimi è buona norma che non siano quelli che gestiscono il sito primario, in quanto potrebbero risultare non disponibili proprio in conseguenza dell'incidente che ha coinvolto tale sito). Il piano deve essere costantemente aggiornato e verificato, cosa che può risultare particolarmente onerosa e complessa.

7. La realizzazione del sito secondario

Se un'azienda ha deciso di attrezzarsi con due siti alternativi, deve seguire dei criteri ben definiti per il loro allestimento. Ad esempio, i siti

primario e secondario devono essere sufficientemente distanti per garantire il non coinvolgimento contemporaneo degli stessi da un evento distruttivo esteso, tipo un terremoto. La scelta del sito secondario dovrebbe inoltre tener conto anche della raggiungibilità del sito stesso da parte del personale che dovrà poi gestirlo.

I tempi di ripartenza dei sistemi in *DR* non sono infatti condizionati solo da aspetti tecnici, ma anche dalla disponibilità del personale incaricato della sua gestione. Di conseguenza, posizionare un sito di *DR* in una località difficilmente raggiungibile, o che richieda tempi di percorrenza molto elevati, può rivelarsi una pessima idea.

Una buona soluzione consiste nel prevedere la possibilità di gestione remota del sito dopo la sua attivazione, cosa che risulta molto favorita dalle scelte che puntano sull'outsourcing del servizio, includendovi anche il supporto del personale tecnico. In questo caso, particolare attenzione va data agli aspetti contrattuali e al tipo di servizio offerto. Molto spesso, infatti, l'outsourcer "vende" spazi e potenza elaborativa da utilizzare in caso di emergenza a più clienti contemporaneamente. Diventa quindi importante valutare quale sia l'effettiva garanzia di continuità offerta dai fornitori, in particolare nei casi in cui molti clienti della stessa area geografica siano interessati da uno stesso evento dannoso e richiedano contemporaneamente l'attivazione del proprio servizio di *DR*.

Le architetture sulle quali impostare il servizio sono numerose, per cui occorre valutare bene quelle che più si addicono alle proprie esigenze.

Si possono distinguere in funzione del fatto che presso il sito di *DR* siano disponibili solo spazi per accogliere i sistemi, che siano presenti sistemi spenti, che siano presenti sistemi attivi ma condivisi, che siano presenti sistemi attivi e continuamente allineati con il sistema di produzione. Per quest'ultima soluzione sono disponibili diverse varianti: ad esempio i sistemi nel sito di *DR* possono essere utilizzati contestualmente a quelli di produzione per bilanciare il carico, oppure possono essere utilizzati per svolgere altri compiti (ad esempio sviluppo e test).

Avere sistemi già attivi nel sito di DR garantisce di solito tempi di ripartenza più contenuti, ma soprattutto garantisce l'azienda circa l'effettivo funzionamento dei sistemi.

Un sito di DR può non contenere tutti gli elementi del sito primario, per un'evidente ragione di costi e opportunità. Per lo stesso motivo un'azienda può decidere di non garantire lo stesso livello di servizio quando questo è offerto dal sito primario o da quello secondario. Rimane tuttavia fondamentale, nella individuazione dei componenti che costituiranno il sito secondario, includere non solo i componenti più critici per l'attività della azienda, ma anche quelli architetturali a loro supporto. È infatti poco utile ripristinare un mainframe con relative applicazioni e dati, se non si ripristina il sistema che consente agli utenti di raggiungerlo (ad esempio il sistema di autenticazione e di instradamento).

I LIVELLI DELLE SOLUZIONI *(Tier LG)*	PRINCIPALI INDICATORI			ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)	
	RTO		RPO max	***Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO***	***Aspetti minimali connessi al sito di DR***
	Min	Max			
Tier 1*:*	7g	>7 gg solari	max 7gg solari	Copia su supporti rimuovibili	Sito esistente ma da attrezzare con risorse elaborative/ server solo reperibili. Il sito di *DR* è predisposto ad accogliere personale e apparecchiature, ma rimane privo di risorse fino al momento di effettiva necessità. Di solito consiste solo di un ambiente fisico dotato di corrente elettrica e di rete dati con idonee misure di sicurezza (es: sistema antincendio ed antifumo; sistema antiallagamento; sistema di alimentazione in grado di garantire l'erogazione di energia elettrica anche a fronte di prolungate interruzioni di alimentazione nella cabina di fornitura; sistema d'aria condizionata per garantire temperatura ed umidità costante; impianto per il ricambio d'aria; sistema di accesso controllato).
Tier 2: .	3g	max 7 gg	max 7 gg solari	Copia su supporti rimuovibili	Il sito dispone di hw e connettività già funzionante ma su scala inferiore rispetto al sito principale o a un sito alternativo sempre disponibile e con replica costante dei dati.
Tier 3:	1g	3g	Max 1 gg	Electronic vaulting: soluzione che comporta il backup dei dati presso il sito alternativo in maniera elettronica, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time più veloce.	Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile e con replica costante dei dati. Il backup avviene in modalità elettronica e quindi sono necessari collegamenti fra i siti tenuto conto della tipologia, quantità e periodicità dei dati da backupare

Tabella 8a. Possibili soluzioni per il DR Fonte: Linee guida per il Disaster Recovery (DR) delle PA

Nella pratica più un sistema è complesso e più è difficile che la ripartenza avvenga senza problemi (salvo il caso in cui i due siti siano contemporaneamente attivi e allineati). Essendo infatti impossibile gestire una ripartenza in blocco di tutti i sistemi e applicazioni di un CED di medie dimensioni si possono generare dei disallineamenti fra i dati in quanto un'applicazione ripristinata potrebbe inoltrare (o aspettare) flussi di dati da applicazioni non ancora ripristinate. Va inoltre considerato che difficilmente un sistema informativo di una certa complessità non scambi flussi con applicazioni di outsourcer e fornitori, che devono essere raggiungibili anche dal sito di *DR.*

I LIVELLI DELLE SOLUZIONI *(Tier LG)*	**PRINCIPALI INDICATORI**			**ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)**	
	RTO		**RPO max**	***Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO***	***Aspetti minimali connessi al sito di DR***
	Min	Max			
Tier 4:	4h	3gg	Max 4 h	Asincrono On line (risorsa storage accesa)	Il sito alternativo è solitamente "un duplicato" del sito originale con tutti i sistemi hardware e la quasi totalità dei backup di dati disponibile. Il sito alternativo può essere pronto ed operativo in alcune ore o meno. Nel caso in cui il personale deve essere spostato fisicamente presso il sito secondario, il sito risulterà operativo solo dal punto di vista del data processing. La piena operatività sarà raggiunta quando anche il personale avrà raggiunto il sito.
Tier 5:	1h	max 4 h	max 5 min	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi ciascuno con capacità sufficiente a prendere in carico il lavoro dell'altro e in cui l'aggiornamento del dato avviene solo quando entrambi i siti hanno completato l'update (con perdita dei soli i dati che in quel momento stanno per essere processati). E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.
Tier 6*:*	0m	1h	Zero min.	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi, ognuno dei quali possiede capacità sufficienti a farsi carico del lavoro dell'altro; in questa soluzione il carico di lavoro da un sito all'altro si trasferisce immediatamente ed automaticamente. E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

Tabella 8b. Possibili soluzioni per il DR Fonte: Linee guida per il Disaster Recovery (DR) delle PA

8. Le soluzioni di business continuity

La *business continuity*, come il nome stesso porta a intuire, si occupa della continuità del *business*.

Si tratta di un tema più ampio e complesso della semplice capacità di ripristinare il sistema informativo di un'azienda.

Banca d'Italia ad esempio ha previsto, nella Circolare 285, che le banche debbano predisporre un piano di *BC* che:

prende in considerazione diversi scenari di crisi basati almeno sui seguenti fattori di rischio, conseguenti a eventi naturali o attività umana, inclusi danneggiamenti gravi da parte di dipendenti:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o indisponibilità di personale essenziale per il funzionamento dei processi aziendali
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari)
- alterazione o perdita di dati e documenti critici
- apparecchiature critiche
- indisponibilità di sistemi informativi critici.

Tali scenari interessano in realtà anche tutte le altre organizzazioni che erogano servizi o per le quali la gestione delle informazioni costituisce una componente essenziale per garantire la produzione. Per le aziende manifatturiere tali scenari andrebbero integrati aggiungendo, ad esempio, l'indisponibilità di una linea di produzione o la mancanza di semilavorati o materie prime.

In generale la capacità di continuare la propria attività è condizionata almeno dai seguenti fattori:

- disponibilità di strumenti
- disponibilità di informazioni
- disponibilità dei collaboratori (in particolare delle figure chiave)

ai quali si aggiungono per le aziende di produzione:

- disponibilità di materie prime, semilavorati, infrastrutture, impianti…

Deve essere inoltre disponibile un edificio con le opportune infrastrutture in cui collocare quanto sopra.

La disponibilità di un sito alternativo di produzione rispetto a quello principale si può configurare con varie modalità, analogamente a quanto avviene per le soluzioni di DR dei sistemi informativi.

È possibile disporre di un sito in cui si svolga effettivamente la produzione nel continuo (non necessariamente dello stesso prodotto), o

che sia semplicemente pronto a farla o che possa ospitare l'attività produttiva.

È anche possibile in alternativa ricorrere a terzi che possano subentrare temporaneamente all'attività mediante un contratto di appalto ovvero individuare i possibili fornitori (e monitorarli nel continuo) presso i quali acquisire in tempi rapidi tutto ciò che serva per far ripartire la produzione.

Quello che conta è che quanto sopra non sia lasciato al caso e che siano allocati i relativi budget.

Molte delle informazioni di cui è necessario disporre per predisporre soluzioni di continuità operativa dovrebbero già essere disponibili presso le organizzazioni in quanto necessarie per il rispetto di normative quali il GDPR che richiede la mappatura di:

- sistema informativo
- archivi elettronici
- documenti
- processi e attività
- struttura organizzativa
- controparti
- …

Le verifiche effettuate nel corso della mia attività di consulenza presso numerosissime organizzazioni dei più disparati settori e dimensioni hanno di fatto evidenziano le seguenti carenze:

- mancanza di documentazione
- assenza di una mappatura e formalizzazione dei processi
- parti di processi chiave non documentate
- eccessivo ricorso a figure chiave, in particolare nelle organizzazioni medio piccole
- ampio uso di applicazioni di operatività individuale in aggiunta al sistema informativo dell'azienda
- dispersione nella archiviazione dei file, molto spesso collocati anche sui singoli pc in uso ai collaboratori
- assenza di un censimento della documentazione presente al di fuori del sistema informativo
- mancanza di qualunque classificazione delle informazioni.

Inoltre molte delle informazioni che servono a un'azienda sono ancora presenti unicamente al di fuori del sistema informativo; vi è ancora un largo uso di documenti, spesso per esigenze legali e contrattuali.

Tali documenti rivestono particolare rilevanza per un'azienda, ma nessuno si preoccupa di custodirne una copia in un luogo diverso dal sito principale (analogamente a quanto dovrebbe avvenire per le copie di *backup*), o di procedere a una loro digitalizzazione o meglio ancora alla loro eliminazione sostituendoli con documenti informatici di analoga valenza legale.

Anche nel caso di una adeguata documentazione quello che si riesce a mappare è comunque solo la componente esplicita del patrimonio informativo dell'azienda, la parte cioè formalizzata. La componente implicita, patrimonio molto spesso di singoli collaboratori, è esclusa da questo censimento, salvo poi costituire l'elemento chiave per consentire o no la ripresa dell'attività.

Anche il legislatore se ne é accorto e uno degli scenari previsti da Banca d'Italia è proprio l'indisponibilità di personale essenziale per il funzionamento dell'azienda.

Nell'accezione bancaria si tratta del personale che presiede i processi critici o vitali (molto spesso legati all'area finanza), che in un corretto piano di *business continuity* è sostituibile con altro personale che abbia le stesse competenze, che possibilmente utilizzi gli stessi strumenti e che possibilmente operi in un'altra località (in questo modo viene coperto anche lo scenario della indisponibilità di un sito, in quanto spesso i due eventi sono fra loro collegati).

Nel caso di una piccola azienda può essere difficile trovare un idoneo sostituto di una figura chiave ed è per questo motivo che, come precedentemente illustrato, i processi critici o vitali dell'azienda dovrebbero essere il più possibile documentati (il tutto da conciliare con le indispensabili esigenze di riservatezza).

Alcune tipologie di servizi conservano rilevanti quantità di documenti, quasi sempre in originale, che in caso di distruzione (incendio, alluvione…) comportano da un lato danni gravissimi per i clienti e dall'altro un costo enorme per la ricostruzione degli stessi (dove possibile) e per la ripresa dell'attività.

Nel caso specifico, un semplice accorgimento come la conservazione delle sole copie (lasciando ai clienti la responsabilità della conservazione degli originali) ridurrebbe drasticamente i rischi e consentirebbe una più agevole ripresa del lavoro.

Altro punto di difficile attuazione per una piccola e media azienda è la predisposizione di soluzioni relative a uno scenario come la distruzione o l'inaccessibilità di strutture nelle quali siano allocate unità operative o apparecchiature critiche. Per una società di servizi parte del problema può essere risolto de localizzando i sistemi presso un outsourcer o facendo ricorso a soluzioni cloud e predisponendo come possibili fonti di accesso postazioni mobili o telelavoro.

Le soluzioni cloud costituiscono probabilmente oggi una delle soluzioni più percorribili per le piccole e medie organizzazioni, per aumentare considerevolmente la propria resilienza esternalizzando i propri sistemi informativi, con la possibilità di includere nel servizio anche la loro continuità operativa.

Non mancano anche esempi concreti di società manifatturiere che hanno saputo esternalizzare molte attività (dalla progettazione alla produzione) concentrando in spazi molto limitati le sole attività di coordinamento e marketing.

Esternalizzazione, diversificazione anche geografica delle unità produttive, così come diversificazione dei fornitori, costituiscono alcune delle possibili strategie di continuità anche per le aziende di produzione.

9. Le attività di test

Le attività di test dovrebbero avere la finalità di confermare il corretto funzionamento delle soluzioni implementate e di individuare le criticità al fine di risolverle. Per tale motivo dovrebbero essere svolte (gradualmente) anche in condizioni che rispecchino situazioni critiche reali, come i periodi di ferie o importanti attività di manutenzioni dei sistemi.

Le possibili attività di test sono molteplici e devono partire dalle verifiche dei singoli componenti di un sistema, sia quelli del sito primario, sia quelli del sito secondario (nel caso in cui sia attivo un sito di *DR*), quali apparati di elaborazione, apparati di archiviazione dati, configurazioni per la ripartenza, fino al test complessivo dell'intero sito.

Vanno testati tutti gli impianti (impianto elettrico, LAN e relativi componenti, connettività esterna, continuità elettrica, condizionamento, controllo accessi e videosorveglianza, antincendio, antiallagamento) e gli elementi ridondati. Tali attività vanno però eseguite con "intelligenza". Emblematico è il caso dei test dei gruppi elettrogeni, che si risolve nella maggior parte dei casi con una prova annuale del loro corretto funzionamento per un tempo molto limitato. La conseguenza di questa modalità di svolgimento del test è che il carburante permane nei serbatoi anche per anni, con effetti deleteri sulle valvole e sul galleggiante che misura il livello di carburante. Il risultato è che in una vera emergenza l'erogazione del carburante può bloccarsi per un malfunzionamento di uno di questi componenti del valore di pochi euro, vanificando così tutto il lavoro svolto.

L'esempio non è un caso isolato. Basta visitare un qualunque CED per trovare accatastati scatoloni di ogni genere in conseguenza delle costanti attività di manutenzione, spesso posizionati nelle vie di fuga o davanti agli ugelli del sistema antincendio.

È piuttosto raro che le organizzazioni, anche molto grandi, dispongano in autonomia di un sito di *DR*; molto più spesso ricorrono a servizi in outsourcing, nel qual caso la possibilità di effettuare dei test è condizionata dalla disponibilità dei tecnici del fornitore e dagli spazi dove allocare le proprie risorse presso l'outsourcer.

Il periodo per compiere i test è pertanto limitato a pochi giorni in un anno. Per ovviare a questo inconveniente è opportuno prevedere lo svolgimento di test anche presso la propria struttura. Ad esempio, la verifica puntuale della leggibilità e capacità di ripristino dei singoli componenti dei sistemi può essere fatta anche in locale, isolando opportunamente porzioni adeguate del sistema.

L'attività di test della continuità operativa per la parte non *IT* deve prevedere ad esempio l'indisponibilità di un edificio o di personale critico. In teoria in mancanza di un edificio sarebbe possibile utilizzare le stesse risorse spostandole in un'area appositamente attrezzata a tale scopo.

Questo tipo di soluzione, peraltro molto diffusa, ha il limite di non prendere in considerazione l'indisponibilità proprio delle risorse. Peraltro tale soluzione potrebbe risultare più costosa della effettiva dislocazione di risorse in luoghi diversi, essendo necessario mantenere

costantemente allineate alle postazioni principali le postazioni di riserva di solito inutilizzate, pagando comunque le relative licenze software e le relative attività di manutenzione. Pur non simulando un malfunzionamento del sistema informativo, l'esperienza ha evidenziato che un test di questo tipo comporta il coinvolgimento di diversi aspetti *ICT*. Come in precedenza accennato, solo durante i test è possibile scoprire se gli utenti utilizzano per la loro operatività strumenti di produttività individuale con cui hanno realizzato file salvati sulle proprie postazioni (spesso con macro e path assoluti), documenti, apparecchiature particolari (ad esempio telefoni con registrazione della chiamata).

Va inoltre considerato il fatto che un evento che comporta il ricorso, ad esempio, allo sgombero di un edificio e alla invocazione del piano di *BC* può accadere in qualunque momento e quindi il personale che dal sito alternativo prende in carico le varie attività troverà delle applicazioni aperte e dei file bloccati. L'*IT* dovrà quindi intervenire per sbloccare da remoto tali situazioni e per attribuire le corrette credenziali al personale subentrante.

Le modalità di svolgimento dei test di continuità operativa possono comprendere anche esercizi prettamente teorici, dedicati in particolare a verificare la preparazione del personale coinvolto e delle procedure di invocazione e gestione della crisi.

In considerazione della interconnessione con altri soggetti è inoltre necessario partecipare anche ai test di terzi e verificare, nel caso in cui due soggetti abbiano entrambi dei siti di DR che in situazioni di emergenza effettivamente funzioni tutte le possibili combinazioni di collegamento fra i siti (primario su DR e DR su DR).

Conclusioni

Garantire la resilienza di un'azienda richiede una attenta valutazione di numerosi fattori (secondo una logica di costi e benefici proporzionali agli obiettivi individuati), molti dei quali riguardano soggetti esterni all'azienda stessa.

Un esercizio complesso, per il quale le organizzazioni sono poco o per nulla attrezzate, ma sempre più necessario in una realtà sempre più interconnessa.

Note

Il testo di questo lavoro riprende stralci del contenuto degli articoli pubblicati dall'autore sulla rivista **Toolnews** (*BC*I - Itware):

- *Business Continuity,* Alta Affidabilità*, Disaster Recovery: limiti e confini*
- *Il Cloud Computing, soluzione ideale per il Disaster Recovery*
- *L'occhio dell'auditor sui piani di Business Continuity, per legge e necessità*