



## Disaster recovery: le attività da non rimandare

Al momento dell'implementazione di un Disaster recovery Pian (DRP) ci si concentra spesso sulle misure tecniche e procedurali per il ripristino dei servizi, tralasciando aspetti fondamentali legati alla comunicazione, all'informazione e agli accordi contrattuali. È invece determinante affrontare a priori tali aspetti per evitare sorprese a giochi ormai conclusi.

Rubrica di Mauro Cosmi

---

IT Security, gennaio-febbraio 2008

### Premessa

L'obiettivo primario delle attività di Disaster Recovery (DR), descritte e gestite tramite un Disaster Recovery Plan (DRP), è di dare garanzie sulla continuità e la sopravvivenza dei processi di business e dei servizi al loro supporto in caso di eventi disastrosi.

Come sinteticamente riportato nell'articolo "Disaster Recovery Life Cycle" presentato nel n. 12 di ICT Security (Maggio 2003), tali attività presuppongono che siano affrontati preliminarmente alcuni aspetti legati alla definizione dei possibili scenari di disastro, all'individuazione dei processi critici e al possibile coinvolgimento delle figure interne di riferimento e dei fornitori già presenti e/o da contattare per l'attuazione del piano.

### Dagli obiettivi teorici alla realizzazione dei presupposti

Anche se per gli addetti ai lavori potrebbe apparire un'affermazione incredibile, non è assolutamente insolito trovarsi in realtà in cui, nonostante il progetto di DR si trovi in uno stato avanzato, non siano ancora stati definiti i presupposti alla sua futura applicazione e si siano tralasciati alcuni aspetti di analisi di base, relativi per esempio:

- alla classificazione dei processi di business e ai possibili impatti derivanti dalla loro indisponibilità
- alla definizione di un processo interno decisionale e di comunicazione che permetta, in caso di evento disastroso, di dare indicazioni oggettive sulla necessità di attivare le procedure di DR
- all'individuazione e applicabilità di eventuali SLA sia verso l'interno che verso l'esterno dell'azienda
- alla definizione dei possibili referenti coinvolti nella comunicazione cliente-fornitori, ai relativi contenuti da comunicare e agli aspetti contrattuali che riguardano le attività da erogare



Un maggior approfondimento, legato all'esperienza maturata in progetti "sul campo" di DR, porta alle seguenti considerazioni.

Spesso l'esecuzione di una Business Impact Analysis (BIA) di dettaglio è considerata un'opzione a cui si cerca di sopperire con altri mezzi più snelli e/o utilizzando "informazioni di corridoio", poi rimaneggiate a quattro mani, con lo scopo di arrivare a delle risultanze definite "accettabili fino a prova contraria".

Tipicamente il danno avviene in relazione ai dati di RTO associati alle informazioni, che non possono essere rispettati, o agli RPO dichiarati che, non tenendo conto di aspetti legati agli effettivi tempi di recovery degli ambienti, spesso vengono disattesi per ovvi motivi. Il problema deriva quindi dalla generazione di informazioni, in sostituzione di quelle ottenibili con una BIA che sono dapprima validate e poi modificate in corso d'opera per "assecondare" il rispetto delle tempistiche dichiarate formalmente nel DRP di progetto.

A regime, anche se l'IT risulta in grado di raggiungere gli obiettivi prefissi, non è detto che RTO ed RPO siano rispettati. Infatti, in assenza della definizione preventiva degli scenari di disastro ed in caso di eventi potenzialmente disastrosi, l'IT attende una dichiarazione di disastro che il management potrebbe non essere in grado di dare con certezza per la mancanza di dati oggettivi atti a valutare l'evento (in termini di possibili impatti) in relazione ai costi di migrazione (totale e/o parziale) da sostenere verso un sito di DR.

Il ritardo che potrebbe derivare dall'attesa di una decisione in merito all'attivazione del DR o l'attivazione dello stesso senza un effettiva necessità potrebbe ovviamente portare a gravi perdite in entrambi i casi. È pertanto assolutamente necessario individuare e specificare a priori il livello e la tipologia di disastro che si desidera affrontare, nonché le modalità per "misurarlo" e quindi riconoscerlo in tempi accettabili.

Qualora l'azienda si appoggi a dei service provider per la gestione dei propri servizi e/o dei servizi di DR, la definizione dei SLA diviene una componente fondamentale della comunicazione. Difatti, è ovvio che senza uno SLA ben definito non ci sia modo di gestire la qualità dei servizi attesi/erogati e le relative performance, né dal punto di vista del cliente né del fornitore. L'aspetto degli SLA viene invece spesso tralasciato fino all'ultimo, non considerando che la parte contrattuale nonché la disponibilità del fornitore (o del fornitore interno di servizi) e la sua capacità di assolvere ai compiti a lui richiesti non possono essere dati per scontati. Infatti potrebbe accadere che:

- non esistano risorse adeguate (in numero e qualità)
- i costi relativi ai servizi necessari risultino troppo elevati
- l'ipotesi di richiedere servizi di DR on-demand sia inapplicabile perché non soddisfacenti i requisiti della BIA (es. in relazione a RTO ed RPO dichiarati in conseguenza di quest'ultima nel DRP)
- l'eventuale manutenzione della documentazione non sia demandabile

La mancata individuazione preventiva dei responsabili della comunicazione e la mancata definizione delle modalità con cui eseguire quest'ultima, sia verso l'interno che verso fornitori e partner, creerà sia al momento della dichiarazione di disastro che durante tutte le attività di test del DR non pochi problemi e ritardi nell'esecuzione



delle attività previste. Se poi si tiene conto che molte delle attività richieste ad eventuali service provider sono generalmente relative alla gestione delle infrastrutture, risulta subito ovvio come il fattore in oggetto possa risultare estremamente bloccante per tutte le attività successive e per il loro tracciamento. Pertanto, pena l'impossibilità di rispondere in modo efficiente e responsabile ad un eventuale disastro:

- eventuali fornitori esterni e referenti interni del DRP team (in genere composto da un management team che possa prendere le decisioni chiave e da funzioni aziendali / esterne che possano supportare / eseguire le attività descritte nel DRP) devono essere allertati sin dai primi momenti della definizione del DRP
- gli aspetti salienti relativi a contratti, reperibilità e disponibilità devono essere discussi e concordati il prima possibile nell'ambito della definizione degli SLA e dei servizi potenzialmente necessari
- le modalità di comunicazione e di scambio delle informazioni necessarie per l'esecuzione del DRP devono essere considerate e discusse appena le macrovoci relative alle tipologie d'intervento risultano formalizzate.
- 

Allo stesso modo andrà valutato attentamente e preventivamente l'utilizzo di risorse interne "delocalizzate" (sia per servizi di base e infrastrutturali che per l'erogazione delle normali attività operative) per non scoprire che quanto teoricamente implementato non risulti applicabile solo sulla carta per mancanza di risorse.

### **L'informazione al contorno**

Un altro aspetto, spesso non considerato nella giusta misura, riguarda la divulgazione delle attività di preparazione e/o manutenzione del DRP nei confronti dei referenti aziendali coinvolti, a pieno titolo o marginalmente, nell'esecuzione delle attività di DR.

Quello che spesso accade è la "costruzione a compartimenti stagni" del DRP: si creano differenti gruppi di lavoro, ognuno specializzato su una particolare tecnologia o ambiente infrastrutturale / applicativo; a questi si danno indicazioni in merito a cosa debba essere creato, ma in genere non si ricorre mai abbastanza a momenti di incontro, di discussione e integrazione di quanto realizzato fino a che non si arrivi al prodotto definitivo (il DRP) e al suo test. Se poi si pensa che spesso progetti di questo tipo riguardano ambienti e dinamiche di gestione complesse, allora è ovvio che ogni gruppo di lavoro dovrà essere allineato su quanto già prodotto e riutilizzabile, nonché sulle modalità di approccio alla soluzione:

- evitando così inutili ridondanze sulle attività descritte nei passi procedurali definiti
- riducendo al minimo la rivisitazione di quanto descritto, mantenendo al contempo un livello di dettaglio uniforme per tutte le procedure e le istruzioni operative prodotte
- ottenendo una maggiore integrazione della documentazione e facilitando la definizione delle priorità di esecuzione delle attività (cosa abbastanza difficile qualora la granularità delle "macroclassi" di attività non sia uniforme per i vari ambienti).



### **Gli aspetti contrattuali**

Come sopra indicato i requisiti nei confronti di eventuali provider esterni e partner nonché i relativi aspetti contrattuali devono essere concordati il prima possibile al fine di:

- poter modificare/integrare la formalizzazione di eventuali attività già sottoposte ad agreement fra cliente e fornitore
- permettere al fornitore di "prepararsi" ad ottemperare alle richieste effettuategli entro i tempi che l'azienda cliente si è prefissa ancor prima di interpellare in merito il fornitore stesso; oltre a quanto già detto il provider potrebbe per esempio non avere il sufficiente know-how degli ambienti da gestire o non essere l'unico owner di questi ultimi, il che lo porterebbe inevitabilmente a rifiutare l'incarico.

### **Concludendo...**

La comunicazione fra le parti coinvolte nell'attuazione del DR e le relative modalità di attivazione/ tracciamento dello stesso nonché la divulgazione delle informazioni esistenti e la definizione degli accordi contrattuali, sono tutte attività che devono essere pensate in modo interconnesso e formalizzate appena possibile all'interno del processo di realizzazione di un DRP, evitando di posticiparle al termine dei lavori. In caso contrario si dovrà mettere in conto che gli obiettivi previsti in termini di risposta ad eventi disastrosi potrebbero molto probabilmente non essere raggiunti, causando danni ingenti, se non addirittura irreparabili.

Giorgio Jandolo Cossu

Etnoteam S.p.A.