

RPO e RT0: come progettare il disaster recovery



In questo articolo parleremo ancora di **business continuity**, ovvero di *business continuity plan* ed in particolare della progettazione delle procedure di **disaster recovery**.

Molte organizzazioni che non predispongono un vero e proprio piano di continuità operativa (o *business continuity plan*, BCP), comunque hanno una **procedura di disaster recovery**, più o meno evoluta. Purtroppo, però, questa attività viene delegata quasi interamente ai responsabili ICT senza coinvolgere il management, i responsabili dei processi primari di business ed in particolare di quelli più critici.

Non che i responsabili ICT non siano in grado di progettare una procedura di *disaster recovery* adeguata, ma spesso sono loro stessi che stabiliscono i requisiti di base del *disaster recovery*, ovvero implicitamente definiscono gli obiettivi **RT0** e **RPO** che dovrebbero essere alla base della procedura.

Riprendiamo le definizioni di questi indici, già esposte in precedenti articoli, per capire meglio di cosa si tratta.

- **Recovery Point Objective** (RPO) ovvero il punto (l'istante nel tempo) al quale le informazioni sono coerenti e possono essere ripristinate per consentire la ripresa delle attività (denominato anche *Maximum Data Loss*).
- **Recovery Time Objective** (RT0): periodo di tempo entro il quale i servizi erogati, la produzione, i servizi di supporto e le funzionalità operative devono essere ripristinati dopo l'incidente che ha generato la discontinuità.

Facciamo un esempio per comprendere meglio il significato degli indici sopra esposti.

Supponiamo che una piccola organizzazione che opera nel settore dei servizi, denominata ALFA srl, decida di effettuare un **backup incrementale** dei propri dati con frequenza giornaliera su un NAS interno, mantenendo le ultime 7 versioni dei dati e che poi, per cautelarsi a fronte di eventuali catastrofi naturali che potrebbero

rendere inutilizzabile il sistema informatico aziendale e tutti i backup salvati su NAS, effettui anche un **backup completo** su nastri DAT con cadenza settimanale. I nastri magnetici dell'ultimo backup settimanale sono conservati a casa del titolare, a 20 km di distanza dalla sede dell'azienda, il quale quando si porta via il backup restituisce quello della settimana precedente.

Qual è il valore di RPO e RT0 per questa azienda?

Occorre distinguere fra diversi tipi di problemi (disastro):

1. Si tratta di un crash del sistema che ha comportato la perdita dei soli dati (eventualmente anche dei supporti di memorizzazione) oppure
2. Si tratta di un evento catastrofico che ha reso inutilizzabile l'intero server e l'infrastruttura informatica della sede di ALFA?

Evidentemente nel primo caso potrebbero essere sufficienti i backup su supporto NAS da ripristinare su un nuovo hard disk, reperibile in tempi brevi. Dunque il RT0 potrebbe essere pari anche ad una sola giornata, dipende dal tempo che si impiega a ripristinare il sistema (tempi di acquisto dei nuovi supporti di memorizzazione, tempi di eventuale reinstallazione del sistema operativo del server e degli applicativi, ecc.). Il RPO invece è pari ad una giornata di lavoro o meno, a seconda dal tempo trascorso dall'ultimo backup giornaliero eseguito. In questo caso per valutare correttamente il RT0 occorre capire quanto tempo si impiegherebbe a reinstallare il sistema, partendo dai supporti originali oppure da un'immagine del sistema creata attraverso l'impiego di macchine virtuali. Questa seconda soluzione, certamente più costosa della prima, potrebbe abbassare drasticamente il RPO.

Nel secondo caso il ripristino dell'operatività dipende anche dai danni generati alla sede dell'organizzazione: che si sia verificato un terremoto che ha reso inagibili i locali oppure un'alluvione i cui danni possano essere riparati entro qualche giorno o settimane la situazione può essere sensibilmente differente e il RT0, anche in questo caso può essere di alcuni giorni o settimane, indipendentemente dalla strategia di backup implementata. Il backup settimanale su nastro, conservato in un luogo sicuro (da valutare se la distanza dalla sede è sufficiente per garantire un'alta probabilità di evitare danni), garantirebbe un RPO di al massimo una settimana di dati persi.

Bisogna capire se questi valori, di RPO e RT0, sono accettabili per l'organizzazione oppure le perdite, in termini di dati e di discontinuità operativa, mettono a repentaglio la sopravvivenza dell'azienda.

Ricordiamo che per alcune attività critiche il verificarsi di eventi disastrosi con RT0 di settimane e di RPO di una settimana potrebbero portare a danni economici ingenti, non coperti da polizze assicurative (ritardi nella consegna di commesse con addebito di penali da parte del committente, perdita di commesse importanti, ecc.).

In questa seconda situazione occorrerebbe certamente un **sito di *disaster recovery***, ovvero un sito alternativo, geograficamente distante dalla sede principale dell'azienda, in grado di consentire la ripresa dell'attività in pochissimo tempo (ore, al massimo una giornata lavorativa) e la perdita dei dati di al massimo una giornata, dunque ottenendo un RT0 = 1 giorno e RPO = 1 giorno. Ciò potrebbe essere ottenuto senza investimenti consistenti in una struttura gemella, ma dotandosi di una infrastruttura tecnologica in *cloud*.

In conclusione la procedura di *disaster recovery* dovrebbe essere progettata da personale competente (responsabile IT, consulenti esterni, ...) basandosi su precisi input da parte della Direzione aziendale, derivanti da obiettivi di RPO e RT0 ritenuti adeguati per l'organizzazione. La procedura di *disaster recovery* progettata avrà dei costi (che possono variare in base alle soluzioni scelte) che la Direzione dovrà mettere a budget per garantirsi gli obiettivi desiderati. Viceversa bisognerà migrare verso obiettivi meno ambiziosi di RPO e RT0, ma la Direzione deve essere consapevole di ciò. In caso di disastri, infatti, nessuno potrà accusare altri di non aver pensato alle giuste contromisure ed ognuno si assumerà le responsabilità che gli spettano.