Evoluzione del Disaster Recovery

Resilienza Operativa e Gestione della Disponibilità

Informazioni documento
Versione 2.0
2 luglio 2026

Ing. Francesco Volani
Computer Systems Engineer - MEng - MBCS - CITP® - CISA® - CISM® - CRISC® - CGEIT® - CDPSE® - CSA STAR™ - CPMA - CPSM - ISO/IEC 27001 LA / 20000 LA / 42001 AI MSA - ISO 22301 LA - ISO 19011 - NIST CSF - COBIT® - ITIL®

Introduzione

Il panorama del Disaster Recovery (DR) ha subìto negli anni una trasformazione radicale, passando da una primaria focalizzazione sulla fornitura di spazi e hardware alternativo a una più recente funzione strategica incentrata sulla gestione della disponibilità delle informazioni (*availability management*).

Inizialmente il settore delle soluzioni di DR era infatti focalizzato sulla creazione di data center di emergenza che potessero affrontare condizioni di *disastro* del sito di produzione secondo scenari predefiniti, evolvendosi successivamente verso un più ampio concetto di “resilienza operativa digitale” che ha integrato concetti quali la gestione del rischio, la gestione degli incidenti, la gestione dei fornitori, così come richiamato sia nella recente normativa europea NIS2 che in quella più specificatamente bancaria DORA.

Nonostante una diffusa percezione che i progressi tecnologici abbiano sostanzialmente risolto il problema del DR, la realtà è che la natura della sfida è mutata: con la migrazione verso il *cloud* e i servizi gestiti in modalità “as a Service” il DR è diventato in gran parte una questione di gestione dei fornitori e di garanzia della disponibilità continua delle informazioni. Più in generale si può affermare che il successo di un DR moderno non deve solo integrarsi nel processo della “continuità operativa aziendale” (*business continuity management*) ma deve evolversi ed inserirsi in un più generale processo di “gestione della disponibilità” (availability management).

Evoluzione Storica del DR

Il percorso del Disaster Recovery è passato attraverso diverse fasi critiche, guidate dalla crescente dipendenza delle aziende dai sistemi informatici. Inizialmente, il recupero dei sistemi

non era percepito come una priorità, perché l'obiettivo primario era focalizzato semplicemente sul corretto funzionamento dei personal computer. Tale aspetto ha definito una primaria organizzazione dei "centri elaborazioni dati" (CED/EDP) intesi quali funzioni prettamente tecniche all'interno delle realtà aziendali.

Con l'aumento della dipendenza dai dati, le organizzazioni hanno iniziato a cercare alternative in caso di ben definiti scenari di disastro, sulla base di una graduale consapevolezza dei rischi collegati all'eventuale indisponibilità delle informazioni. I primi tentativi, come i consorzi di backup e i "cold site" si rivelarono ben presto poco pratici o troppo lenti, rappresentando soluzioni più "sulla carta" che effettivi servizi operativi in caso di reale necessità. Anche il dichiarato impegno di eseguire test periodici di funzionalità delle soluzioni implementate ha gradualmente confermato un limitato spettro delle verifiche e la sostanziale inefficacia nel rappresentare uno scenario di reale disastro (si pensi ai *tabletop test* oppure ai test su specifiche funzionalità slegate da un più complesso scenario di fermo).

L'approccio di maggior successo è stato l'adesione a servizi che offrivano computer e reti alternative "chiavi in mano". Sebbene in parte limitati da distanza, test e compatibilità, questi servizi sono stati ampiamente adottati ed hanno rappresentato una prima vera soluzione con un rapporto costi/benefici più bilanciato rispetto a soluzioni fatte in casa.

Con la graduale riduzione dei costi dell'hardware, le aziende sono infine passate a data center ridondanti di proprietà e più di recente soluzioni di "Disaster Recovery as a Service" (DRaaS) basate su cloud pubblico, che offre separazione geografica, sicurezza e scalabilità nativa.

Il cambio di paradigma: DRaaS

L'avvento del cloud e della miniaturizzazione dell'hardware ha spostato il fulcro del problema evidenziando i seguenti tre macro-aspetti:

1. Scomparsa dei data center aziendali: i costi delle infrastrutture fisiche (meccaniche, elettriche, idrauliche) hanno iniziato a superare quelli dei computer stessi, portando alla contrazione dei data center on-premises verso siti di colocation o il cloud;
2. Il ruolo dei vendor: il compito del DR non è più fornire piattaforme alternative, ma gestire i fornitori (*vendor management*): le organizzazioni si affidano a servizi "as a Service" gestiti;
3. Il limite degli SLA: i Service Level Agreement (SLA) hanno sostituito i piani di recupero tradizionali, presentando in ogni caso limiti significativi: spesso offrono solo il rimborso dei canoni di abbonamento e non coprono i danni consequenziali derivanti da un fallimento del sistema.

Il Disaster Recovery nel contesto attuale

Oggi il DR deve elevarsi da funzione operativa a ruolo tattico e strategico, collaborando strettamente con altre funzioni aziendali. Il DR deve svolgere un ruolo di garanzia della qualità nell'acquisizione di nuovi sistemi, verificando se i prodotti soddisfano le metriche di recovery e possano rispettare gli obiettivi di ripristino stabiliti dalla BIA (in particolare RPO e RTO). La parte di

sviluppo deve garantire che la resilienza sia integrata nei nuovi sistemi dalla fase di progettazione (con particolare riferimento al paradigma *security by design)*.

La modalità di verifica delle capacità di recovery (ovvero il test del DR) è cambiata profondamente, almeno in questi tre aspetti:

- Efficienza: non sono più necessari mesi di pianificazione logistica per test in siti distanti durante il fine settimana;
- Flessibilità: grazie al cloud, i test possono essere eseguiti direttamente dall'ufficio e su singole applicazioni in modo rotativo;
- Scalabilità: nonostante la facilità dei test cloud, rimangono necessari test annuali su larga scala per verificare l'efficacia operativa complessiva.

Verso la gestione della disponibilità

Il Disaster Recovery si sta evolvendo in una specializzazione più ampia denominata *availability management* ovvero "gestione della disponibilità". Caratteristiche di questo macro-processo possono essere riassunte nella seguente tabella:

Caratteristica	**Descrizione**
Obiettivo	Garantire la disponibilità continua del flusso di informazioni necessario per condurre il business
Ambito	Dalle sorgenti di dati (interne o esterne) fino all'utente finale
Natura	Funzione di tipo strategico
Requisiti	Richiede competenze specifiche del personale, che i manager senior devono valutare caso per caso

Questa evoluzione rappresenta un vero cambio di paradigma: non si tratta più solo di recuperare sistemi dopo un disastro, ma di assicurare che l'informazione sia disponibile in ogni circostanza, attraverso sistemi alternativi che garantiscono resilienza intrinseca.