©deepai.org

Garantire la continuità operativa con il giusto Disaster Recovery.

Nell'odierno panorama aziendale, la resilienza di fronte a disastri o interruzioni è fondamentale .
Un piano di continuità operativa BCP *(**Business Continuity Plan**)* solido, è essenziale per garantire la continuità delle attività aziendali in caso di eventi imprevisti.
Un elemento chiave di ogni BCP efficace è la scelta più adeguata del sito dove mantenere una copia speculare di dati e applicazioni aziendali, ovvero il sito di **Disaster Recovery** (DR) .

La selezione del tipo di sito DR appropriato, dipende da molteplici fattori; tra cui le esigenze aziendali prioritarie, le risorse finanziarie disponibili e i requisiti di conformità normativa.

Di seguito alcune delle principali tipologie di DR, con l'indicazione dei loro lati positivi e negativi e un esempio di scenario d'uso reale:

DR Attivo: Si tratta di un DR che **replica l'infrastruttura IT** sita presso la sede aziendale, pertanto è formato da apparati, applicativi, configurazioni, tutti pronti all'uso immediato in casi di blocco del sito primario. Nel sito di DR è presente in modo continuativo anche personale tecnico, che conosce il sistema aziendale ed è in grado di gestire e manutenere completamente il recovery.

Lati positivi

- Tempo di ripristino (RTO) rapido e minimo impatto sulla produttività aziendale.
  Es.: Riduzione al minimo, del tempo di inattività per un'impresa del settore

finanziario, garantendo così la continuità delle transazioni finanziarie e prevenendo gravi perdite.

- Replica speculare del sito primario, garantendo una transizione fluida. *Es.: Mantenimento delle operazioni di un sito web di e-commerce durante un picco di traffico inaspettato, senza compromettere l'esperienza utente.*

- Ideale per organizzazioni che richiedono tempi di down-time minimi.
  Es.: Società di telecomunicazioni, ospedali, enti governativi che gestiscono servizi critici etc.

Lati negativi

- Costo elevato di implementazione, manutenzione e gestione. Richiede investimenti significativi iniziali, e ridondanza di apparati, applicativi, licenze software, etc,
- Necessita di personale qualificato per la gestione e il mantenimento del DR, con conoscenza specifica della situazione tecnologica del sito primario e delle procedure da attivare nella contingenza.

Es.: Un istituto finanziario con elevate transazioni giornaliere, richiede un RTO minimo per prevenire gravi perdite finanziarie. Un DR attivo rappresenta la scelta ideale per garantire la continuità del servizio in caso di disastri come incendi, inondazioni, terremoti etc.

DR stand-bay: A differenza del DR attivo, questa tipologia di DR ha un'infrastruttura predisposta (spazio, reti, alimentazioni), ma gli apparati **non replicano totalmente** quelli presenti nel sito primario ed è privo dell'aggiornamento degli applicativi e delle configurazioni, elementi necessari per un'immediata replica del sito primario in down.

Lati positivi

- Costi inferiori rispetto ad un DR attivo, con risparmi significativi in termini di apparati, applicativi, costi iniziali di configurazione, aggiornamenti e gestione continuativa.

- Maggiore flessibilità per personalizzare l'ambiente di DR in base alle specifiche esigenze, con relativo adattamento a diversi tipi di carichi di lavoro.

Lati negativi

- Tempo di ripristino più lungo rispetto ad un DR attivo, a causa della configurazione e dell'attivazione dei vari elementi che costituiscono l'infrastruttura, con un potenziale impatto sul business aziendale.

- Necessità di risorse tecniche con specifiche competenze IT in grado di gestire in tempi ridotti il deployment.

Es.: Un'azienda che ha picchi intensi di attività in determinati periodi, potrebbe utilizzare un DR stand-bay per gestire l'aumento del traffico durante questi periodi, attivandolo il DR solo quando necessario. In questo modo, l'azienda può beneficiare di una soluzione DR scalabile ed economica senza dover sostenere i costi costanti di un DR attivo.

DR Passivo: In questo caso il DR ha anch'esso un'infrastruttura di base dedicata (spazio, alimentazione, connettività), ma richiede che tutti gli altri elementi necessari al recovery, **vengano implementati al momento** in cui il sito primario risulti essere in emergenza.

Lati positivi

- Risulta essere la soluzione di DR meno impegnativa economicamente, con costi relativi all'infrastruttura iniziale.

- Ideale per organizzazioni con budget limitati o per un DR di sistemi non critici.

Lati negativi

- Tempo di ripristino non certi, con potenziali periodi di inattività prolungati.

- Necessità di risorse tecniche con competenze IT anche non specifiche, le quali collaboreranno, in team con il personale tecnico dell'azienda, nel momento in cui il DR passivo andrà attivato.

- Non risulta adatto a organizzazioni che richiedono tempi di ripristino immediati o estremamente rapidi.

Es.: Un'azienda con ridotte esigenze di disaster recovery (es: PMI), o con risorse finanziarie limitate, potrebbe utilizzare un DR passivo per proteggere i propri dati essenziali, accettando tempi di ripristino più lunghi in caso di emergenza.

Alle tre tipologie di DR esposte, può ormai essere aggiunta anche la categoria di DR che fa uso del Cloud, o più precisamente di un **Private Cloud**, per offrire soluzioni di "**Disaster Recovery as a Service**" (DraaS), scalabili e con costi basati sulle effettive risorse occupate, nel momento del duo utilizzo.

DR - DRaaS

Lati positivi

- Scalabilità per soddisfare le esigenze di DR mutevoli nel tempo.
- Accessibilità al DR da remoto (sicurizzato tramite VPN o soluzioni similari).
- Modello di costi in base alle risorse utilizzate in un dato range di tempo.
- DR di primo approccio per evolvere ad altre tipologie di DR.

Lati negativi

- Attenta valutazione nella scelta in merito alla sicurezza e alla privacy dei dati.
- Dipendenza da un fornitore esterno.
- Necessità di connettività aziendale in fibra di alto livello (Fibra dedicata o in capacità, con linea secondaria di backup).

Come indicato inizialmente, la selezione e la scelta del tipo di DR appropriato, dipende da molti fattori interni ed esterni alla singola azienda. Tutte le valutazioni sono **tanto più importanti quanto maggiore è la criticità aziendale** circa la continuità della sua attività.
Uno dei consigli rimane quello di affidarsi sempre ad aziende con elevata esperienza e con un team di **tecnici specializzati** nelle aree IT pertinenti al DR. E' inoltre necessario non considerare prioritariamente i costi, ma **valutarli come un investimento**, volto a non far subire all'azienda, in caso di eventi negativi, perdite dirette o indirette come ad esempio rivalse da parte della sua clientela che potrebbero sfociare in azioni legali, o intervento di autorità relativi alla privacy.

IPnext
Siamo partner tecnologici di molte imprese italiane.
Insieme a loro progettiamo e gestiamo le soluzioni ICT più evolute, per continuare a crescere insieme.

- *IPnext sito Web*

- *IPnext documentazione & soluzioni*
- *IPnext LinkedIn*
- *IPnext Newsletter "Verba Volant"*

#disasterrecovery #resilienza #draas #arista #paloalto #veeam #ipnext