CASE STUDY - IT RESILIENCY LIFECYCLE MANAGEMENT

Resilienza evoluta di Backup & Recovery per oltre 550 punti vendita retail

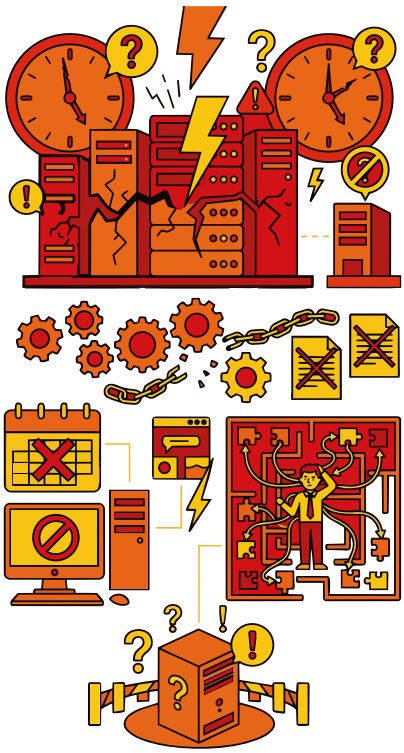
Progetto su larga scala | Durata: 1 anno

PANORAMICA

Un primario gruppo retail italiano ci ha incaricato di ricostruire integralmente la propria capacità di Disaster Recovery (DR). Il risultato è un'operatività di DR multi-vendor, pienamente governata e collaudata, che copre 17 aree tecnologiche distribuite su due siti geograficamente separati. L'efficacia della soluzione è stata validata attraverso una simulazione completa di failover dal sito primario.

LA SFIDA

A seguito di un grave disservizio infrastrutturale che ha richiesto mesi per essere ripristinato, è emersa una criticità strutturale: il cliente disponeva di un sito di DR, ma non di una reale capacità operativa di Disaster Recovery.



- **Assenza di RTO e RPO definiti** per l'intero portafoglio applicativo: gli obiettivi di continuità operativa non erano formalizzati né affidabili.
- **Mancanza di processi formali, procedure codificate** o documentazione storica di DR.
- **Nessun ciclo recente di test di DR** e preparazione interna limitata nella gestione di eventi e incidenti critici.
- **Team IT interno sovraccarico**, impegnato a orchestrare un ecosistema di fornitori ampio, frammentato e ad elevata complessità operativa.
- **Un nuovo sito di DR in fase di attivazione**, ma mai collaudato in condizioni operative reali.

STACK TECNOLOGICO

Infrastruttura
Multi-cloud Iaas | PaaS

Rete
Check Point | Palo Alto Networks | Fastweb

Virtualizzazione
VMware

Piattaforma di Gestione Applicativa:
Red Hat | OpenShift

Gestione Database
Oracle | SQL Server

Backup & Data Protection
Commvault

Identity Management
Microsoft

DELIVERABLE DI PROGETTO

1. **Strategia, Piano e Governance**
Redazione della Strategia e del Piano di DR enterprise. Istituzione del comitato di crisi/DR (tecnico, business, governance) con una chiara matrice RACI. Esecuzione della BIA (Business Impact Analysis) e mappatura di servizi e asset critici per stabilire RTO/RPO coerenti.

2. **Orchestrazione Multi-Team**
Coordinamento di oltre 15 team interni e fornitori esterni tramite gruppi di lavoro verticali dedicati.

3. **Armonizzazione Multi-Vendor**
Introduzione di una governance collaborativa strutturata tra 6 diversi vendor tecnologici terzi.

4. **Nuovo Sito di DR e Hardware**
Provisioning e collaudo dell'hub secondario a Settimo Milanese (MI), sincronizzando le logiche di replica e ripristino su tutti i livelli.

5. **430 Test e Validazioni di DR**
Una campagna intensiva di validazione, culminata nella simulazione completa di failover dal sito primario.

6. **Documentazione Completa e Conforme**
Suite documentale allineata ai template aziendali: strategia di DR, piano di test, architettura, procedure di ripristino, checklist pre/post attivazione, definizione degli RTO, tiering applicativo, piani di comunicazione, report di simulazione e piano di revisione periodica.

7. **Modernizzazione Opportunistica**
Upgrade di JBoss alla versione 8 e rinnovamento dell'infrastruttura dei Domain Controller, integrati con successo senza estendere le tempistiche di consegna.

IMPEGNO POST-PROGETTO (CONTINUOUS SERVICE)

La resilienza IT è una disciplina continua, non un traguardo isolato.
Il nostro presidio continuativo comprende:

- **DR Annuale:** esecuzione del master runbook in ambiente isolato ("bubble") per massimizzare il tasso di successo al primo tentativo.
- **Revisioni Periodiche:** verifica degli standard, gestione dei ruoli e supporto operativo al comitato di crisi.
- **Aggiornamento del Piano di DR:** riallineamento costante a ogni mutamento architetturale e tecnologico.
- **Backup & Restore:** automazione costante dei backup e ottimizzazione continua dei tempi di ripristino.

Garantiamo la tempestiva disponibilità di un piano di riavvio sempre efficace e aggiornato.



RISULTATI IN SINTESI

1 anno
durata del progetto

89,7%
Successo RTO
(305/340) su tutta la simulazione

4 giorni
Test di **ripristino** in failover

430
Test di validazione DR

17
domini tecnologici per la **copertura operativa**

100%
delle applicazioni critiche con RTO/RPO formalizzati in **Governance**