Axsym
IT COUNSELING

IFInet
LA SICUREZZA. IN INTERNET.

Disaster Recovery, Business Continuity e... GDPR

La Partnership

- CONSULTANCY & COMPLIANCE
- GOVERNANCE IT
- RISK & BUSINESS IMPACT ASSESSMENT
- PRIVACY & DPO SERVICES
- TRAINING

Massimo Licari
AXSYM – Cybersecurity Consultant
massimo.licari@axsym.it
+393403542740 - @maslicar

- DIGITAL TRANSFORMATION
- SYS INTEGRATION
- IT SECURITY
- CLOUD & NETWORKING
- SUPPORT & MAINTENANCE

Andrea Scarabelli
IFInet – CTO, Solutions Architect
a.scarabelli@ifinet.it
+39 3929393476 - @scarabellia

Perché Axsym

Nuovo player nel mercato delle consulenze IT a valore, Axsym si propone a supporto delle figure professionali impegnate nell'Information Technology come naturale elemento di crescita e valorizzazione del patrimonio e dei servizi informatici delle Organizzazioni.

Il nostro metodo

Axsym propone l'approccio "Risk-based" thinking, finalizzato ad aumentare il livello di consapevolezza e sensibilizzazione in ambito sicurezza, coinvolgendo tutto il personale dell'azienda. Le attività di consulenza sono ritagliate "su misura" per garantire la rapida individuazione dei punti di maggior vulnerabilità sia in termini tecnologici che organizzativi.

Aiutare a servire gli interessi degli stakeholder

Competenze

I professionisti presenti in Axsym vantano diverse tra le principali certificazioni delle competenze in materia di Security:

- Certified Privacy Officer
- Data Protection Officer
- Lead Auditor ISO 27001 – ISO 22301
- ISACA – CISA – Certified Information Systems Auditor
- ISACA – CISM – Certified Information Security Manager
- ISC² – CISSP – Certified Information Systems Security Professional
- BCI – AMBCI – Associate Member of the Business Continuity Institute
- ITIL – Foundation v3

Attività a portafoglio

- Data Protection Officer (General Data Protection Regulation)
- Privacy Consultant
- Information Systems (IS) Audit
- Enterprise IT Governance, Service Governance
- Establishing BC/DR Plans
- Risk Assessment
- IT Strategy Consulting
  - ✓Supporto strategico per singoli progetti
  - ✓Percorsi di formazione per i vari ambiti IT
  - ✓Supporto per raccordare l'IT alle normative

Regolamento UE 679/2016 e

Business Continuity & Disaster Recovery

Mamma, ho perso il dato personale

Cosa stiamo trovando nelle aziende – 1

-IT manager
-Legal
-Organization

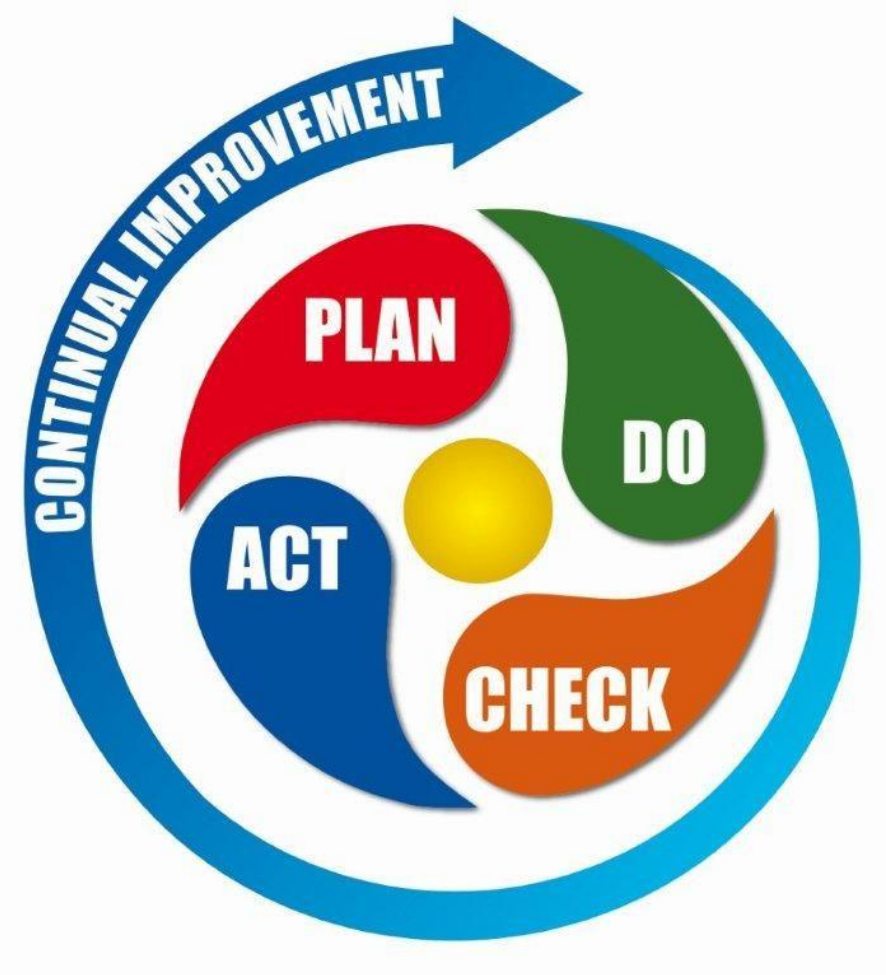
Cosa stiamo trovando nelle aziende – 2

Il Top Management
la proprietà
si passa dal disinteresse
ad una ostilità più o meno
manifesta

Come considerare l'adeguamento al Regolamento UE

Elevare il livello di sicurezza del sistema di gestione delle Informazioni partendo da un obbligo normativo

Il Sistema di Gestione della Sicurezza delle Informazioni



Il Sistema di Gestione della Sicurezza delle Informazioni

Business Continuity & Disaster Recovery

Mamma, ho perso il dato personale

Diverso atteggiamento?

Business Continuity

=

continuità del business

=

sopravvivenza dell'azienda

Cosa prevede il Regolamento UE? – 1

Articolo 4 punto 12

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Cosa prevede il Regolamento UE? – 2

Articolo 15

Diritto di accesso dell'interessato

Articolo 16

Diritto di rettifica

Articolo 20

Diritto alla portabilità dei dati

Cosa prevede il Regolamento UE? – 3

Articolo 24

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Cosa prevede il Regolamento UE? – 4

Articolo 32

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;

c) la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare **dalla distruzione, dalla perdita**, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Le parole del Regolamento

Disponibilità = misura l'attitudine di un'entità o sistema ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante (es. fornire un servizio ad un utente)

Resilienza = capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati

Ripristino = azione che consiste nel riportare qualcosa ad uno stato antecedente ad un determinato evento

Business Continuity vs Disaster Recovery

Il BCP assicura che le principali funzioni di business siano operative durante e dopo un disastro

Esempio di test: se avessimo perso questo edificio, come avremmo ripreso il business?

Il DRP è un piano tecnico sviluppato per consentire di recuperare una specifica funzione aziendale. Il DRP più noto è quello dei sistemi IT

Esempio di test: se avessimo perso i servizi IT, come li avremmo recuperati?

Come affrontare BC & DR

È un tema che riguarda i processi e la tecnologia

Cosa stiamo trovando nelle aziende

Soluzioni parziali, che spesso riguardano solo l'IT e nemmeno tutto

Soluzioni che non si basano sulle reali esigenze dell'organizzazione ma sulla percezione che ne ha chi le sceglie e le implementa

Cosa stiamo trovando nelle aziende

Abbiamo trovato:

Backup ogni 24 ore con processi critici che hanno un RPO di 4 ore

Backup ogni 24 ore che hanno tempi di ripristino superiori a 12 ore con RPO di 8 ore

Soluzioni di ripristino che passano attraverso l'acquisto dell'HW

Soluzioni ridondanti che non hanno tenuto conto di Single Point of Failure che le rendono inutili

Lo standard di riferimento

ISO 22301 – Societal security - Business continuity management systems - Requirements

ISO 22313 – Societal security - Business continuity management systems – Guidance

Approccio alla Business Continuity e al Disaster Recovery

Un sistema di gestione per la continuità operativa BCMS (Business Continuity Management System) sottolinea l'importanza di:

- capire le esigenze della organizzazione e la necessità di predisporre politiche e obiettivi per la continuità operativa;
- attivare e operare controlli e misure in grado di gestire la capacità complessiva dell'organizzazione di fronteggiare eventi destabilizzanti;
- monitorare e riesaminare la prestazione e l'efficacia di un sistema di gestione per la continuità operativa; e
- un continuo miglioramento basato su misure oggettive

Business Impact Analysis

Intervistare i responsabili di processo

Capire la dipendenza del processo dall'IT

Capire l'impatto di un eventuale blocco sul business aziendale

Valutare i reali costi – benefici

Capire le esigenze dell'organizzazione

Process info | Process Zones | Process Assets | Process Ctrl Lists | Legenda (#001) | SYSTEM

Process Code: 0011

Process Name: Gestione dell'offerta

Process Owner: Mario Rossi

Process Description or notes:

4 RTO* desired — 7 Employees needed to bring the process forward

4 RPO* desired — 25 Users served by the process (1st level of sub processes)

Organitazion Process criteria

- (•) Primary process
- ( ) Secondary Process
- [ ] * Select if the process is running 24h (always active/reactive)
- [x] Select if the process is considered critical for the Company
- 6 Confidentiality of the data handled by the process

Cumulative impact after (and in between):

(time range considered by Risk Matrix)

"24h" process type-> "8-18" process type ->	< 15min	up to 1h	up to 4h	up to 8h (1 day)	up to 24h (1-3 w/d)	up to 48h (3-6 w/d)	up to 72h (6-9 w/d)	up to 120h (9-15 w/d)	up to 192h (15-24 w/d)	up to 240h (24-30 w/d)	up to 360h (30-45 w/d)	GT 360h (>45 w/days)	
Loss of revenue	0	0	0	0	1	2	3	4	5	6	7	8	[ ] n.a.
Additional expenses	0	0	0	1	2	3	4	5	6	7	8	8	[ ] n.a.
Customer Service	0	0	0	1	2	3	3	3	4	4	5	6	[ ] n.a.
Regulatory and Legal	0	0	0	0	0	0	5	6	7	8	8	8	[ ] n.a.
Reputat. and Goodwill Loss	0	0	0	0	1	2	3	4	5	6	7	8	[ ] n.a.

- Loss of Revenue: redditi generati dal processo, nella finestra temporale considerata.
- Additional Expenses: considerare i maggiori costi/spese che sarà necessario affrontare in caso di evento destabilizzante.
- Regulatory & Legal: considerare tutti i rischi derivanti da violazione delle normative e dai regolamenti cogenti (locali, nazionali ed europee), dalle normative o regolamenti non cogenti e da tutti gli accordi contrattuali.
- Customer Services: considerare la perdita di clienti in caso di evento destabilizzante e interruzione di uno o piu attività (o prodotti o servizi) erogati dal processo.
- Reputat. and Goodwill Loss : prevedere l'impatto reputazionale, sia interno che nei confronti dei principali clienti/fornitori.

Il processo di gestione della BC & DR

Costruire un processo di gestione

Valutare e decidere prima di un incidente:

- ciò che è necessario fare;
- chi decide e cosa;
- chi deve essere coinvolto per cosa;
- come gestire la comunicazione

Il processo di gestione della BC & DR

Formalizzare il processo di gestione BC&DR

Formare le persone che saranno parte attiva e passiva del processo

Testare il funzionamento del processo

Il Sistema di Gestione della Continuità di Business

Il Sistema di Gestione della Sicurezza delle Informazioni

Disaster Recovery

Sottolineiamo che anche il Disaster Recovery deve essere un processo gestito con procedure, istruzioni, controlli e test

Dettaglio Servizio Axsym per DR&BC

Cosa fa axsym in pratica (affiancamento IT, misura rischio, ecc)

Disaster Recovery

La continuità di business e in particolare il Disaster Recovery hanno comunque un'anima tecnologica molto importante.

Stiamo parlando di garantire la continuità o il ripristino di sistemi che garantiscono la continuità del business.

IT Disaster Recovery – possibili architetture

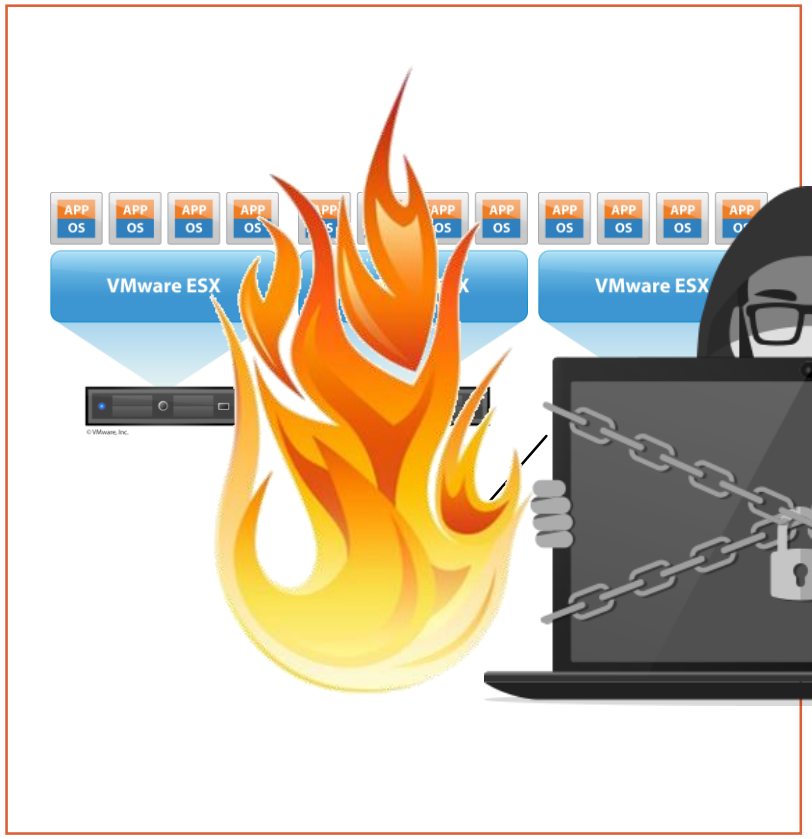
A. Backup (DR «a freddo»)

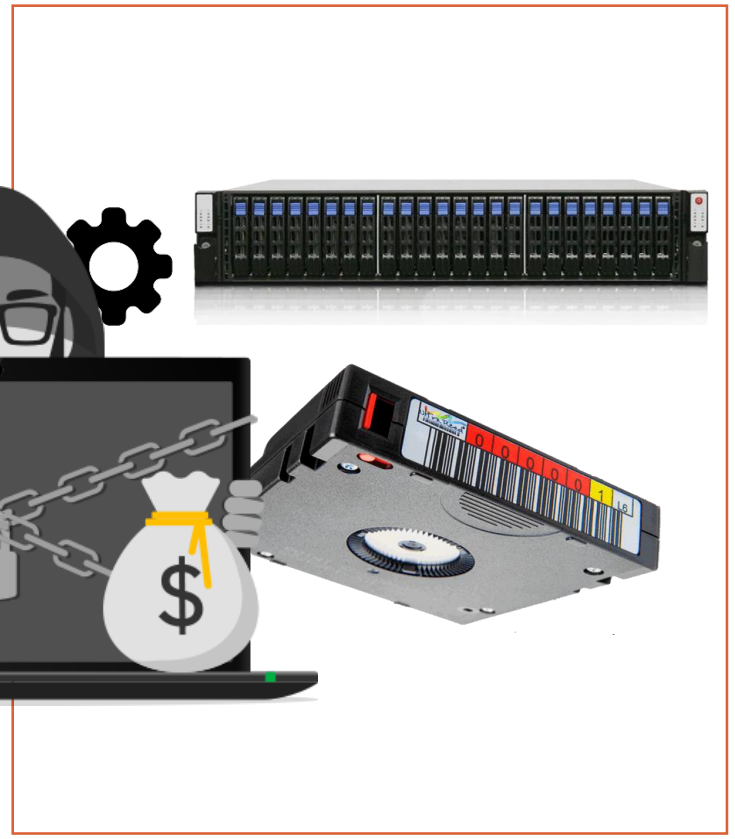
B. Active / Passive (DR)

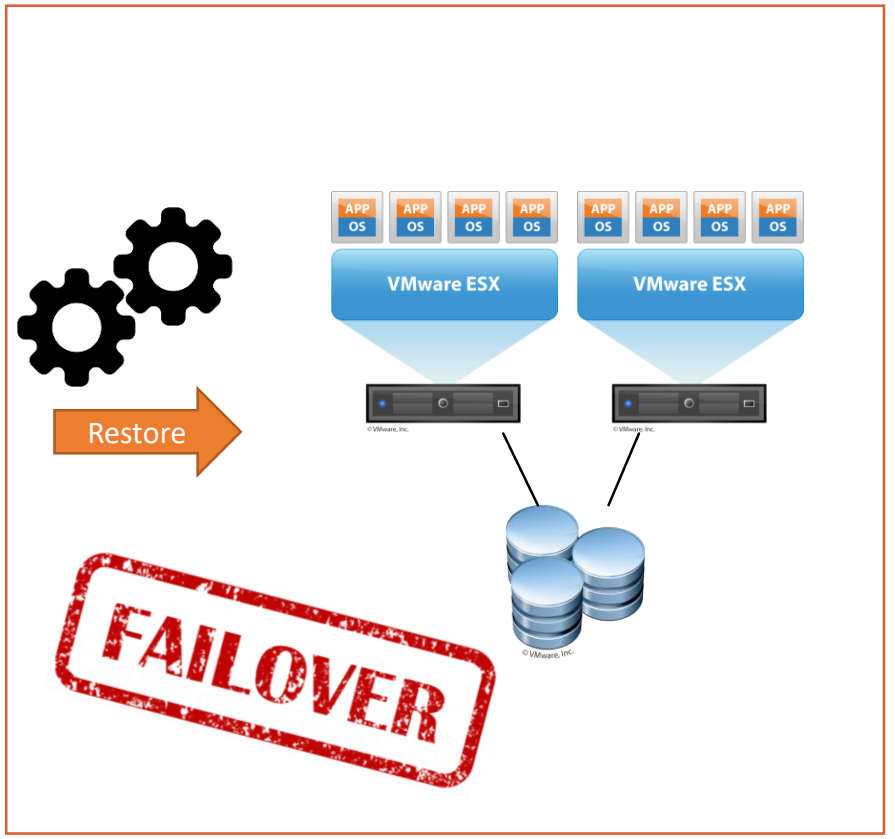
C. Il ruolo del Cloud

D. Stretched Cluster

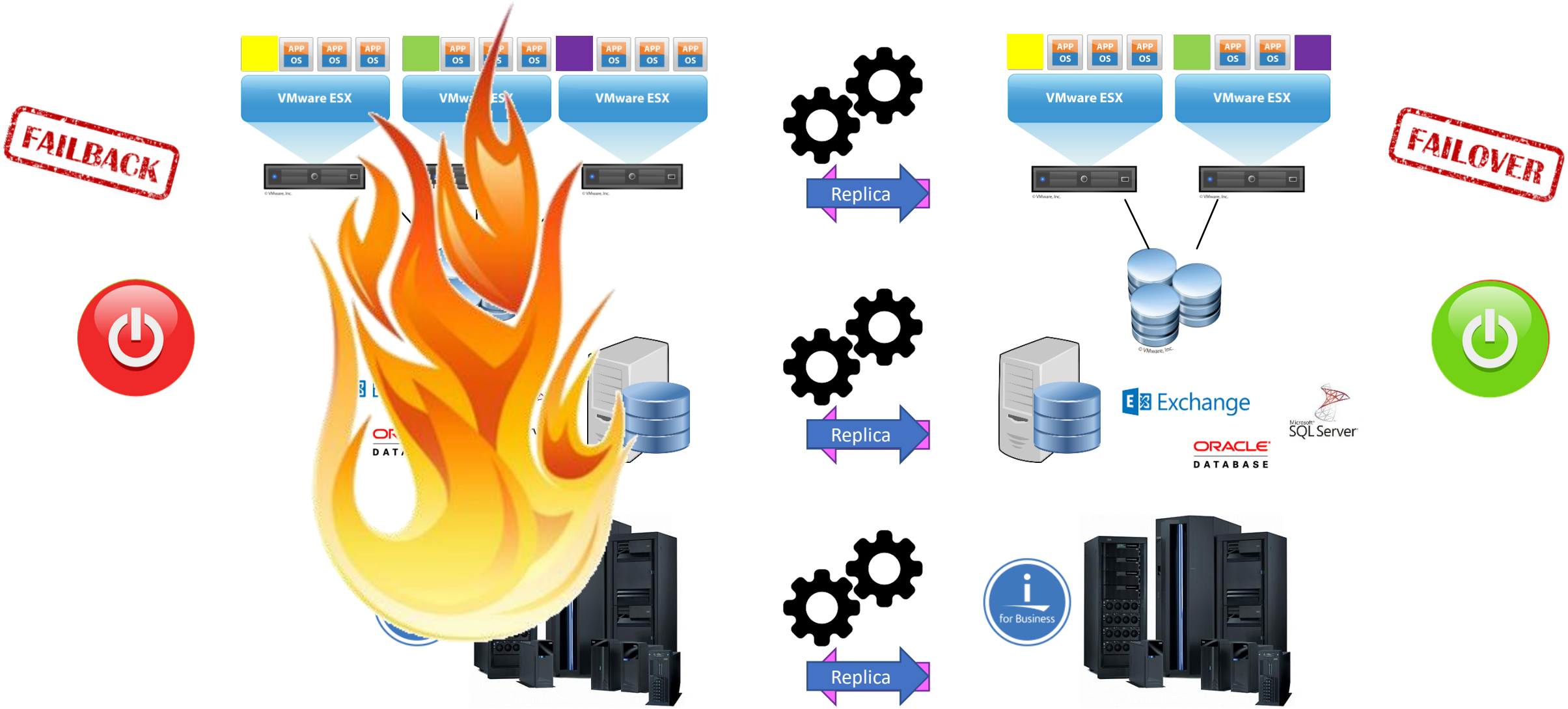
Disaster Recovery – Backup (DR «a freddo»)



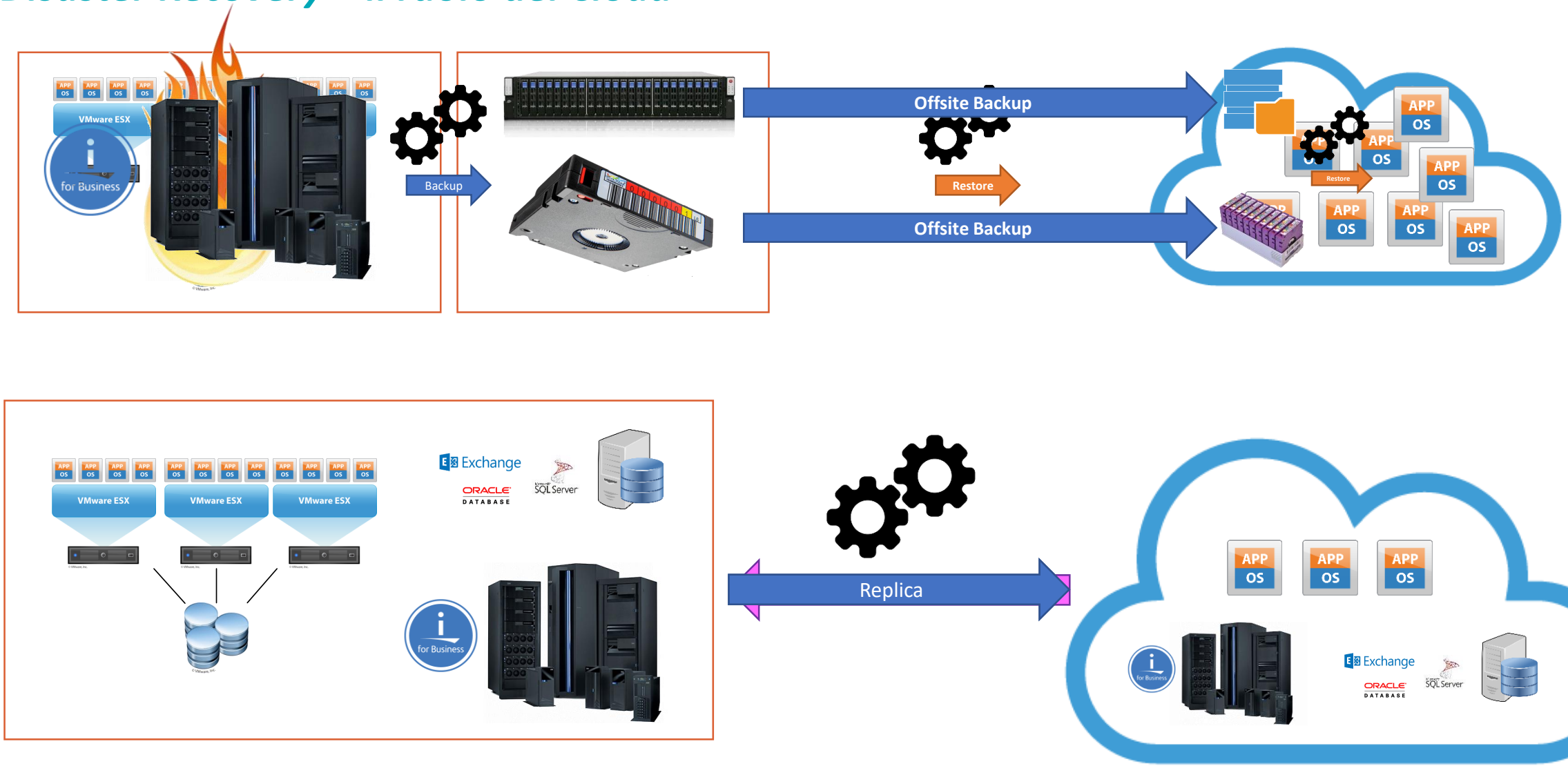




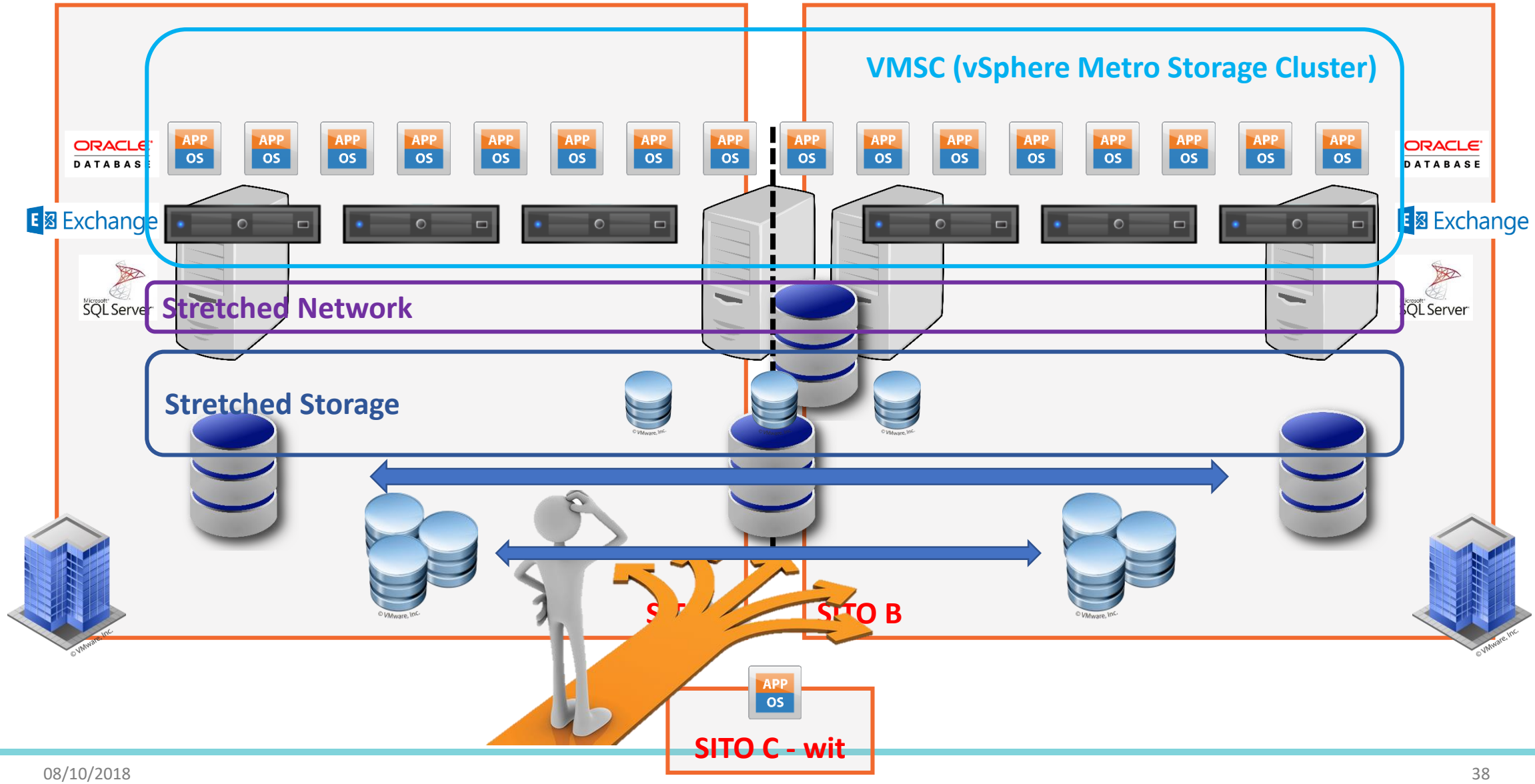
Disaster Recovery – Active/Passive



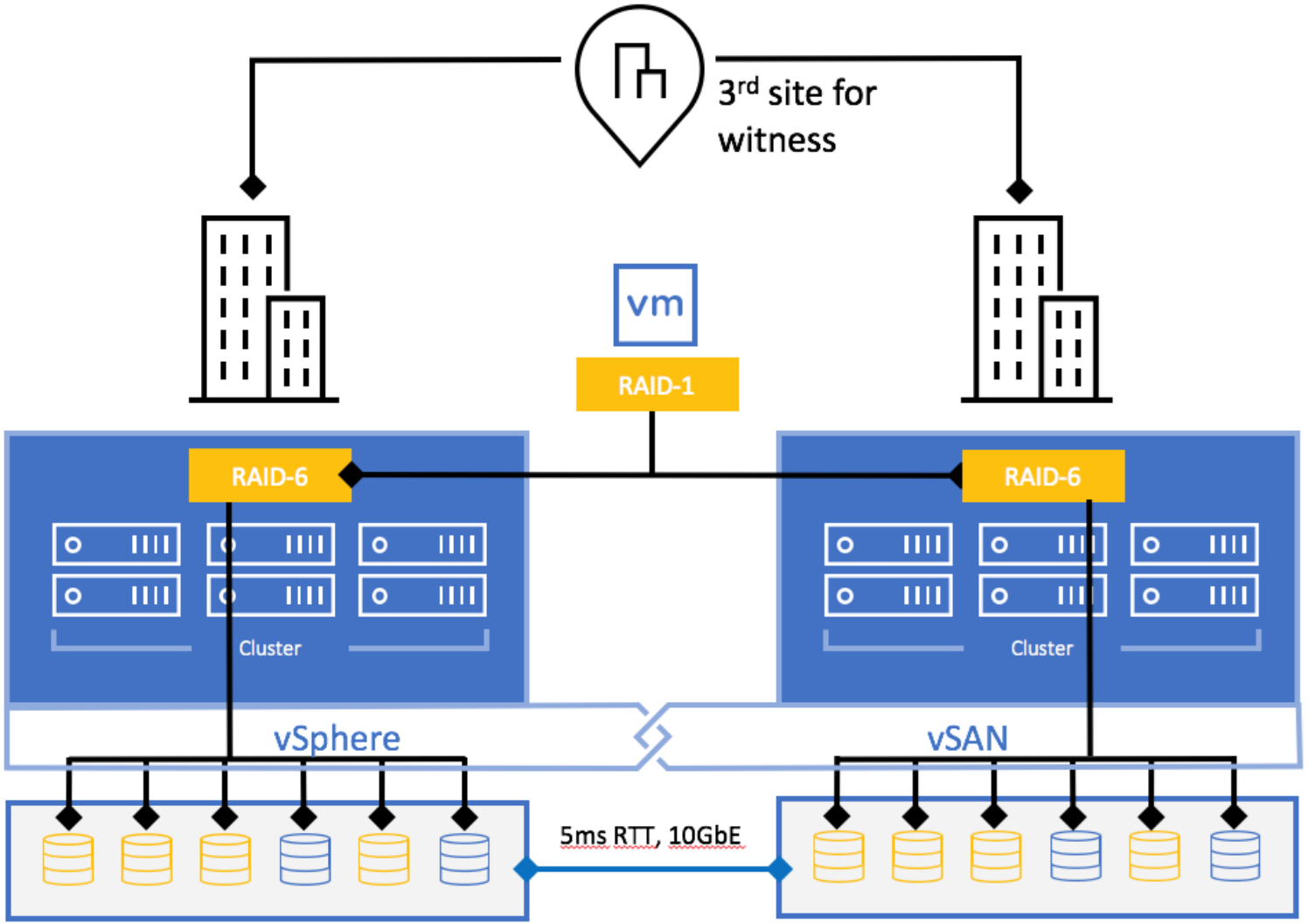
Disaster Recovery – il ruolo del Cloud



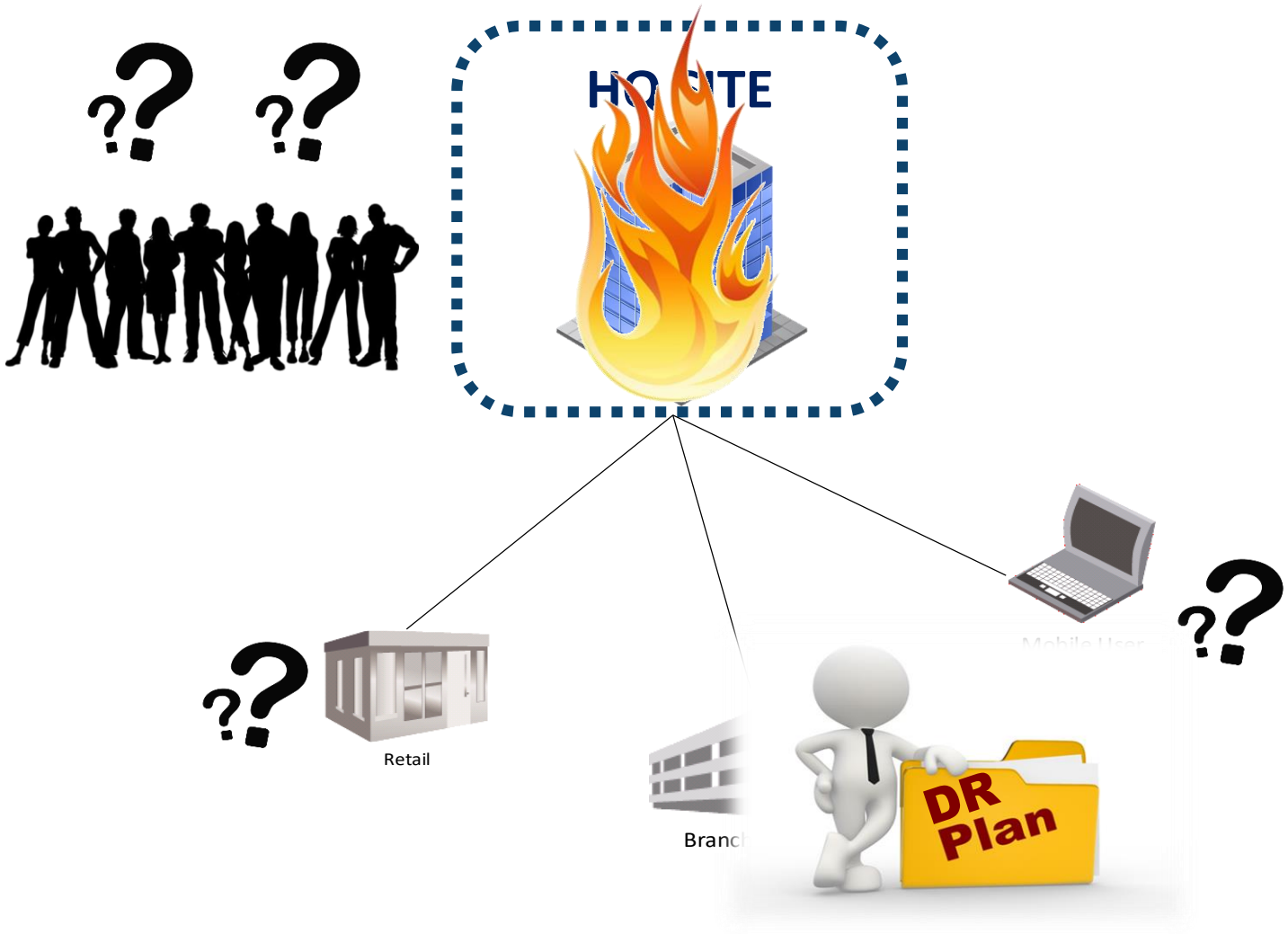
Disaster Recovery – stretched cluster

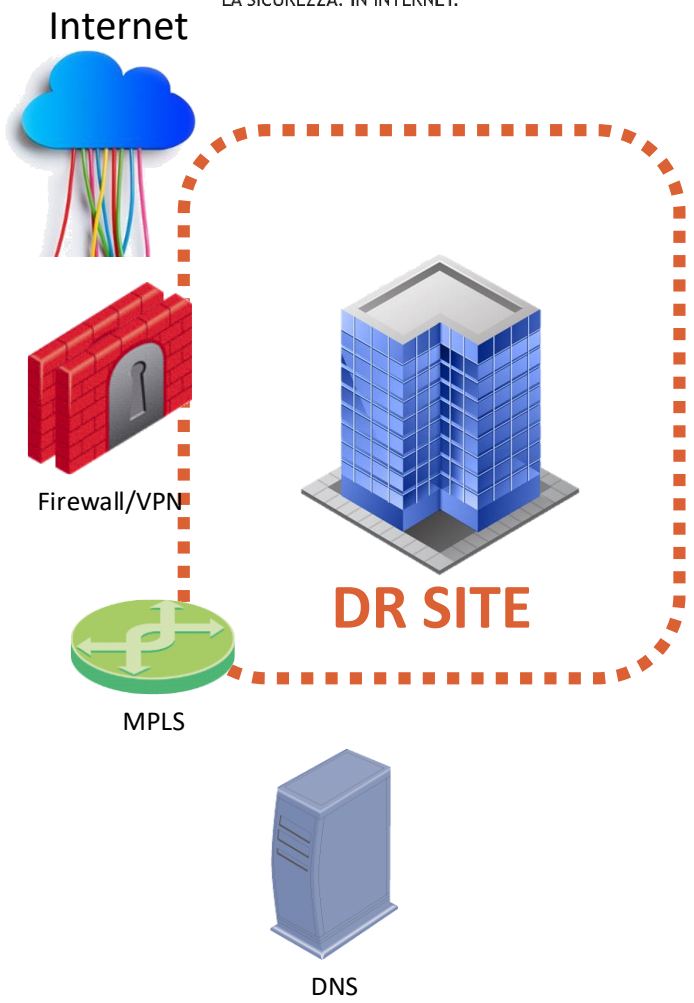


Disaster Recovery – stretched cluster con HCI (VMware vSAN)



Disaster Recovery – raggiungibilità dei dati





inizio test DR:	14/06 22.3		
# attività	ora inizio prevista	ora inizio effettiva	durata prevista (h)
1	14/06 22.30	22.30	
2	14/06 22.30	22.30	0,50
3	14/06 23.00	16.53	1,00
4	15/06 00.00	22.55	
5	15/06 00.00	23.00	7,00
6	15/06 07.00	5:07	
7	15/06 07.00		2,50
8	15/06 09.30	9.30	1,00
9	15/06 10.30	11.45	0,50
10	15/06 11.00	12.02	
11	15/06 11.00	12.05	1,00
12	15/06 12.00	12.25	1,50
13	15/06 13.30		0,50
14	15/06 14.00	15.00	1,00
15	15/06 15.00		2,00
16	15/06 17.00	15.20	
17	15/06 17.00	19.00	
18	15/06 17.00	19.00	0,50
19	15/06 17.30	19.30	7,00
20	16/06 00.30		
21	16/06 00.30		9,00
22	16/06 09.30		1,00
23	16/06 10.30	8.45	0,50
24	16/06 11.00	8.45	1,00
25	16/06 12.00	11.32	1,50
26	16/06 13.30		0,50
27	16/06 14.00		2,00

→ 13.00 PRANZO
14.00 RESTART
COPIE
FAILBACK

[redacted] - Disaster Recovery Plan
Italian Datacenter

Table of Contents

IFnet Andrea Scarabelli

	esito
	✓
	✓
	✗
	✓
	✓
	✓
	✓
umentazione	✗
umentazione	

RUNBOOK v.1

Failback

GRAZIE PER L'ATTENZIONE!

AXSYM

massimo.licari@axsym.it

www.axsym.it

+39 045 5118570

IFInet

a.scarabelli@ifinet.it

www.ifinet.it

+39 045 595699