FARETE 2016
DALLA MAIL ALLA STRETTA DI MANO

ACANTHO
Società del Gruppo Hera

Cloud è bello, ma se piove?

Le opportunità per migliorare l'affidabilità del proprio sistema informatico aziendale

Disastro e rischio

Disaster Recovery

Il disaster recovery (brevemente DR), in informatica ed in particolare nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese a fronte di gravi emergenze che ne intacchino la regolare attività (Wikipedia https://is.gd/BWMcfv).

C'è disastro se c'è rischio

Rischio = Minaccia x Vulnerabilità x Impatto

Tutto matematico? e l'incertezza?

Il calcolo del rischio è condizionato dalla incertezza sui vari aspetti e in effetti dovremmo considerare nel calcolo anch'essa.

La gestione del rischio ha basi metodologiche ma si perfeziona costantemente tramite le esperienza

Mitigare e prevenire

Impatto e frequenza

Una guerra dovrebbe mantenere una frequenza bassa con impatti totali; alluvioni e terremoti hanno una relativa frequenza (rispetto alle guerre e al contesto geografico) mentre danni o attacchi informatici hanno maggiori frequenza con minore impatto; non trascuriamo l'effetto umano con errori, danni e furti

Una matrice impatto / frequenza aiuta a valutare la consistenza del piano

Basso impatto – alta frequenza

queste sono le tipiche aree di ***prevenzione***, a cui il sistema IT si adegua

Alto impatto – bassa frequenza

queste sono le aree in cui occorre invece una ***mitigazione***, non si evitano, creando un piano di disaster recovery

Un piano di DR non evita il disastro, ma perlomeno permette di essere preparati

Analisi degli economici

Analisi sia delle perdite finanziarie sia degli impatti sul business; questo permette di valutare la consistenza dei valori di RPO e RTO

Alcuni economici da valutare:

personale improduttivo – fatturato – costi generali – processo commerciale - delivery

Individuare le metriche

RPO: Recovery Point Objective (quanti dati puoi perdere)

RTO: Recovery Time Objective (quanto ci metti a ripartire)

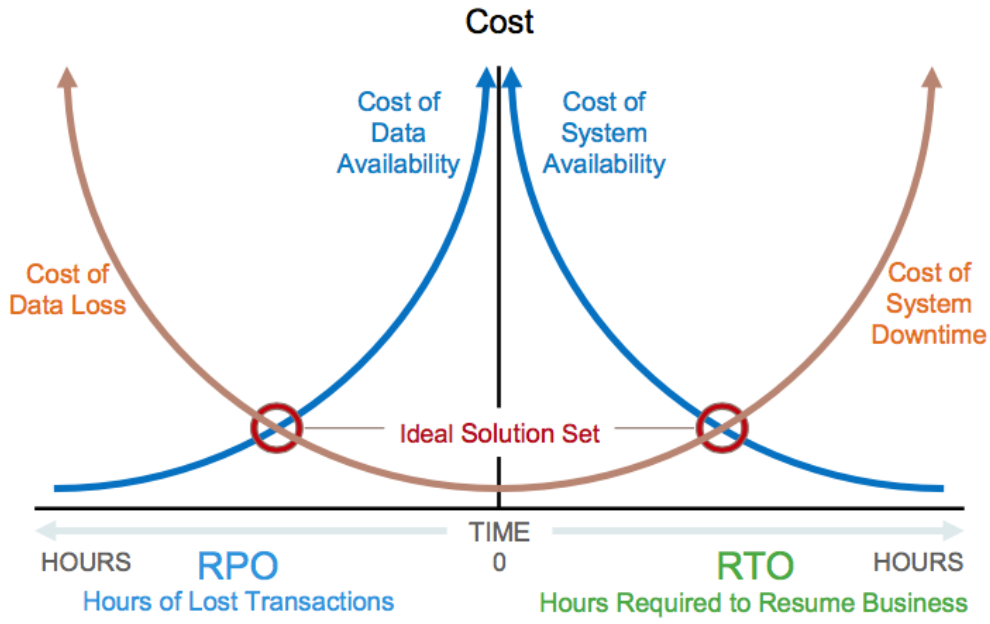
costo perdita del dato vs costo della disponibilità del dato

costo del downtime vs costo della disponibilità sistema

E' il punto di equilibrio l'obiettivo

definire i recovery time objectives

https://is.gd/3tJZdH



ACANTHO®

Quanti 9?

oltre i tre 9 (99,9%)

costo – tecnologie – organizzazione variano non proporzionalmente rispetto ai “9”
il budget di DR o BC determina la classe

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% ("one nine")	36.5 days	72 hours	16.8 hours	2.4 hours
95%	18.25 days	36 hours	8.4 hours	1.2 hours
97%	10.96 days	21.6 hours	5.04 hours	43.2 minutes
98%	7.30 days	14.4 hours	3.36 hours	28.8 minutes
99% ("two nines")	3.65 days	7.20 hours	1.68 hours	14.4 minutes
99.5%	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes	1.44 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes	43.2 seconds
99.99% ("four nines")	52.56 minutes	4.38 minutes	1.01 minutes	8.66 seconds
99.995%	26.28 minutes	2.16 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds	864.3 milliseconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	604.8 milliseconds	86.4 milliseconds
99.99999% ("seven nines")	3.15 seconds	262.97 milliseconds	60.48 milliseconds	8.64 milliseconds
99.999999% ("eight nines")	315.569 milliseconds	26.297 milliseconds	6.048 milliseconds	0.864 milliseconds
99.9999999% ("nine nines")	31.5569 milliseconds	2.6297 milliseconds	0.6048 milliseconds	0.0864 milliseconds

Disaster Recovery: precisazioni

Distanza

Su quanto debba essere la distanza fra i due siti non vi è, al momento, una posizione definitiva

- la ISO 22301 (Business continuity management systems) non prescrive le distanze (https://is.gd/vIKLpo)
- La FINMA, ente Svizzero che sancisce le normative Bancarie, non pone l'attenzione sulla distanza effettiva, ma sull'analisi del rischio di evento catastrofico contemporaneo in entrambi i siti
- Uptime Institute prescrive per certificazione le ridondanze di sistemi, non le distanze
- SEC consiglia 200 miglia

Comunque una elevata distanza (oltre i 100 Km) non permette soluzione di BC con real time, in quanto il ritardo di trasmissione inizia ad essere sensibile

Raddoppio delle risorse

con le soluzioni di DR / BC cloud ovvero con VM active / passive il sito di DR occupa frazioni di risorsa rispetto alla situazioni normale, e attiva le risorse solo in caso di disastro

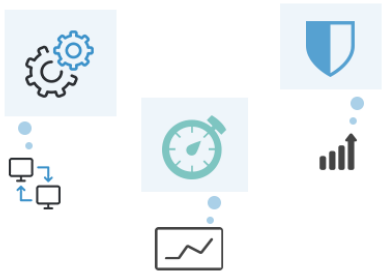
Un buon backup

Un backup strutturato è una condizione necessaria al DR, ma non risolve il problema della operatività dopo il disastro, ovvero oltre al backup avrò bisogno di risorse IT per ripristinare l'ambiente di produzione

Disaster recovery plan: infografica

ACANTHO®

Disaster recovery plan: infografica



4

Define
recovery objects.

Think about Recovery Time Objective (RTOs) and Recovery Point Objectives (RPOs).

5

Determine the
right tools & techniques.

Remember to include offsite protection and automate and stramline where possible.

6

Get
Stakeholder buy-in.

Collaboration, consensus, and support is vital to your disaster recovery plan's success.

Disaster recovery plan: infografica

7

Document
&Communicate your plan

Share the document with others
and store it in a safe place.

8

Test
& practice
your disaster recovery plan

Find and rectify problems to execute
faster and more accurately.

9

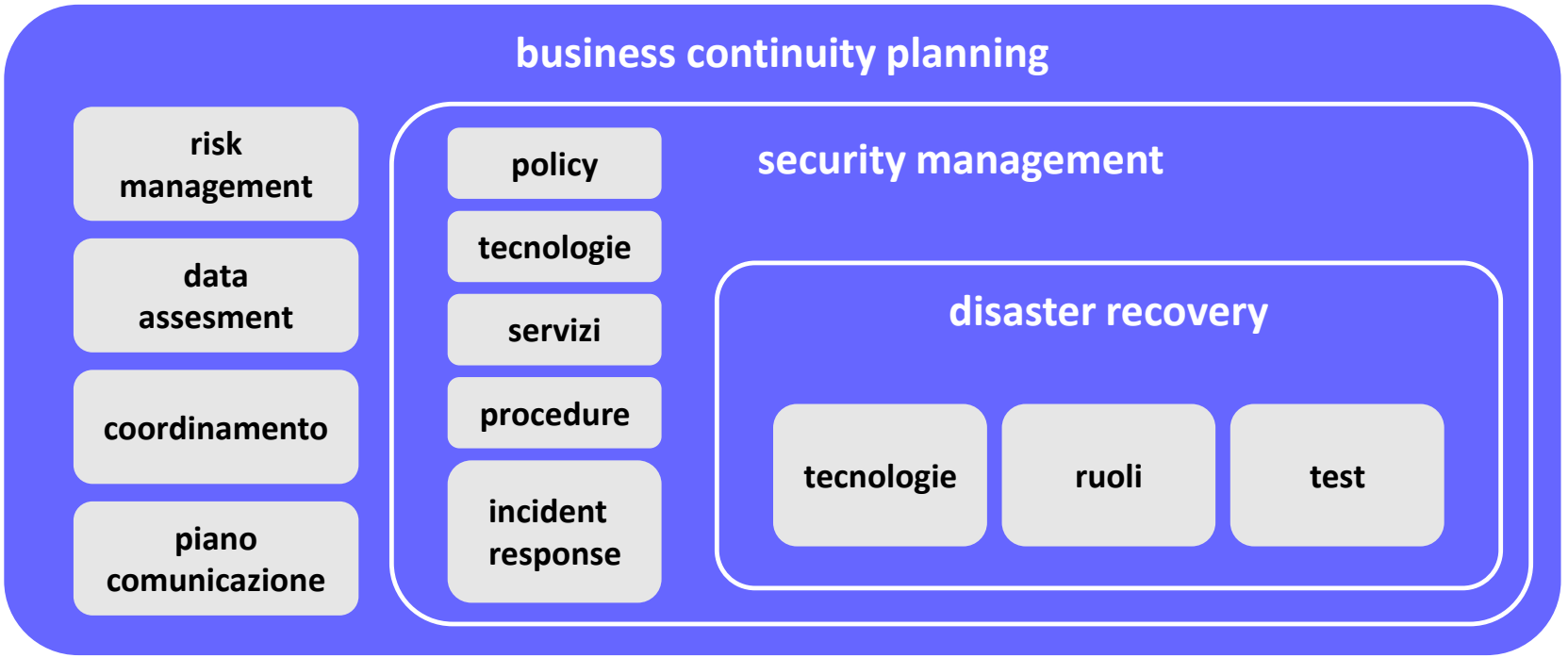
Evaluate
& Update
your plan

Regularly review your plan due to
ever-chaning business environments.

Business Continuity o Disaster Recovery?

BC è tutta questione di “9”? Il DR è una BC “lenta”?
No è un piano complesso che comprende anche il disaster recovery; infatti occorre considerare

- contact list e piano di comunicazione - set di attività urgenti (mente fredda)
- centro operativo minimo
- GAP di operatività (attesa e fornita)
- Policy: verificabili, chiare, documentate e decisive
- HA (normalmente 99,9% o ,99%) è 24x7 ma comprende tutte le componenti dell’ecosistema?
- Scenari “what if” e attenzione ai cigni neri



ACANTHO®

Approccio al disaster recovery

Tutto chiaro ma da dove iniziare?

- valutare il grado di “dipendenza digitale” dell’impresa
- valutare soprattutto le funzioni “core” dell’azienda per la dipendenza digitale
- a livello di processi valutare le dipendenze fra i vari sistemi IT
- individuare scenari minori: ramsomware, perdita / rottura PC, virus, guasto alla email aziendale
- individuare 3 scenari globali: 1 - 3 - 10 giorni di fermo sistema IT
- non occorre riferirsi a scenari apocalittici, solo semplice interruzioni di servizi
- stimare per questi scenari le perdite economiche dirette
- valutare gli altri aspetti di impatto sul business non diretti: perdita dati, ritardi nel flusso commerciale e nel delivery, immagine, costo della “ripartenza”

Con questa analisi si attua una prima stima degli economici e degli impatti sul business per delle interruzioni del servizio qualificabili e si stima il budget ovvero costo del rischio

Questo aspetto assieme ad una architettura virtualizzata (o virtualizzabile) permette di approcciare le nuove soluzioni di DR / BC in cloud, con costi / tempi competitivi rispetto alle soluzioni tradizionali

DR / BC: due approcci

Approccio classico

Assessment

Analisi azienda

- territorio
- caratteristiche IT
- organizzazione
- gestione
- sicurezza

Analisi obiettivi

- processi critici
- definizione RPO RTO

Analisi infrastruttura

- scenari recovery
- architetture
- sistemi operativi
- risorse DC di DR

Soluzione di DR

- SLA - vincoli
- design
- costi – tempi
- impatti organizzativi

Implementazione

- copia dati
- risorse (IT & network)

Approccio cloud based

Assessment

- servizi / VM
- risorse (vCPU – RAM – storage)
- sistemi operativi
- network

Setup

- SW sync lato cliete
- SW sync data center
- alert e policy
- 1° data backup

Delivery

- test network & sync
- sleep virtual data center
- sync engine run

Test

- test annuale
- update

Cloud DR / BC: valutazione

I vantaggi

- Il DR diviene una OPEX, e non un CAPEX, modulabile anno per anno secondo le esigenze
- Le tecnologie sono sempre aggiornate
- Il data center di DR ha tutte le caratteristiche di alta affidabilità, resilienza e sicurezza (ISO 27001 – TIIER 3)
- Modelli di servizio in relazione ai parametri di RPO – RTO desiderati
- servizio su infrastruttura Vmware dedicata
- data center italiano di proprietà e conforme alle normative

I limiti

non tutta l'infrastruttura IT può essere virtualizzata e sincronizzata in cloud, alcuni casi:

- chiavi HW
- porte di comunicazione non standard
- real time app
- licensing non virtualizzabile
- sistemi non virtualizzabili

Cloud DR / BC: un modello di servizio

Una soluzione semplice ad alta affidabilità, nel data center Acantho

Cloud DR / BC

- Replica dell'intero ambiente operativo
- Ripristino rapido delle funzionalità
- classi di RPO / RTO
- configurazioni di sistema automatiche o semi-automatiche (classi di avvio e gruppi VM sync)
- per testare release / upgrade o change-management
- differenti recovery point e journaling del file sistem
- multi hypervisor
- anche per soluzioni di cloud ibrido

Cloud backup

- Backup di interi ambienti on-premise (a livello immagine Virtual Machine)
- Monitoraggio e invio di promemoria
- Dati su storage di classe enterprise in alta affidabilità
- Backup programmabili quotidiani più frequenti
- possibilità di avere il virtual data center di replica in caso di incidente

Modello pricing

modello di pricing in relazione al perimetro (numero VM e storage) e classi di DR (RPO/RTO) o solo backup; canone una tantum in caso di disastro e per test

grazie

gianluca.ulisse@acantho.com

ACANTHO

Società del Gruppo Hera