

Resilienza

PPM



Consideraciones solución

antes → Resiliencia: Backup

Negocio	dif. estrategia negocio con IT
Organización	Gestión Usuarios y Personal de Soporte
Procesos	
Aplicaciones	Plan de Contingencias para Apps
Datos	Recuperación rápida & Protección ante pérdidas
Tecnología	Soluciones tecnológicas
Instalaciones	Soluciones para Prestos de trabajo

antes "experimenta y reacciona"

ahora "Anticiparse y Ajustar"

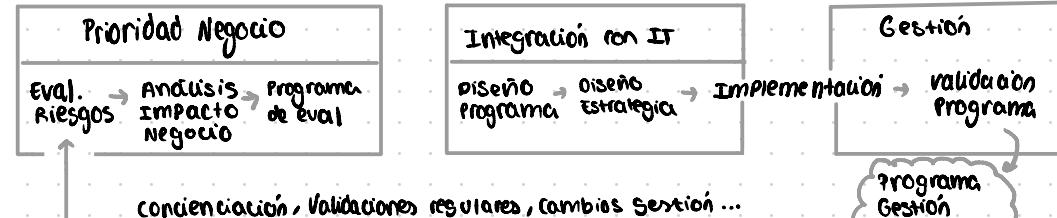
Resiliencia → $\frac{2}{3}$ se note lo menos posible → impacto

¿Qué nos aporta Resiliencia?

- ↳ Evaluar + manip + mitigar, impacto riesgos
- ↳ Responder normativas (reguladoras legales)
- ↳ Garantizar datos
- ↳ Lograr objetivos disponib → ∇ interrupciones
- ↳ Documentar Plan de continuidad para recuperarse en el \rightarrow responder
- ↳ Plantear soluciones tecnológicas en $\langle \rightarrow \rangle$ requisitos

Alta disponib? disponib continua? Recuperación ante desastres?

Requisitos de Resiliencia



Protección de Datos IT
Alta disponib op continuas
Recuperación ante desastres

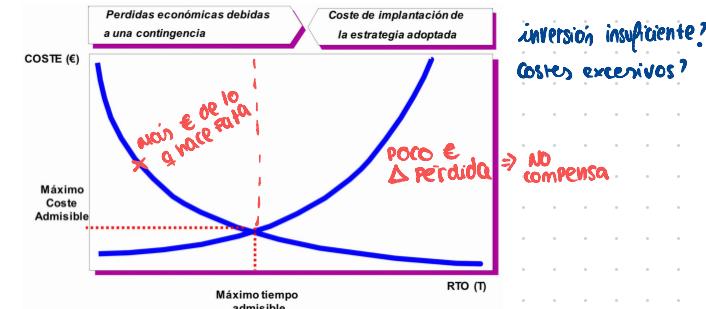
RTO & RPO

RTO: Recovery Time objective \rightarrow ∇ de inactividad aceptable

RPO: Recovery Point objective \rightarrow cantidad datos perdida

U copia cada 24 h \rightarrow RPO / min: 24 h

Balance coste solución \leftrightarrow pérdidas por contingencia



Normativa y Mejores Prácticas

→ Ley Resiliencia Operativa Digital (DORA)

- Gestión Riesgos
- Notificación incidentes
- Prueba Resiliencia Operativa Digital
- Riesgo de terceros en materia de TIC
- Intercambio de inteligencia

→ BS 25999 / ISO 22301

• Prácticas y Soluciones → Gestión Continuidad Negocio

Fase Inicial

- Identif requisitos
- Obj & Alcance
- Tratamiento Riesgos

Implement. Sistema

- Análisis impacto riesgos
- Estratégica
- Implementación PCN
- Sensibilización Promoción
- Documentación

análisis de riesgos cada vez es más difícil de PREDECIR
↳ IMP: hacer un BIA → Business Impact Analysis

Revisión & Mantenim.

- Ejercitación PCN
- Análisis resultado
- Planes Comunicación
- Acciones correctivas
- Revisión & Mantenimiento

Resiliencia

Diseño y Recuperación de un PCN

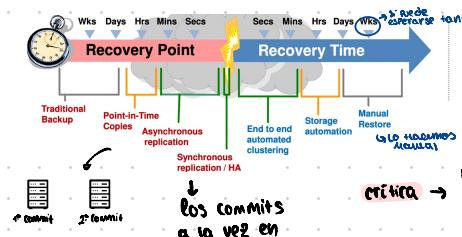
Diseño PCN

Negocio
APP
Infraestruct

Resolución PCN

wando largo
una contingencia
fire document

RTO y RPO: Marco Rel.



disponib 99.999%

redundancia total

RTO - min
RPO - casi 0

disponib 99.999% si se duplicados

disponib 99.9%
RTO < 24h
RPO - min

capacidad libres/espaci

disponib 99.5%
RTO > 24h
RPO - horas

op de recuperación

→ ISO 22316: 2017 Seguridad y Resiliencia

→ ISO 22316: 2020 Seguridad y Resiliencia

- Resiliencia Organizacional
- Norma → Mayor capacidad anticipar riesgos/vulnerab.
- Mayor coordinación disciplinas de gestión para mejorar coherencia de actuación
- Recomendación: hacer BIA Análisis de Impacto al Negocio
↳ guía para seguir proceso + documentar

capacidad de una empresa para absorber y adaptarse a los imprevistos, sin dejar de cumplir su obj o alcanzar

- 1 Compromiso de los órganos de Dirección
- 2 Estructura de gobierno
- 3 Assegurar inversión en actividades de resiliencia organizacional
- 4 Sistema de soporte a la gestión
- 5 Evaluación continua
- 6 Comunicación

Escalabilidad de Soluciones

Tier 1

Bunkers donde guardan cartuchos
millones de datos

Tier 2

Hot-site → Cartuchos +

Tier 3

Envío telemático de la copia Respaldo

No críticas

→
Point In Time Backup

Recup. rápida datos + mínima perdida

Tier 4 → PIT

Copias más inteligentes / diarias incrementales y en un momento determinado

Tier 5 → integración aplicación / BBDD

Copias exigentes → basadas en SW
+ identif. consistencia por transacción

Perdida datos en (x) → f copia

Algo critico
2º Site dormiente

Tier 6

replicación continua
datos en 0 real delay

Disk Mirroring

síncrono o asíncrono 0 delay

RPO = 0

Tier 7

Hot site y remoto totalmente desacoplados

0 perdidas y 0 delay

RTD tiende a 0
RPO = 0

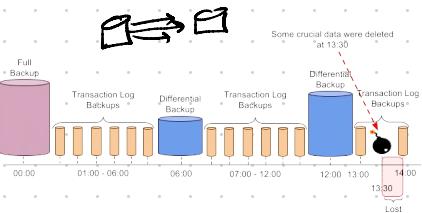
APP muy críticas
Balanceo larga

Resiliencia

Soluciones Copia

Point In Time

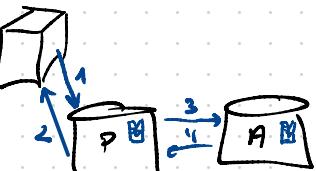
Copias → totales
incrementales
discos = tipo
No garantiza consistencia datos



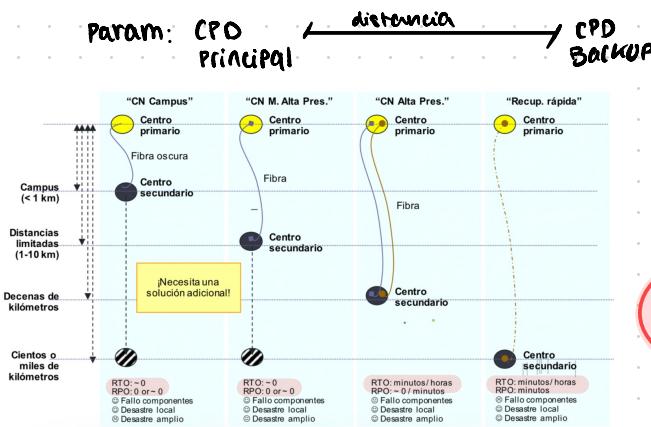
Síncrona



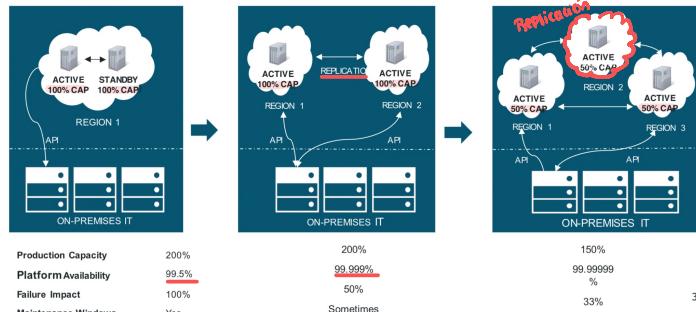
Asíncrona



SOLUCIONES DE RECUPERACIÓN ANTE DESASTRES



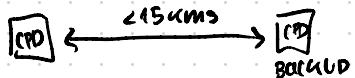
Sustituir CPD por cloud



Resiliencia

ESTRATEGIAS BCRS

2 Centros con HA



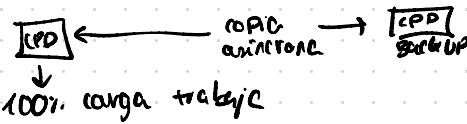
2 centros soportan 100% trabajo
50% 50%

Centros espejados
inversión alta

Pruebas contingencia &

RPO { tiende a 0
RTO

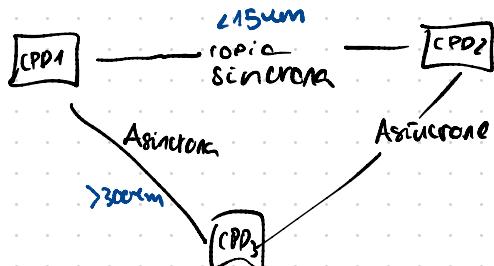
Centros a larga distancia



Soluciones HA
RPO ⇒ segundos
RTO ⇒ en ((x)) operatividad sist

→ descarte regional sobrevive

3 CPDs con 2 en HA



7000s los datos copiados (CPD1 y CPD2)

RPO { tiende a cero
RTO