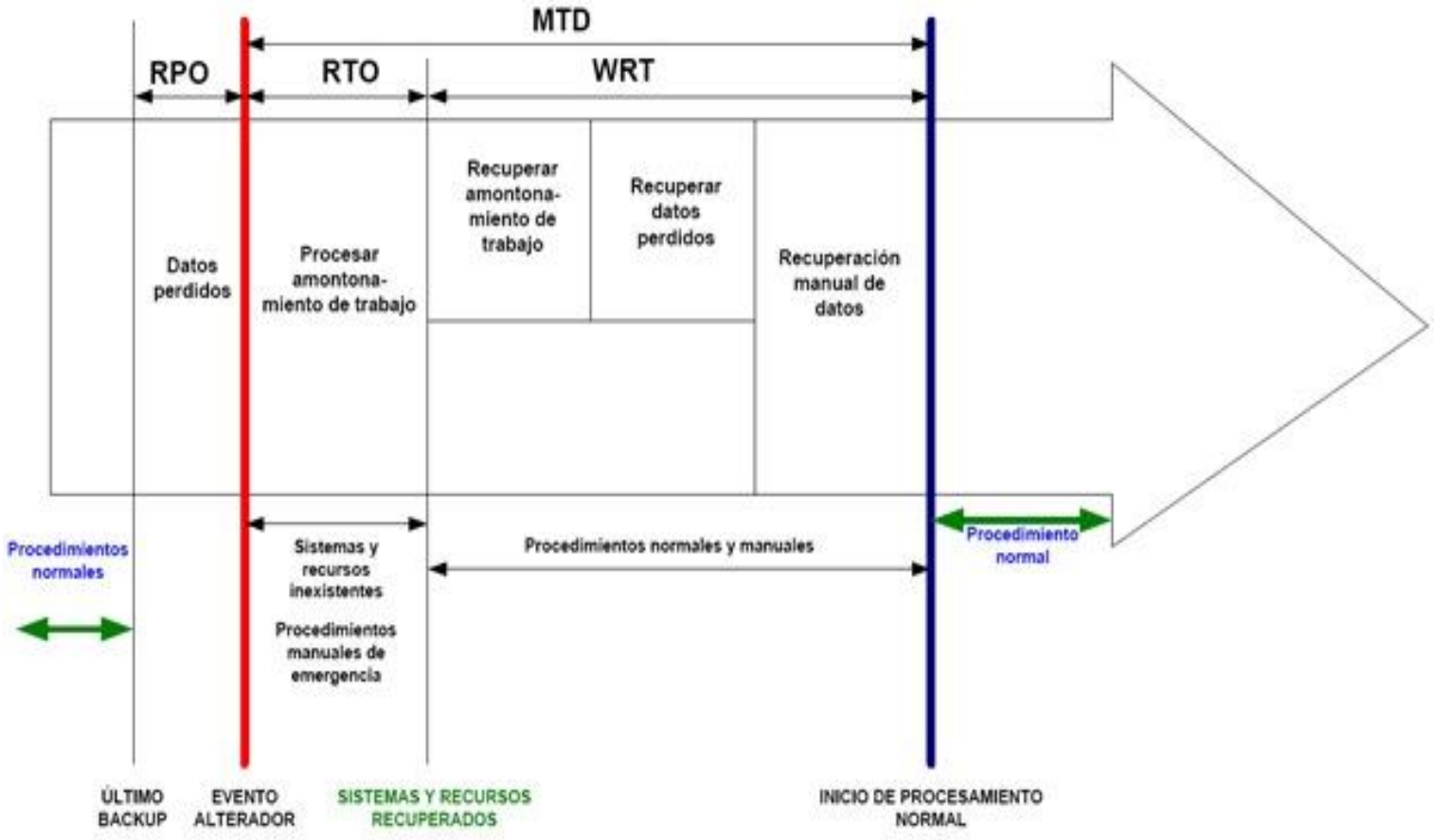
Soporte Eficiente en Tecnologías de la Información y la Comunicación

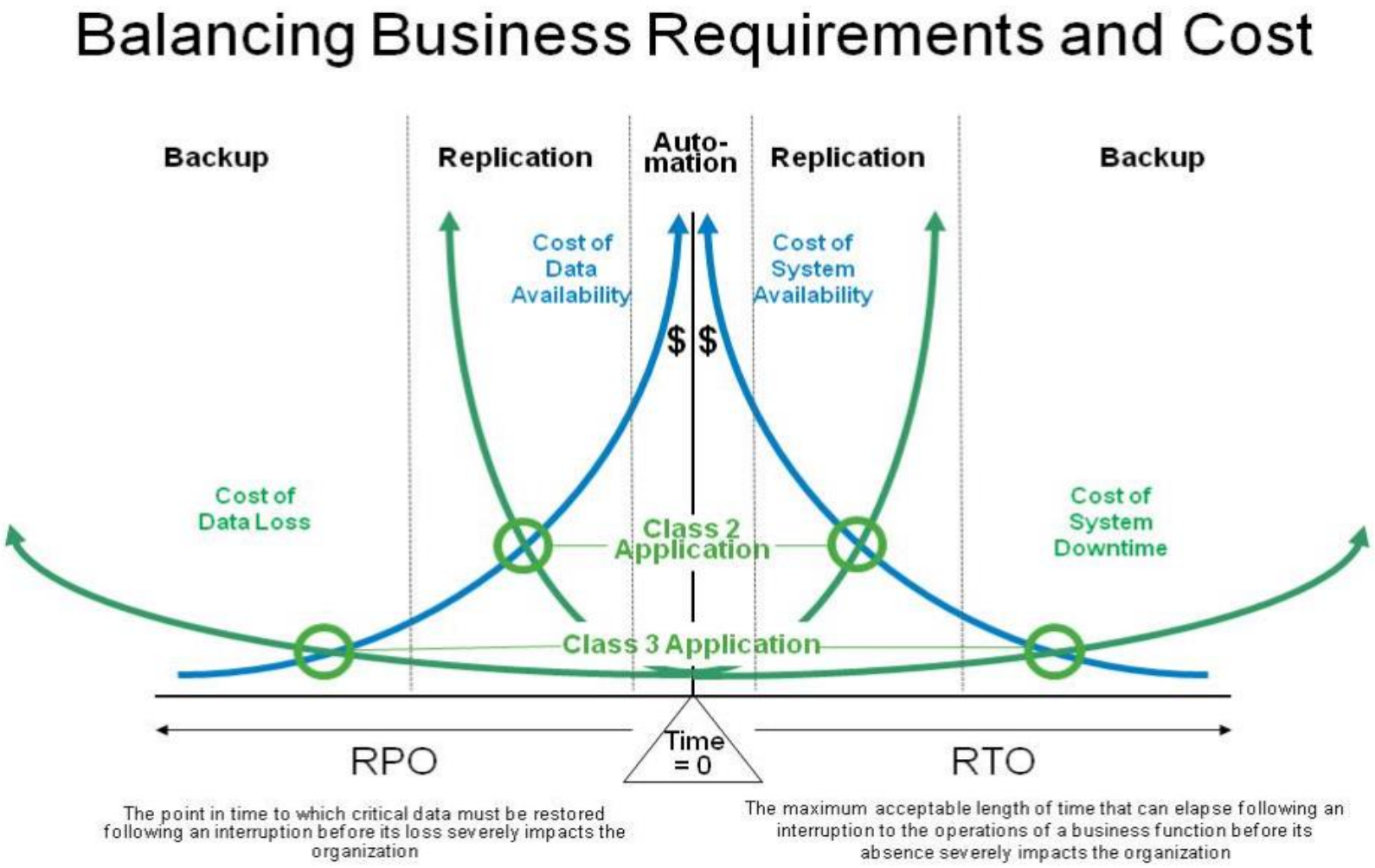
The concept of IT (BCDR)

IT Business Continuity and Disaster Recovery

The concept of IT (BCDR)



The concept of IT (BCDR)



The concept of IT Business Continuity and Disaster Recovery (BCDR)

- ✓A business continuity plan
- ✓A disaster recovery plan
- ✓An IT disaster recovery plan

The concept Business Continuity (BC)

Un plan de continuidad de negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre

> One in three companies has declared a disaster during the past five years.[2]
>
> - **Forrester**

Disaster Recovery Plan (DRP)

Un plan de recuperación de desastres es un subcomponente de su plan de continuidad de negocio. Describe el proceso, las políticas y los procedimientos para prepararse para la recuperación y la continuación de las operaciones de negocio e infraestructura en caso de un corte de energía, falla del equipo, incendio, inundación u otro incidente perturbador.

IT Disaster Recovery Plan (IT DRP)

Un plan de recuperación de desastres de TI es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos

> Cloud-based recovery services have evolved from traditional, managed disaster recovery (DR) services adopted by enterprises and online backup services adopted by small or midsize businesses.[3]
>
> - **Gartner**

7 reglas de BCDR

1. Planee con anticipación y documente
2. Replicar aplicaciones
3. Establecer protección en el sitio y fuera del sitio
4. Automatizar los procedimientos de recuperación
5. Pruebe con regularidad
6. Proteja su entorno de copia de seguridad
7. Seleccione su socio de BCDR

> Automate, automate, automate. The complexity of today's technology is beyond what humans can manage.[2]
>
> - **Forrester**

1. Planee con anticipación y documente

- ✓Documentación disponible
- ✓Procedimientos detallados
- ✓Contratos proveedores SLAs
- ✓Información de copias de seguridad
- ✓Cuando y quien declara una incidencia?
- ✓Cual es la perdida aceptable de información?
- ✓Donde se almacena el Software, Claves y copias de seguridad?
- ✓Tiempo de recuperación?

2. Replicar aplicaciones

- ✓Los datos solos son inútiles
- ✓Recuperar un servidor desde cero toma tiempo
- ✓Tener un servidor preinstalado
- ✓Tener un sitio alterno para replicas
- ✓Contratar un DRaaS.

Tener replicadas las aplicaciones disminuye el tiempo de recuperación.

3. Establecer protección en el sitio y fuera del sitio

Protección en sitio

- ✓Acceso rápido y ágil a la información
- ✓Tiempo menor en retención de datos
- ✓Afectación en un evento critico.

Protección fuera de sitio

- ✓Retención de datos a largo plazo.
- ✓Geo disponibilidad

Solución hibrida donde las copias locales se repliquen a sitio alterno o nube.

4. Automatizar los procedimientos de recuperación

- ✓No dependencia de las personas
- ✓Probabilidad mayor de error bajo presión alta
- ✓Varias tareas al mismo tiempo
  (recuperar, revisar consolidar. Etc)
- ✓Afectación familiar
- ✓Puede lograrse un mayor ROI
- ✓Flujos de trabajo manuales claros con notificación de ejecución

5. Pruebe con regularidad

- ✓Pruebe
- ✓Pruebe a menudo
- ✓Vuelva a probar
- ✓Los cambios de la plataforma afectan el plan
- ✓Las actualizaciones de hardware y software, la red, las personas.
- ✓Utilizar entornos de prueba aislados.

6. Proteja su entorno de copia de seguridad

- ✓La seguridad es una prioridad
- ✓Copias de seguridad custodiadas
- ✓Copias de seguridad cifradas
- ✓Sistema de copias independiente
- ✓Revisar la seguridad de DRaaS

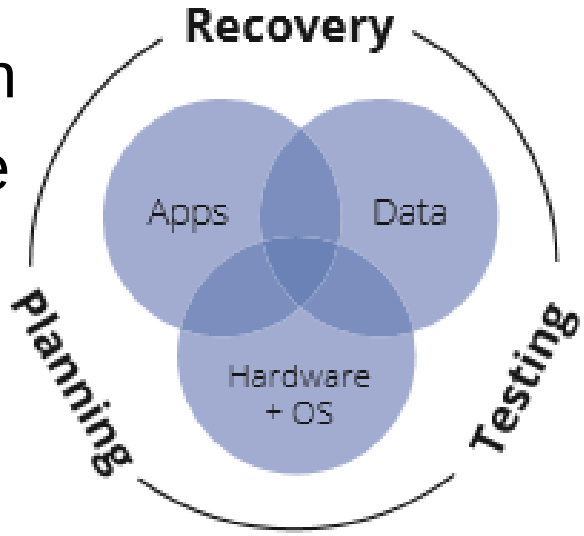
7. Seleccione su socio de BCDR

- ✓Contar con un aliado estratégico
- ✓Ayude a desarrollar el BCDR
- ✓Que conozca de tecnología
- ✓Que entienda de la solución
- ✓Que cuente con herramientas

The concept of IT Disaster Recovery

Pasos para un DRP

- ✓Establecer un grupo de planificación
- ✓Realizar una evaluación del riesgo e inventario TI
- ✓Establecer prioridades
- ✓Desarrollar estrategias de recuperación
- ✓Desarrollar documentación, criterios de verificación y procedimientos
- ✓Pruebe el plan
- ✓Implementar el plan
- ✓Mantener la infraestructura de TI

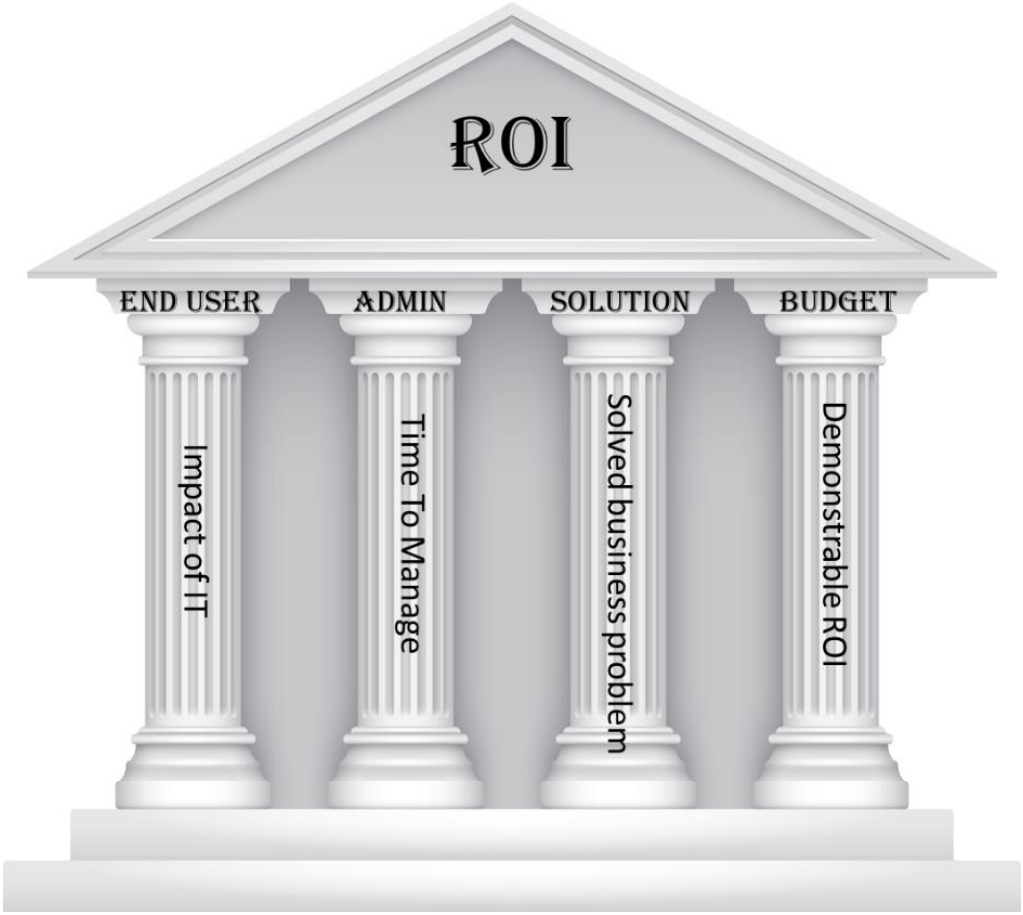


Disaster Recovery Plan

Que debe tener un plan?

1. Introducción
2. Funciones y responsabilidades
3. Datos de contacto
4. Respuestas a los incidentes
5. Planificación de activación
6. Volver al funcionamiento
7. Historial del documento
8. Procedimientos
9. Pruebas
10. Anexos (Documentación)

ROI of IT DISASTER RECOVER



ROI of IT DISASTER RECOVER

Como se calcula el ROI

- ✓Tiempo de inactividad sin protección
- ✓Tiempo de inactividad protegido
- ✓Determine la pérdida de tiempo de inactividad no protegida y las pérdidas de tiempo de inactividad protegidas
- ✓Calcular la pérdida evitada

Avoided Loss = Unprotected Downtime Loss – Protected Downtime Loss

ROI = (Avoided Loss – DR Solution Costs) / DR Solution Costs x 100%

= RATE (# of years, —Annual DR Solution Costs, 0, Avoided Loss, 1)

ROI of IT DISASTER RECOVER

Caso Real: (2 semanas sin información no podían operar 250 empleados a nivel nacional)

- ✓Costo de Empleados
- ✓Dejar de facturar
- ✓Dejar de fabricar
- ✓Dejar de cobrar
- ✓Reproceso del sistema
- ✓Incumplimiento de pedidos
- ✓Sanciones por incumplimiento
- ✓Costos de informática forense
- ✓Costo de Hardware y Software nuevo

ROI of IT DISASTER RECOVER

ROI a 1 año

ROI = (500.000 USD Loss – 20.000 USD Costs) / 20.000 USD x 100% = 2400%

Ahorro de 480.000 USD

ROI a 5 años

ROI = (500.000 USD Loss – 100.000 USD Costs) / 100.000USD x 100% = 400% Ahorro de 400.000 USD

Tasa se retornó anual a 5 años

=TASA(5;-20000;0;500000;1)

Se obtiene 59,51%

Conclusión

Un plan de recuperación de desastres puede hacer la diferencia de su organización. Considere las razones por las que es importante contar con un plan de DR.

La creación de un plan de recuperación de desastres es el primer paso para proteger a su empresa de los desastres naturales o incidentes causados por el hombre.

Next Step

Si aún no ha implementado un plan de DR y no tiene una solución para apoyar ese plan, debe hacerlo inmediatamente. Utilice el cálculo del ROI para apoyar su propuesta a su equipo directivo y recuerde presentarla como una inversión, no como un costo puro.

Dudas comentarios?

Sh*t happens (next time Backup)

MUCHAS GRACIAS!