DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Fundamentos de ciberseguridad

Recuperación ante desastres (DRP)

Profesor
Juan Ignacio Iturbe A.

Introducción

- Nunca se sabe las contingencias que pueden ocurrir:
  - Ataque terrorista al *World Trade Center* (2001)
  - Tsunami en el océano índico (2004)
  - Huracán Katrina (2005)
  - Tsunami en Fukushima (2011) y posterior catástrofe nuclear.
  - Terremoto 8.8 en Chile (2011), posteriores robos y vandalismo.
  - Cada año, miles de negocio son afectados por inundaciones, incendios, tornados, ataques terroristas y otros desastrosos eventos.

Introducción

- Las compañías que sobrevivieron a estos traumas, son:
  - Las que pensaron y se adelantaron a los hechos
  - Planearon para lo peor,
  - Estimaron los posibles daños que pueden ocurrir y
  - Colocaron los necesarios controles en su lugar para protegerse así mismos.

Disaster Recovery Plan (DRP).

- El objetivo de la recuperación ante desastres es:
  - minimizar los efectos de un desastre o un trastorno.
  - manejar el desastre y sus ramificaciones justo después que este ocurre
- Se toman los pasos necesarios para asegurar que los recursos, personal y el proceso de negocio este disponible para reanudar las operaciones en un tiempo acotado.
- Por ejemplo:
  - Define las acciones a tomar en los casos en que una determinada contingencia inhabilite el centro de cómputos.
  - Permite recuperar las operaciones críticas definidas de IT.

Diferencia entre un BCP y un DRP

- DRP
  - Lleva todo a cabo en modo de emergencia
  - Enfrenta por ejemplo:
    - “Oh!, los servidores están todos abajo, no hay servicio!”
    - Se pueden cambiar de lugar los sistemas críticos.
    - Llevar el negocio en un modo diferente mientras se llega a las condiciones regulares.
- BCP
  - Toma un acercamiento mas amplio al problema.
  - Enfrenta por ejemplo:
    - “Ok, los servidores están abajo. Ahora, ¿que hacemos nosotros con el negocio, mientras alguien sube los servicios?”.

Disaster Recovery Plan

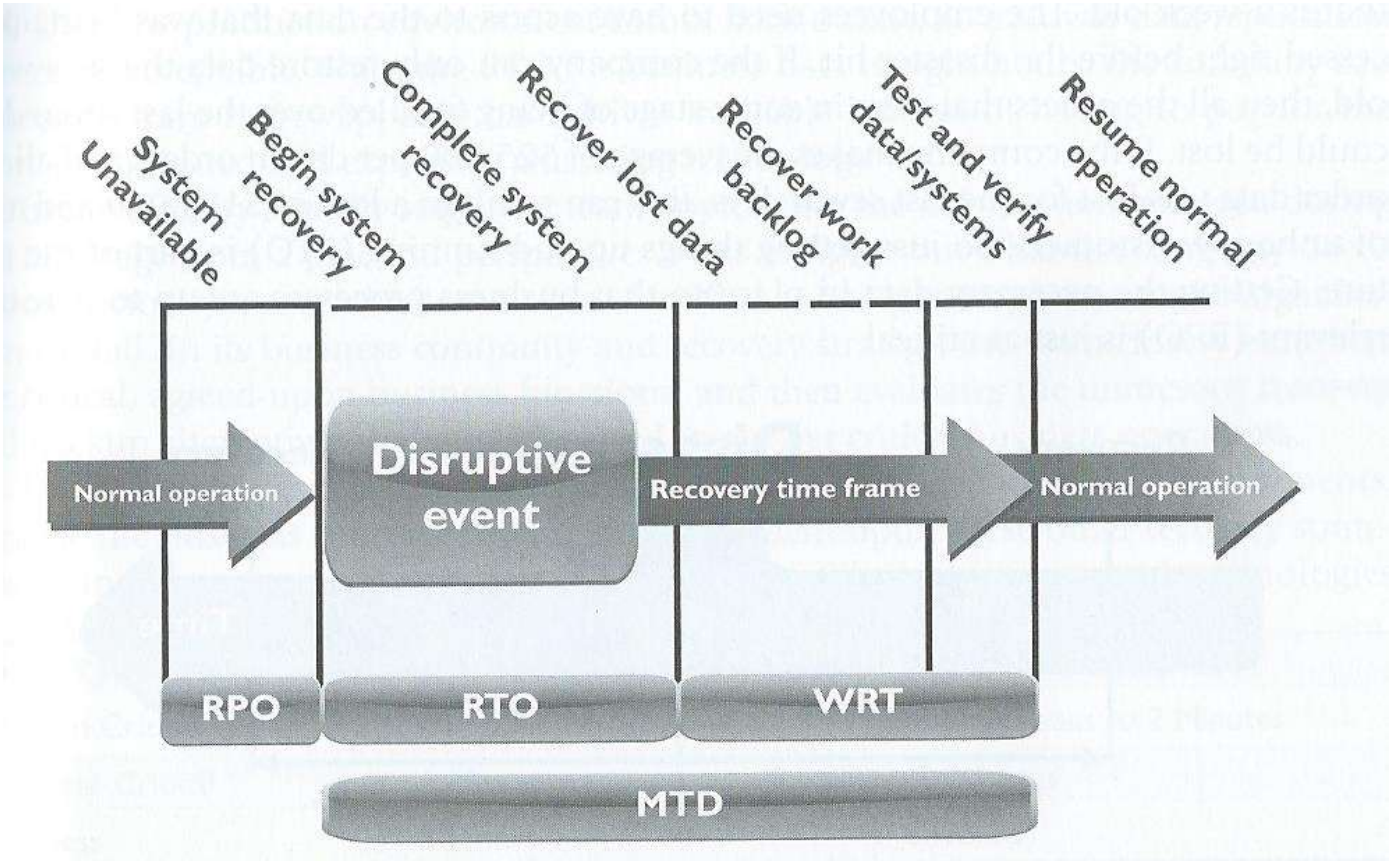
- Objetivos
  - Proteger a la organización de fallas generales de los servicios de información.
  - Minimizar el riesgo generado por la demora en la provisión de servicios.
  - Garantizar la confianza de los sistemas de backup a través de pruebas y simulaciones.
  - Minimizar la toma de decisiones del personal durante una contingencia.

Estrategias de recuperación

- Anteriormente se discute los valores de MTD.
- Es un buen valor para comenzar, pero este no es suficiente granular. Por ejm:
  - Si se tiene definido el MTD del servicio web de atención al cliente en 48 hrs.
  - Esta no es suficiente información para saber que soluciones de respaldo o soluciones redundantes se necesitan.
  - MTD provee un *deadline* básico, que significa que si el servicio no se recupera en 48 hrs, la compañía no se podrá recuperar.

Estrategias de recuperación

- Se necesitan las métricas para volver los sistemas de producción a un funcionamiento normal.
  - RTO, Tiempo de recuperación objetivo:
    - es el tiempo más temprano que un proceso de negocio debe ser restaurado después de que un desastre tenga inaceptables consecuencias.
    - El RTO asume que existe un tiempo de *downtime* aceptable.
    - Lidia con subir toda la infraestructura y sistemas
  - RPO, Punto de recuperación objetivo:
    - es la aceptable cantidad de perdida de datos medida en el tiempo.
  - WRT, Tiempo de recuperación del trabajo:
    - lidia con la restauración de los datos, prueba de los procesos, etc.



- RPO: Punto de recuperación objetivo
- RTO: Tiempo de recuperación objetivo
- WRT: Tiempo de recuperación del trabajo
- MTD: Tiempo máximo tolerable de caída

Ejemplo

- Si una compañía desarrolla procesos manuales en caso que la solución automatizada falla
- Pero le toma 24 horas comenzar con la solución manual
- La compañía puede sufrir perdidas tal que esta no pueda volver totalmente recuperada.

¿RPO o RTO?

Ejemplo

- Por otra parte, si la solución manual funciona en tiempos adecuados, pero solamente el proceso. Se puede tener un problema crítico.
- Por ejemplo, en un sistema de compras online, si solamente se recuperan los datos de las ordenes de compra de hace una semana.
- Y la compañía factura $10.000.000 diarios.
- Se tendrá un gran perdida semanal y muchos clientes insatisfechos

¿RPO o RTO?

Tipo de datos	RPO	RTO
Misión Criticos	Continuo a 1 minuto	Instantáneo a 2 minutos
Negocio Críticos	5 minutos	10 minutos
Negocio	3 horas	8 horas

Procesos del DRP

- Planificación de la continuidad del procesamiento de datos.
  - Acuerdos de ayuda mutua.
  - Servicios de Subscripción.
    - Hot Site. (Full, +$$ y - HH)
    - Warm Site. (Parcial, -$$ y +HH)
    - Cold Site. (Sin servicios,--$$ y ++HH)
  - Centros múltiples.
  - Centros Móviles.
  - Servicios de provisión de HW/SW.

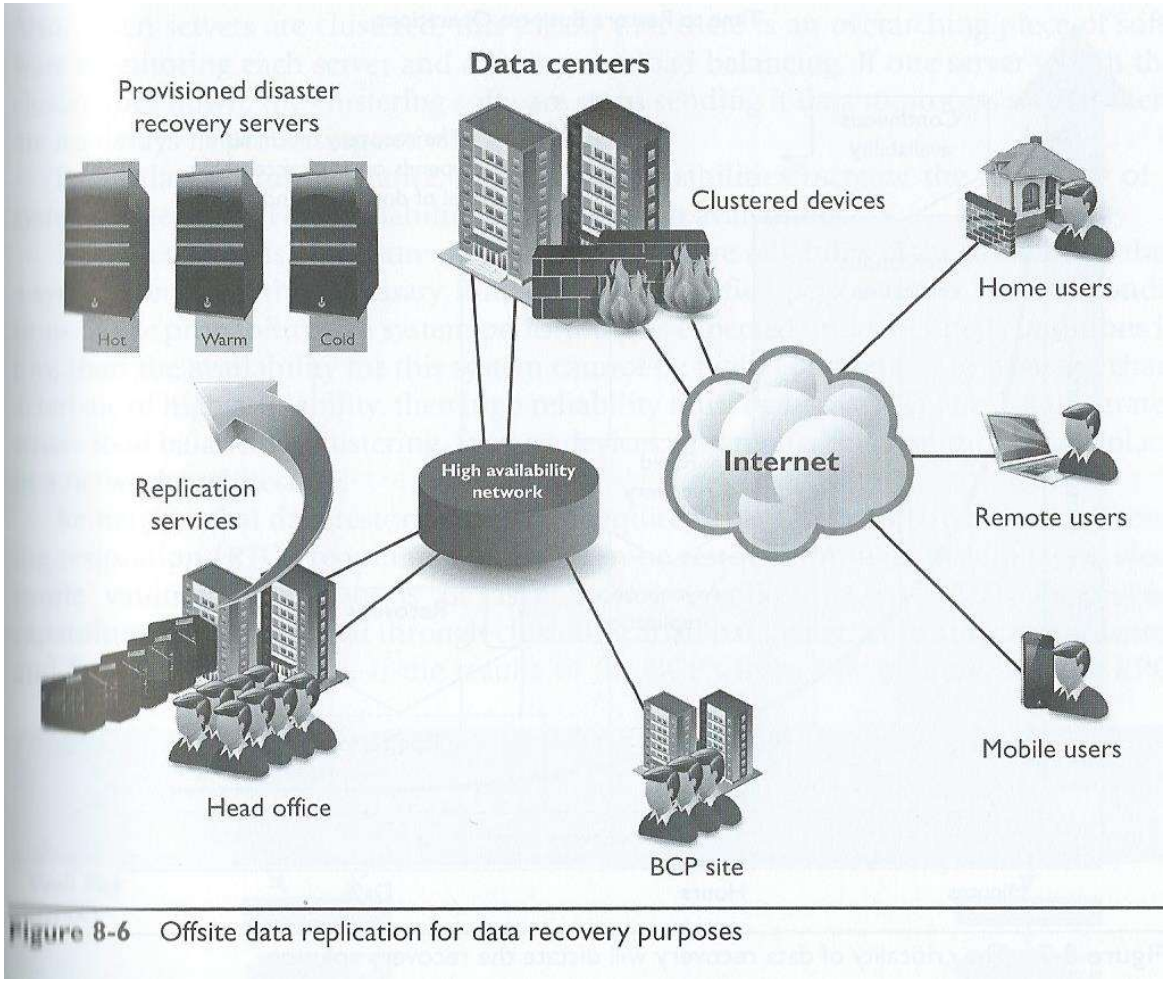


Figure 8-6 Offsite data replication for data recovery purposes

Mantenimiento del plan

- El plan es un documento vivo .
- Asegurar que solo la copia mas reciente del plan sea distribuida. Evitar la existencia de múltiples versiones.
- Asegurar que la información de contactos este actualizada.
- Asegurar que ante la adquisición o modificación o eliminación de elementos críticos, estos sean incorporados al plan.

Testeo de los Planes

- Checklist.
  - Copias del plan son distribuidas a las gerencias para su revisión.
- Seguimiento estructurado (*structured walk-through*).
  - Gerentes de las áreas afectadas se reúnen para revisar el plan.
- Simulación.
  - Todo el personal de soporte se reúne en una sesión de práctica.

Testeo de los Planes

- Prueba en Paralelo.
  - Los sistemas críticos son ejecutados en el sitio alternativo.
- Interrupción completa.
  - Todos los sistemas en producción son interrumpidos. Se procede a ejecutar el plan en condiciones reales.

Testeo de los Planes

- Otras consideraciones.
  - Las pruebas del plan deben realizarse alternando el personal a cargo.
  - No es absolutamente necesario efectuar siempre pruebas completas.
  - La periodicidad de las pruebas dependerá del grado de movilidad del plan y/o del personal a cargo.
  - Toda prueba que haya sido 100% exitosa fue mal realizada.
  - Todo resultado de una prueba debe servir como feedback para mejorar el plan.

Equipos de trabajo

- Equipo de Recuperación.
  - Responsable de ejecutar los procedimientos de recuperación ante la declaración de un desastre.
- Equipo de Salvatage.
  - Responsable de volver el sitio primario a sus niveles operativos normales.
- Equipo de Reanudación de Operaciones.
  - Responsable de volver las operaciones al sitio primario.
  - No siempre es un equipo adicional.

Otros aspectos a considerar

- Relación con grupos externos (emergencias, policía, bomberos, etc).
- Relaciones con empleados.
- Fraude y crímenes.
- Desembolsos financieros.
- Relaciones con los medios de prensa/ tv/ radio.

Importante!

- Ambos planes, BCP y DRP, deben mantenerse actualizados.
- El personal responsable debe estar preparado para entrar en contingencia.
- Toda la compañía debe conocer y entender los objetivos de los planes.
- Pruebas periódicas de los planes, BCP y DRP, deben realizarse. Estas deberían estar a cargo de entidades independientes a las áreas involucradas:
  - Auditoría Interna
  - Ó Consultores Externos.

FIN