Taller de Administración de Servidores Linux

CC5308

Clase 29: 24 de mayo de 2011

Business Continuity Planning

Luis León Cárdenas Graide
lcardena [at] nic . cl

Objetivos BCP

- Reducir Riesgo Operacional
- Abarca Administración de Crisis
  - BRP: Business Recovery Planning
  - DRP: Disaster Recovery Planning
- Gestión de Riesgo Operacional es parte de BCP
- Fail-safe vs Safe-fail
- Evolución conjunta con Security Policies
  - Empezar por lo simple: manual impreso en almacén seguro con nombres, direcciones, teléfonos; contactos de staff, clientes, proveedores, copias de contratos y seguros

Tolerancia a Fallos

- Fail-safe: No fallar
  - ¿Realista? Siempre: Riesgo > 0
  - Ineficiencia: Probabilidad → 0 => Costo → infinito
  - ¡Fallará! => Mitigar
- Safe-fail: Asumir falla
  - Gracefull faliure
  - Fallas controladas
  - Desenlaces previsibles
    - Gestionable

Ciclo de Vida BCP

- Análisis
- Diseño de Solución
- Implementación
- Prueba y Aceptación Organizacional
- Mantenimiento

Ciclo BCP: 1 - Análisis

- Análisis de Impacto (BIA)
  - Funciones/actividades: Críticas vs no-Críticas
    - Identificar Críticas
    - Consecuencias inaceptables para dueño
  - Inaceptabilidad: ránking de costo c/r mitigación
    - Leyes
  - Recovery Point Objective (RPO)
    - Latencia recuperación datos
    - MTDL: Maximum Tolerable Data Loss
  - Recovery Time Objective (RTO)
    - Tiempo a reestablecer función
    - MTPD: Maximum Tolerable Period of Disruption
  - Requerimientos técnicos/negocio recuperación función

Ciclo BCP: 1 - Análisis

- Análisis de Amenazas
  - Naturales
    - Terremoto, Inundación, Huracán
  - Accidentales
    - Incendio, Averías, Apagones
  - Intencionales
    - Robo, ciber-ataque, Sabotaje, Terrorismo
  - Negligencias
    - Errores, Omisiones, Olvidos
  - Biológicas
    - Enfermedades, Muerte

Ciclo BCP: 1 - Análisis

- Definición de Escenarios de Impacto
  - Priorización: Impacto amplio vs acotado
  - Considerar costo extra de reacción durante operación
- Documentación Requerimientos de Recuperación
  - Requiere documentación de Activos y disponibilidad
    - Físicos y de Información
  - Plazas de trabajo. Múltiples dependencias físicas
  - Contactos de personal involucrado en recuperación
  - Insumos de trabajo críticos en cada dependencia
  - Claridad sobre inoperatividad máxima permitida

Ciclo BCP: 2 - Diseño Solución

- Maximizar costoefectividad de soluciones
  - Requerimientos mínimos de datos y aplicaciones
  - Margen de tiempo en que deben estar disponibles
- Estructura administración de mando
- Ubicación dependencia de trabajo 2daria
- Interrelación entre 1ª y 2ª
  - Arquitectura telecomunicaciones
  - Metodología de replicación de datos
  - Aplicaciones
  - Insumos de trabajo físico

Ciclo BCP: 3 - Implementación

- Llevar a cabo Diseño :)

Ciclo BCP: 4 - Testing y Aceptación

- Poner a prueba Implementación
  - Poner a prueba que Organización lo haya incorporado
- ¿Funciona equipo de respuesta a crisis?
  - ¿Sigue funcionando organización?
- Ensayo técnico de intercambio entre dependencias
  - De 1aria a 2daria y viceversa
- Probar que aplicaciones sigan funcionando después de cada cambio
- Probar que negocio siga funcionando después de cada cambio

Ciclo BCP: 5 - Mantención

- Testing periódico + retroalimentación ante cambios
- Actualización de información
- Verificación de soluciones técnicas
- Procedimientos de recuperación
  - ¿Siguen funcionando labores críticas?
  - ¿Cambios en sistemas de soporte a labores críticas?
  - ¿Documentación actualizada, significativa y útil?
  - Cumpliendo procedimiento, ¿se alcanzan límites establecidos de inoperabilidad?

Parámetros Cuantificables

- MTBF: Mean Time Between Failures
- MTTR: Mean Time to Recovery
  - ¿Cumple RTO?
- SPF: Single Point of Failure
  - Redundancia
- Niveles de Servicio tolerables
  - Máximos/Mínimos, Varianzas, Indisponibilidad, Latencias, Tasas, Costos

Nivel de Servicio

- Proveedor vs Contratante
- Parámetros Cuantificables
- SLA: Service Level Agreement
  - Responsabilidades mutuas: Derechos y Deberes
  - "Best effort" / Garantías
  - Renovaciones / Caducidades / Nulidades
  - Multas = Sincerar Fracaso
  - Barreras de entrada y de salida
- Estandarización
  - British Standards Institution (BS): BS 25999-{1,2}
- ¡Para todo negocio, no sólo informático!

Actividad Personal

- Documéntese sobre el SLA contratado a sus distintos proveedores
  - Internet: ¿dedicado, asimétrico, inalámbrico?
  - Telefonía: ¿fija vs celular? ¿tiempos, tonos, latencias?
  - Sanitaria: ¿presión, químicos, tiempos?
  - Electricidad: ¿tiempos, voltaje, frecuencia?
  - TV: ¿abierta vs pagada? ¿canales o carrier?
- ¿Qué ofrecen?
- ¿Voluntarios u obligados por ley? ¿Qué ley?
- ¿Cumplen? ¿Pasa algo si no? ¿Qué? ¿Cuánto $?