DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Fundamentos de ciberseguridad

Continuidad del negocio y recuperación ante desastres

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

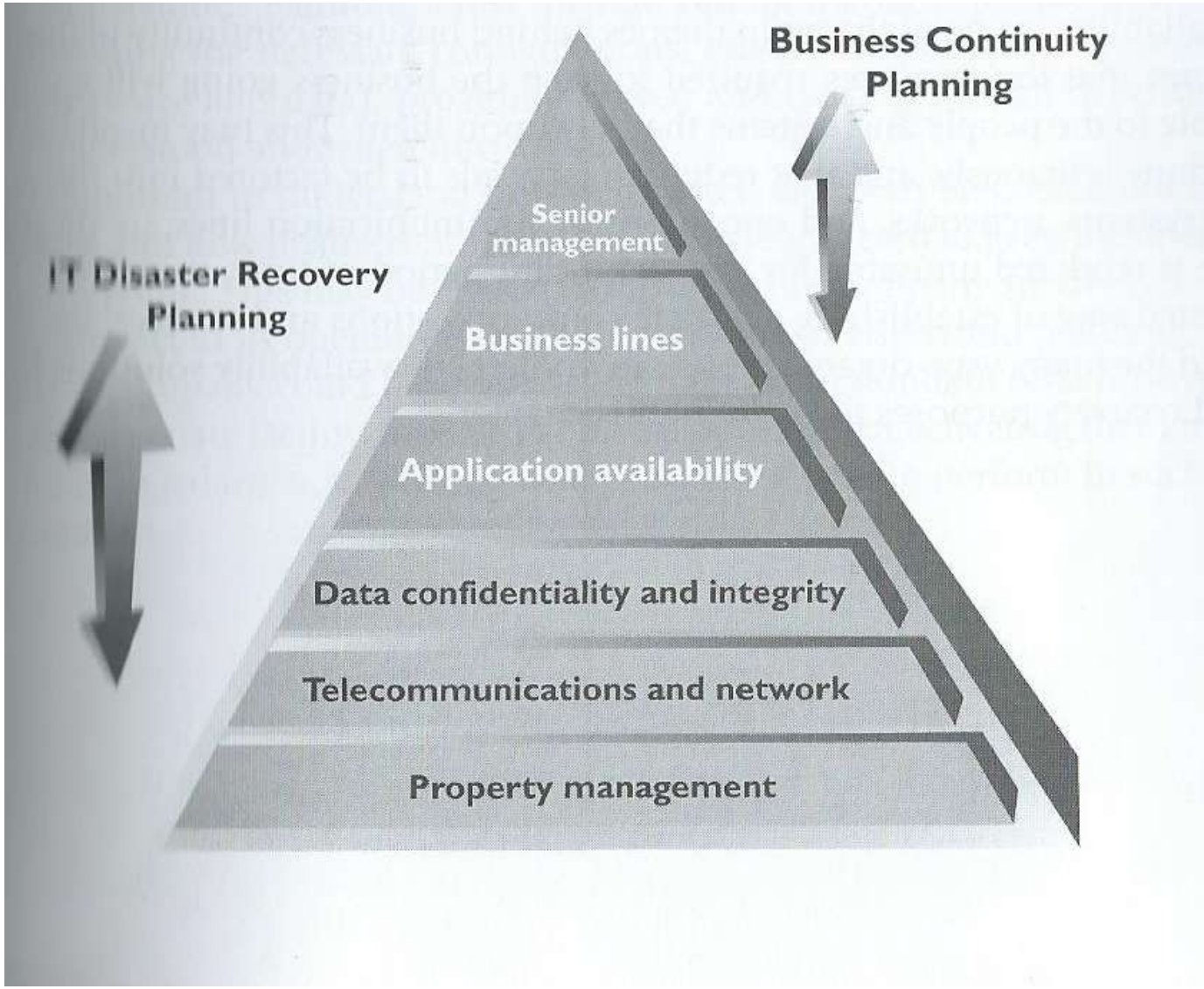
- Las compañías que sobrevivieron a estos traumas, son:
  - Las que pensaron y se adelantaron a los hechos
  - Planearon para lo peor,
  - Estimaron los posibles daños que pueden ocurrir y
  - Colocaron los necesarios controles en su lugar para protegerse así mismos.

Business Continuity Plan (BCP)

- Provee métodos y procedimientos para enfrentar cortes o desastres de una manera oportuna.
- Define las acciones a tomar en los casos en que una determinada contingencia inhabilite algún área de operaciones o tecnología.
- Permite recuperar las operaciones críticas definidas del negocio.
- Incluye el DRP.
- Es a largo plazo

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?”.


Business Continuity Planning
IT Disaster Recovery Planning
Senior management
Business lines
Application availability
Data confidentiality and integrity
Telecommunications and network
Property management

Recuperación ante contingencias

- BCP y DRP, incluyen tareas a efectuar:
  - Antes de que ocurra una interrupción.
  - Durante la ocurrencia de la interrupción.
  - Después de que ocurrió la interrupción.
- Toda planificación de Recuperación ante Contingencias debe ser realizada antes de la ocurrencia de los eventos.
  - Proactivo en lugar de Reactivo.

Razones para tener un plan

- Mas vale prevenir que curar
  - Proactivo en lugar de Reactivo.
- Mantener el negocio funcionando.
  - Ahorro de tiempo, $$, errores y stress.
  - Que el dinero siga entrando.
  - Pérdida de negocios a corto y largo plazo.
- Efecto en clientes.
  - Imagen pública.
- Requerimientos legales/ contractuales.

Recuperación ante Contingencias

- La prioridad número 1 de la recuperación de contingencias es:

La gente siempre está primero.

Estándares y buenas prácticas

- El instituto nacional de estándares y tecnología (NIST), genero una de las primera guías NIST 800-34
- La guía *“Continuity Planning Guide for Information Technology Systems”, tiene siete pasos.*

Política de continuidad

- Integrar requerimientos de la ley y regulaciones
- Definir alcance, objetivos y roles
- La autoridad aprueba la política

BIA

- Identificar las funciones críticas
- Identificar los recursos críticos
- Calcular el MTD para los recursos
- Identificar amenazas
- Calcular riesgos
- Identificar soluciones de respaldo

Identificación de controles preventivos

- Implementar controles
- Mitigar riesgos

Desarrollar estrategias de recuperación

- Procesos de negocios
- Instalaciones
- Suministros y tecnología
- Usuarios y ambiente del usuario
- Datos

Desarrollar el BCP

- Documentar
  - Procedimientos
  - Soluciones de recuperación
  - Roles y tareas
  - Respuesta de emergencia

Ejercitar, probar y repetir

- Probar plan
- Mejorar plan
- Entrenar empleados

Mantener el BCP

- Integrar dentro del proceso de control de cambios
- Asignar responsabilidad
- Actualizar plan
- Distribuir después de actualizar

Continuity Planning Guide for Information Technology Systems

Estándares y buenas prácticas

- Otros estándares son:
  - BS 25999-1 y 25999-2, para la gestión de la continuidad del negocio (BCM)
  - ISO/IEC 27031:2011
  - ISO 22301 reemplaza la 25999-2
  - Business Continuity Institute's Good practice Guideline (GPG), las mejores prácticas para BCM divididas entre aspectos de gestión y técnicos.
  - DRI Internacional Institute's Professional Practices for Business Continuity Planner,

Contingencias

- Eventos Naturales.
  - Huracanes, inundaciones, terremotos, incendios.
    - Interrupción de servicios básicos (electricidad, comunicaciones, etc).
    - Incendios, explosiones o derramamiento de toxinas.
- Eventos desatados por personas.
  - Sabotaje, bombardeo u otros ataques intencionales.
  - Huelgas, accidentes.
  - Errores.

Plan de continuidad del negocio

- Etapas
  - Definición de Alcance e Inicio del Plan.
  - Evaluación del Impacto en el Negocio (Business Impact Assessment, BIA).
  - Desarrollo del Plan.
  - Aprobación e Implantación del Plan.
  - Prueba y Mantenimiento del Plan.

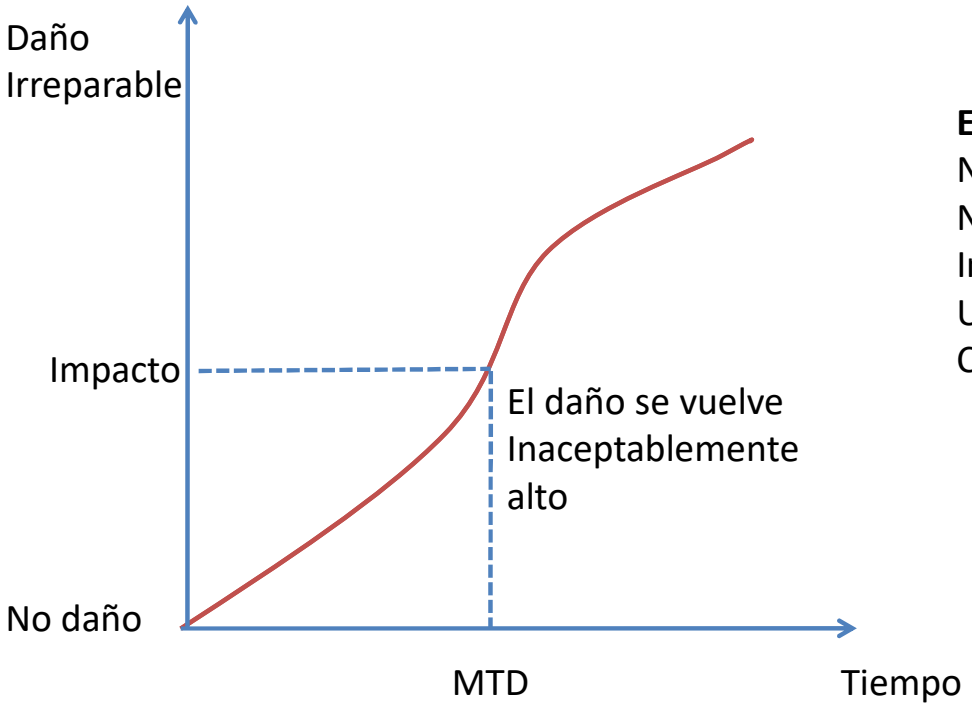
Plan de continuidad del negocio

- Roles y Responsabilidades
  - Alta Gerencia.
    - Inicia el proyecto, da la aprobación final y apoya la iniciativa a lo largo de todo su ciclo de vida.
  - Gerencia de Unidades de Negocio.
    - Identifican y priorizan los sistemas/ operaciones críticas del negocio.
  - Comité de BCP.
    - Dirige los procesos de planificación, implantación y prueba del BCP.
  - Unidades Funcionales:
    - Participa en la implantación y las prueban del plan.

Etapas del BCP

- Evaluación del Impacto en el Negocio (BIA)
  - Objetivos.
    - Priorización en base a la criticidad de los procesos/ sistemas.
    - Estimación de tiempo máximo de tolerancia (*Maximum Tolerable Downtime, MTD ó Maximum Period Time of Disruption*).
    - Requerimientos de Recursos.

Impacto versus Tiempo



Ejemplos de MTD's:

No esencial	30 días
Normal	7días
Importante	72 horas
Urgente	24 horas
Critico	Minutos a horas

Análisis del impacto en el negocio (BIA)

1. Selección de los individuos a entrevistar para la obtención de datos.
2. Seleccionar técnicas para la obtención de los datos (encuestas, cuestionarios, acercamientos cualitativos y cuantitativos).
3. Identificar las funciones del negocio criticas para la empresa.
4. Identificar los recursos en los cuales dependen estas funciones.

Análisis del impacto en el negocio (BIA)

5. Calcular cuanto tiempo estas funciones pueden sobrevivir sin estos recursos.
6. Identificar vulnerabilidades y amenazas de estas funciones
7. Calcular el riesgo para cada diferente función del negocio.
8. Documentar lo encontrado y reportarlo a la gerencia.

Etapas del BCP

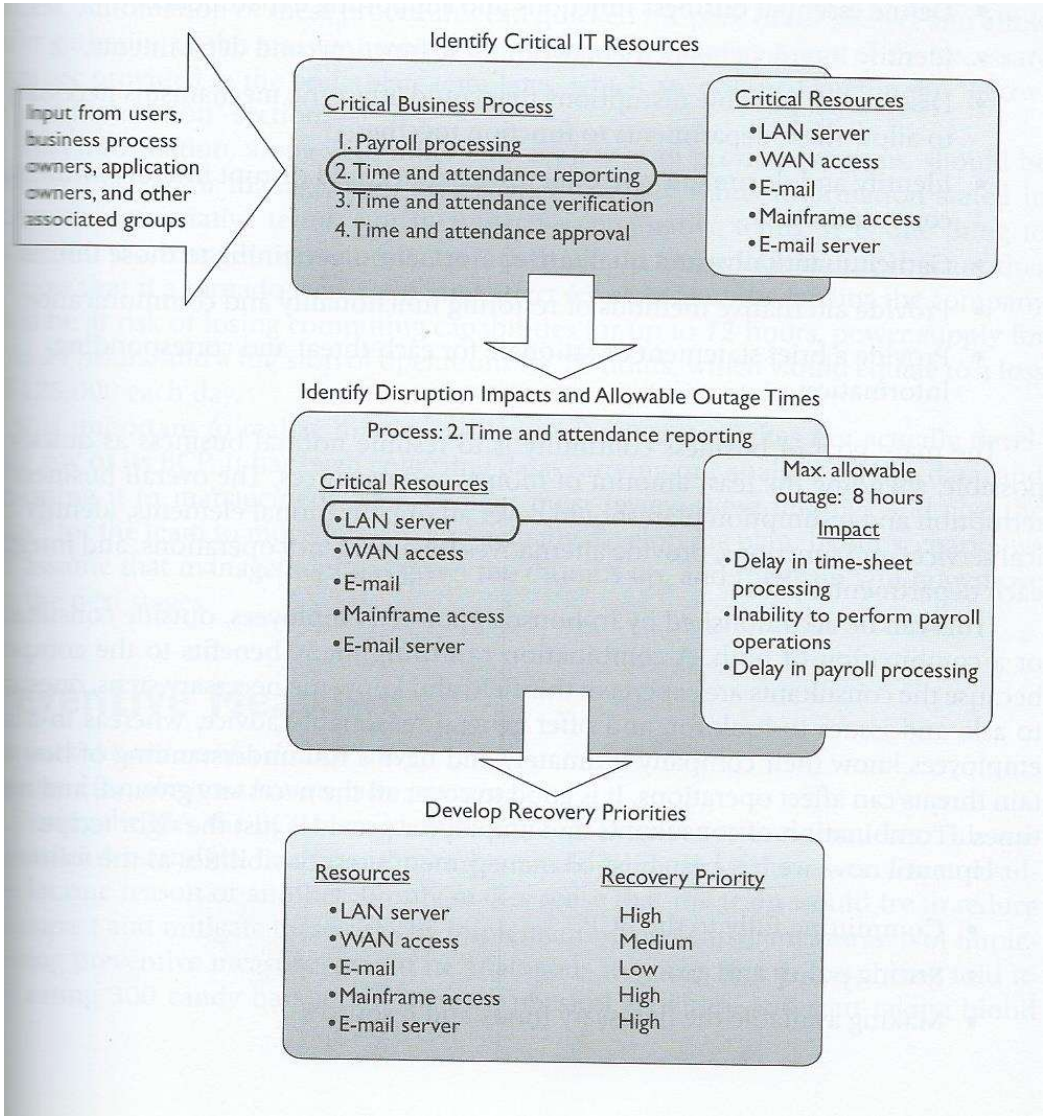
- Evaluación del Impacto en el Negocio (BIA)
  - Tareas.
    - Obtención del material necesario para realizar el análisis.
    - Desarrollo de una evaluación de vulnerabilidades.
    - Análisis de la información obtenida.
    - Documentación y reporte de resultados y recomendaciones.

Etapas del BCP

- Evaluación del riesgo
  - Identificación de escenarios de fallas potenciales.
  - Probabilidad de falla.
  - Costo de la falla (análisis de impacto).
    - Costo monetario.
    - Gastos operativos adicionales.
    - Violación de contratos o requerimientos legales.
    - Pérdida de ventaja competitiva, confianza del público

Etapas del BCP

- Evaluación del riesgo/Análisis
  - Estimación de Pérdida Anual.
  - Suposiciones del peor de los casos
  - El BCP se basará en el modelo de procesos de negocios o en IT exclusivamente?
  - Identificación de funciones críticas y recursos necesarios para soportar dichas funciones.
  - Balance del impacto vs. costo de los controles/ contramedidas.


Identify Critical IT Resources
Input from users, business process owners, application owners, and other associated groups
Critical Business Process
1. Payroll processing
2. Time and attendance reporting
3. Time and attendance verification
4. Time and attendance approval
Critical Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Identify Disruption Impacts and Allowable Outage Times
Process: 2. Time and attendance reporting
Critical Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Max. allowable outage: 8 hours
Impact
•Delay in time-sheet processing
•Inability to perform payroll operations
•Delay in payroll processing
Develop Recovery Priorities
Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Recovery Priority
High
Medium
Low
High
High

Ejemplo

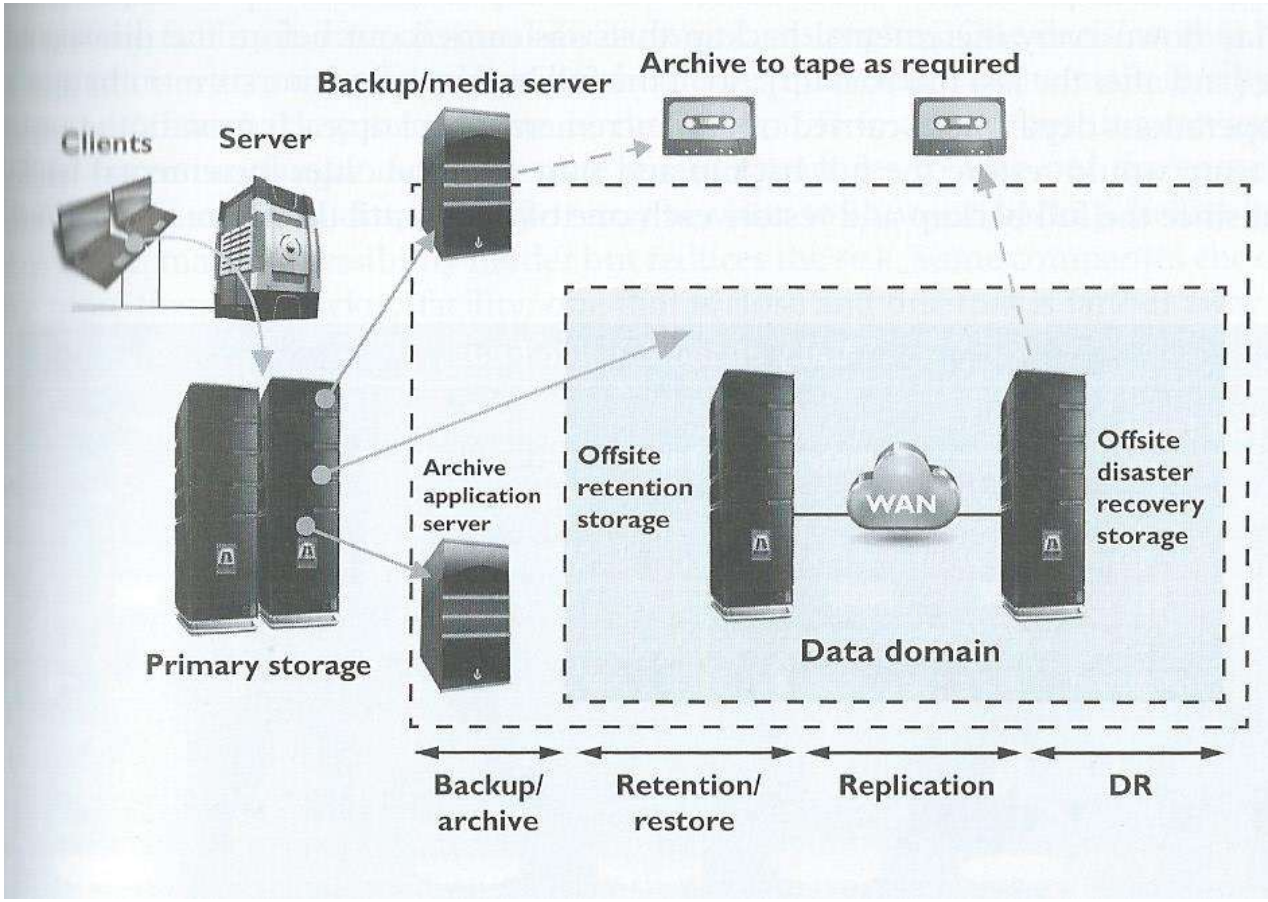
- Si tengo una compañía cuya principal actividad es la venta a artículos vía una página web.
  - ¿Cuáles serían los recursos principales que soporta el negocio?
  - Por ejem, ¿Cuánto tiempo podría estar abajo el sitio web? ¿En que me afectará mientras se encuentre abajo?
  - ¿Cuales son los recursos que tendrían mayor prioridad de ser atendidos?

Etapas del BCP

- Desarrollo de la Estrategia (Selección de Alternativas)
  - Soporte/ Apoyo de la Gerencia Ejecutiva.
  - Estructura del/ los equipos.
  - Selección de la estrategia.
    - Costo - efectivo.
    - Trabajable/ Implementable.

Definición de la Estrategia de Continuidad

- Recursos Informáticos.
  - Hardware, software, comunicaciones, aplicaciones, datos.
- Locaciones.
  - Locaciones alternativas para equipamiento y personal.
- Personal.
  - Cada persona asignada al BCP tendrá funciones específicas para llevar a cabo la ejecución del plan en forma exitosa.
- Equipamiento y suministros.
  - Papel, formularios, energía, equipamiento de seguridad específico, etc.


Backup/media server
Archive to tape as required
Clients
Server
Archive application server
Offsite retention storage
WAN
Offsite disaster recovery storage
Primary storage
Data domain
Backup/ archive
Retention/ restore
Replication
DR

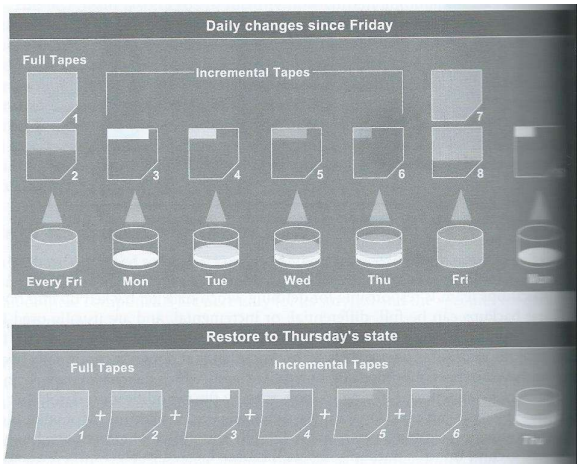
Etapas del BCP

- Implantación (Desarrollo del Plan)
  - Especificación de los recursos necesarios para efectuar la recuperación.
  - Negociación de aquellos aspectos que no serán soportados inhouse.
  - Mitigación de debilidades.

Etapas del BCP

Prevención/ Mitigación de Riesgos.

- Programa de administración de riesgos.
- Seguridad física y acceso a información.
- Controles ambientales.
- Redundancia Backups/ Recuperación.
  - Journaling (recuperación de transacciones), Mirroring, Shadowing (snapshots).
  - On-line/near-line/off-line.
- Seguros (Insurance).
- Planes de respuestas ante emergencias
- Procedimientos.
- Entrenamiento.



Etapas del BCP

- Toma de decisiones.
  - Costo efectivas
  - Requerimientos con intervención humanas
    - Las funciones manuales en general tiene debilidades
  - Sobreescrituras y valores por defecto
    - Capacidad de Shutdown.
    - Por defecto toda solución debe ser de no access .

¿Qué se incluye en el BCP?

- Almacenamiento Off-site.
- Sitio Alternativo de Procesamiento.
- Procesamiento de Backups.
- Comunicaciones.
- Espacio para trabajar (oficinas).
- Equipamiento de oficina,documentación y artículos de escritorio.
- Seguridad.
- Procesos de Negocio/ Administrativos críticos.
- Pruebas.
- Proveedores - información de contratos, negociaciones, etc.
- Equipos de trabajo -información de contacto, transportación, etc.
- Procedimientos de retorno a operaciones normales
- Otros recursos necesarios.

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