Sesión # 213

De la teoría a la práctica:

CobiT aplicado para asegurar la **continuidad de las operaciones**

José Ángel Peña Ibarra

japi@ccisa.com.mx

Consultoría en Comunicaciones e Informática, S.A. de C.V.

Agenda

1. **Introducción**
   - Continuidad de TI y continuidad de los negocios.
   - Que es el DS4 y su relación con otros estándares.
2. **Establecimiento del marco de referencia: (DS4.1)**
3. **Estrategia y filosofía de continuidad de TI, alineada con la estrategia de continuidad de negocios (DS4.2)**
4. **Identificación de los procesos críticos y análisis de impacto, BIA (DS4.2,DS4.10)**
5. **Contenido del Plan de Continuidad (DS4.3) (DS4.4) (DS4.9)**
6. **Estrategias de continuidad. (DS4.2)**
7. **Almacenamiento off-site, sitios alternos. (DS4.11, DS4.12)**
8. **Pruebas y actualización del Plan (DS4.5, DS4.6)**
9. **Entrenamiento y distribución del Plan de Continuidad (DS4.7, DS4.8)**

1. Introducción

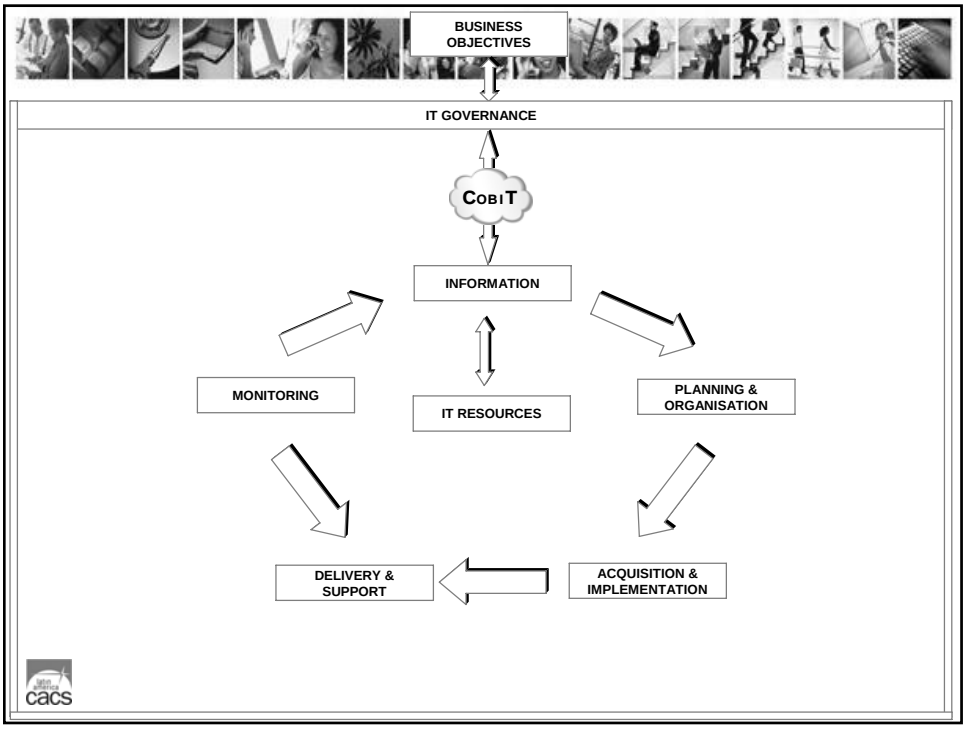
Introdución

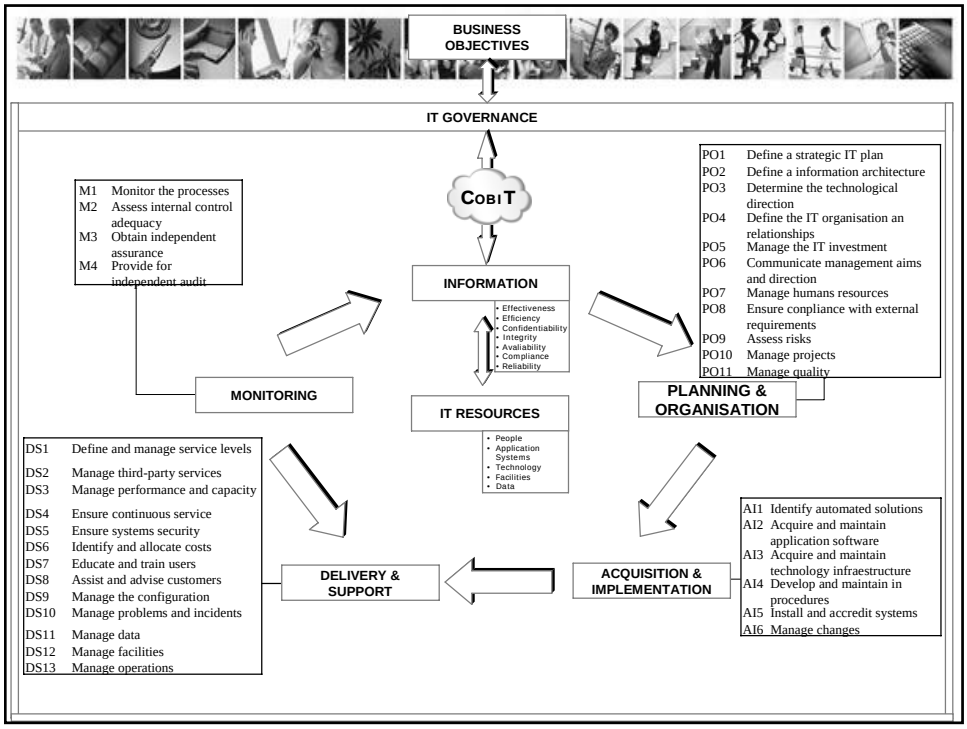
- **Necesidad de continuidad:** El ambiente de negocios actual, obliga a las empresas a mantener una adecuada administración de la continuidad de las operaciones.
- **Nuevas Aplicaciones:** Cada día se tienen más aplicaciones de negocio, que se basan en la tecnología de información, por lo que las organizaciones en prácticamente todos los sectores se han hecho más dependientes de TI, provocando que cualquier falla de esta les puede afectar severamente.
- **Nuevas Amenazas:** Ya no son suficientes los controles por ignorancia, ahora mucha más gente tiene los conocimientos necesarios para afectar los sistemas de información. Es un fenómeno mundial el hecho de que las nuevas generaciones adquieren conocimientos de TI siendo cada vez más jóvenes.

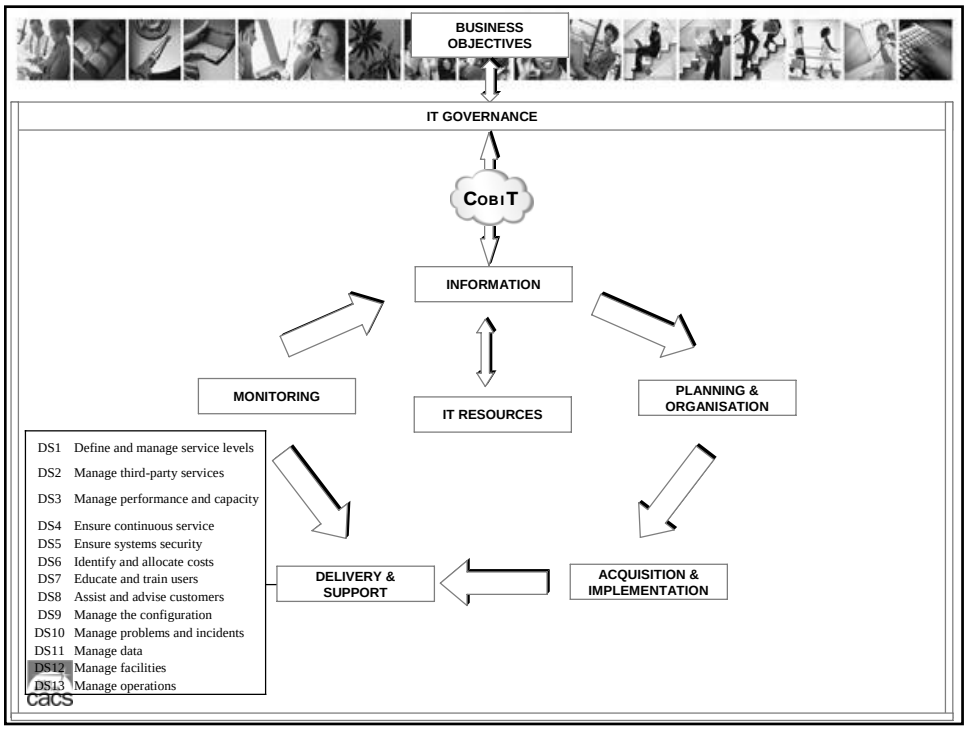
DS4 CobiT

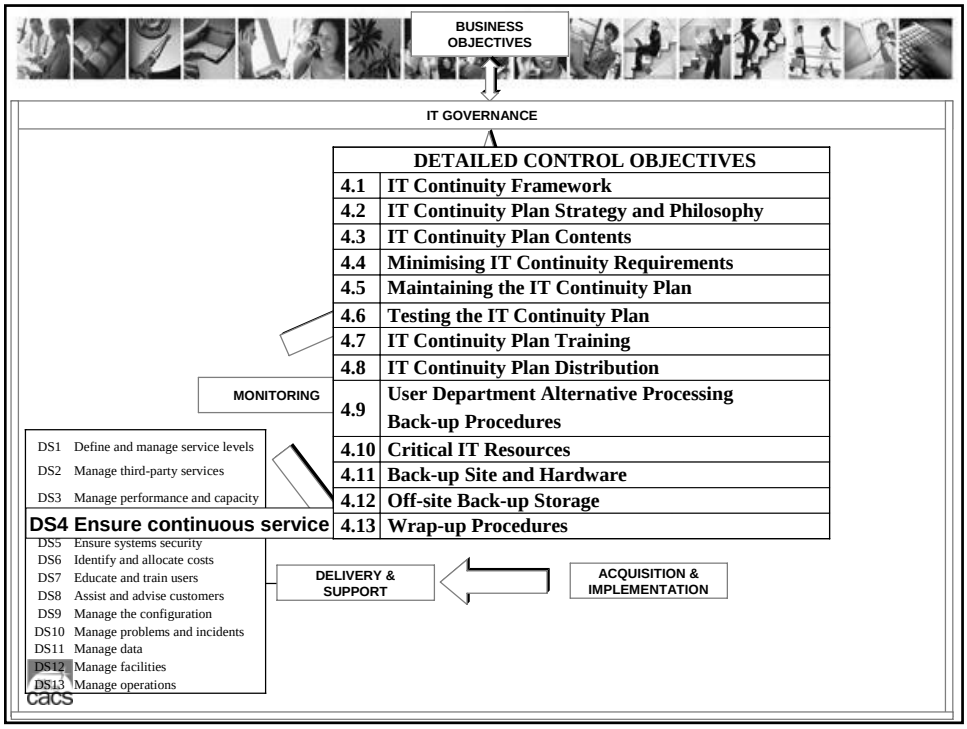
- Una de las herramientas que nos pueden ayudar a tener un adecuado enfoque para la continuidad de las operaciones es el **CobiT**, el cuál tiene 4 dominios, los cuáles se muestran en las láminas siguientes.

- En el dominio de Delivery and Support, se tiene el proceso **DS4,** el cuál incluye 13 objetivos detallados de control, los cuáles, permitirán asegurar la continuidad del servicio y por lo tanto, mantener la continuidad de las operaciones




BUSINESS OBJECTIVES
IT GOVERNANCE
COBIT
M1 Monitor the processes
M2 Assess internal control adequacy
M3 Obtain independent assurance
M4 Provide for independent audit
INFORMATION
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability
PO1 Define a strategic IT plan
PO2 Define a information architecture
PO3 Determine the technological direction
PO4 Define the IT organisation an relationships
PO5 Manage the IT investment
PO6 Communicate management aims and direction
PO7 Manage humans resources
PO8 Ensure conpliance with external requirements
PO9 Assess risks
PO10 Manage projects
PO11 Manage quality
MONITORING
IT RESOURCES
• People
• Application Systems
• Technology
• Facilities
• Data
PLANNING & ORGANISATION
DS1 Define and manage service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and allocate costs
DS7 Educate and train users
DS8 Assist and advise customers
DS9 Manage the configuration
DS10 Manage problems and incidents
DS11 Manage data
DS12 Manage facilities
DS13 Manage operations
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire and maintain technology infraestructure
AI4 Develop and maintain in procedures
AI5 Install and accredit systems
AI6 Manage changes
DELIVERY & SUPPORT
ACQUISITION & IMPLEMENTATION


BUSINESS OBJECTIVES
IT GOVERNANCE
COBIT
INFORMATION
MONITORING
IT RESOURCES
PLANNING & ORGANISATION
DS1 Define and manage service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and allocate costs
DS7 Educate and train users
DS8 Assist and advise customers
DS9 Manage the configuration
DS10 Manage problems and incidents
DS11 Manage data
DS12 Manage facilities
DS13 Manage operations
DELIVERY & SUPPORT
ACQUISITION & IMPLEMENTATION



2. Establecimiento del marco de referencia

Marco de Referencia

- Para asegurar una adecuada administración de la continuidad de las operaciones, se debe establecer todo un marco de referencia, que incluya la definición de los **roles y responsabilidades** que tendrán, tanto los responsables de TI, como los dueños de los procesos y la Gerencia de la organización.

- El marco de referencia incluirá las **políticas y lineamientos necesarios** para guiar las acciones de prevención de desastres y para asegurar que se cuenta con los planes y entrenamiento necesarios para enfrentar y recuperarse de un desastre, con el menor impacto para la organización.

Marco de Referencia

- El marco de referencia incluirá la definición del esquema de **análisis de riesgos y del enfoque metodológico** a utilizar para lograr la adecuada continuidad de las operaciones.

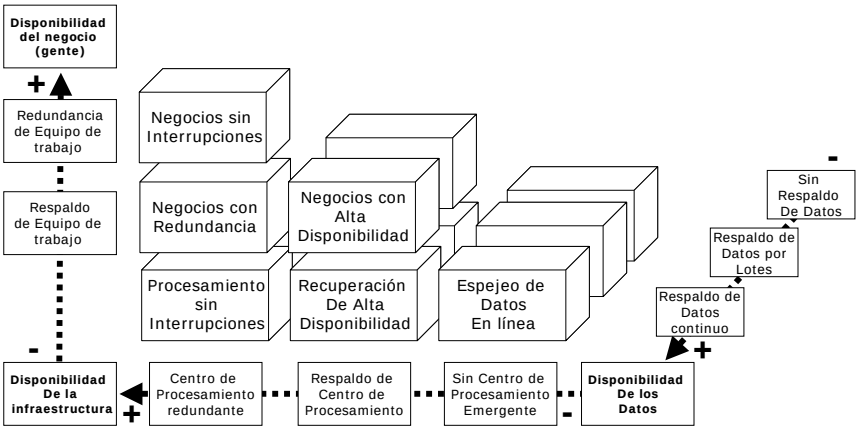
- También se incluirán las **reglas y estructuras para documentar y distribuir los planes**, así como los correspondientes **procedimientos de aprobación**.

3. Estrategia y filosofía de continuidad de TI, alineada con la estrategia de continuidad del negocio

Alineamiento de estrategias

- El plan de continuidad de TI debe estar en línea con el Plan General de Continuidad del Negocio, para asegurar consistencia.
- El análisis de las estrategias de continuidad se hace considerando los objetivos globales de la organización, respecto a las tres dimensiones fundamentales para la disponibilidad:
  - **Datos,**
  - **Infraestructura tecnológica y**
  - **Gente.**

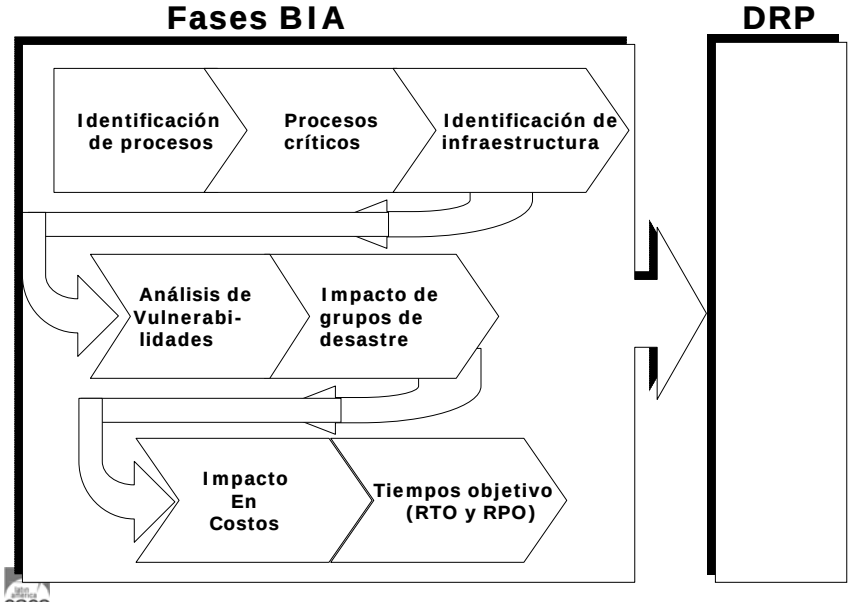
Filosofía de continuidad en las Tres Dimensiones de Disponibilidad



4. Identificación de los procesos críticos y análisis de impacto al negocio (BIA)

BIA

- El Análisis de Impacto al Negocio, BIA, nos permite identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre. Identifica los sistemas críticos y estima el tiempo que la compañía puede tolerar en caso de un desastre.
- Conociendo el impacto al negocio, se pueden **dimensionar** las medidas de prevención y recuperación, de acuerdo a las necesidades de la organización, evitando la sobre inversión o la sub inversión.



BIA

- Durante el BIA se identifica la infraestructura relacionada con los procesos críticos, lo que permite **enfocar** los esfuerzos de prevención y recuperación sobre los elementos críticos de la infraestructura.
- Los *procesos* serán *críticos,* dependiendo de la organización de que se trate, por ejemplo:

Banca: *Tarjetas de débito, mesa de dinero..*
Aerolíneas: *Reservaciones, plan de vuelos..*
Manufactura: *Inventarios, Control de la producción..*
Servicios: *Facturación, cobranza..*

BIA

- La infraestructura crítica será entonces, la que se utiliza para la operación de un proceso crítico, por ejemplo:

Proceso Mesa de dinero

Infraestructura:
- Sistema de Mesa de dinero
- Servidor de aplicación Mesa de dinero
- Router para comunicar con entidades externas
- Switch de red local
- Conmutador telefónico
- Gerente de mesa de dinero

BIA

- Una vez identificada la infraestructura crítica, se hace un análisis de sus vulnerabilidades.

- Se pueden encontrar ***vulnerabilidades*** como:

  -Servidor de aplicación no tiene respaldo.

  -No se tiene respaldo de información off-site

  -Solamente una persona conoce todos los procedimientos

  -El switch de red local no tiene respaldo ni contrato de servicio.

BIA

- Conociendo las vulnerabilidades, se puede hacer un análisis para identificar la probabilidad y el impacto (severidad) de posibles amenazas.

- Las amenazas se pueden agrupar por grupos de impacto, por localidad, por sitio estratégico o según se requiera para obtener conclusiones adecuadas.

BIA

- Asimismo, se estima el tiempo durante el cuál un proceso puede estar sin operar, antes de sufrir pérdidas considerables.
- Con base en lo anterior, se fija un Tiempo de Recuperación Objetivo, RTO por sus siglas en inglés, que también es conocido como MTD (maximum tolerable downtime).

BIA

- Otro factor que es muy importante conocer es la “frescura” o nivel de actualización que debe tener la información, una vez que se pueda operar el sistema.
- Con eso se define el Punto de Recuperación objetivo de la información, RPO, por sus siglas en inglés.

El Reto de la Recuperación

Objetivo del Tiempo de Recuperación (RTO)

" ¿Cuál es la tolerancia al downtime? "

Seg Min Hrs Días Sem

Tiempo de Recuperación

cacs

El Reto de la Recuperación

Punto de Recuperación Objetivo (RPO)

" ¿Qué tan actualizados necesitan estar los datos? "

Tiempo de Recuperación Objetivo (RTO)

" ¿Cuál es la tolerancia al downtime? "

Sem Días Hrs Min Seg

Punto de Recuperación

Seg Min Hrs Días Sem

Tiempo de Recuperación

cacs

BIA

- Podemos concluir que, el BIA es una etapa imprescindible para **alinear** el Plan de Recuperación de Desastres, DRP, con los objetivos de la organización.

5. Contenido del Plan de continuidad

Basados en la estrategia seleccionada, el Plan debe considerar al menos los siguientes factores:

1. Guía en como utilizar el Plan

2. Procedimientos de emergencia para asegurar la seguridad del personal, incluyendo procedimientos de evacuación.

3. Condiciones para declarar un desastre.

4. Identificación de los procesos de negocio y recursos de TI que deben ser recuperados.

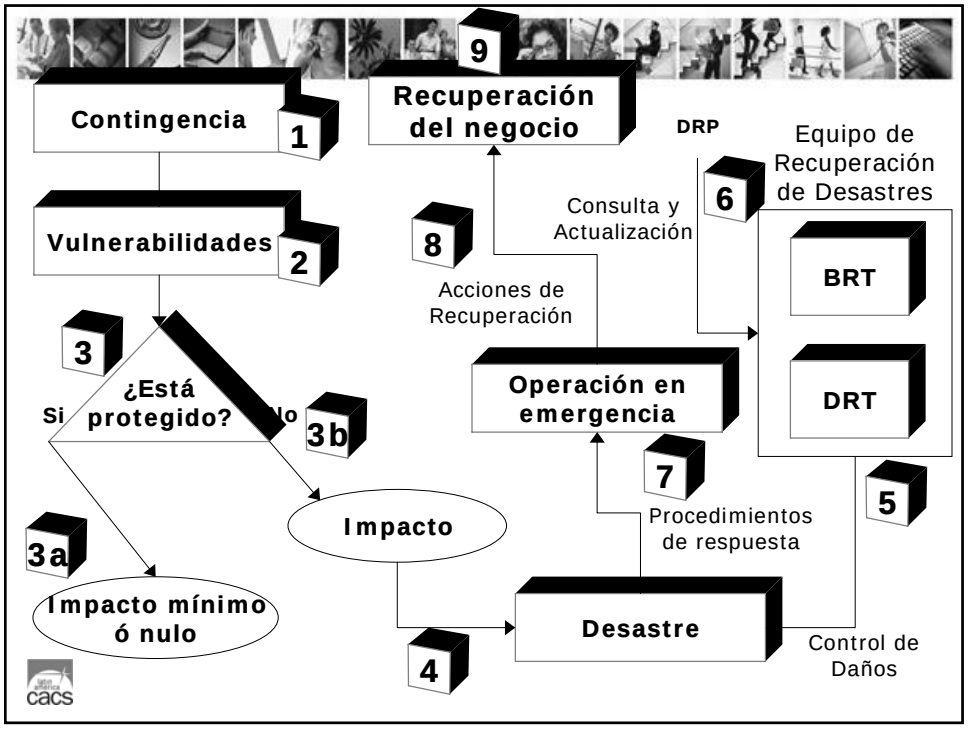
5. Información crítica de personas afectadas y de los responsables por cada función del Plan, incluyendo sus datos de contacto.

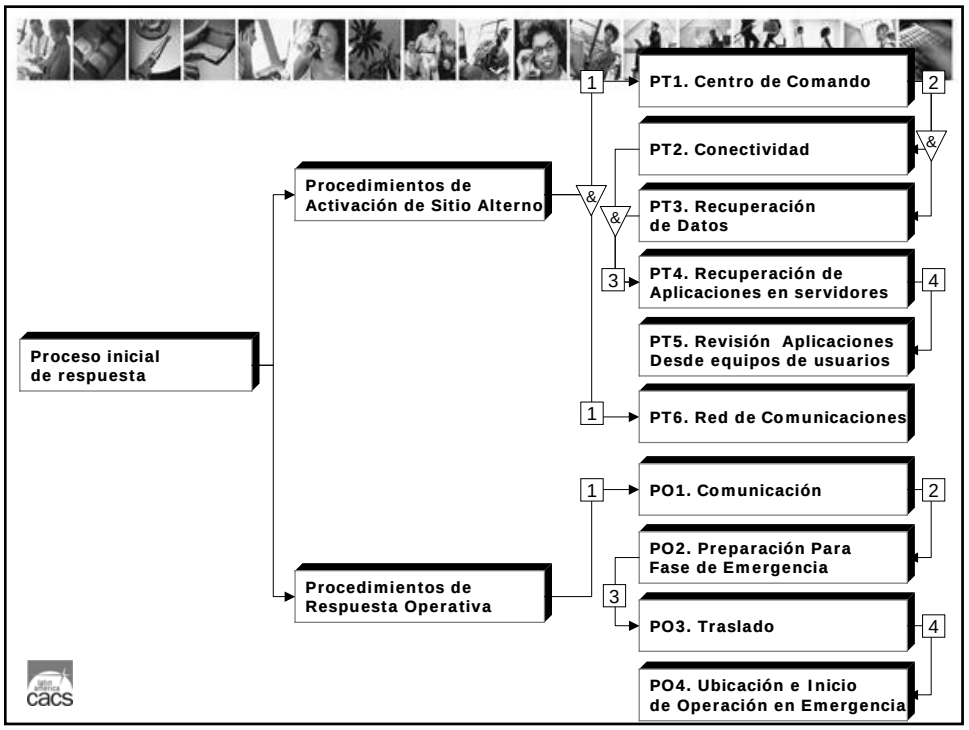
6. Clara identificación de información de contratos.

7. Explicación paso por paso de los procedimientos de respuesta que incluyen los procedimientos de operación en estado de emergencia.

8. Guía de puntos para reconstruir el sitio e infraestructura de operación normal.

9. Procedimientos de comunicación con empleados, autoridades, clientes y público en general.


9
Recuperación del negocio
Contingencia
1
DRP
Equipo de Recuperación de Desastres
6
Consulta y Actualización
Vulnerabilidades
2
8
Acciones de Recuperación
BRT
3
¿Está protegido?
Si
lo
3b
Operación en emergencia
DRT
7
5
Procedimientos de respuesta
Impacto
3a
Impacto mínimo ó nulo
Desastre
4
Control de Daños
cacs


1
PT1. Centro de Comando
2
PT2. Conectividad
&
Procedimientos de Activación de Sitio Alterno
&
&
PT3. Recuperación de Datos
3
PT4. Recuperación de Aplicaciones en servidores
4
PT5. Revisión Aplicaciones Desde equipos de usuarios
Proceso inicial de respuesta
1
PT6. Red de Comunicaciones
1
PO1. Comunicación
2
PO2. Preparación Para Fase de Emergencia
Procedimientos de Respuesta Operativa
3
PO3. Traslado
4
PO4. Ubicación e Inicio de Operación en Emergencia
cacs

- En todo caso, los procedimientos deben ser claros, no confusos, para evitar malas interpretaciones.

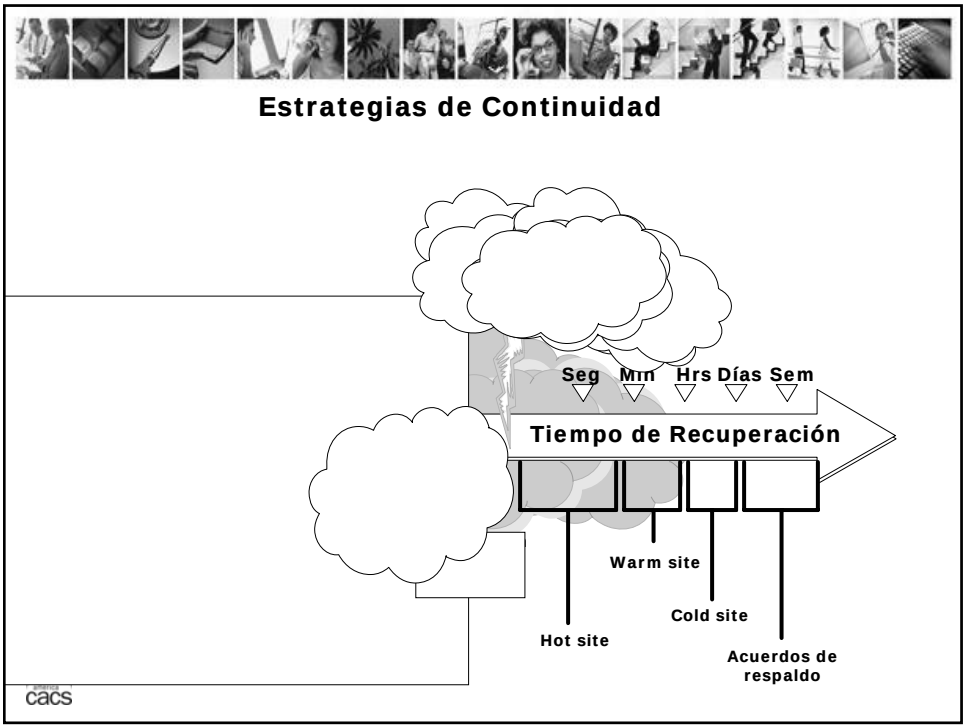
- Los procedimientos deben considerar medidas adecuadas a las situaciones de emergencia, con soluciones oportunas, que permitan continuar las operaciones, según los objetivos de la organización.

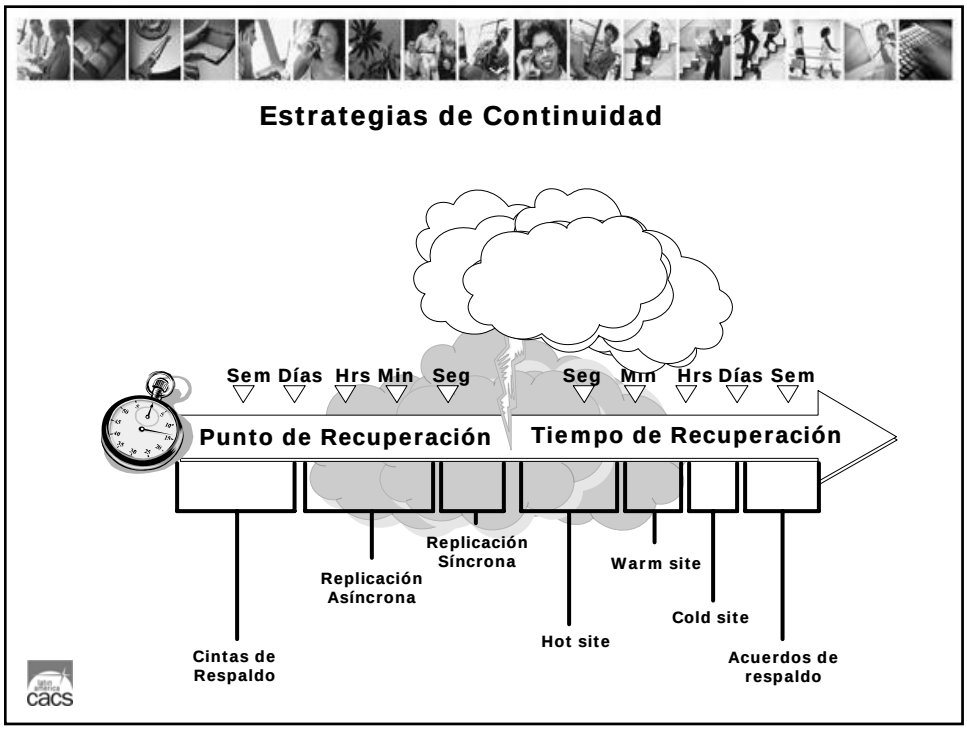
6. Estrategias de continuidad

Estrategias de Continuidad

- Es necesario identificar las diferentes estrategias de continuidad y seleccionar la más adecuada para la organización.

- La selección de la estrategia depende de:
  - La criticidad del proceso a proteger.
  - El costo de la estrategia.
  - El tiempo de recuperación objetivo.
  - El punto de recuperación objetivo.


Estrategias de Continuidad
Seg Min Hrs Días Sem
Tiempo de Recuperación
Warm site
Cold site
Hot site
Acuerdos de respaldo
cacs


Estrategias de Continuidad
Sem Días Hrs Min Seg
Seg Min Hrs Días Sem
Punto de Recuperación
Tiempo de Recuperación
Replicación Síncrona
Replicación Asíncrona
Warm site
Cold site
Hot site
Cintas de Respaldo
Acuerdos de respaldo
cacs

Estrategias de Continuidad

- A final de cuentas, la selección de la estrategia de continuidad, dependerá del nivel de riesgo que la organización este dispuesta a afrontar.
- Algo importante es que las estrategias de continuidad, se ubiquen de acuerdo al contexto y necesidades de la organización, para evitar paradojas.

7. Almacenamiento off-site, sitios alternos

Almacenamiento off-site, sitios alternos

- **Hot site**. Listo para operar en pocas horas, tiene el equipo, red y sistemas necesarios. Solo falta el staff, datos y documentación.
- **Warm site**. Puede operar en menos de un día. Está parcialmente configurado, con conexiones de red y equipo periférico seleccionado. Con capacidad de CPU menor a la de producción normal.
- **Cold site**. Tiene solo la infraestructura básica: suministro eléctrico, aire acondicionado, etc. Está listo para recibir equipo de cómputo y comunicaciones. Puede tardar varios días en operar.

Almacenamiento off-site, sitios alternos

- **Acuerdos recíprocos**. Son acuerdos de respaldo entre dos ó más organizaciones, para apoyarse cuándo sucede una emergencia.
- El almacenamiento fuera de sitio es muy importante, para mantener la continuidad de las operaciones.
- Los sitios alternos se pueden mantener “vivos” utilizándolos para este almacenamiento.

8. Pruebas y actualización del Plan de continuidad

Pruebas y actualización del Plan

- El Plan de Recuperación de Continuidad debe ser probado, con el fin de determinar si funciona adecuadamente ó si hay partes del Plan que deben ser actualizadas.
- Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones a la operación normal sean mínimas, como los fines de semana.

- Las pruebas deben comprender lo elementos críticos y simular condiciones de proceso lo más parecidas a las normales de operación, aunque se realicen fuera de horas.

Pruebas y actualización del Plan

Las pruebas deben incluir las siguientes tareas:

1. Verificar la totalidad y precisión del Plan
2. Evaluar el desempeño del personal involucrado.
3. Evaluar la coordinación entre los miembros del B/DRT y proveedores y otros terceros
4. Medir la capacidad del sitio de respaldo, para ejecutar el proceso requerido.

Pruebas y actualización del Plan

5. Identificar la capacidad de recuperar registros e información vital.
6. Evaluar el estado y cantidad del equipo y suministros que han sido movidos al sitio de recuperación.
7. Medir el desempeño de los sistemas operativos y computacionales.

- Tipos de Pruebas :
- **Check list test**. Las diferentes áreas revisan el Plan y hacen sus comentarios para asegurarse de que nada falte.
- **Structured Walk-Trough test**. Representantes de las diferentes áreas se reúnen y “caminan” a través del Plan, evaluando diversos escenarios desde el principio al fin .
- **Simulation test**. Este toma más gente y planeación. Se revisa un escenario específico y se ejecutan los pasos que se indican en el plan, simulando incluso la relocalización hacia un sitio alterno.

- Tipos de Pruebas :
- **Parallel test**. Se hace para asegurarse de que los sistemas trabajen de acuerdo a lo esperado en el sitio alterno. Se procesa en el sitio alterno y se comparan los resultados con los que se obtienen en el sitio de producción.
- **Full interruption test**. Esta es una prueba real dónde el sitio de producción es detenido y se debe trabajar en las instalaciones y facildiades alternas.

Fases de proceso de Full-Interruption Test

Fase 1:
PRETEST

- Acciones para preparar las condiciones de prueba.
- Aviso a usuarios
- Check list de condiciones, contactos, equipo etc.
- Definición de medidas de retorno por si algo falla en la prueba y afecta fuertemente la operación.

Fase 2:
TEST

- Prueba real.
- Movimiento de personal.
- Traslado de equipo y datos.
- Simulación de condiciones de desastre
- Ejecución de procedimientos del Plan

Fase 3:
POST-TEST

- Regresar todo a su lugar.
- Desconectar equipos.
- Regresar personal.
- Documentar y evaluar resultados.

9. Entrenamiento y distribución del Plan de Continuidad

cacs

- **Entrenamiento:** La administración de la continuidad debe asegurar que todas las personas involucradas reciban entrenamiento sobre los procedimientos a seguir en caso de desastres.
- Además de entrenamiento teórico, se debe hacer que el personal participe en las pruebas y simulacros del Plan.
- **Distribución:** El Plan de continuidad contiene mucha información sensitiva, por lo que debe ser distribuido solo a las personas autorizadas.
- El Plan se dividirá en secciones, las cuáles se entregarán sobre la base de “necesita saber” solamente.
- **Mejora continua:** Con base en las pruebas y experiencias reales, el plan deberá ser mejorado continuamente, aprendiendo de los errores cometidos.

¡Gracias!

José Ángel Peña Ibarra

japi@ccisa.com.mx