



Sesión #313

**Planes de Contingencia,
Recuperación de Desastres.**

José Ángel Peña Ibarra

Contenido:

- **Antecedentes**
- **Marco Metodológico ISO 17799**
- **Análisis de Impacto al Negocio**
- **Estrategias de Recuperación**
- **Plan de Recuperación de Desastres**
- **Pruebas y Actualización del Plan**
- **Conclusiones**

Contenido:

- **Antecedentes**
- **Marco Metodológico ISO 17799**
- **Análisis de Impacto al Negocio**
- **Estrategias de Recuperación**
- **Plan de Recuperación de Desastres**
- **Pruebas y Actualización del Plan**
- **Conclusiones**

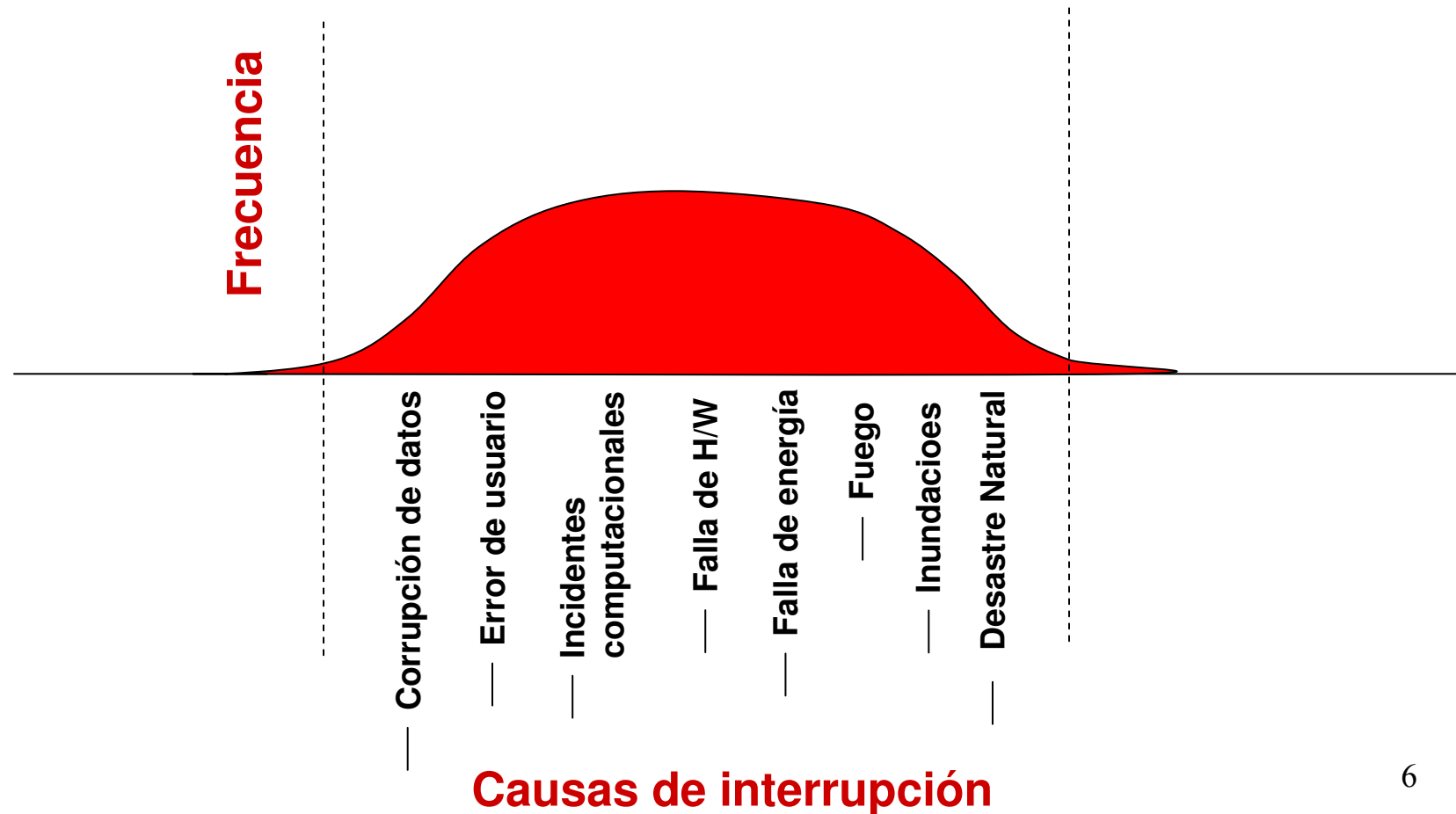
- Considerando que la mayoría de los procesos de una empresa, dependen de los sistemas de información para operar, cualquier falla de estos **puede interrumpir la operación** de una parte de una organización o en caso extremo de toda ella.
- Por lo tanto, se deben definir medidas preventivas para reducir los riesgos de interrupción y desarrollar los procedimientos de recuperación necesarios, en caso de que un desastre ocurra. Es decir, se debe lograr una adecuada **Administración de la Continuidad del Negocio.**

Antecedentes

- A pesar de los efectos negativos en las organizaciones, muchas empresas aún no toman medidas para contar con planes que les permitan lograr **la Continuidad del Negocio**.

- **72% de todos los negocios tienen alguna de estas condiciones:**
 - No tienen Plan de Continuidad del Negocio.
 - Si lo tienen, nunca lo han probado.
 - Su Plan falló cuándo lo probaron.
- **Solamente 18% de los datos de usuario final están protegidos. ***

Entre las causas más frecuentes de caídas de sistemas se tienen:



- De hecho, las causas pueden variar de una empresa a otra o de una región a otra dentro de una misma empresa.
- Puede haber instalaciones en zonas sísmicas o en zonas de conflictivas o marginadas, etc.
- Lo importante entonces es tomar una **actitud pro-activa** e identificar los factores más importantes para apoyar la continuidad del negocio.

Antecedentes

Dentro de los factores clave para tener una buena administración de la continuidad se tienen:

- Desarrollar una rigurosa **planeación** de la continuidad de las operaciones.
- Identificar los **procesos y activos críticos** para la operación del negocio.
- **Reducir el riesgo** de interrupciones a los procesos de negocio críticos.
- **Asegurar la continuidad** del nivel de servicio mínimo necesario para las operaciones críticas.
- Obtener el **compromiso de la alta dirección**.



Antecedentes



El proceso de planeación de la continuidad debe incluir al menos lo siguiente:

- **Análisis de impacto al negocio.**
- **Estrategias de recuperación de las operaciones.**
- **Desarrollo de un Plan detallado.**
- **Implementación del Plan**
- **Pruebas y actualización del Plan**

Contenido:

- **Antecedentes**
- **Marco Metodológico ISO 17799**
- **Análisis de Impacto al Negocio**
- **Estrategias de Recuperación**
- **Plan de Recuperación de Desastres**
- **Pruebas y Actualización del Plan**
- **Conclusiones**

- El conjunto de recomendaciones **ISO 17799**, que fue desarrollado por la ISO, con el propósito de contar con un conjunto de mejores prácticas en el campo de seguridad de la información.
- El **ISO 17799** incluye 10 dominios, uno de los cuáles es el llamado **Administración de la continuidad de las operaciones**.

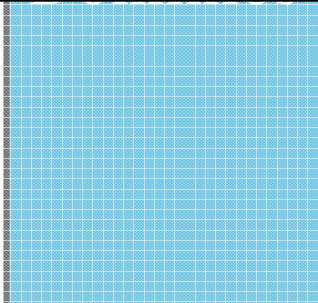
- Dentro de este dominio de continuidad de las operaciones, se encuentran dos herramientas fundamentales que son el **Análisis de impacto al negocio, BIA**, y el **Plan de recuperación de desastres, DRP**.

Marco Metodológico ISO 17799

Dominios 	Políticas de Seguridad
	Seguridad en la organización
	Control y clasificación de activos
	Seguridad en el personal de la organización
	Seguridad física y ambiental
	Administración de operaciones y comunicaciones
	Control de accesos
	Desarrollo y mantenimiento de sistemas
	Administración de la continuidad de las operaciones del negocio
	Acatamiento de leyes y normas

Modelo ISO 17799

Marco Metodológico ISO 17799

Aspectos de la administración de la continuidad de la operación del negocio	Análisis de impacto y continuidad de la operación del negocio (BIA)
	Elaboración de planes de recuperación en caso de desastres, para mantener la continuidad de las operaciones (DRP)
	Implementación de planes de continuidad (DRP)
	Marco de planeación de continuidad de la operación del negocio
	Pruebas, mantenimiento y reevaluación de planes de continuidad de la operación del negocio
	Desarrollo y mantenimiento de sistemas
	Administración de la continuidad de las operaciones del negocio
	Acatamiento de leyes y normas

Modelo ISO 17799

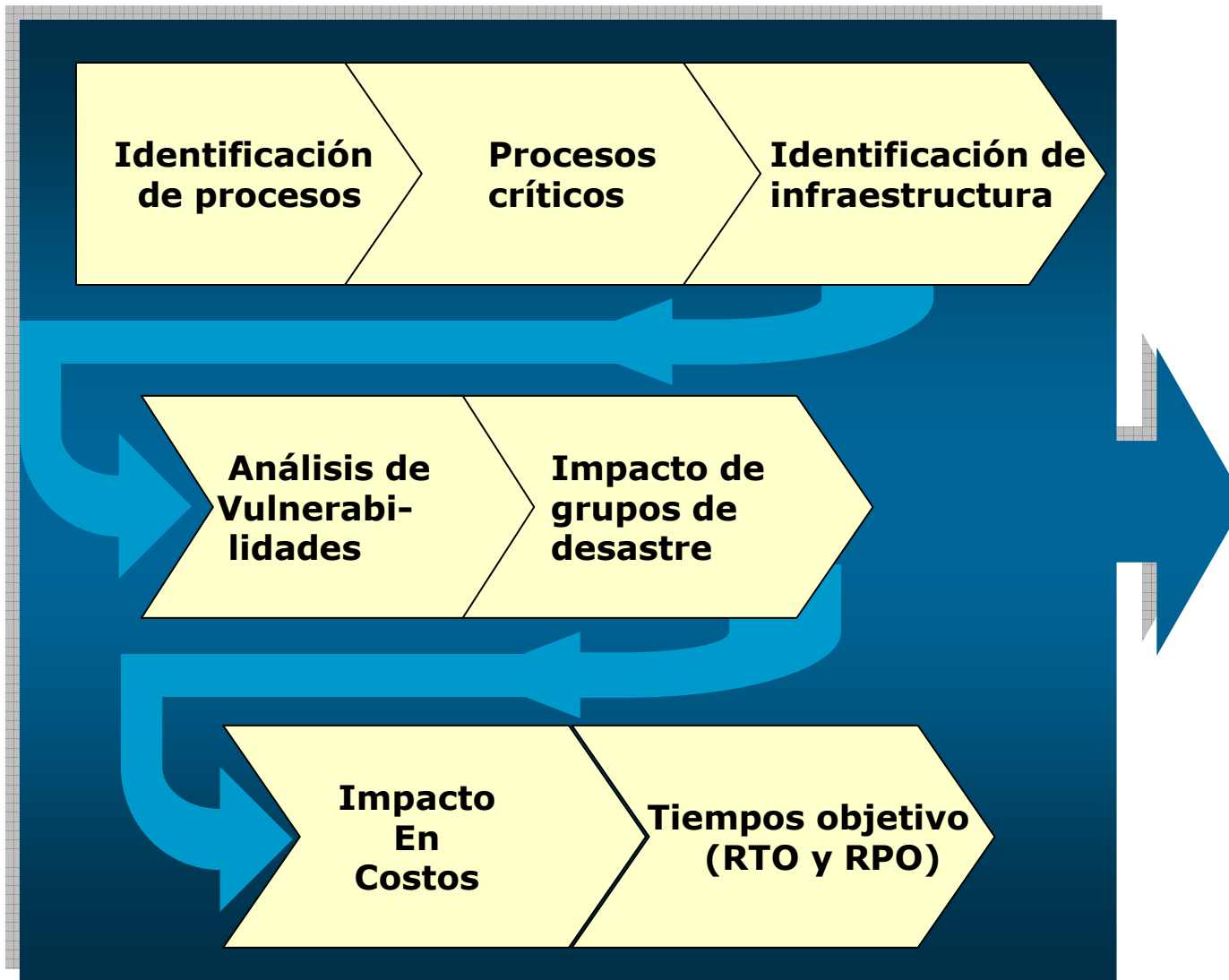
Contenido:

- **Antecedentes**
- **Marco Metodológico ISO 17799**
- **Análisis de Impacto al Negocio**
- **Estrategias de Recuperación**
- **Plan de Recuperación de Desastres**
- **Pruebas y Actualización del Plan**
- **Conclusiones**

- El Análisis de Impacto al Negocio, BIA, nos permite **conocer** el estado actual de respuesta en caso de desastres, nos ayuda a identificar el impacto económico de cada desastre, y también permite a la organización identificar impactos intangibles, que pueden ser muy relevantes.
- 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.

Fases BIA

DRP



- 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..*

Clasificación de procesos

Críticos

- Sus funciones no pueden ser ejecutadas a menos que sean remplazadas por recursos idénticos.
- No se pueden utilizar métodos manuales.
- Costo de interrupción es muy alto.

Vitales

- Sus funciones pueden ser ejecutadas manualmente durante un periodo corto.
- Mayor tolerancia a las interrupciones .
- Costos de interrupción menores si caída es menor a 3 d.

Sensitivos

- Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo.
- Mientras se hace manualmente requiere staff adicional.
- Costos de interrupción medios.

NoCríticos

- Sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún costo.

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

Proceso Mesa de dinero

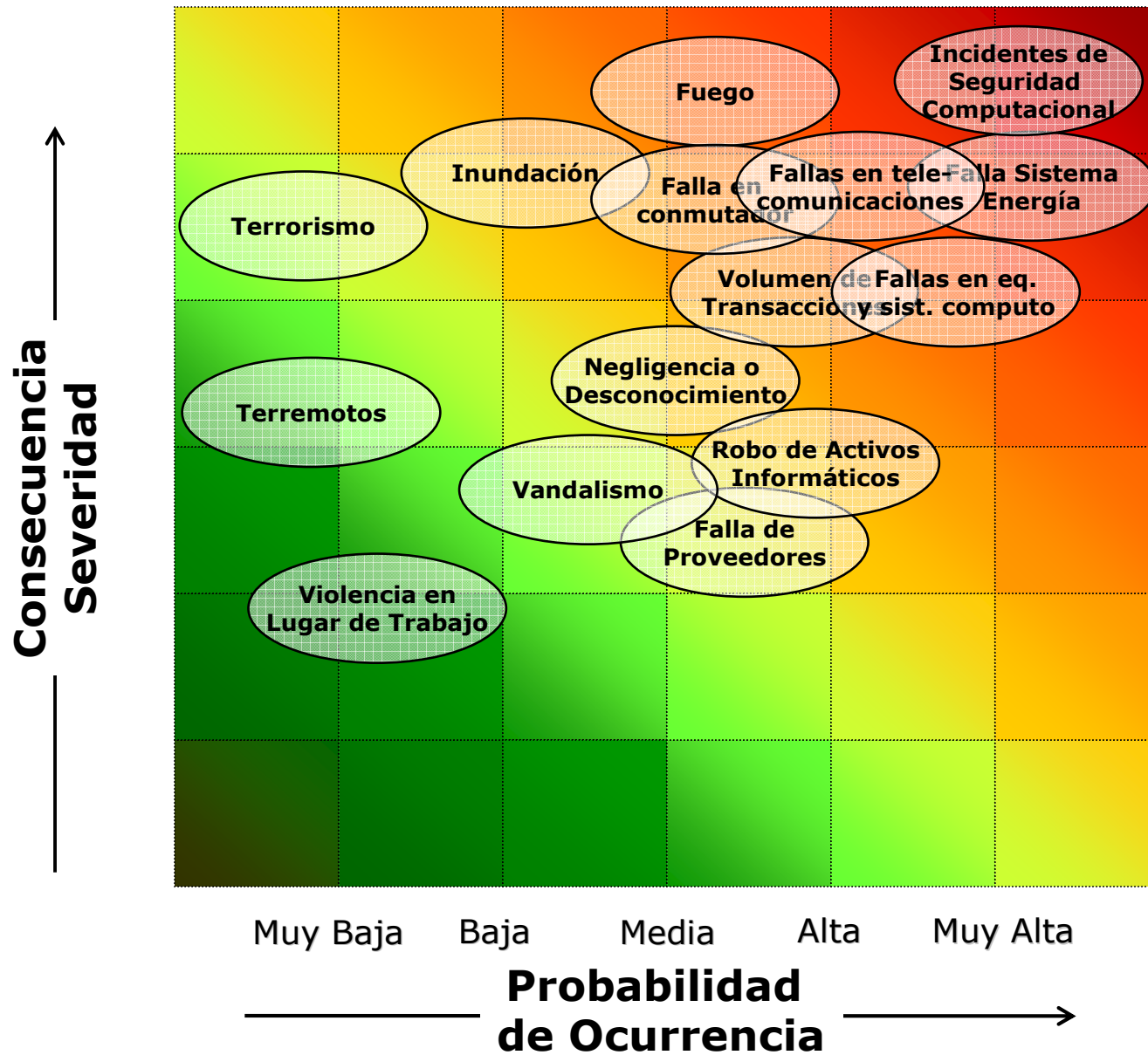
Infraestructura:

- 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

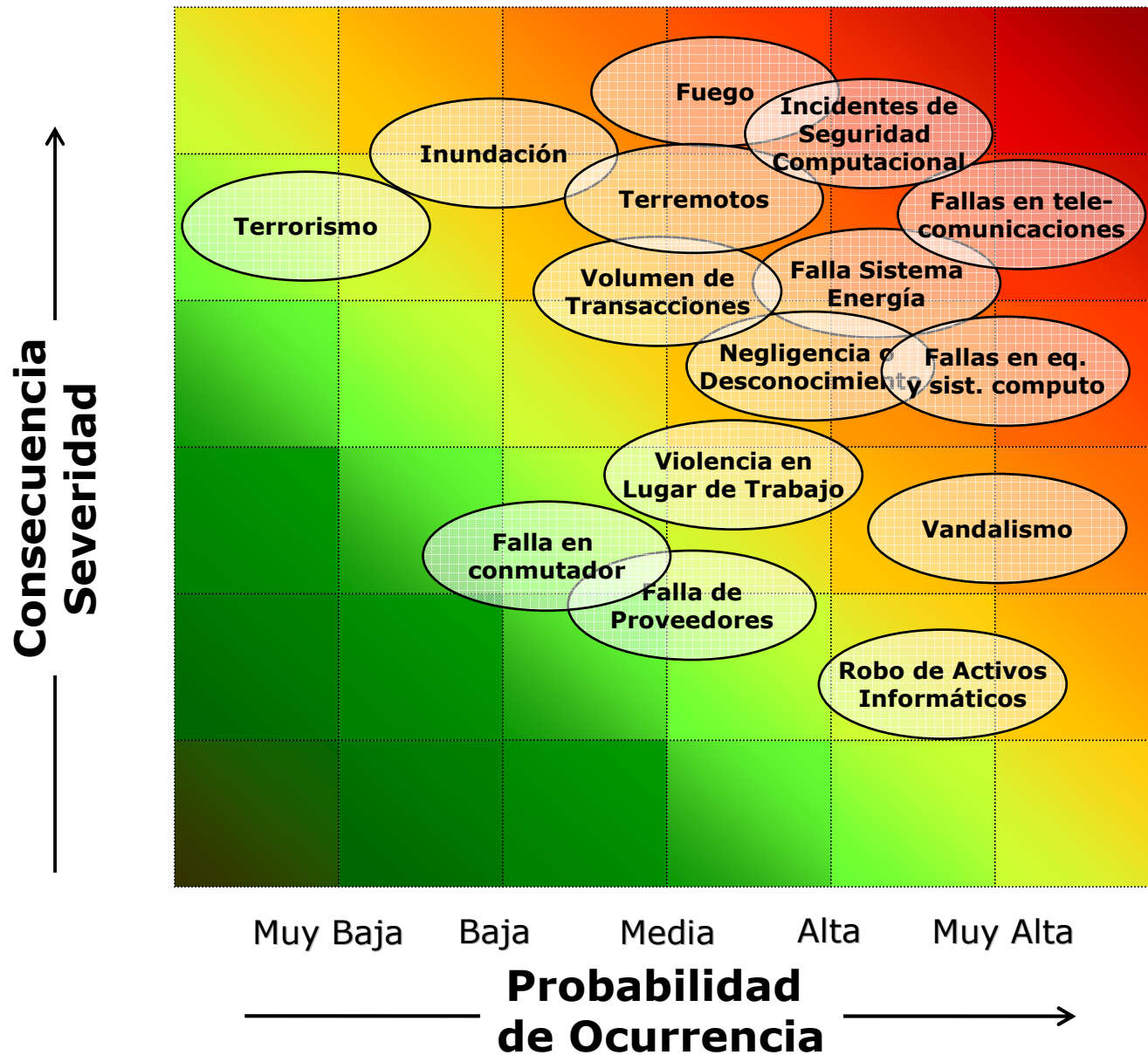
- Una vez identificada la infraestructura crítica, se hace un análisis de sus vulnerabilidades.
- Se pueden encontrar **vulnerabilidades** como:
 - *Servidor de aplicación no tiene respaldo.*
 - *No se tiene respaldo de información off-site*
 - *Solamente una persona conoce todos los procedimientos*
 - *El switch de red local no tiene respaldo ni contrato de servicio.*

- 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.

Probabilidad y Consecuencia de Amenazas Corporativo Valle



Probabilidad y Consecuencia de Desastres Sucursales Cd. de México



Durante el BIA se deben identificar los impactos financieros, es decir los **costos asociados a la continuidad de las operaciones**. Se tienen dos tipos de costos:

1. Costos derivados de la suspensión de las operaciones:

- Caída de ventas
- Falta o retraso de cobranza
- Recursos ociosos
- Imagen....

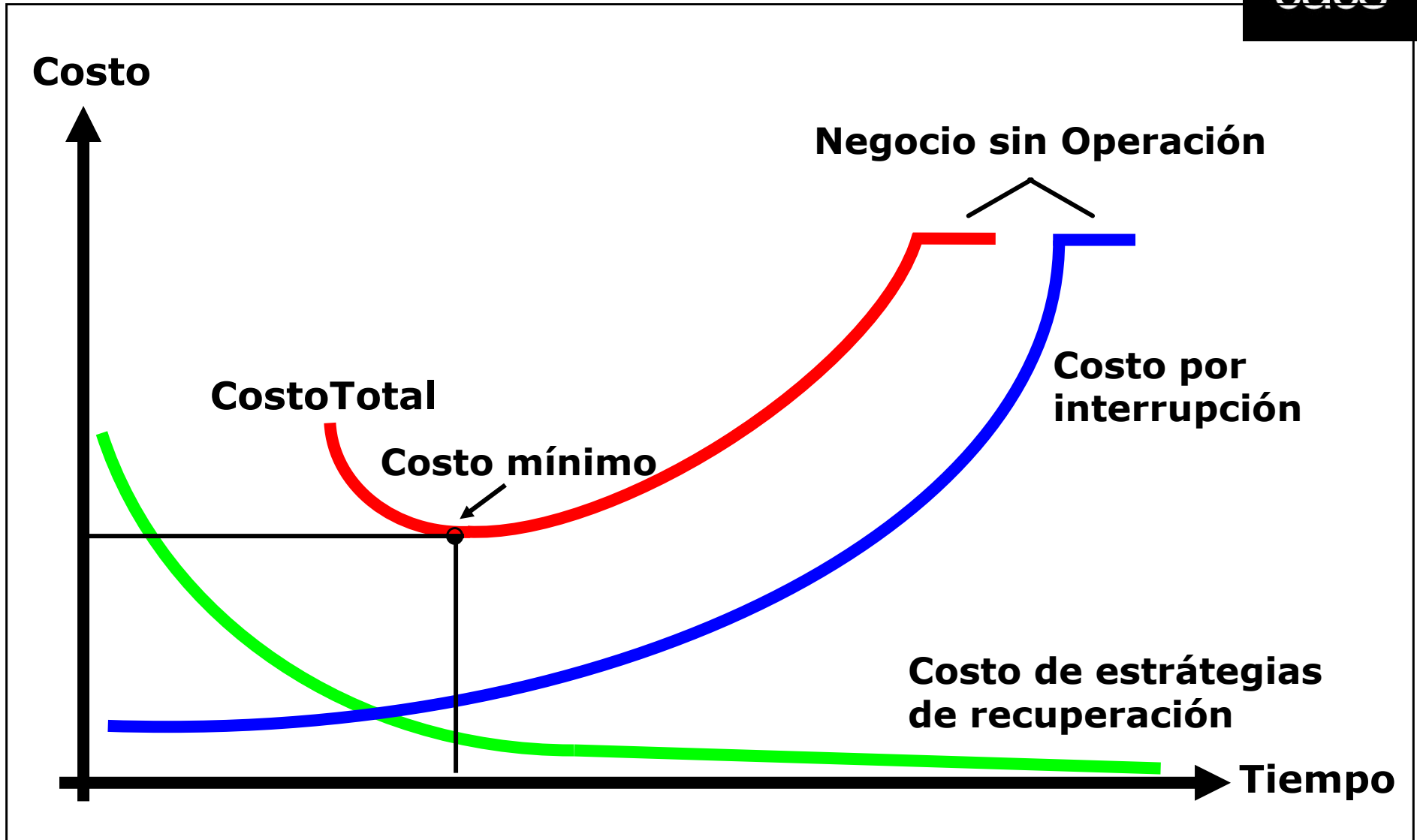
Estos costos aumentan con el “down time”

2. Costos de estrategias de corrección y prevención:

- Costo de los sitios alternos
- Costo de equipos de respaldo
- Seguros

Si estamos dispuestos a aceptar un mayor “down time” entonces estos costos disminuyen.

En la siguiente página se muestra una gráfica dónde se observa que, conociendo los dos tipos de costo mencionados, se puede saber el punto de costo mínimo.



- La gráfica de costos se puede hacer para cada proceso crítico. La suma de todos los procesos dará la información de costos total.
- 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.

- 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? ”



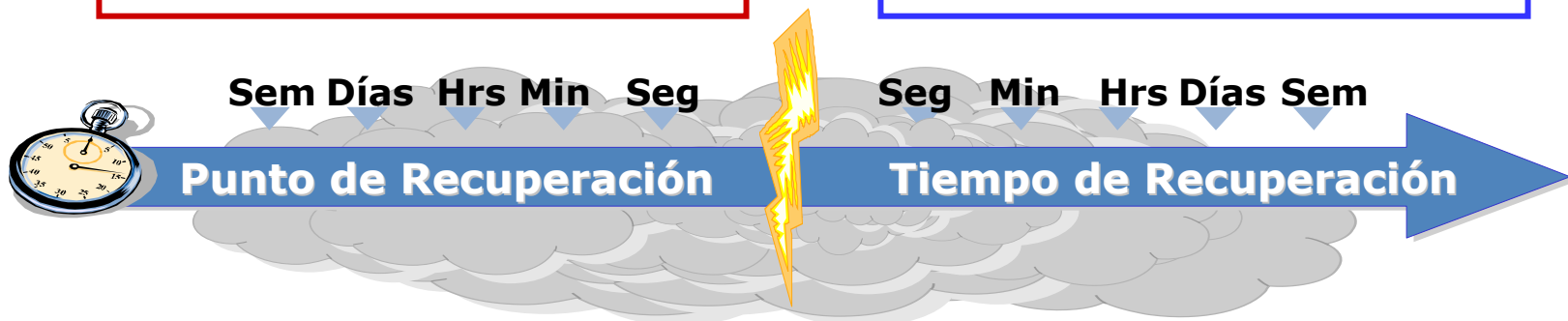
El Reto de la Recuperación

Objetivo del Punto de Recuperación (RPO)

“ ¿Qué tan actualizados necesitan estar los datos? ”

Objetivo del Tiempo de Recuperación (RTO)

“ ¿Cuál es la tolerancia al downtime? ”





BIA



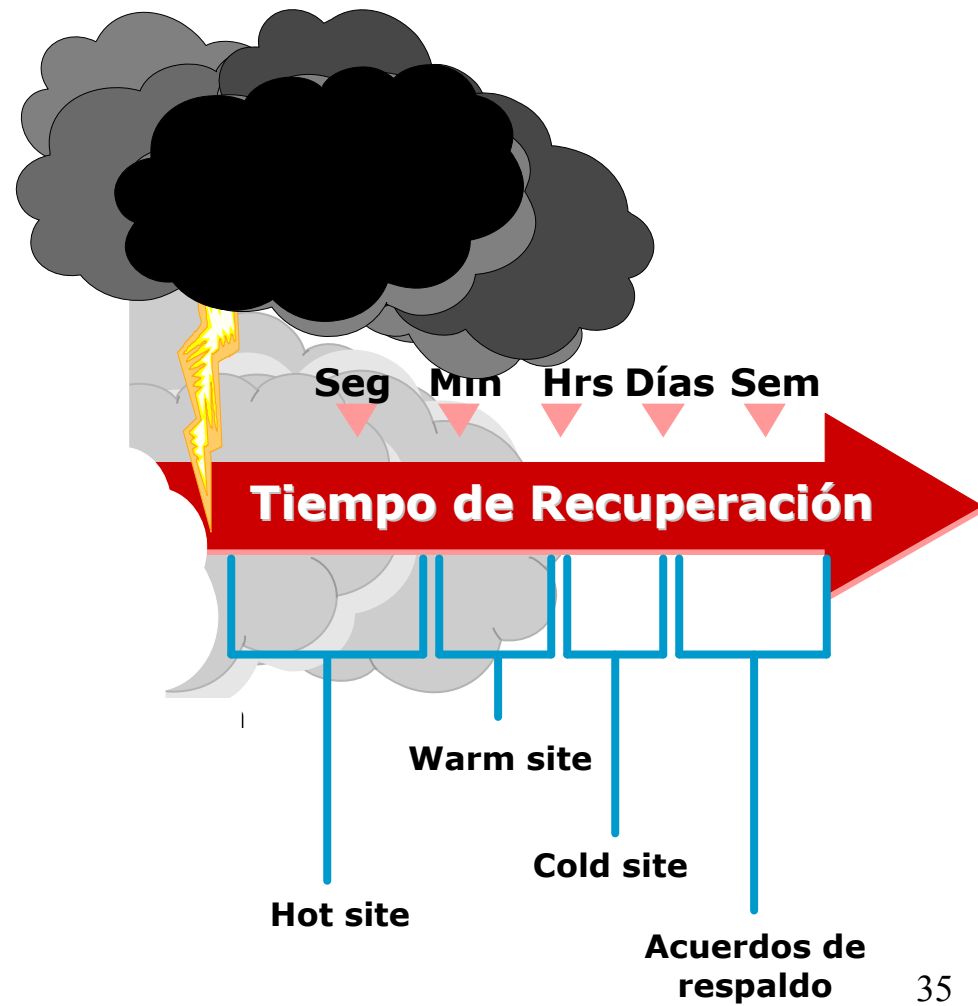
- Podemos concluir que, el BIA es una etapa imprescindible para **alinear** el Plan de Recuperación de Desastres, DRP, con los objetivos de la organización.

Contenido:

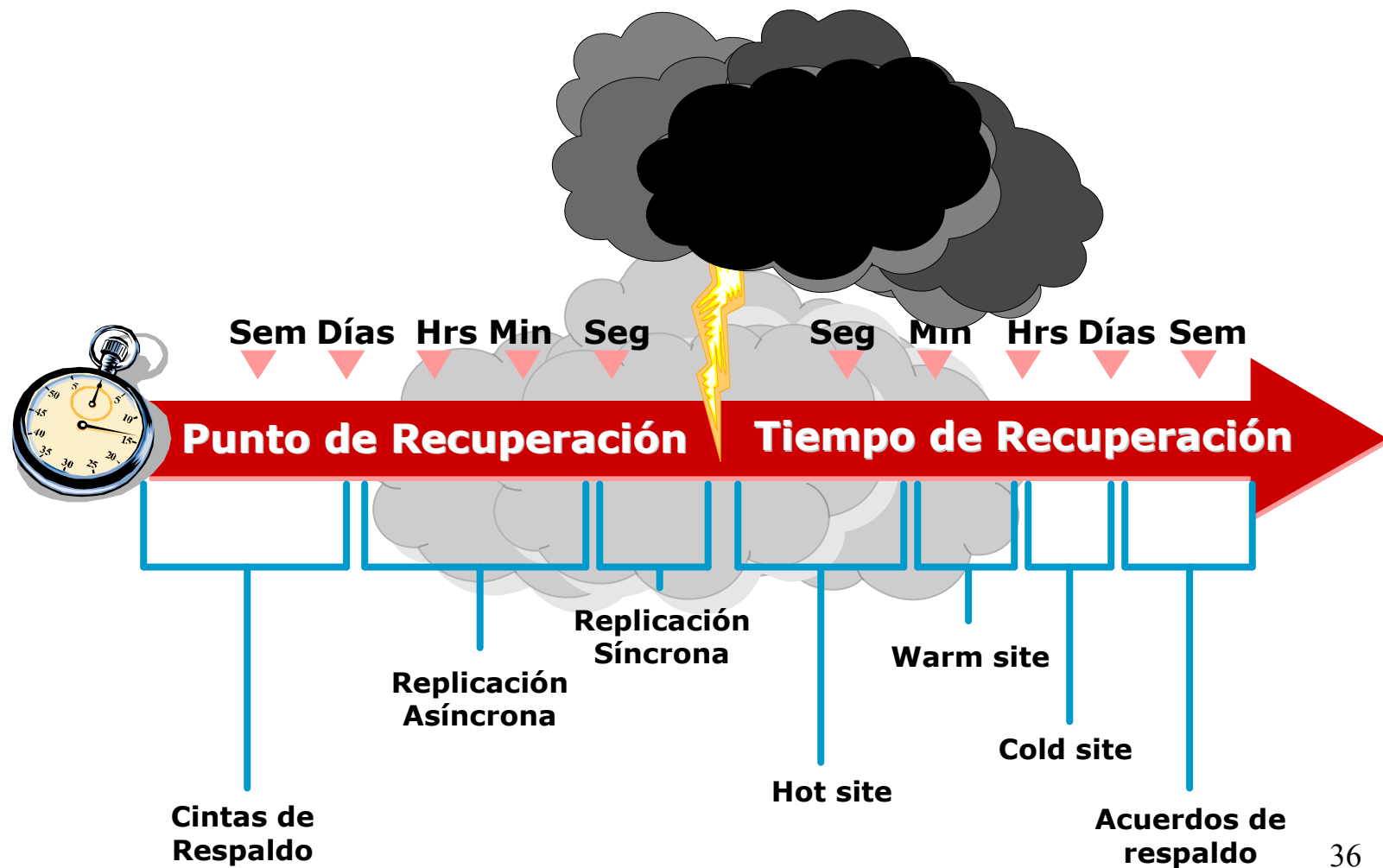
- **Antecedentes**
- **Marco Metodológico ISO 17799**
- **Análisis de Impacto al Negocio**
- **Estrategias de Recuperación**
- **Plan de Recuperación de Desastres**
- **Pruebas y Actualización del Plan**
- **Conclusiones**

- El siguiente paso en el desarrollo de un Plan de Continuidad es identificar las diferentes estrategias de recuperación 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 Recuperación



Estrategias de Recuperación



- **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.



Estrategias de Recuperación



- **Acuerdos recíprocos.** Son acuerdos de respaldo entre dos ó más organizaciones, para apoyarse cuándo sucede una emergencia.

Estrategias de Recuperación en redes de telecomunicación

- **Redundancia.** Se tiene capacidad extra, como trayectorias múltiples entre los ruteadores. En las LAN se tiene un cable adicional. Se tienen configuraciones de respaldo.
- **Ruteo alternativo.** Se tienen medios alternos para enviar la información, como cable o fibra óptica. Los medios alternativos pueden ser VPN's o dial up como alternativa a circuitos dedicados.



Estrategias de Recuperación en redes de telecomunicación



- **Ruteo diverso.** Se envía el tráfico a través de facilidades divididas o duplicadas. Pueden ser cables dobles viajando en el mismo tubo conduit.
- **Protección de última milla.** Se tiene redundancia solo para el segmento que une el domicilio del usuario con el carrier.

Contenido:

- Antecedentes
- Marco Metodológico ISO 17799
- Análisis de Impacto al Negocio
- Estrategias de Recuperación
- **Plan de Recuperación de Desastres**
- Pruebas y Actualización del Plan
- Conclusiones



Plan de recuperación de desastres



- El Plan de Recuperación de desastres, DRP, nos permitirá contar con las definiciones y los **procedimientos** necesarios, para recuperar la operación en caso de algún problema, enfocándose en lo más relevante.
- En el desarrollo del DRP se analizarán las estrategias y escenarios de recuperación.
- Se definirán las **responsabilidades**, tanto de los administradores de la infraestructura, como de los dueños de los procesos de negocio, debiendo definirse un **Disaster Recovery Team** y un **Business Recovery Team**.

BIA

Fases DRP



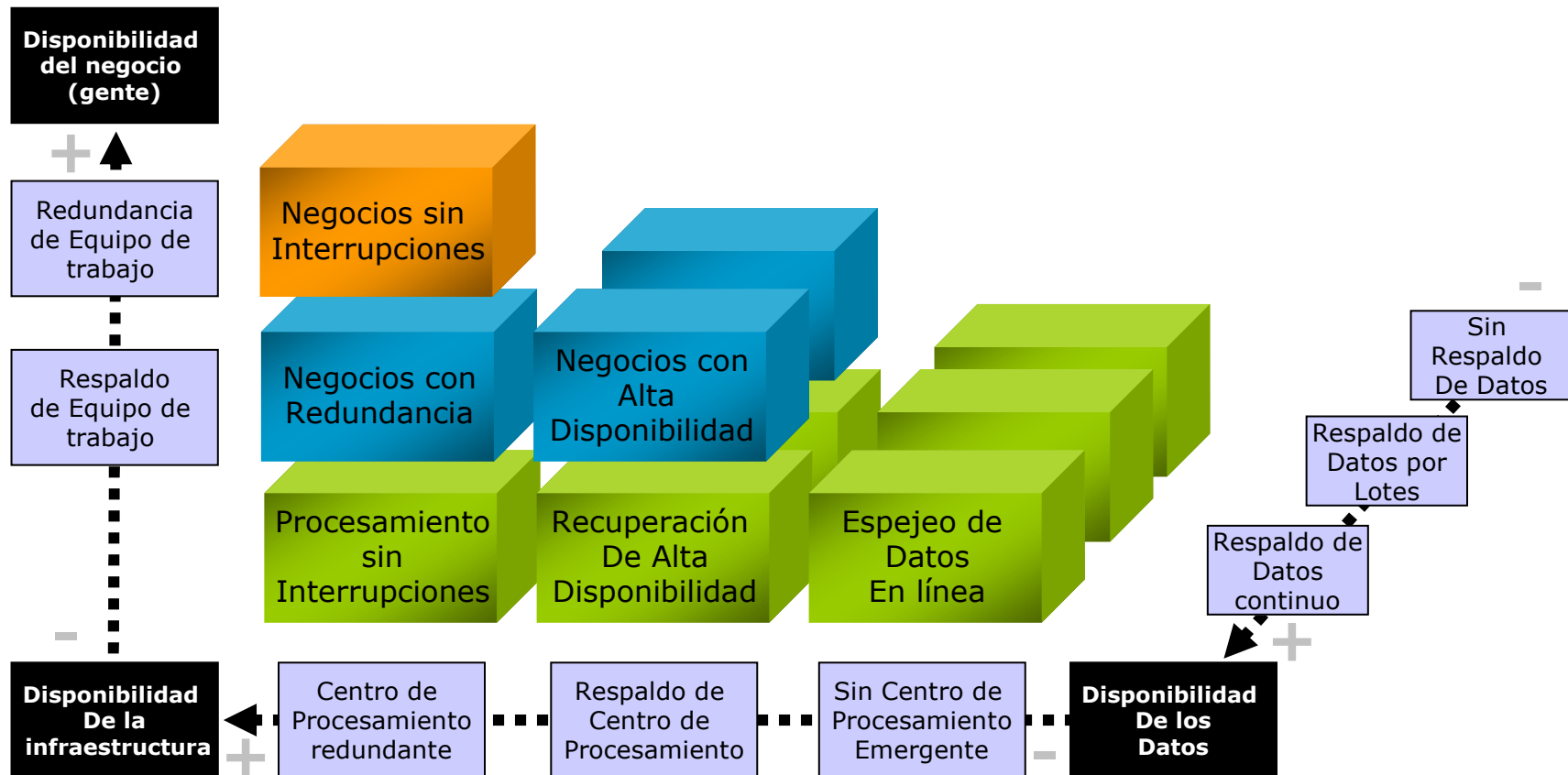


Plan de recuperación de desastres



- El análisis de las estrategias de recuperación se hace considerando los objetivos globales de la organización, respecto a las tres dimensiones fundamentales para la disponibilidad:
 - **Datos,**
 - **Infraestructura tecnológica y**
 - **Gente.**

Tres Dimensiones de Disponibilidad





Plan de recuperación de desastres



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

- 1.** Acciones preventivas.
- 2.** Procedimientos de evacuación.
- 3.** Condiciones para declarar un desastre.
- 4.** Identificación de los procesos de negocio y recursos de TI que deben ser recuperados.



Plan de recuperación de desastres

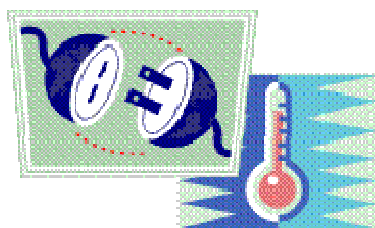


- 5.** Clara identificación de personas responsables por cada función del Plan, incluyendo sus datos de contacto.
- 6.** Clara identificación de información de contratos.
- 7.** Explicación paso por paso de los procedimientos de recuperación.
- 8.** Clara identificación de los recursos requeridos.

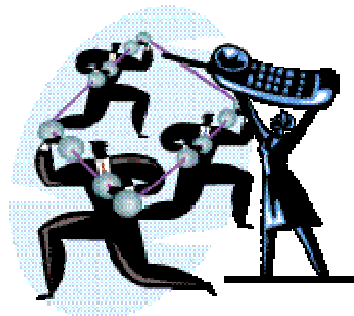




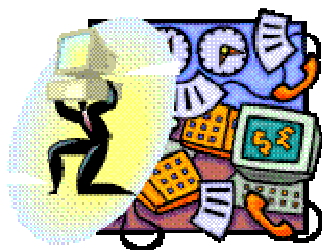
1. Sitio de operaciones disponible



2. Instalaciones eléctricas y climatización



3. LAN y Telefonía



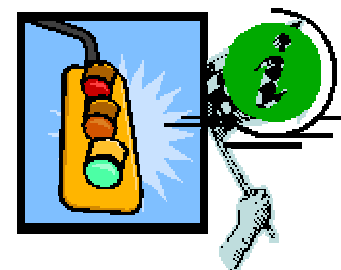
4. Equipo de cómputo crítico



5. Software operativo y crítico



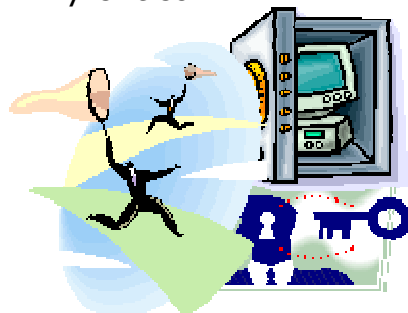
6. Datos



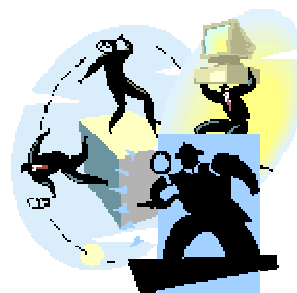
10. Regreso a operación normal y cierre DRP



7. Telecomunicaciones



8. Infraestructura de seguridad



9. Pruebas de operación

Contenido:

- Antecedentes
- Marco Metodológico ISO 17799
- Análisis de Impacto al Negocio
- Estrategias de Recuperación
- Plan de Recuperación de Desastres
- Pruebas y Actualización del Plan
- Conclusiones



Pruebas y actualización del Plan



- El Plan de Recuperación de Desastres 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:

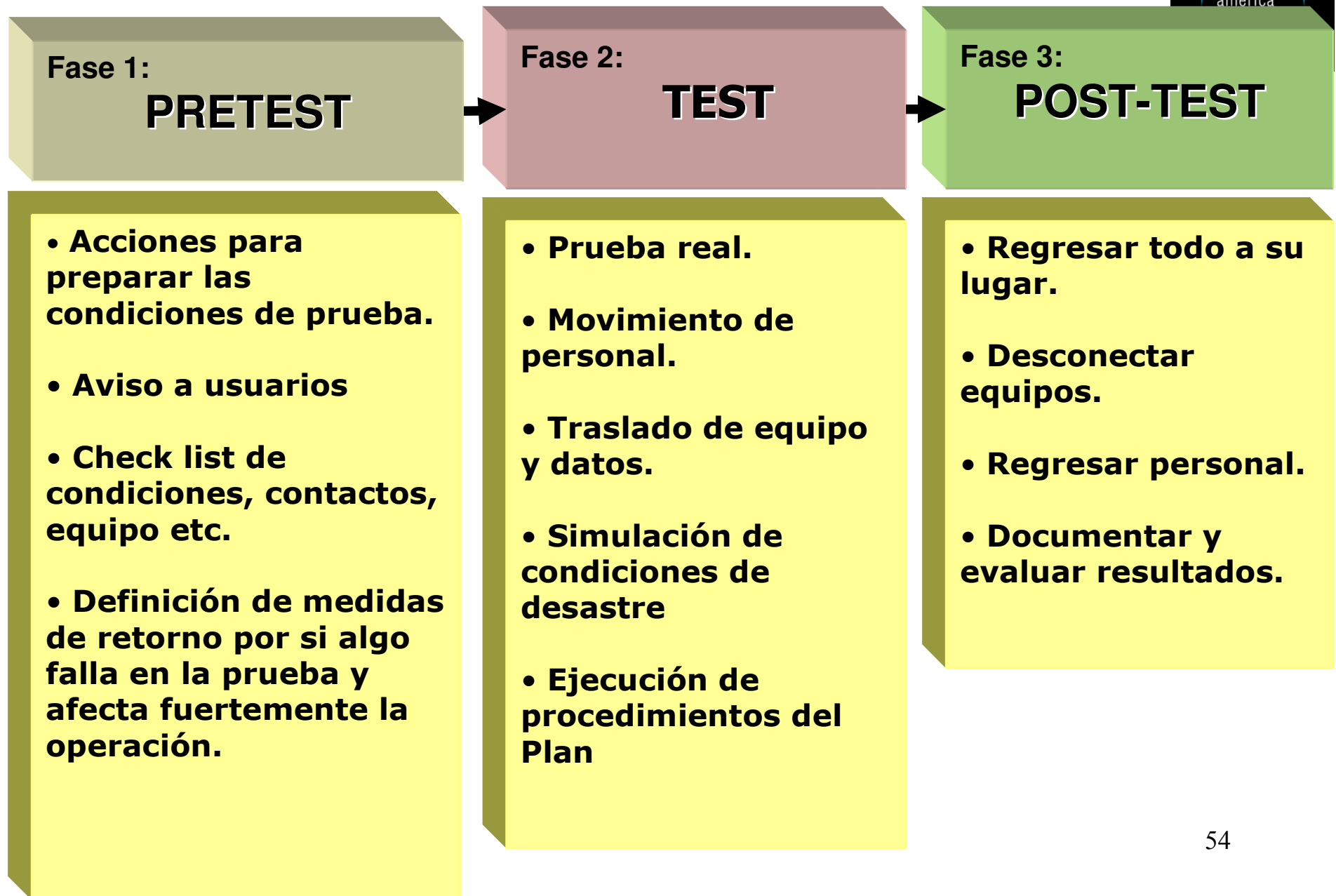
1. Verificar la totalidad y precisión del Plan
- 2.** Evaluar el desempeño del personal involucrado.
- 3.** Evaluar la coordinación entre los miembros del B/DRT y proveedores y otros terceros
- 4.** Medir la capacidad del sitio de respaldo, para ejecutar el proceso requerido.



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 :
- **Prueba de papel.** Es una revisión en papel del posible comportamiento del Plan en determinadas circunstancias. Puede incluir todo el Plan o partes de él.
- **Prueba preparatoria.** Se prueban solo partes del plan, ya con equipos y sistemas reales, para obtener una evidencia gradual de cómo funcionará el Plan.
- **Prueba operacional completa.** Es lo más cercano a una interrupción real. Se recomienda que antes se hayan efectuado pruebas de papel y pruebas preparatorias parciales.

Contenido:

- Antecedentes
- Marco Metodológico ISO 17799
- Análisis de Impacto al Negocio
- Estrategias de Recuperación
- Plan de Recuperación de Desastres
- Pruebas y Actualización del Plan
- Conclusiones

Conclusiones

- La **Planeación de Continuidad** incluye dos fases muy importantes: El Análisis de Impacto al Negocio y el Plan de Recuperación de Desastres.
- Se debe enfocar el Plan a **mantener la continuidad de los procesos críticos** de la organización.
- El Plan se debe **probar periódicamente**, para ver si los procedimientos corresponden a la realidad y si dan los resultados esperados.
- Si el Plan no se **actualiza**, no servirá para nada.



Gracias

José Ángel Peña Ibarra

japi@ccisa.com.mx

www.ccisa.com.mx

