

Planes de Contingencia y Respaldo

Ernesto Rivera Pitti

Director Nacional de Administración

Comisión Nacional de Valores

República de Panamá



VI Jornadas Iberoamericanas sobre Tecnología y
Mercado de Capitales

Quito, 1 al 3 de marzo de 2004





Agenda

- Generalidades de los Planes de Contingencia
- Desarrollando un Plan de Contingencia
- Prepararse para “Pequeñas Emergencias”
- Recomendaciones finales



Planes de Contingencia

- Una serie de actividades tendientes a restablecer la operación normal, en el evento de una calamidad (interna o externa).
- Recuperabilidad vs. Irrecuperabilidad
COSTO de los Planes y Programas de contingencia vs. la probabilidad de asumir el COSTO del DESASTRE



Planes de Contingencia

- En el pasado...
 - Los procesos de misión crítica no estaban soportados por sistemas informáticos
 - Había menos complejidad en los equipos (Mainframes, terminales)
 - Había sistemas operativos más estables y menos expuestos a contaminación o intromisión
 - Había más tiempo para reaccionar
 - Solo se involucraba a personal de sistemas



Planes de Contingencia

- En la actualidad
 - Procesos de misión crítica están soportados por DIFERENTES sistemas informáticos
 - Mayor complejidad en la **interacción** de diferentes equipos (redes internas, externas, servidores, PC's, firewalls, etc.)
 - Se exige respuesta INMEDIATA
 - Es requerida la participación de TODOS los involucrados dentro (y a veces fuera) de la organización



Planes de Contingencia

- Todo esto da a lugar a:
 - Establecer planes de contingencia que tomen en cuenta la interacción con todas las áreas de la organización
 - Revisar y actualizar constantemente estos planes
 - Practicar y poner a prueba los planes de contingencia



Planes de Contingencia

- Complejidad del sistema
- Necesidad real de “uptime”
- Presupuesto
- Personal de Tecnología

Planes de Contingencia

Principales Causas de Problemas en las Empresas

Catástrofes

18%

Fuego, Inundaciones,
Tormentas, Sabotaje,
Terrorismo

82 días en promedio

82%

Fallos de sistema y
Software

7 días en promedio

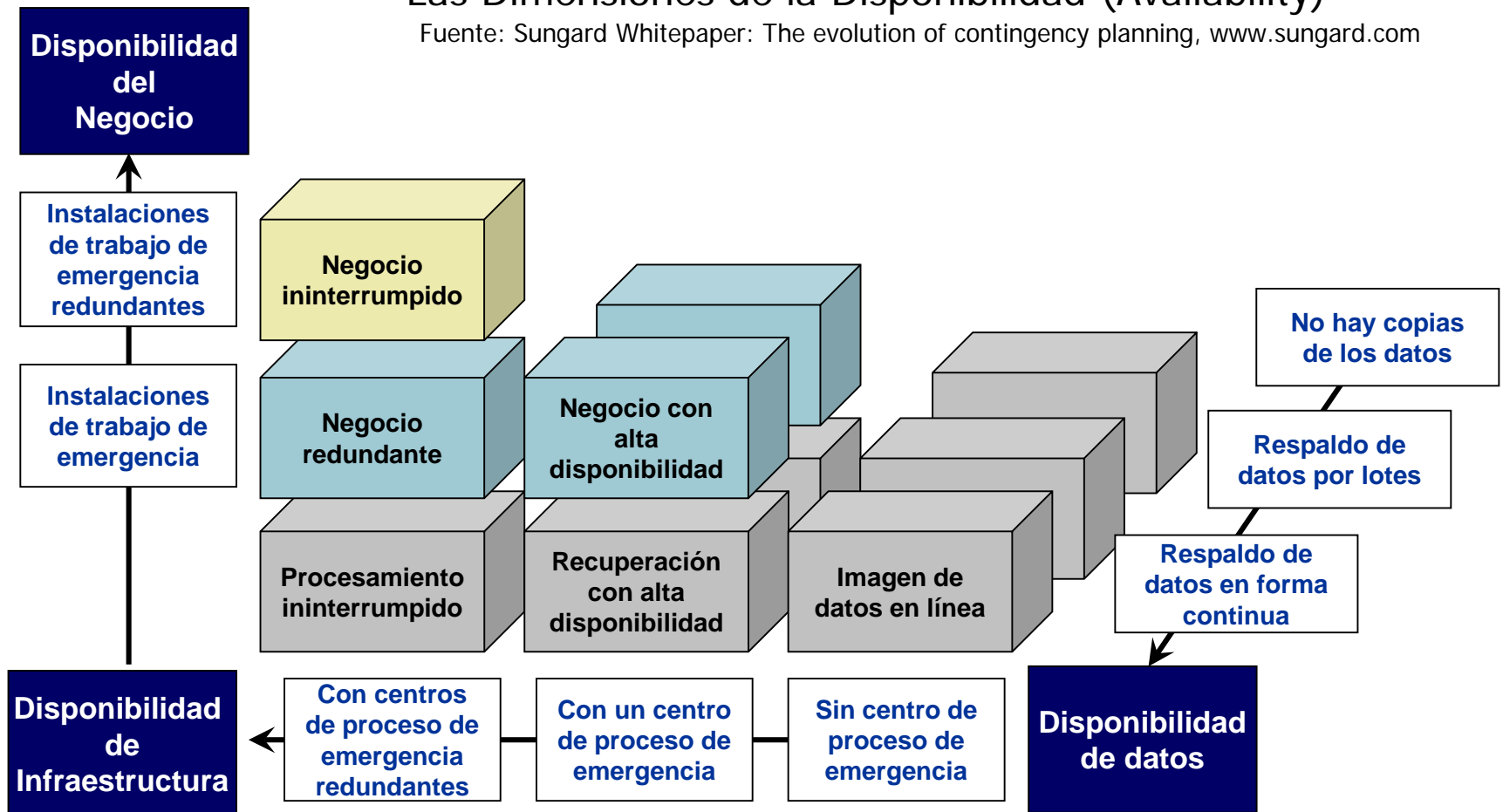
Pequeñas
Emergencias

Fuente: ComputerWorld, 14 al 20 de diciembre de 2001
Artículo: Foro Cibernos TV, La Seguridad Adquiere un Claro
Protagonismo en la Empresa

Planes de Contingencia

Las Dimensiones de la Disponibilidad (Availability)

Fuente: Sungard Whitepaper: The evolution of contingency planning, www.sungard.com

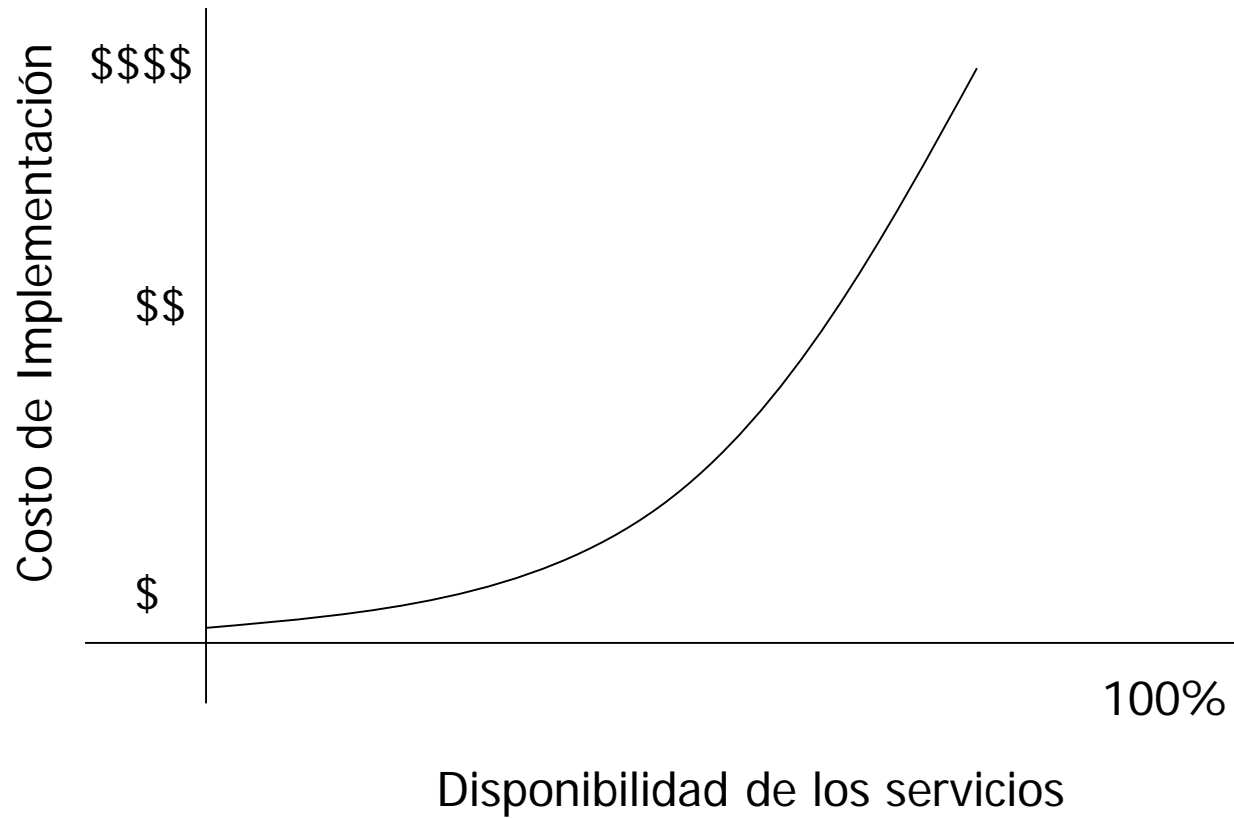




Planes de Contingencia

- En un plan de contingencia se presume que hay **una para de un tiempo**, tiempo sobre el cual se declara la emergencia, y entran a operar una serie de procedimientos que permiten que el servicio se restablezca en el menor tiempo posible
- Un plan de continuidad tiene como objetivo tratar de alcanzar una **disponibilidad de cinco nueves (99.999%)** para la infraestructura crítica, lo que implica que el sistema siempre estará disponible

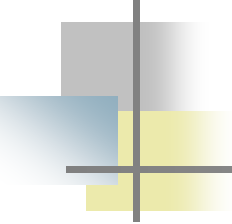
Planes de Contingencia





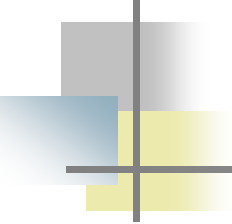
Planes de Contingencia

- ¿Existen procesos en sus instituciones que no pueden estar “fuera de línea”?
- ¿Existe el presupuesto para costear un Plan de Continuidad?
- ¿El personal directivo esta consciente de las posibles limitantes?



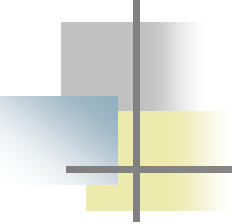
Desarrollo de un Plan de Contingencia

- Aspectos a tener en cuenta:
 - Definir que procesos son esenciales para la operación y concentrar los esfuerzos iniciales en esos procesos
 - La mayor parte de los problemas son causados por situaciones relativamente pequeñas y localizadas
 - Se debe concienciar al personal directivo y definir que nivel de “uptime” se necesita o el que el presupuesto permita.



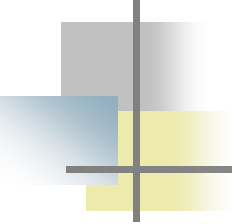
Desarrollo de un Plan de Contingencia

- Obtener el apoyo de los directivos
 - Justificar los fondos necesarios y tenerlos dentro del presupuesto
 - Apoyar las medidas que sean requeridas para hacer y mantener el Plan de Contingencia
 - Facilitar el trabajo y tener muy claro el rol a seguir durante una emergencia



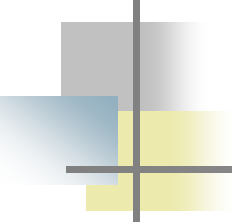
Desarrollo de un Plan de Contingencia

- Seleccionar a un “dueño” del proceso
 - Es la persona más importante durante un desastre
 - Debe coordinar un equipo multifuncional de personas para desarrollar y mantener el plan de contingencia
 - En nuestras organizaciones normalmente este rol pudiera recaer en el Gerente Administrativo o Secretario General en algunos casos



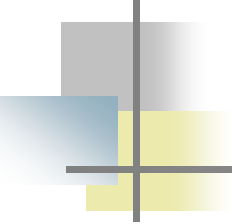
Desarrollo de un Plan de Contingencia

- Crear el equipo multifuncional
 - Personal de diferentes áreas
 - Normalmente el equipo es compuesto por: Tecnología (operadores, desarrolladores, DBA's, etc.), personal de seguridad y de mantenimiento de instalaciones y sobre todo, representantes de los USUARIOS.
 - Desarrollan el Plan de Contingencia.



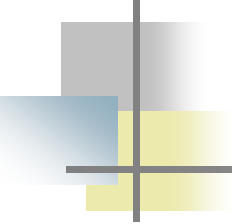
Desarrollo de un Plan de Contingencia

- Realizar un Análisis de Impacto en las Operaciones
 - No es posible darle la misma importancia a todos los procesos
 - Hay que hacer un inventario y priorizar los procesos críticos de la institución
 - Podemos definir procesos que deben ser reanudados en:
 - 24 horas como A
 - 72 horas como B
 - Más de 72 horas como C



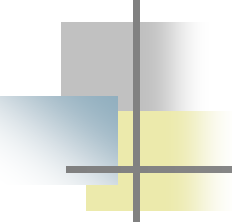
Desarrollo de un Plan de Contingencia

- Identificar y priorizar requerimientos
 - Identificar los requerimientos de operaciones, técnicos y logísticos
 - **Operaciones:** incluye definir cuales criterios determinan un desastre y que procesos deben ir primero y en que tiempo
 - **Técnicos:** incluye definir cuales plataformas serán utilizadas para recuperación
 - **Logísticos:** cuanto tiempo se permite para declarar un desastre y arreglar aspectos como transporte para buscar back ups, coordinación con proveedores externos, etc.



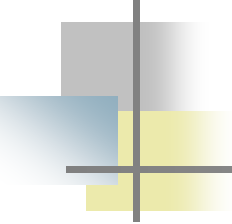
Desarrollo de un Plan de Contingencia

- Definir estrategias de continuidad
 - ¿cómo seguir adelante con las operaciones?
 - Outsourcing o comprar todo internamente
 - Buscar sitios remotos, collocations de servidores



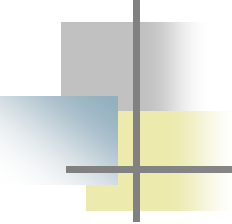
Desarrollo de un Plan de Contingencia

- Escoger a los participantes y definir roles en un Equipo de Recuperación
 - Hay que incluir, a parte de los seleccionados, personal directivo y personal de proveedores externos
 - Roles y responsabilidades deben estar claros, documentados y comunicados



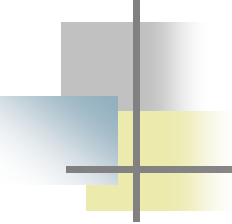
Desarrollo de un Plan de Contingencia

- Documentar el Plan de Contingencia
 - Última actividad del Equipo Multifuncional
 - El Equipo de Recuperación deberá mantenerlo al día
 - Debe incluir diagramas de configuración del hardware, software y componentes de red involucrados en la recuperación



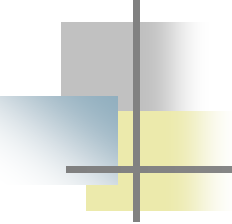
Desarrollo de un Plan de Contingencia

- Planificar y practicar regularmente pruebas al Plan
 - Deben ser probados como mínimo una vez al año
 - Comparar el tiempo utilizado en levantar los sistemas vs. el tiempo definido
 - Hacer pruebas progresivas vs. completas



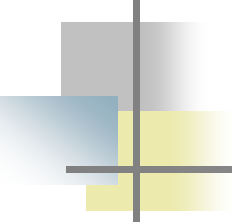
Desarrollo de un Plan de Contingencia

- Hacer evaluación de cada prueba
 - Definir que se hizo bien y que requiere mejorar o actualizarse



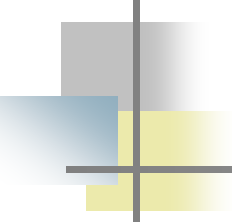
Prepararse para “Pequeñas Emergencias”

- Una “pequeña emergencia” puede no ser una “catastrofe” pero es capaz de inhabilitar uno o más sistemas
- Tecnología debe tener definidos planes de acción para situaciones que pueden afectar a usuarios



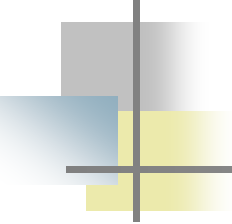
Prepararse para “Pequeñas Emergencias”

- Tener a mano la lista de contactos importantes:
 - Personas o empresas que se requieran para atender situaciones urgentes
 - Tener sus números de teléfono, celular



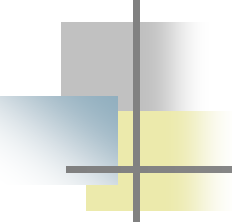
Prepararse para “Pequeñas Emergencias”

- Tener en cuenta las necesidades de los “clientes internos”
 - Tener claros las dependencias entre los sistemas existentes y los departamentos que los usan
 - Estar en comunicación con los usuarios afectados para calmar la ansiedad



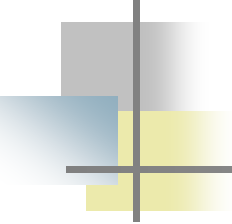
Prepararse para “Pequeñas Emergencias”

- Mantener todo lo demás funcionando
 - Recordar que aunque uno o dos sistemas hayan dejado de funcionar, el resto debe seguir andando o tendremos realmente una “catastrofe”.



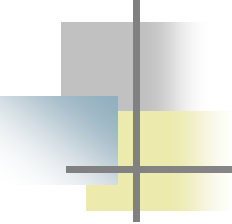
Prepararse para “Pequeñas Emergencias”

- Documentar los Planes de Acción
 - Tener documentados pequeños “Planes de Contingencia Internos” y tener el personal preparado para seguirlo.



Prepararse para “Pequeñas Emergencias”

- Entrenamiento cruzado
 - Mantener por lo menos dos personas entrenadas en cada sistema existente en la organización, en especial aquellos de misión crítica



Prepararse para “Pequeñas Emergencias”

- Mantener la calma
 - Dependiendo del problema, recordar que muchas veces un incidente dentro de Tecnología es invisible para el usuario, por lo que este se impacienta fácilmente.
 - Hay que comunicarse y sobre todo, mantenerse “frío” para pensar mejor.



Recomendaciones finales

- Obsérvese que en esto NO HAY DECISIONES DEFINITIVAS. Hay que revisar constantemente, ¡Estar al día, valorar y anticipar las influencia del ambiente para poder alertar a la Gerencia y se tomen los correctivos necesarios!
- Conversar con el equipo directivo para determinar hasta donde se quiere llegar con el Plan de Contingencia y alinear sus expectativas con la realidad



Recomendaciones finales

- Comunicar efectivamente el Plan de Contingencia a todos los miembros de la institución
- Evaluar el outsourcing del servicio de respaldo y continuidad. Definir muy bien los proveedores y experiencias previas en el mercado.

Fin de Presentación

Planes de Contingencia y Respaldo



Ernesto Rivera Pitti
Director Nacional de Administración
Comisión Nacional de Valores
República de Panamá