IAN STORKEY
INTERNATIONAL CONSULTANT

Taller de Intercambio de Experiencias en Implantación del Plan de Continuidad de Negocios en el Área de Tesorería Pública

Desarrollo e Implementación de un Plan de Continuidad de Negocios

15 de abril de 2013

PERÚ Ministerio de Economía y Finanzas

Lima, 15 y 16 de abril de 2013

Esquema de la presentación

1. Proceso de seis pasos para PCN y PRD
2. Prueba de revisión
3. Simulacro en vivo


Colombia 2011


Brazil 2011


Chile 2010


Mexico 1985

Proceso de seis pasos para PCN y PRD

1. Documentar procesos y sistemas críticos
2. Emprender análisis de impacto en el negocio
3. Desarrollar PCN y PRD
4. Implementar o actualizar PCN y PRD
5. Incorporar PCN y PRD en las operaciones de Tesorería
6. Realizar pruebas y actualizaciones periódicamente

Esquema del proceso de gestión de riesgos (caso de Chile)

Paso 1 Política de riesgo	Paso 2 Proceso de análisis	Paso 3 Elaboración de la matriz
Paso 4 Establecer orden de clasificación	Paso 5 Establecer un plan de tratamiento	Paso 6 Monitoreo y examen

Procesos y sistemas críticos

Sistema	Período de tiempo (minutos, horas, días)	Localidad de Servidor (sitio primario)	Respaldo de Datos (tiempo y ubicación)	Localidad de Acceso (sitio o centro de datos alternativo)
SIAF/SIIF				
SIAD/SDP				
MS Office				
Bloomberg				

Proceso o Sistema Crítico del Negocio #< >: <insertar nombre del proceso>	
Actividades	
Recursos	
Personas	
Instalaciones (incluyendo edificios y equipos)	
Tecnología (incluyendo sistemas de TI y aplicaciones)	
Telecomunicaciones	
Registros importantes (incluyendo físico y medio electrónico)	
Procesos interdependientes (incluyendo internos y externos)	
Otros	

Proceso 1.

Personas que intervienen:
Persona crítica 1:
Persona crítica 2:
Persona crítica 3:
Persona crítica 4:
Persona crítica 5:
Persona crítica 6:
Persona crítica 7:
Persona crítica 8:

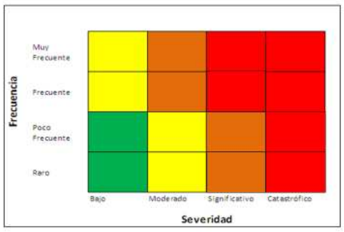
Id	Actividad crítica	Sistema(s)	Descripción
1.1			
1.2			
1.3			

Procesos críticos por tiempo

Prioridad	Tesorería	Interno	Externo	Operaciones
Crítico (dentro de los siguientes 15 minutos)				
Inmediato (dentro de la siguiente hora)				
Muy alta (dentro de las siguientes 2 horas)				
Alta (dentro de las siguientes 4 horas)				
Moderado (dentro de las siguientes 8 horas)				
Baja (> 8 horas)				

Análisis de impacto en el negocio

Fallas de Infraestructura y de Tecnología		
Falta de energía eléctrica	Falla del equipo	Falla del Software
Corrupción de datos incluyendo virus	Fallas en LAN/WAN/Intranet/Internet	Inundación Interna (rociadores, ductos)
Falla de la red de Voz	Robo de Equipo	Robo de datos / información
Mantenimiento deficiente	Daño Accidental	Sabotaje
Incidentes donde se Niega Acceso al Sitio		
Peligro de inundación o incendio	Violación a la salud y a la seguridad	Accidente por productos químicos peligrosos
Fugas de gas o productos químicos	Acciones industriales o disturbios	Amenaza de bomba o de terroristas
Incendio o explosión en la instalación	Inundación interna/externa	Sabotaje o terrorismo
Dependencias de Proveedores de Servicios Clave o Fallas de Recursos		
Falla de proveedores de servicios clave (teléfono, internet, banca, etc.)	Proveedores externos (Banco Central y otras operaciones subcontratadas)	Impacto de incidentes en los equipos o grupos críticos (pandemias, incidente de grupo, en viajes)
Fallas de Personal, Administración y Humanas Relacionadas		
Error humano (que puede deberse a mala capacitación o supervisión inadecuada)	Mala capacitación o supervisión inadecuada (que puede llevar a error o ejecución de operaciones no autorizadas)	No se respeta el código de conducta o las pautas sobre conflicto de intereses
Falta de guía de políticas (que puede llevar a tomar malas decisiones o a realizar actividades no autorizadas)	Entendimiento deficiente del ambiente de riesgos (que puede ocasionar riesgos innecesarios o desconocidos)	Delegaciones mal especificadas (que puedan llevar a la ejecución de operaciones no autorizadas)
No se sigue o se cumple las prácticas administrativas (lo que puede causar errores en el procesamiento)	Riesgo de personas clave (que puede llevar a error humano cuando la persona clave está ausente)	Prácticas fraudulentas, corruptas o deshonestas (que pueden llevar a pérdidas financieras y situaciones políticas embarazosas)
Falla en el Cumplimiento de Obligaciones Reglamentarias, Legales, de Recursos Humanos y Otras		
Obligaciones legales/reglamentarias (Ej. cumplimiento con los contratos de préstamos)	Directrices administrativas (Ej. políticas y procedimientos internos)	Manuales de Procedimientos y facultades delegadas
Obligaciones de presentar reportes (Ej. a autoridades superiores e instituciones internacionales)	Obligaciones contractuales (Ej. obligaciones del servicio de la deuda)	Reglamentos de Salud y Seguridad (Ej. leyes o reglamentos laborales nacionales)
Grandes desastres regionales y naturales		
Terremotos severos	Huracán, ciclón o tornado	Tsunami
Erupción volcánica	Incendios graves	Disturbios civiles
Fuerte inundación	Huaicos	Terrorismo



Evaluación de Impacto	Impacto Reputacional	Reportes e Impacto a los Recursos	Impacto a las Operaciones de Endeudamiento y Tesoro
Catastrófico	Pérdida de confianza del gobierno Pérdida de confianza del mercado Pérdida de confianza, Ej. Regiones y Ministerios Amplia cobertura de los medios Investigación a alto nivel del Ministerio [o renuncia] Sanciones financieras y legales	Se reporta al Presidente o al Congreso Gran cantidad de tiempo dedicado a manejar el impacto (Ej. Más de 20 días hombre)	Significativa variación del presupuesto para el servicio de deuda (más del 10%) Retraso significativo en conseguir los objetivos presupuestarios incluyendo los requerimientos para la obtención de préstamos Se deja de hacer pagos de alta prioridad a su vencimiento (personal, servicio de deuda, reintegro de impuestos, Regiones) Se incurre en pagos erróneos como acreditar fondos en la cuenta equivocada o entregarlos después de la fecha de vencimiento Se incurre en pago de sanciones (como recurso no presupuestario) como servicio de deuda, reintegro de impuestos, planillas y transferencias a entidades (con impacto político) Se sobregira una cuenta bancaria No se puede transferir fondos entre las cuentas del Tesoro debido a una falla en los sistemas de pago del BN No se puede recibir ni tener acceso a los fondos. No se puede operar con divisas (recibir, comprar, vender o invertir) No se puede tener acceso a las cuentas bancarias del Tesoro o a sus saldos y operaciones

Desarrollar PCO/PCN y PRD

Ministerio de Economía y Finanzas — Plan de Continuidad de Operaciones

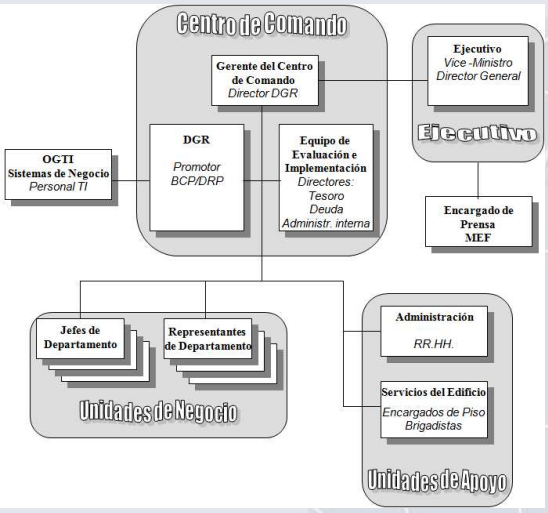
PLAN DE CONTINUIDAD DE OPERACIONES

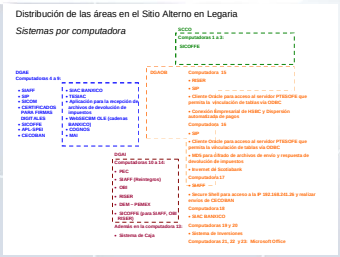
PERU
MINISTERIO DE ECONOMÍA Y FINANZAS

Página 1

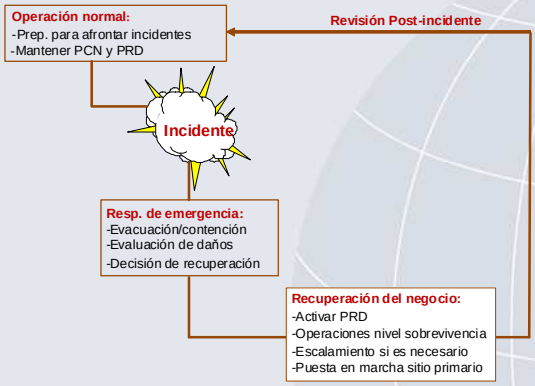
PLANILLA: ÍNDICE DEL PCO/PRC	
Sección	**Información incluida**
Portada	Título y versión Declaración breve del objetivo del PCO/PRC Aprobación por parte de la alta gerencia
Índice	Contenido del PCO/PRC
Activación	Medidas que se adoptarán inmediatamente después de que se produzca el incidente o evento (respuesta de emergencia) Proceso de intensificación Criterios para la activación del PRC
Funciones y responsabilidades	Estructura del centro de mando Funciones y responsabilidades de todos los equipos
PRC	Planes para reunir al equipo de personal (*team assembly arrangements*) Pasos de la recuperación (procedimientos, listas de tareas y medidas) Reubicación en el emplazamiento alternativo
Necesidades de recursos	Personal Instalaciones (incluidos los edificios y el equipo) Tecnología (incluidos los sistemas y aplicaciones informáticas) Telecomunicaciones Registros clave Interdependencias Otras
Comunicación	Protocolo de comunicación Muestreo de las comunicaciones (por ejemplo, mensaje de activación, comunicado de prensa, emisiones del personal, etc.) Contacto con los medios de comunicación
Registro de eventos	Planilla del registro de eventos
Listas de contactos	Lista de contactos para servicios de emergencia Listas de contactos del equipo interno Lista de contactos de las organizaciones dependientes Listas de contactos de las partes interesadas y de contactos externos Listas de contactos del personal
Otra información	Instrucciones, mapas, diagramas y otra información útil para el personal

Implementar el PCN y PRD





Pruebas y actualizaciones periódicas



Mantenimiento	Cronograma
Revisión y actualización de la documentación del Plan de Continuidad de Operaciones	cada seis meses
Prueba de recuperación de la tecnología	cada seis meses
Prueba de conocimiento básico del personal	anualmente
Pruebas de escenarios (pizarrón blanco)	anualmente
Prueba completa (incidente simulado)	anualmente

Muy recomendable: realizar prueba durante las operaciones normales

Prueba del PCN y PRD

¿Qué tan bien preparada esta su Tesorería?
Pongámoslo a prueba

Escenarios de prueba para el PCN/PRD:

- Escenario 1: Falla del sistema
- Escenario 2: Evacuación del edificio
- Escenario 3: Daño al predio
- Escenario 4: Pandemia

Escenario 1: Falla del sistema

- A las 4pm se cae el sistema y se afectan todos los servidores del MHCP. En la evaluación inicial realizada por sistemas (TI) se determina que se necesitará por lo menos el resto del día y toda la noche para remplazar los servidores y reinstalar los sistemas operativos, las aplicaciones y los datos a partir de la fuente de respaldo más reciente. El Director y el Director Encargado de Sistemas y el Director de la subdirección de Riesgo no están en el edificio en el momento del incidente.

Escenario 2: Evacuación del edificio

- A las 11am las autoridades municipales requieren una evacuación total del edificio del MHCP debido al posible riesgo de una explosión. Se acordonan varias manzanas alrededor del edificio y el personal es evacuado de inmediato y llevado fuera de la zona. Las autoridades no tienen claridad sobre la duración del incidente, pero esperan que asegurar el área y permitir que el personal retorne al edificio puede durar más de un día. El incidente ocurre en el día de una subasta de títulos del tesoro.

Escenario 3: Daño al predio

- Durante la noche hay un incendio en el edificio y éste sufre daños graves, incluidos daños de importancia debido al humo y al agua en el área de la tesorería. Los bomberos no permiten acceso alguno al edificio debido a los daños estructurales y el riesgo para cualquiera que pudiera entrar en el edifico. Los funcionarios que llegan al área acordonada a las 7:30am son los primeros en darse cuenta de los daños.

Escenario 4: Pandemia

- Una pandemia afecta el país (parecida al virus H1N1 del 2009). Parte del personal decide quedarse en casa para evitar contagiarse con el virus. El personal que sí viene a la oficina está bajo un monitoreo constante, y tan pronto como muestran signos de contagio son enviados inmediatamente a casa. Al finalizar la semana, por lo menos el 50% de los funcionarios están afectados o han decidido permanecer en casa. Todo el personal de tesorería está afectado y el 80% del personal de operaciones también está afectado. Después de ser diagnosticados con el virus, el personal debe quedarse en casa por lo menos 10 días.

Prueba del PCN/PRD

- Una vez PCN/PRD está en su lugar, necesita probar regularmente
- La prueba deberá simular una situación "en vivo"
- Usaremos el siguiente ejemplo de una prueba en vivo para mostrar la forma como Tesorería puede manejar una interrupción grave

Simulacro en vivo #1

- En la subestación que provee de energía al centro de la ciudad hubo esta mañana una explosión a las 9:45am provocando un apagón en todo el centro de la ciudad. Según la primera evaluación de los danos realizada por la empresa de servicios públicos, el daño es grave y se necesitara al menos una semana de tiempo para completar las reparaciones y restablecer el fluido eléctrico en su totalidad.
- Debido a restricciones presupuestarias del MHCP y a la utilización reciente de la planta eléctrica, hay pocas reservas de diesel las cuales quizás alcancen para unas 3-4 horas. A causa del apagón, la demanda de diesel se ha disparado, de manera que quizás pasen varios días antes de poder recibir el reabastecimiento.

Simulacro en vivo #2

- El MHCP ha decidido que se utilizara la planta solamente para dar energía a las dos salas donde están los servidores hasta tanto se agote la reserve del combustible. Con esto, el personal de sistemas podrá correr las operaciones criticas y tomar las medidas necesarias para el traslado al centro de datos.
- El apagón también afecto las torres de transmisión de telefonía celular del centro de la ciudad, de manera que la cobertura es limitada en esa zona de la ciudad. La utilización de los teléfonos celulares se debe reducir a un mínimo y utilizar texto en lugar de voz, por ejemplo.
- En el centro de la ciudad se han visto afectados los establecimientos comerciales, y será necesario cerrar los restaurantes y demás negocios de comidas debido a la falta de electricidad para mantener las neveras.
- La tesorería ha convocado a esta reunión de emergencia para activar el PRD.

Conclusiones

- Creciente dependencia de las tecnologías de información y comunicación (basados en internet)
- Los tiempos se han acortado
- Se ha reducido la tolerancia del incumplimiento
- Critico para Tesorería para asegurar un mínimo de fallas y proteger la reputación del gobierno
- Es fundamental que Tesorería cuente con un PCN/PRD que este plenamente integrado a las operaciones cotidianas
- Es necesario someter el PCN/PRD a pruebas periódicas

IAN STORKEY
INTERNATIONAL CONSULTANT

Taller de Intercambio de Experiencias en Implantación del Plan de continuidad de Negocios en al área de Tesorería Pública

Desafíos en la implantación de un Plan de Continuidad de Negocios

15 de abril 2013

PERÚ Ministerio de Economía y Finanzas

Lima, 15 y 16 de abril de 2013

Esquema de la presentación

1. Principales limitaciones o barreras
2. Principales lecciones de la experiencia internacional
3. Algunas sugerencias

Principales Limitaciones o Barreras

- Frecuente descuido de la alta gerencia:
  - "eso jamás nos sucederá" sigue muy vigente
- Asignación insuficiente de recursos para desarrollar, implementar y mantener el PCN/PRD
- Visto como una prioridad baja
- Es frecuente que la responsabilidad sea delegada al Departamento de Tecnología o a un funcionario de nivel medio
- Visto como un proyecto, más que como un programa continuo integrado a la operación
- Ausencia de regulación del MHCP

Principales lecciones de América Latina

- El ciclo político de América Latina dificulta la implementación del PCN/PRD
  - necesidad de renegociar los arreglos con terceros
- El MHCP sujeto a limitaciones presupuestales
- Persiste la idea generalizada de "por qué pagar para cubrir algo que tal vez no suceda?"
- Sigue siendo visto como TI, no como un riesgo operacional que afecta todas las operaciones de Tesorería

Como abordar la limitación de recursos

- Administración se compromete a implementar PCN/PRD e integrarlo en todas las operaciones
- Nombrar un funcionario de la unidad de riesgo como “defensor” o “facilitador” del PCN/PRD, de tiempo completo
- Cada sub-dirección asume la responsabilidad de sus propias operaciones y asignar recursos cuando sea necesario
- Trabajar en estrecha colaboración con TI y el Banco Central

Integración con las operaciones

- PCN/PRD es un componente de gestión del riesgo operacional
- Todos los riesgos deben ser controlados y gestionados diariamente
- MHCP lo debe integrar en todas las políticas y procedimientos

TI versus operaciones

- El PCN/PRD es visto a menudo como una copia de seguridad para la recuperación de datos
- Sigue siendo importante por la dependencia de la tecnología
- El PCN/PRD cubre todas las operaciones, particularmente los procesos críticos, los sistemas y las personas más importantes

Algunas sugerencias #1

1. El MHCP debe contar con un PCN/PRD para cada una de sus operaciones
2. El PCN/PRD debe ser administrado por una unidad de riesgo y no por el Departamento de Tecnología
   - es fundamental tener una estrecha coordinación con Tecnología
3. El PCN/PRD debe ser visto dentro del marco de la Gestión del Riesgo Operacional

Algunas sugerencias #2

4. El MHCP debe promover una cultura de la continuidad del negocio y recuperación de desastres como una actividad cotidiana y se incluye en todas las decisiones relacionadas con las operaciones del MHCP
5. El MHCP debe ampliar el ámbito de aplicación del PCN/PRD a todas las direcciones de MHCP
6. El PCN/PRD debe ser probado al menos cada 12 meses
   - preferiblemente trimestralmente y/o utilizar el sitio alterno periódicamente

Otras sugerencias #1

El MHCP debe:

- asegurar que un miembro del personal de la unidad de riesgo sea asignado de tiempo completo al PCN/PRD en el papel de “defensor” o “facilitador”
- definir la estructura y recursos para manejar incidentes que requieren activar el PRD, incluido el establecimiento de una estructura de centro de mando
- el PCN/PRD debe abarcar los procesos de reubicación, incluyendo la recuperación de la infraestructura y los recursos necesarios en el sitio alterno, conexión con terceros, la sensibilización y capacitación del personal, y las pruebas periódicas

Otras sugerencias #2

El MHCP debe:

- desarrollar un plan de continuidad de negocio global de pruebas incluyendo pruebas “en vivo”
- identificar las causas de los fracasos recurrentes mediante el mantenimiento de un registro de todos los incidentes de este tipo
- mantener una base de datos estadística de fallas recurrentes y desarrollar acciones preventivas para hacer frente a las debilidades y evitar o reducir este tipo de incidentes
- garantizar que todos los terceros que proporcionan servicios críticos para MHCP tener una adecuada PCN/PRD en su lugar

IAN STORKEY
INTERNATIONAL CONSULTANT

Taller de Intercambio de Experiencias en Implantación del Plan de Continuidad de Negocios en el Área de Tesorería Pública

Experiencias internacionales del
Plan de Continuidad de Negocios

16 de abril 2013

PERÚ Ministerio de Economía y Finanzas

Lima, 15 y 16 de abril de 2013

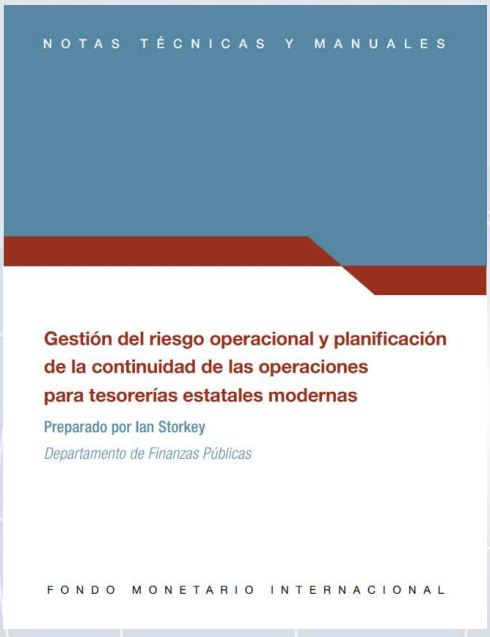
Esquema de la presentación

1. Normativa internacional
2. Experiencias internacionales
3. Los casos de México y Colombia

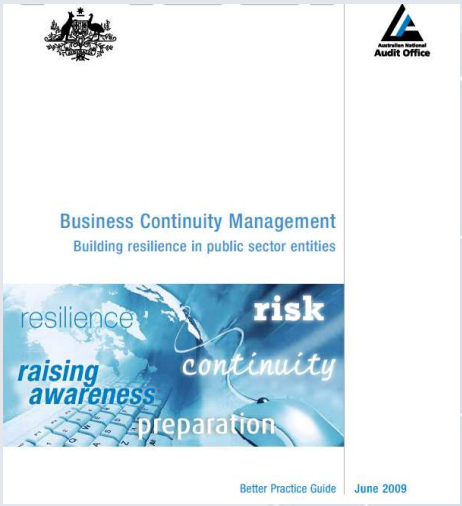
Normativa internacional

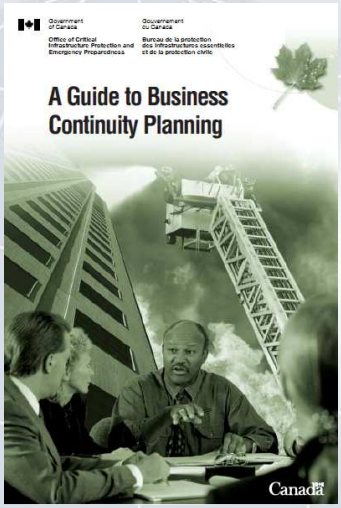
- El PCN/PRD se debe elaborar de conformidad con la normativa internacional denominada ISO 22301 sobre Gestión de Continuidad de Operaciones
  - reemplaza la norma BS25999

FMI notas técnicas y manuales

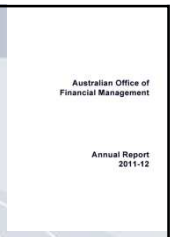


Gobiernos de Australia y Canadá





Australia (AOFM)



- El AOFM cuenta con planes de continuidad de negocios y pandemias para asegurar que sus actividades continuen en caso de perturbaciones o pandemias de influenza
- Esto incluye contar con copias y sitios de respaldo que se pueden implementar cuando la oficina de la AOFM no puede ser utilizada o su personal no puede realizar tareas clave
- También cuenta con un plan de recuperación de TI (sistemas) que pone en marcha los procesos requeridos para restablecer las funciones de TI luego de una interrupción significativa
- Se ha probado y actualizado los planes de continuidad de negocios

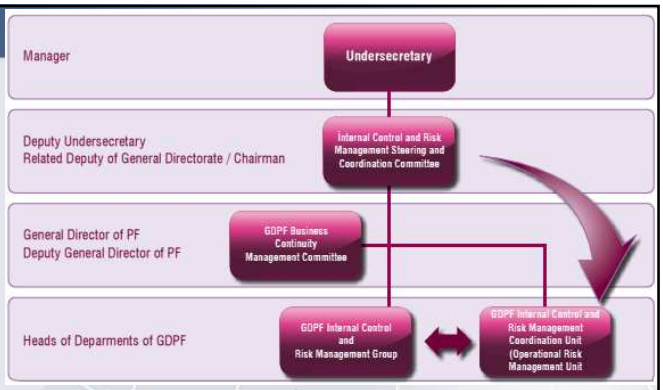
Francia (Agence France Trésor)

- El plan de continuidad de negocios comprende tres etapas que se activan dependiendo de la criticidad de la situación presentada
- Estas etapas siguen una secuencia geográfica:
  - **Back-up (respaldo) local:** diseñado para asegurar la continuidad del servicio cuando se presenta un incidente donde solo se verán afectadas algunas áreas del sitio principal
  - **Back-up (respaldo) cercano:** diseñado para contrarrestar una interrupción parcial o de muy corta duración en el sitio (máximo 48 horas) con reubicación a una sede alterna cercana
  - **Back-up (respaldo) regional:** abarca todos los recursos y procesos requeridos para respaldar el sitio principal mediante un traslado completo a un sitio ubicado en un lugar regional
- Se realizan pruebas técnicas y pruebas de usuario periódicamente a lo largo del año

Reino Unido (DMO)

- El Plan de Continuidad de Negocios (PCN), Recuperación de Desastres (RD) y otros arreglos de DMO son sometidos continuamente a revisión y actualización
- DMO ejecutó un programa de pruebas de Recuperación de Desastres en el 2011 y se aseguró que los arreglos de PCN que respaldan las subastas fueran observados durante el año por los equipos que trabajan desde el sitio RD durante las sesiones de subasta
- La evaluación de los requerimientos de continuidad de negocios es requisito indispensable para todo proyecto nuevo y toda iniciativa de negocios de gran importancia
- DMO contrató un especialista en continuidad de negocios en el 2011 con el fin de mejorar y promover la planificación a lo largo y ancho de la organización

Turquía (DGPF)



En el 2011, como resultado de estudios iniciados por el Comité de Continuidad de Negocios constituido con la aprobación de la Subsecretaría, se elaboró el documento "Política de Gestión de la Continuidad de Operaciones de Tesorería". La Dirección General de Finanzas Públicas (DGPF) realizó sus labores de conformidad con este documento. Estudios relacionados fueron llevados a cabo por el Comité de Control Interno y Gestión de Riesgo de Tesorería creado con el fin de identificar normas de control interno específicas dentro de la Subsecretaría y así asegurar la implementación efectiva del sistema de control interno y gestión de riesgo.

También se creó el "Comité de Gestión de la Continuidad de Negocios" como sub-componente de la DGPF. Dicho Comité es responsable por la gestión de la deuda, cartera y caja de Tesorería. El Comité tiene por objeto asegurar la continuidad de las operaciones prioritarias de gestión de activos y pasivos durante una situación de emergencia.

El caso de México: TESOFE plan de continuidad de operaciones

TRIARA Centro de Datos de TI de Querétaro

Tesorería de la Federación

Banco de México

Sitio Alterno en Legaria

El caso de Colombia: DGCPTN plan de continuidad de operaciones

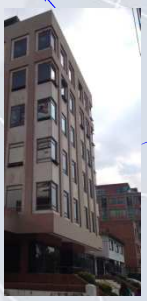
TRIARA
Centro de Datos de Bogotá 10km al noroeste del aeropuerto

Ministerio de Hacienda y Crédito Público

Banco de la República

MHCP tiene contrato con SONDA

SONDA
Sitio Alterno en el norte Bogotá



Opción 1: bajo costo

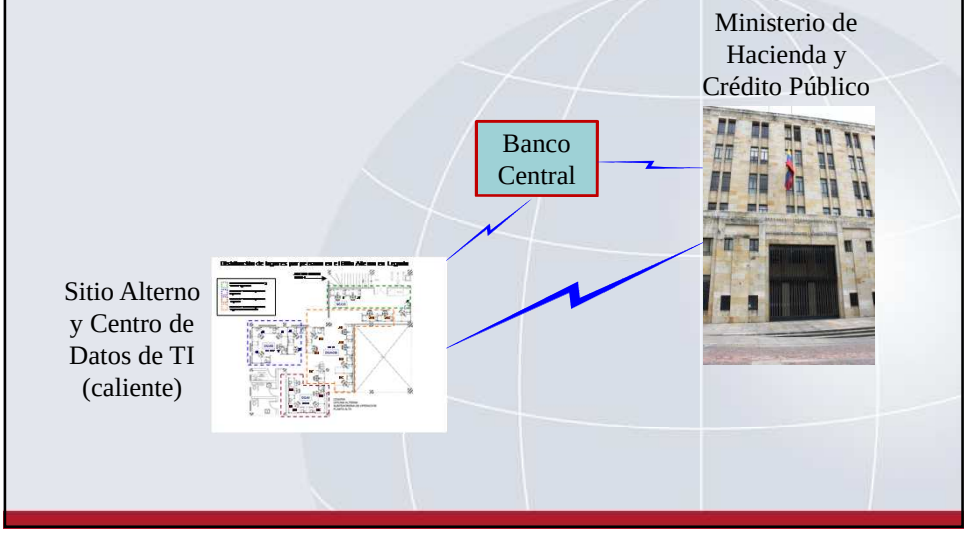
Ministerio de Hacienda y Crédito Público

Banco Central

Sitio Alterno
(frío-caliente)

Transferencia de datos

Opción 3: costo intermedio



Opción 2: costo alto