



Taller de gestión de la continuidad operativa en entidades del sector Economía

Desarrollo e implementación de un plan de continuidad de negocios



Lima, 12 de noviembre 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



Chile 2010



Perú 2007



México 1985

Proceso de seis pasos para PCN y PRD

1. Documentar procesos y sistemas críticos
2. Empezar 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 MEF
6. Realizar pruebas y actualizaciones periódicamente

A menudo es necesario hacerlo de manera simultánea para ciertas etapas

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

	Procesamiento de la información	Información sobre riesgos críticos	Control básico
Proceso			
Subproceso			
Etapas			
Objetivo			
Riesgo crítico			
Probabilidad			
Impacto			
Gravedad			
Control			
Diseño			
Eficacia del control			
Exposicional riesgo			

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:

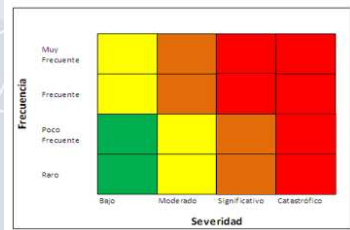
Id	Actividad crítica	Sistema(s)	Descripción
1.1			
1.2			
1.3			

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)				

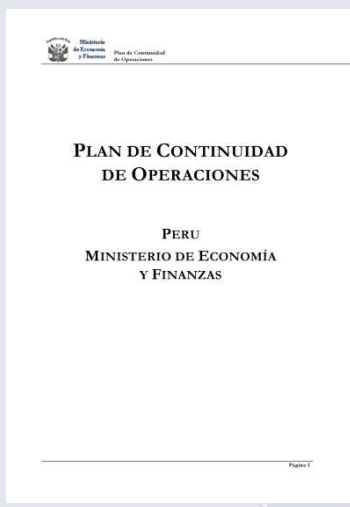
Análisis de impacto en el negocio

Fallos de Infraestructura y de Tecnología		
Falta de energía eléctrica	Falta del equipo	Falta del Software
Corrupción de datos incluyendo virus	Fallas en LAN/WAN/Internet/Intranet	Inundación Interna (servidores, datos)
Falta de la red de Voz	Buho de Equipo	Buho de datos / información
Mantenimiento deficiente	Dialo accidental	Sabotaje
Incidentes donde se NINGA Acceso al Sitio		
Riego de inundación o incendio	Violación a la salud o a la seguridad	Accidente por productos químicos peligrosos
Pugas 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
Dependencia de Proveedores de Servicios Clave o Fallos de Recursos		
Falta de proveedores de servicios clave (teléfono, internet, banca, etc.)	Proveedores externos (Banco Central o otras operaciones subcontratadas)	Impacto de incidentes en los socios o grupos críticos (partenariats, incidente de grupo, etc.)
Fallos de Personal, Administración y Finanzas		
Error humano (que puede llevar a mala asignación o supervisión inadecuada)	Mala capacitación o supervisión inadecuada que puede llevar a error o omisión de operaciones en actividades	Rotación de personal
Falta de plan de política (que puede llevar a mala asignación de recursos o mala supervisión)	Excesivo tiempo dedicado del personal de tiempo que puede llevar a mala asignación de recursos o mala supervisión	Dispersión mal asignada que puede llevar a mala asignación de recursos o mala supervisión
No se sigue el ejemplo de prácticas gubernamentales (que puede llevar a mala asignación de recursos o mala supervisión)	Rango de personas clave (que puede llevar a mala asignación de recursos o mala supervisión)	Prácticas gubernamentales, políticas y procedimientos que pueden llevar a grandes impactos o subestimar prácticas gubernamentales
Falta en el Cumplimiento de Obligaciones Regulatorias, Externas, de Relaciones Públicas y Otras		
Obligaciones legales regulatorias (Ej. cumplimiento con las condiciones de préstamo)	Obligaciones regulatorias (Ej. cumplimiento con las condiciones de préstamo)	Obligaciones de Prudencia y Función del Estado
Obligaciones de gobierno corporativo (Ej. integridad de la información)	Obligaciones de gobierno corporativo (Ej. integridad de la información)	Obligaciones de Integridad (Ej. Integridad de la información)
Grupos de Interés regionales y nacionales		
Transacciones comerciales	Financiera, créditos o transacciones	Financiera
Empleos voluntarios	Relaciones públicas	Dimensiones críticas
Planes de continuidad	México	Financiera



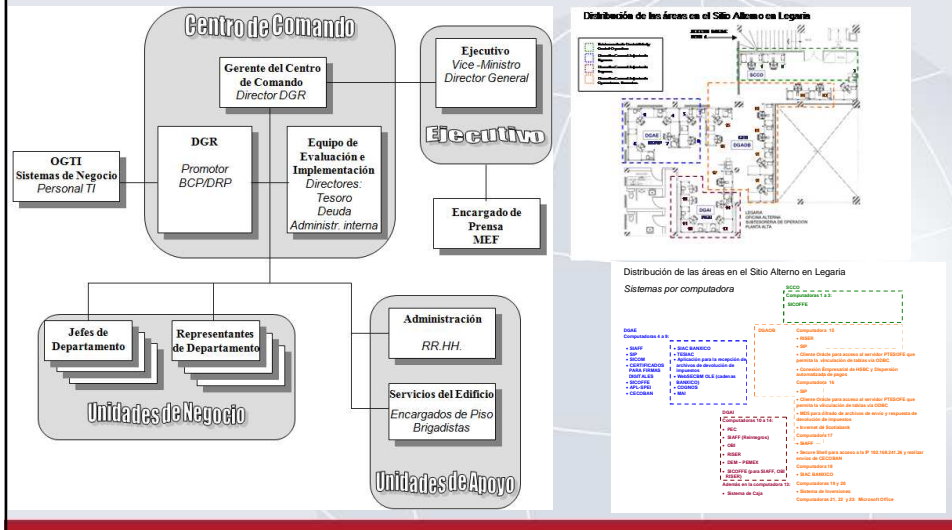
Evaluación de Impacto	Impacto Reputacional	Respuesta a Impactos o los Recursos	Impacto a las Operaciones de Endeudamiento y Tesoro
Catástrofico	Pérdida de confianza del gobierno Pérdida de confianza del consumidor Pérdida de confianza de proveedores, El Regulatorio y Ministerios Amenaza coherente de los miembros Investigación o alto nivel de atención (o escándalo) Dimensiones financieras y legales	Se reporta al Presidente o al Director Grave cantidad de tiempo dedicado a manejar el impacto (Ej. más de 20 días hábiles)	Significativa reducción del presupuesto para el servicio de deuda (más del 10%) Retraso significativo en conseguir los recursos comprometidos incluyendo los compromisos para la obtención de préstamos Se deja de hacer pagos de alta prioridad a los proveedores (general, servicio de deuda, proveedores de seguros, Regulatorio) Se incurre en pagos adicionales como resultado de la cuenta de equidad o entregados después de la fecha de vencimiento Se incurre en pago de comisiones (como resultado de pagos, entrega de garantías, planillas y transferencias a entidades (con impacto positivo)) Se subestima una cuenta bancaria No se puede transferir fondos entre las cuentas del Tesoro debido a una falla en los sistemas de pago del BCR No se puede recibir ni hacer efectivo a los fondos. No se puede operar con divisas (ventas, compras, ventas o compras) No se puede operar con las cuentas bancarias del Tesoro o a sus hijos y operaciones

Desarrollar PCO/PCN y PRD

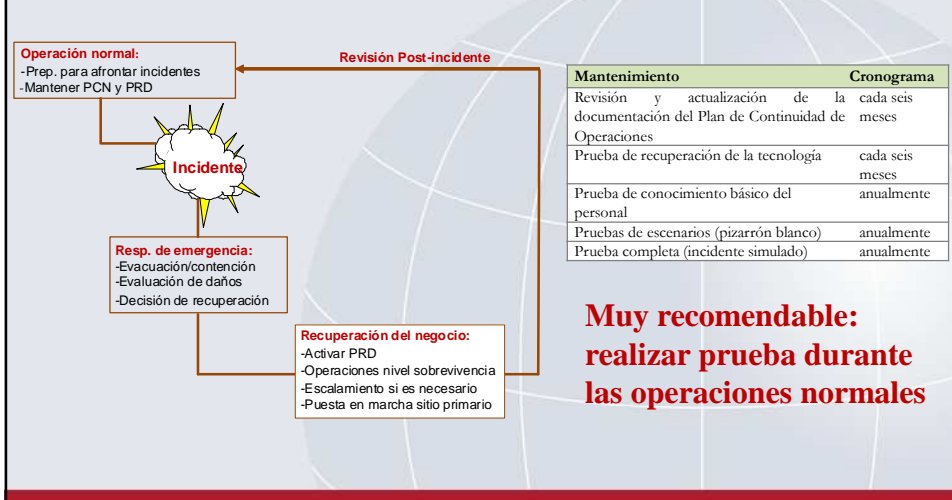


PLANILLA: INDICE DEL PCO/PRC	
Sección	Información incluida
Portada	Título y versión Declaración breve del objetivo del PCO/PRC Aprobación por parte de la alta gerencia
Índice	Contenido del PCO/PRC
Activación	Medidas que se adoptarán inmediatamente después de que se produzca el incidente o evento (respuesta de emergencia) Proceso de identificación 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) Flexibilidad 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 Muestra de las comunicaciones (por ejemplo, mensaje de activación, comunicado de prensa, emisiones del personal, etc.) Contacto con los medios de comunicación
Registro de eventos	Plantilla del registro de eventos
Listas de contactos	Lista de contactos para servicios de emergencia Lista de contactos del equipo interno Lista de contactos de las organizaciones dependientes Lista de contactos de las partes interesadas y de contactos externos Lista 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



Prueba del PCN y PRD

¿Qué tan bien preparada esta su DGETP?
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 MEF. 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 reemplazar 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 MEF 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 DGETP. Los bomberos no permiten acceso alguno al edificio debido a los daños estructurales y el riesgo para cualquiera que pudiera entrar en el edificio. 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 DGETP está afectado y el 80% del personal BN de operaciones para MEF 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 DGETP 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 daños 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 MEF 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 MEF 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 críticas 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.
- DGETP 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 DGETP para asegurar un mínimo de fallas y proteger la reputación del gobierno
- Es fundamental que DGETP 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

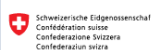
Taller de gestión de la continuidad operativa en entidades del sector Economía

Desafíos en la implantación de un plan de continuidad de negocios



PERÚ

Ministerio de Economía y Finanzas



Lima, 12 de noviembre 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, no urgente
- Es frecuente que la responsabilidad sea delegada al Departamento de Tecnología o a un funcionario de nivel medio o de un área administrativa
- Visto como un proyecto, más que como un programa continuo integrado a la operación
- Ausencia de regulación del tema (general e interna)

Principales lecciones de América Latina

- El ciclo político de América Latina dificulta la implementación del PCN/PRD
 - necesidad de renegociar los arreglos con terceros
 - parálisis antes y después de elecciones, o cambios de Ministros y otros funcionarios clave
- El Ministerio sujeto a limitaciones presupuestales y a normas que impiden actuar con rapidez
- 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 del Ministerio

Como abordar la limitación de recursos

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

Integración con las operaciones

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



No es solo un tema de TI

- El PCN/PRD es visto a menudo como una copia de seguridad para la recuperación de datos, lo que es erróneo
- 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 MEF 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
 - Pero es fundamental tener una estrecha coordinación con Tecnología
3. El PCN/PRD debe ser visto dentro del marco de la Gestión del Riesgo Operacional. No se debe relajar estándares (calidad de construcción, ubicación y conectividad) de sedes alternas y centros de respaldo TI.

Algunas sugerencias #2

4. El MEF 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 MEF
5. El MEF debe ampliar el ámbito de aplicación del PCN/PRD a todas las direcciones de MEF
6. El PCN/PRD para todo el MEF debe ser probado al menos cada 3 meses
 - preferiblemente mensualmente y/o utilizar el sitio alternativo periódicamente o permanentemente

Otras sugerencias #1

El MEF debe:

- asegurar que por lo menos 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 alternativo, conexión con terceros, la sensibilización y capacitación del personal, y las pruebas periódicas

Otras sugerencias #2

El MEF 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 MEF tener una adecuada PCN/PRD en su lugar



IAN STORKEY
INTERNATIONAL CONSULTANT

Taller de gestión de la continuidad operativa en entidades del sector Economía

Experiencias internacionales del plan de continuidad de negocios



PERÚ

Ministerio de Economía y Finanzas



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Lima, 12 de noviembre 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 mínimo en conformidad con la normativa internacional denominada ISO 22301 sobre Gestión de Continuidad de Operaciones
 - reemplaza la norma BS25999



FMI notas técnicas y manuales

NOTAS TÉCNICAS Y MANUALES

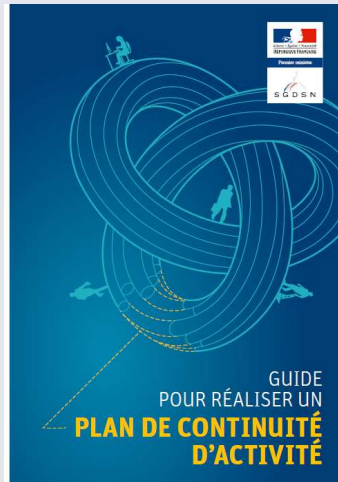
Gestión del riesgo operacional y planificación de la continuidad de las operaciones para tesorerías estatales modernas

Preparado por Ian Storkey

Departamento de Finanzas Públicas

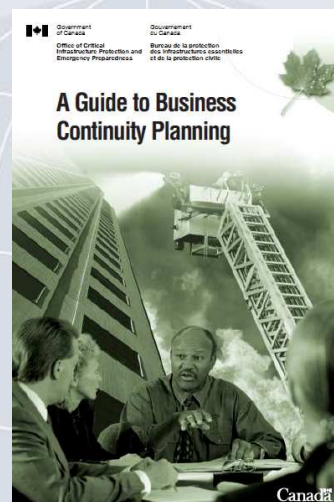
FONDO MONETARIO INTERNACIONAL

Francia: Secretariado General de la Defensa y Seguridad Nacional (del despacho del Primer Ministro)



- Estos son lineamientos que deben utilizar todos los Ministerios y Entidades Públicas clave
- Los “Ministerios Económicos”, liderados por el de Economía y Finanzas, tienen un coordinador común para los temas de continuidad operativa, seguridad de la información, y defensa y seguridad nacional, que tiene un reporte funcional al SGDSN, además de reportar al MEF
- Su alcance va más allá de la Continuidad de estos Ministerios. El enfoque es el de la articulación de la resiliencia de las actividades económicas que cubren (por ejemplo, comercio exterior y producción de energía) y se articulan con el sector privado.

Gobiernos de Australia y Canadá



Australia (AOFM)

Australian Office of Financial Management
Annual Report 2011-12

- 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)

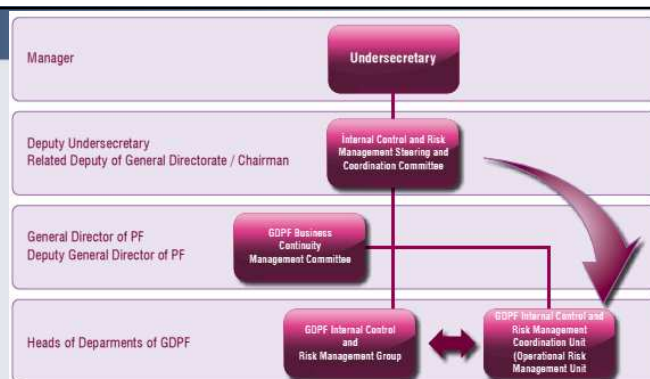
ANNUAL REPORT 2011
AGENCE FRANCE TRÉSOR

- 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)



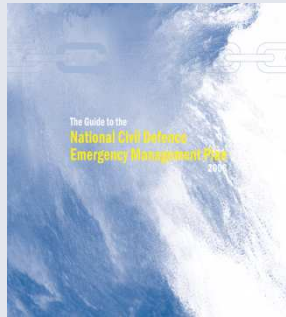
En el 2011, como resultado de estudios iniciados por el Comité de Continuidad de Negocios constituido con la aprobación de la Subsecretaría, se elaboró el documento “Política de Gestión de la Continuidad de Operaciones de Tesorería”. La Dirección General de Finanzas Públicas (DGPF) realizó sus labores 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.

Nueva Zelanda

4 fases:

- reducción
- preparación
- respuesta
- recuperación

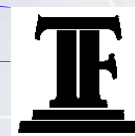


El caso de México: TESOFE plan de continuidad de operaciones

TRIARA
Centro de Datos
de TI de
Querétaro



Tesorería de la
Federación



Banco de
México



Centro Alterno
de Datos



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



**MHCP
tiene
contrato
con
SONDA**

SONDA
Sitio Alterno
en el norte
Bogotá



Banco de la
República

Ministerio de
Hacienda y
Crédito Público



Opción 1: bajo costo

Sede Alternativa
(frío o caliente)



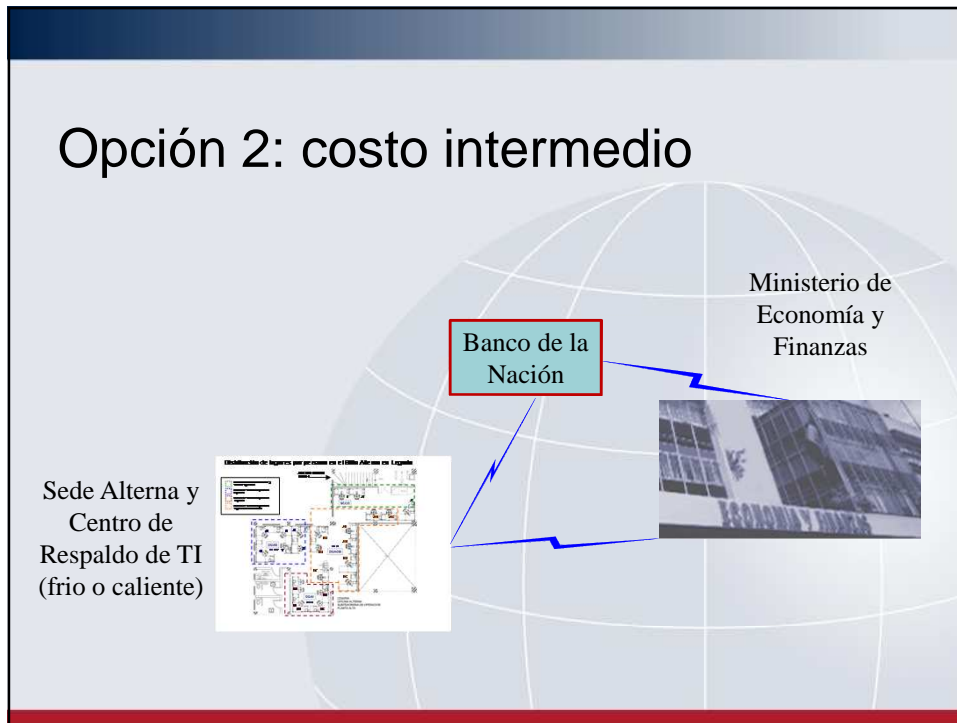
Banco de la
Nación

Ministerio de
Economía y
Finanzas



Transferencia de datos

Opción 2: costo intermedio



Opción 3: costo alto

