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

FONDO MONETARIO INTERNACIONAL

Departamento de Finanzas Públicas

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

Preparado por Ian Storkey

Distribución autorizada por Sanjeev Gupta

Noviembre de 2011

Números de clasificación JEL:	H12, H60, H63, H83
Palabras clave	continuidad de las operaciones, plan de recuperación en caso de desastres, riesgo operacional, gestión del riesgo operacional, operaciones de tesorería
Dirección electrónica del autor	ian@storkeyandco.com

This page intentionally left blank

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

Preparado por Ian Storkey

En esta Nota Técnica[1] se abordan las siguientes cuestiones:

- Definición de gestión del riesgo operacional y su aplicación a las operaciones de tesorería.
- Definición de planificación de la continuidad de las operaciones y de la recuperación en caso de catástrofe y su importancia para las operaciones de tesorería.
- Formulación y puesta en práctica de un plan de continuidad de las operaciones y de recuperación en caso de catástrofe mediante un proceso de seis pasos prácticos, e incorporación del plan en las operaciones cotidianas de tesorería.
- Factores necesarios para la activación del plan de recuperación en caso de catástrofe y procedimientos básicos de activación.

INTRODUCCIÓN

La gestión del riesgo financiero es un aspecto muy importante de las operaciones de tesorería de todo ministerio de Hacienda. Sobre el ministerio de Hacienda recae la responsabilidad de gestionar una cantidad muy importante de activos y pasivos y numerosas transacciones de alto valor, probablemente muchas más que cualquier otro ministerio o dependencia del gobierno. El elevado importe de las operaciones significa que cualquier exposición al riesgo puede tener consecuencias financieras negativas para el presupuesto y el balance del gobierno en general. Pero los errores o las fallas también pueden ocasionar graves daños de reputación y de índole política al ministerio de Hacienda, puesto que las operaciones de tesorería son competencia de este.

El ministerio de Hacienda está potencialmente expuesto —y tendrá un particular apetito de exposición— a una amplia gama de riesgos. En el gráfico 1 se ilustran los riesgos percibidos:

[1]Nota: Ian Storkey es un asesor internacional especializado en operaciones de gestión de deuda pública y caja del gobierno y figura en la lista de expertos que contrata el Departamento de Finanzas Públicas (FAD). Esta Nota Tecnica se ha enriquecido con los comentarios de Mario Pessoa (FAD), Israel Fainboim (FAD), Mike Williams (asesor) y la Tesorería de la Federación de México. El autor asimismo quisiera agradecer a los gobiernos de Australia, Chile, Turquía y el Reino Unido por la información facilitada.

Gráfico 1. Riesgos de tesorería percibidos

- **Riesgos financieros:** Tradicionalmente son gestionados por una unidad de gestión de riesgo ubicada en el ministerio de Hacienda; la categoría abarca los riesgos de mercado, de liquidez y de crédito.
- **Riesgos de negocio:** Como leyes nuevas, cambios de gobierno, evolución macroeconómica y cualquier otro factor que afecte el entorno del ministerio de Hacienda; la gestión de estos riesgos suele formar parte del proceso de planificación empresarial.
- **Riesgos operacionales:** Abarcan una gama de peligros, desde la pérdida de personal esencial, fallas de liquidación de pagos e incumplimiento, hasta el robo, la falla de sistemas y los daños de las instalaciones. La gestión del riesgo operacional tiene por objeto garantizar la integridad y la calidad de las operaciones del ministerio de Hacienda y las actividades de tesorería mediante el uso de diversas herramientas, como auditorías, políticas de contratación, sistemas de control y planes de continuidad de las operaciones.

En muchos países la noción del riesgo operacional no es muy conocida, y son muy pocos los ministerios de Hacienda que cuentan con un plan de continuidad de las operaciones y recuperación en caso de catástrofe (PCO/PRC). A menudo un plan de ese tipo se percibe como algo aplicable solo al sector privado y no atrae mayormente la atención de la alta gerencia. Esto se debe a que este tipo de planificación no se considera importante ni se reconoce como una prioridad; a que se asignan recursos insuficientes al establecimiento y mantenimiento de un marco de gestión del riesgo operacional, incluido el PCO/PRC; a que la responsabilidad se delega en los encargados de la tecnología de la información, y a que se convierte en un proyecto especial y no en una parte integrante de las operaciones cotidianas de tesorería. La negligencia de la gerencia a menudo se debe a la creencia de que "eso no nos pasará a nosotros".

El problema obviamente es que la gestión del riesgo operacional abarca una gran cantidad de aspectos, y a menudo se considera que cubre prácticamente todo, con excepción de los riesgos de mercado, liquidez y crédito. A diferencia del riesgo de mercado o de crédito,

el riesgo operacional es un riesgo endógeno del ministerio de Hacienda. Aparte de eventos externos como catástrofes naturales, el riesgo está ligado al entorno operativo, a la naturaleza y complejidad de las operaciones de tesorería, a los procesos y sistemas vigentes y a la calidad de la gestión y de los flujos de información. No suele existir una presión de tipo regulatorio a favor de la adopción de medidas adecuadas para vigilar y controlar los riesgos operacionales y mantener un PCO/PRC, como sucede en el caso de los bancos centrales.

En el presente documento se sobreentiende que las referencias al ministerio de Hacienda (MH) comprenden las operaciones de tesorería (gestionadas por el tesorero), a pesar de que algunos países cuentan con un departamento o un organismo aparte encargado de las actividades de tesorería. Una unidad de gestión de la deuda también puede formar parte del ministerio de Hacienda o puede estar constituida independientemente (por ejemplo, como una oficina de gestión de la deuda). La unidad o la oficina de gestión de la deuda pueden realizar algunas de las operaciones de tesorería, como la gestión de caja, aunque estas por lo general se realizan en coordinación con el ministerio de Hacienda.

Introducción a la gestión del riesgo operacional

Definición

En el Acuerdo Basilea II elaborado por el Banco de Pagos Internacionales (BPI)[2], el riesgo operacional se define como "el riesgo de pérdidas debidas a deficiencia o fallas en los procesos, el personal y los sistemas internos o a acontecimientos externos". La definición incluye explícitamente el riesgo jurídico, pero excluye el riesgo estratégico y el riesgo de reputación. Si bien esta definición y las prácticas adecuadas establecidas por el Comité de Basilea de Supervisión Bancaria y el COSO, y ampliadas útilmente por entidades como TransConstellation, han sido formuladas principalmente para el sector bancario y financiero, los principios rectores bien pueden aplicarse a las operaciones de tesorería[3]. Lo que se necesita es un marco de gestión del riesgo operacional que se adapte al alcance y la naturaleza de las operaciones de tesorería y al entorno operativo.

Para fines de tesorería, las categorías de riesgos, como riesgo de mercado (riesgo cambiario y de tasa de interés), riesgo de liquidez y riesgo de crédito son relativamente bien conocidas; sin embargo, el riesgo operacional no lo es. Los tesoreros del gobierno están empezando a comprender la gestión del riesgo operacional y la importancia que reviste para sus tesorerías. En el recuadro 1 figura un resumen de los riesgos operacionales que afectan a la tesorería. Los planes de continuidad de las operaciones deben ser una parte integrante del marco de gestión del riesgo operacional de tesorería.

[2]Acuerdo Basilea II "Convergencia internacional de medidas y normas de capital. Marco revisado. Versión integral", publicado por el Banco de Pagos Internacionales en junio de 2004.

[3]El Comité de Supervisión Bancaria de Basilea está integrado por representantes de 28 países, que conforma un foro del BPI para actividades regulares de cooperación sobre cuestiones relacionadas con la supervisión bancaria. El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) es una iniciativa conjunta de cinco organizaciones del sector privado, y está enfocado en el elaboración de marcos y directrices sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude. TransConstellation es un organismo belga sin fines de lucro que se dedica al procesamiento de transacciones financieras, y sus miembros incluyen entidades como Banksys, Euroclear, Fin-Force, SWIFT y The Bank of New York (oficina de Bruselas).

Recuadro 1. Riesgos operacionales típicos de tesorería

- Fallas de infraestructura y tecnología relacionadas con sistemas informáticos, energía, telecomunicaciones, datos y registros físicos.
- Incidentes de imposibilidad de acceso a las instalaciones, ya sea por inaccesibilidad o daño de las instalaciones.
- Dependencia de otros proveedores de servicios clave, como el banco central o bancos comerciales, proveedores de telecomunicaciones y servicios de Internet y otras operaciones tercerizadas, o fallas de recursos debidas a incidentes como las pandemias.
- Errores o fallas humanas debidas a falta de recursos, conocimientos, capacitación, políticas, procedimientos, delegaciones, códigos de conducta y deficiencias en la gestión.
- Incumplimiento de obligaciones reglamentarias, jurídicas o contractuales, laborales o de otro tipo, incluidos los objetivos de la gerencia y la obligación de declaración de información.
- Catástrofes naturales y regionales relacionadas con terremotos, tsunami, inundaciones fuertes, huracanes/tifones, erupciones volcánicas, incendios graves, derrumbamientos, disturbios civiles o actos de terrorismo.

¿Qué es la gestión del riesgo operacional (GRO)?

El tesorero debe ser consciente de que los aspectos principales de los riesgos operacionales constituyen una categoría aparte de riesgos que deben ser gestionados, y debe aprobar y revisar periódicamente el marco de gestión del riesgo operacional aplicable a la tesorería. El marco debe definir el riesgo operacional y debe sentar los principios para la determinación, evaluación, vigilancia y control o mitigación de los riesgos operacionales. Puede establecerse un comité de riesgos que se encargue de la supervisión de este proceso.

La alta gerencia de la tesorería debe encargarse de aplicar el marco de gestión del riesgo operacional. El marco debe aplicarse de manera coherente en todas las operaciones de tesorería, y todos los niveles del personal deben comprender sus responsabilidades con respecto a la gestión del riesgo operacional. La alta gerencia asimismo debe encargarse de formular políticas, procesos y procedimientos para gestionar los riesgos operacionales en todas las actividades, procesos y sistemas de tesorería y debe cerciorarse de que antes de que se introduzcan o se emprendan actividades, procesos y sistemas, los riesgos operacionales inherentes se sometan a una evaluación y gestión adecuadas.

La tesorería debe implantar un proceso para efectuar un monitoreo regular de los incidentes que puedan perturbar las actividades o que puedan repercutir gravemente en las operaciones de tesorería. Debe realizarse un reporte periódico de información pertinente al tesorero y a funcionarios de alto rango en el ministerio de Hacienda. La tesorería debe contar con políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales potencialmente más graves; asimismo, debe examinar periódicamente el marco de GRO y modificar sus estrategias de limitación y control del riesgo en función de la estrategia y los objetivos generales de gestión del riesgo del gobierno. La tesorería debe disponer de un plan de con-

tinuidad de las operaciones y de recuperación en caso de catástrofe, a fin de garantizar su capacidad para funcionar ininterrumpidamente y limitar las pérdidas en el caso de cualquier perturbación de las operaciones.

Una vez que se haya establecido sólidamente un marco para la gestión del riesgo operacional, la tesorería debe considerar recurrir a auditores internos y externos para examinar y evaluar el marco de manera independiente. En circunstancias ideales, los auditores deberían realizar periódicamente, de manera directa o indirecta, una evaluación independiente de las políticas, los procedimientos y las prácticas de tesorería en función de los riesgos operacionales.

La gestión del riesgo operacional aplicada a las operaciones de tesorería

Como se señala en la introducción, el riesgo operacional es una categoría amplia, que a menudo parece abarcar todo menos los riesgos de mercado, liquidez y crédito. La formulación de un marco de GRO puede ser un proceso evolutivo, ya que implica la inversión de tiempo y esfuerzo no solo para determinar y comprender los riesgos, sino también para formular técnicas de mitigación en un entorno de cambio constante. No es necesario tratar de lograr la perfección desde el comienzo. El marco puede desarrollarse y aplicarse de manera escalonada, a medida que mejoren las técnicas y que el personal de tesorería comprenda mejor los riesgos y las técnicas de mitigación. Para que el marco tenga éxito, es sumamente importante desarrollar una cultura de consciencia del riesgo en todos los aspectos de tesorería y cerciorarse de que todo el personal participe en la formulación y la aplicación del marco.

En la primera etapa de desarrollo del marco, la alta gerencia debe comprender y transmitir al personal la importancia asignada a la gestión del riesgo operacional y la necesidad de que el personal participe y coopere constantemente. Los principios descritos anteriormente que se aplicarán a la gestión del riesgo operacional deben ser trasmitidos de manera clara al personal y deben incorporarse en las actividades cotidianas de tesorería. Cada gerente de departamento tiene que responsabilizarse de la gestión del riesgo operativo en el ámbito que le corresponda.

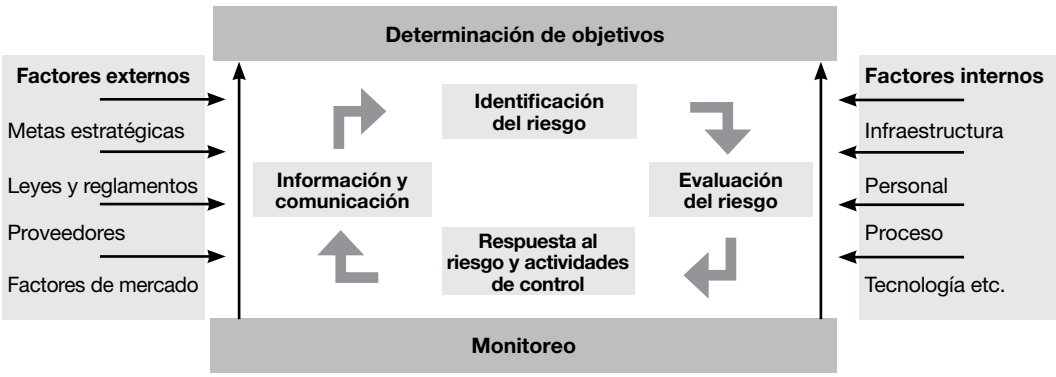
Se recomienda designar a un "responsable de la gestión del riesgo" que asuma la gestión del riesgo operacional en general. El responsable impulsará y guiará el proceso en toda la tesorería, coordinará la declaración de datos al tesorero y a la alta gerencia y formulará las políticas y los procedimientos de GRO adecuados y el entorno de control. En teoría, el responsable debería tener antecedentes y experiencia pertinentes, si bien esto a menudo no será posible. No obstante, existen oportunidades de capacitación profesional en gestión de riesgo operacional y planificación de la continuidad de las operaciones que podrían considerarse.

Una vez establecida la estructura, el desarrollo y mantenimiento de un marco de GRO para la tesorería deben seguir un proceso de seis pasos[4]:

- Comprender y documentar las actividades de negocio.
- Determinar, evaluar y medir los riesgos.
- Formular estrategias de gestión del riesgo.

[4]Puede consultarse más información sobre estos pasos en "Guidance for Operational Risk Management in Government Debt Management", publicado por el Banco Mundial en marzo de 2010.

Gráfico 2. Modelo de gestión de riesgo operacional de Turquía



- Aplicar políticas de gestión de riesgos, límites y controles.
- Monitorear los resultados y el cumplimiento de las políticas, límites y controles.
- Establecer procesos para la mejora continua del marco de GRO.

En el gráfico 2 y el recuadro 2 figuran ejemplos del proceso de GRO del ministerio de Hacienda de Turquía y Chile, respectivamente[5].

En el caso de las operaciones de tesorería, los proveedores de servicios, como el banco central y los bancos comerciales, deben demostrar que cuentan con controles y salvaguardias adecuadas para el almacenamiento o procesamiento de datos relacionados con los sistemas bancarios. La tesorería debe analizar con el banco central este requisito y debe recomendar el uso de la Norma Internacional sobre Contratos de Aseguramiento (ISAE) No. 3402, denominada Informe de Aseguramiento de Controles en una Organización Prestadora de Servicios, que es una norma de auditoría ampliamente reconocida y formulada por la Junta Internacional de Estándares de Auditoría y Aseguramiento (International Auditing and Assurance Standards Boards, IAASB)[6]. Los exámenes de auditoría de servicios realizados conforme a la ISAE No. 3402 son ampliamente reconocidos, ya que demuestran que una organización que presta servicios ha sido sometida a una auditoría exhaustiva de sus objetivos y actividades de control, la cual suele incluir controles de tecnología de la información y procesos conexos. La ISAE No. 3402 es una directriz de fuente fidedigna en virtud de la cual el banco central y los bancos comerciales pueden divulgar a la tesorería sus actividades y procesos de control en un formato uniforme.

La gestión del riesgo operacional debe ser una responsabilidad que todo el personal de tesorería debe compartir y comprender. El personal debe tener una noción de la exposición al riesgo operacional en sus respectivos ámbitos de competencia y de cómo podría afectar la continuidad de las operaciones, y debe encargarse de gestionar las exposiciones que estén dentro de su propio control. Los altos funcionarios deben encargarse de detectar y monitorear los riesgos en sus respectivas unidades y de garantizar que las actividades de control funcio-

[5]Hakan Tokaç y Mike Williams (2011, de próxima publicación).

[6]El 15 de junio de 2011, la ISAE No. 3402 reemplazó la Declaración de Normas (o Estándares) de Auditoría (SAS) No. 70, sobre Organizaciones que prestan Servicios, que había sido elaborada por el Instituto Estadounidense de Contadores Públicos Autorizados (American Institute of Certified Public Accountants, AICPA).

Recuadro 2. El caso de Chile: Esquema del proceso de gestión de riesgos

El objetivo principal es "contar con un sistema de control interno eficiente y cumplir con un proceso de gestión del riesgo estructurado, coherente y coordinado con miras a alcanzar de forma eficaz y eficiente las metas y los objetivos institucionales".

La gestión de riesgos tiene los siguientes objetivos:

- Determinar riesgos y oportunidades
- Analizar los riesgos del proceso
- Evaluar los riesgos
- Establecer el tratamiento de los riesgos
- Monitorear y examinar (retroalimentación, comentarios)
- Elaborar la matriz de riesgo

Paso 1: Política de riesgo

- Definir funciones y responsabilidades de los procesos de gestión de riesgos
- Determinar los procesos fundamentales para la mejora de la calidad del servicio
- Comunicar y publicar la política, que ha de ser coherente con la Política de Calidad del Servicio

Paso 2: Proceso de análisis

- Plantear los procesos propuestos por la Política de Calidad del Servicio
- Identificar y clasificar los riesgos según tipo

Paso 3: Elaboración de la matriz

- Clasificar los procesos transversales
- Establecer ponderaciones de procesos y subprocesos
- Determinar el tipo de riesgo
- Justificar la ponderación estratégica

Paso 4: Establecer orden de clasificación (*ranking*)

- Establecer un orden de clasificación según el proceso
- Establecer un orden de clasificación según subprocesos

Paso 5: Establecer un plan de tratamiento

- Establecer medidas, cronogramas, responsabilidades, impacto potencial (reducción, aceptación, evasión, distribución) e indicadores de desempeño, medir el objetivo del período

Paso 6: Monitoreo y examen

- Generar informes
- Monitorear
- Formular diagnósticos y propuestas de mejora

Matriz estratégica de riesgo

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

nen de la manera prevista y conforme a las prioridades fijadas por el tesorero. La experiencia internacional demuestra que, para que todo esto funcione bien, la GRO es más eficaz si se designa a un "responsable de la gestión del riesgo" que esté ubicado en la unidad de gestión del riesgo que lleve a cabo también otras funciones de gestión del riesgo.

La unidad de gestión del riesgo, incluido el responsable de la gestión del riesgo, cumple dos funciones. En primer lugar, promueve el desarrollo del proceso de gestión del riesgo, monitorea los resultados y la ejecución y presenta informes al tesorero. En segundo lugar, asesora a los altos funcionarios en la identificación de los riesgos y la planificación de las actividades de control. En la práctica, la unidad suele evolucionar con el tiempo, y de ser el factor principal que impulsa el establecimiento del marco de gestión del riesgo operacional, incluido el PCO/PRC, pasa a cumplir una función de facilitación o asesoramiento una vez que el marco está funcionando fluidamente.

Planes de continuidad de las operaciones y recuperación en caso de catástrofe

Introducción de planes de continuidad y recuperación en caso de catástrofe

La planificación o la gestión de la continuidad de las operaciones comprende la formulación, la implementación y el mantenimiento de las políticas, los marcos y los programas para ayudar a la tesorería a hacer frente a perturbaciones que afecten a las operaciones y a desarrollar la capacidad de recuperación de la tesorería. Esa capacidad se desarrolla abordando la probabilidad de que se produzcan perturbaciones y haciendo frente a las consecuencias cuando efectivamente se produzcan las perturbaciones. De ahí que sea importante contar con un marco de GRO y de planificación de la continuidad de las operaciones. Esa planificación ayuda a evitar incidentes o eventos perturbadores, a prepararse y a responder ante su impacto y a gestionar las consecuencias y la recuperación.

La continuidad de las operaciones implica mantener disponibles de manera ininterrumpida todos los recursos necesarios para apoyar el desempeño de las operaciones esenciales de tesorería. Las estrategias y las decisiones operativas de tesorería se basan en el supuesto de la continuidad de las operaciones. Un evento que viole esa suposición representa un acontecimiento significativo en la vida de cualquier tesorería, e incide en su capacidad para cumplir sus objetivos operacionales y en la reputación de la tesorería y el gobierno. Entre otros aspectos, la planificación de la continuidad de las operaciones consiste en adoptar medidas con el objeto de evitar de antemano que ocurran eventos que provoquen la interrupción de las operaciones. También abarca el establecimiento de medidas de respuesta adecuadas en caso de que ocurra un evento.

Por lo tanto, los planes de continuidad de las operaciones son la parte de la GRO que establece medidas eficaces en función de los costos (costo-efectivas) en caso de que se produzca un evento. Como tales, los planes están relacionados con eventos reales —un riesgo materializado— y las medidas de respuesta necesarias. En tal sentido, complementan el proceso general de gestión del riesgo operacional, que guarda relación, ante todo, con la posibilidad de que

eventos de riesgo puedan materializarse, y con el análisis y la gestión activa de tales eventos. La tesorería se enfrenta a varios riesgos. Estos pueden ser de origen externo, en cuyo caso están en gran medida fuera del control inmediato de la tesorería, o de origen interno. Los riesgos internos surgen tanto a nivel estratégico (todos los ámbitos del ministerio de Hacienda) o a nivel operacional (procesos de negocio).

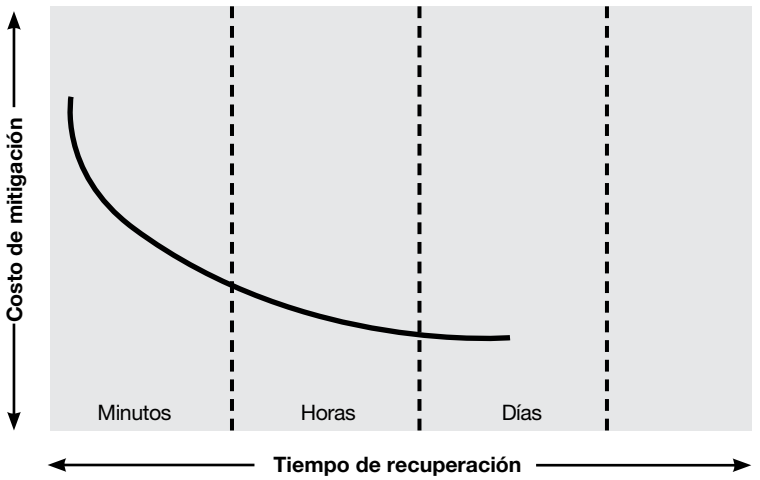
Los planes de continuidad de negocios deben abordar un subconjunto de riesgos operacionales en los que factores ambientales o la deficiencia de los controles operacionales elevan el potencial de pérdida o daño en las operaciones de tesorería (incluido personal, información, infraestructura e instalaciones). Con el apoyo de todo el personal, la tesorería debe mantener un PCO/PRC que tanto el gobierno como las contrapartes externas consideren una práctica sólida, y que cumplirá un papel importante en la gestión del riesgo operacional. El PCO/PRC se centra en mejorar la capacidad de recuperación y en garantizar que se hayan adoptado técnicas de mitigación en aspectos en que se haya determinado que existe una combinación de probabilidades altas o muy altas y un impacto fuerte o catastrófico. También se recomienda cubrir incidentes de baja probabilidad pero que pueden tener un impacto fuerte o muy fuerte. La definición de estos incidentes se expone en la sección sobre el análisis de impacto en las actividades que aparece más adelante.

La tesorería debe seleccionar el método de intervención en el riesgo que sea más eficaz en función de los costos y más idóneo para cada actividad, usando una o más de las siguientes estrategias:

- **Prevención y evasión,** para reducir o eliminar la probabilidad de que ocurra un evento, por ejemplo, mediante la instalación de generadores de energía de respaldo, el uso de más de un proveedor de servicios de telecomunicaciones, la capacitación del personal y la adopción de políticas y procedimientos para prevenir el fraude.
- **Transferencia,** para transferir los riesgos a terceros mediante seguros o contratos en que los PCO/PRC están incorporados en acuerdos de nivel de servicio.
- **Contención,** para que el impacto potencial de un evento se limite a las primeras etapas, mediante el uso de controles u otras técnicas basadas en la aplicación de políticas y procedimientos de detección de fraude, el establecimiento de procedimientos jerarquizados para que la gerencia de la tesorería pueda responder de inmediato en el caso de que un evento comience a agravarse y la designación de más de una persona encargada de realizar una tarea o actividad en particular.
- **Aceptación y recuperación,** para que aun en el caso de que ocurra un evento o interrupción, las operaciones de tesorería puedan reanudarse satisfactoriamente mediante un plan de recuperación en caso de catástrofe, plan que es sometido a pruebas periódicas en el emplazamiento de recuperación (un emplazamiento alternativo).

Algunas estrategias pueden llevarse a cabo a un costo mínimo, pero habrá que tener en cuenta las ventajas y desventajas relativas entre el costo de prevención y/o recuperación y el tiempo de recuperación que necesita la tesorería. Por lo tanto, un aspecto clave que la tesorería debe considerar es la disyuntiva entre el costo y el tiempo de recuperación, como se puede observar en el gráfico 3. Esa disyuntiva no será lineal, ya que el costo de acortar el tiempo de

Gráfico 3. Ventajas y desventajas relativas entre costo y tiempo de recuperación



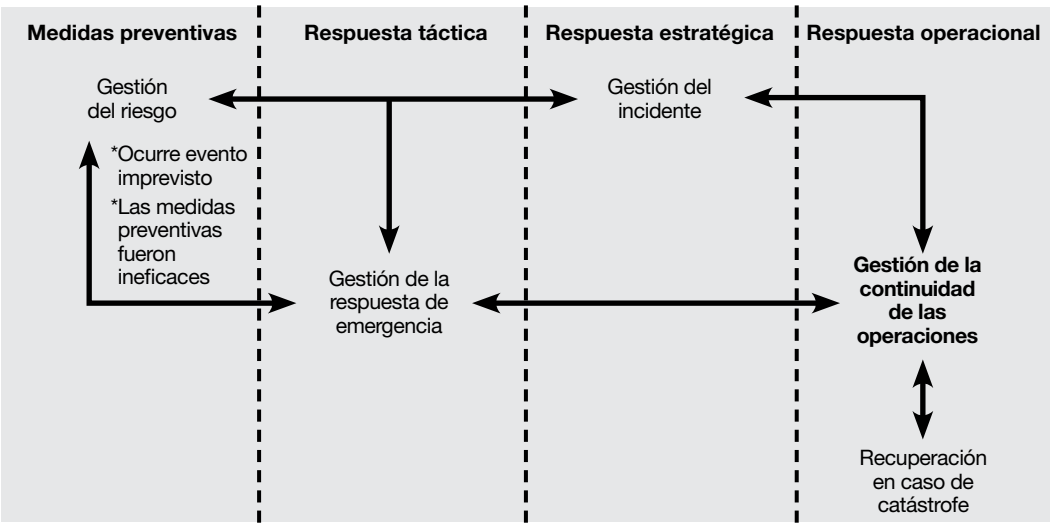
Este gráfico se extrajo de la página 4 del documento de la Australian National Audit Office (2009), con una modificación para reflejar el carácter no lineal de los costos, dado que el costo de mitigación tenderá a aumentar exponencialmente si el tiempo de recuperación se reduce a minutos, en lugar de horas y días.

recuperación, particularmente si es necesario que las actividades, los procesos y los sistemas críticos se recuperen en minutos, implicará una inversión significativa en duplicación de sistemas, replicación de datos, redundancia de comunicaciones e infraestructura y la habilitación de un emplazamiento alternativo que pueda activarse rápidamente.

El costo de establecer y mantener un emplazamiento secundario podría ser alto, no solo en lo que se refiere a la inversión inicial en instalaciones y todo el equipo necesario, sino también en lo que atañe al mantenimiento de cada sistema y la renovación de los equipos cuando se efectúan cambios o actualizaciones en el emplazamiento primario. También es importante garantizar que el emplazamiento alternativo se encuentre a una distancia suficientemente alejada del emplazamiento primario, para que la probabilidad de que los dos emplazamientos se vean afectados por el mismo incidente o evento sea muy baja. Por ejemplo, sería importante garantizar que el emplazamiento alternativo esté ubicado en una red de energía diferente o reciba servicio de un proveedor diferente, además de pertenecer a una red o un proveedor de servicio telefónico diferente, de manera que los dos emplazamientos no se vean afectados simultáneamente. El uso regular del emplazamiento alternativo para capacitación y pruebas puede generar algunos beneficios que compensen el costo.

La recuperación de las actividades, los procesos y los sistemas más críticos de la tesorería puede tomar horas o, para ciertas actividades, entre uno y dos días, aunque podrían existir algunas actividades o procesos que quizá deban concluir forzosamente al final de la jornada. En estos casos es posible que resulte más eficaz en función de los costos preparar procesos manuales que puedan activarse en caso de que se produzca una perturbación. La disyuntiva entre costo y tiempo de recuperación debe considerarse en el análisis del impacto en las operaciones y de las estrategias de mitigación que ponga en práctica la tesorería.

Gráfico 4. Relaciones en la gestión de una perturbación de las operaciones



Fuente: Australian National Audit Office (2009), pág. 2.

Importancia del PCO/PRC para las operaciones de tesorería

En el gráfico 4 se muestra la relación entre el riesgo operacional, la respuesta de emergencia, el incidente y la gestión o planificación de la continuidad de las operaciones tras una perturbación o un evento. Estas actividades de gestión pueden dimensionarse de acuerdo con el contexto operativo de la tesorería. Es posible que en una tesorería pequeña, no compleja, o en que las consideraciones de tiempo son menos críticas, una parte o la totalidad de estas actividades estén combinadas. En una tesorería grande, compleja o dispersa geográficamente, el uso de diferentes equipos de respuesta de emergencia, gestión del incidente y gestión de la continuidad de las operaciones hace más necesaria la definición de funciones y responsabilidades claras así como una comunicación eficaz. La presente Nota Técnica (TNM) se centra en la gestión o planificación de la continuidad de las operaciones.

Las políticas de la tesorería con respecto a los planes de continuidad de las operaciones deben cumplir las siguientes condiciones:

- Realizar un análisis de impacto en las actividades y formular estrategias de mitigación, que garanticen la continuidad de las actividades, las operaciones y los componentes tecnológicos en caso de que el entorno existente no esté disponible.
- Elaborar y mantener un plan integral de continuidad de las operaciones y recuperación en caso de catástrofes (PCO/PRC) para garantizar la capacidad de recuperación de las actividades esenciales o críticas de tesorería.
- El PCO/PRC debe elaborarse conforme a normas internacionales, como la norma de gestión de la continuidad de las operaciones BS-25999 o la norma ISO-27031 de la Organización Internacional de Normalización.
- Presentar al tesorero y a la alta gerencia del ministerio de Hacienda un informe anual sobre el estado del PCO/PRC.

El PCO/PRC de la tesorería debe ser una parte integrante del marco de gestión del riesgo operacional y debe elaborarse para garantizar el cumplimiento de los siguientes objetivos:

- Protección de los intereses del gobierno en términos de reputación, reporte e impacto sobre los recursos, e impacto sobre las operaciones de tesorería.
- Cumplimiento por parte del gobierno de todas las obligaciones reglamentarias, contractuales y de mercado.
- En el caso de que una actividad esencial o crítica se vea perturbada por un incidente o evento, restablecimiento de la actividad dentro del lapso de recuperación estipulado en el plan de recuperación en caso de catástrofe.
- EL PCO/PRC es una parte integrante de las operaciones cotidianas de la tesorería y se actualiza regularmente mediante capacitación permanente del personal y la realización de pruebas.

Proceso de seis pasos para la elaboración de un PCO/PRC

Para la elaboración de un PCO/PRC se recomienda seguir el siguiente proceso de seis pasos (cada paso se describe en más detalle en la siguiente sección):

- **Paso 1:** Documentar las operaciones y los procesos y sistemas críticos.
- **Paso 2:** Realizar un análisis de impacto en las operaciones para evaluar la probabilidad y el impacto.
- **Paso 3:** Elaborar un PCO/PRC (incluir terceros).
- **Paso 4:** Implementar o actualizar el PCO/PRC.
- **Paso 5:** Capacitar para implantar el PCO/PRC en las operaciones cotidianas de la tesorería.
- **Paso 6:** Realizar pruebas y actualizaciones (anuales).

Elaboración de un PCO/PRC

Paso 1: Documentar las operaciones

El primer paso consiste en que la tesorería comprenda plenamente las actividades, los procesos y los sistemas y determine los riesgos clave que podrían incidir en las operaciones. Para este fin se pueden usar mapas de procesos y análisis de flujo, además de los manuales de procedimientos existentes. El funcionario responsable de la gestión del riesgo, recomendado anteriormente, puede supervisar este proceso para garantizar que las operaciones se comprendan ampliamente y que el enfoque y la terminología sean coherentes. Esto se debe hacer de manera que se logre un equilibrio entre el grado de detalle y de utilidad para la alta gerencia y el proceso en general.

Lo esencial es identificar los procesos y sistemas críticos y el período de tiempo en que estos procesos y sistemas son requeridos. Así se determinará el carácter crítico de cada actividad, proceso y sistema, en función del lapso (minutos, horas o días) en que la tesorería no es capaz de mantener las operaciones esenciales o críticas. La tesorería debe elaborar y mantener un cuadro de sistemas esenciales o críticos (véase un ejemplo en el cuadro 1, más adelante).

La tesorería especificará el período en que cada sistema es necesario, los datos que se recuperarán del sistema de respaldo y el lugar donde se puede acceder al sistema en caso de que se produzca un incidente.

CUADRO 1. SISTEMAS CRÍTICOS DE LA TESORERÍA			
Sistema	**Lapso (minutos, horas o días)**	**Respaldo de los datos (momento y ubicación)**	**Lugar de acceso (emplazamiento alternativo o centro de datos)**

Paso 2: Análisis de impacto en las operaciones

Un análisis del impacto en las operaciones (*business impact analysis*) abarcará a todas las personas responsables de las operaciones de tesorería, incluido el personal subalterno, ya que ayuda a comprender los riesgos y a desarrollar una cultura de consciencia del riesgo dentro de la tesorería. Esto se puede lograr mediante seminarios y sesiones de "lluvia de ideas" para cada una de las funciones de tesorería. Para cada categoría de riesgo operacional y cada incidente que pueda afectar a la tesorería, como se indica en el cuadro 2, la tesorería debe evaluar las exposiciones al riesgo derivadas de un incidente o evento que incida en sus operaciones. Para esto es necesario evaluar por separado la probabilidad y el impacto, por ejemplo, usando una combinación de probabilidad Muy alta / Alta / Mediana / Baja / Muy baja, y de impacto Catastrófico / Importante / Moderado / Secundario / Insignificante desde la perspectiva de la reputación, el reporte (la declaración de datos) y los recursos, o el impacto en las operaciones de la tesorería, como se explica en el cuadro 3.

No todos los riesgos operacionales tendrán la misma importancia para la tesorería, ya que la importancia dependerá específicamente del entorno y de los riesgos que se enfrenten. En el caso de la tesorería, hay tres tipos de impacto que quizá deban considerarse en el análisis:

- **Impacto reputacional:** Que puede dar origen a una pérdida de confianza por parte del gobierno, pérdida de confianza del mercado, cobertura por parte de los medios de comunicación y/o una investigación ministerial o parlamentaria de alto nivel.
- **Impacto en el reporte (la declaración de datos) y en los recursos:** Que pueden ser reportados al gobierno o la alta gerencia dentro del gobierno —o externamente a reguladores—, y/o tiempo considerable dedicado a este problema.
- **Impacto en las operaciones de la tesorería:** Que puede dar origen al incumplimiento de los pagos y otras obligaciones de la tesorería y a la interrupción de las actividades de tesorería necesarias para el funcionamiento eficaz del gobierno.

CUADRO 2. INCIDENTES QUE PUEDEN AFECTAR A LA TESORERÍA		
Fallas de infraestructura y tecnología		
Interrupción de energía	Falla de hardware	Falla de software
Corrupción de datos, incluidos virus	Falla de LAN/WAN/Intranet/ Internet	Inundación interna (aspersores, tuberías)
Falla de la red de telecomunicación de voz	Robo de equipos	Robo de datos o de información
Mantenimiento deficiente	Daño accidental	Sabotaje
Incidentes que impiden el acceso a las instalaciones		
Peligro de inundación o incendio	Infracción sanitaria y de seguridad	Accidente con sustancias químicas peligrosas
Fuga de gas o sustancia química	Acción industrial o motín	Bomba o amenaza terrorista
Incendio o explosión en el edificio	Inundación interna/externa	Sabotaje o terrorismo
Fallas de proveedores de servicios esenciales o recursos de los que se depende		
Falla de proveedores de servicios clave (teléfono, internet, bancos, etc.)	Terceros (entidades) proveedores de servicios (banco central y otras operaciones tercerizadas)	Impacto del incidente en equipos o grupos críticos (pandemia, viajes, incidentes en grupos)
Fallas de personal, gerencia y otras fallas humanas		
Error humano (que puede obedecer a capacitación deficiente o supervisión inadecuada)	Capacitación deficiente o supervisión inadecuada (que puede dar origen a error humano o ejecución de transacciones no autorizadas)	Incumplimiento del código de conducta o de las directrices sobre conflicto de intereses
Falta de orientación sobre las políticas (que puede dar origen a decisiones desacertadas o actividades no autorizadas)	Escaso conocimiento del entorno de riesgo (que puede dar origen a riesgos innecesarios o desconocidos)	Delegación deficiente de funciones (que puede dar origen a ejecución de transacciones no autorizadas)
Incumplimiento de las prácticas administrativas (que puede dar origen a errores de procesamiento)	Riego de persona clave (que puede dar origen a error humano cuando esa persona está ausente)	Prácticas fraudulentas, corruptas, o deshonestas (que pueden dar origen a pérdidas financieras y desprestigios políticos)
Incumplimiento de obligaciones reglamentarias, jurídicas, laborales y otras obligaciones		
Obligaciones jurídicas/ reglamentarias (por ejemplo, cumplimiento de contratos de préstamos)	Directivas de administración (por ejemplo, políticas y procedimientos internos)	Manuales de procedimientos y autoridades delegadas
Obligaciones de declaración de datos (por ejemplo, a autoridades superiores o instituciones internacionales)	Obligaciones contractuales (por ejemplo, obligaciones de servicio de la deuda)	Normas sanitarias y de seguridad (por ejemplo, leyes y regulaciones nacionales sobre el trabajo)
Catástrofes naturales y regionales		
Terremoto fuerte	Huracán, ciclón o tornado	Tsunami
Erupción volcánica	Incendios graves	Disturbios civiles
Inundación grave	Derrumbamientos	Actos de terrorismo

En cada uno de estos tres casos, la tesorería debe evaluar los factores que provocarán el impacto conforme a cada una de las cinco categorías de evaluación. En el cuadro 3 se presenta un ejemplo. Obviamente, este cuadro variará según las actividades que le competen a la tesorería y las prioridades asignadas o implícitas en las operaciones de la tesorería.

CUADRO 3. MÉXICO: MARCO DE CRITERIOS PARA DETERMINAR EL IMPACTO			
Evaluación del impacto	**Impacto reputacional**	**Impacto en el reporte (la declaración de datos) y los recursos**	**Impacto en las operaciones de la tesorería**
Catastrófico	Pérdida de confianza del gobierno Pérdida de confianza del mercado Pérdida de confianza, por ejemplo, estados, y ministerios Amplia cobertura mediática Investigación ministerial de alto nivel [o dimisión] Sanciones financieras o legales	Declarados al presidente o al congreso Cantidad considerable de tiempo dedicada a hacer frente a este impacto (es decir, más de 20 personas-días)	Incumplimiento de pagos de alta prioridad en la fecha de vencimiento (personal, servicio de la deuda, devolución de impuestos, a Estados, impuestos) Errores de pago, como acreditación de fondos en una cuenta equivocada o entrega después de la fecha de vencimiento Incurrir en sanciones por incumplimiento de pago (como recurso no presupuestario) en servicio de la deuda, devoluciones de impuestos, nómina y transferencias a entidades (con repercusiones políticas) Sobregiro en cuenta bancaria Imposibilidad de efectuar transferencias entre cuentas de tesorería debido a falla de los sistemas de pago del banco central y los bancos comerciales Imposibilidad de recibir ingresos o acceder a los ingresos Imposibilidad de efectuar transacciones en moneda extranjera (recibir, comprar, vender o invertir) Imposibilidad de acceder a las cuentas bancarias de la tesorería o a sus balances y operaciones
Importante	Deterioro de las relaciones del gobierno Pérdida temporal de la confianza del mercado Cobertura mediática moderada Investigación ministerial Relaciones deterioradas con contribuyentes y renuencia a pagar impuestos	Declarados al ministerio Cantidad importante de tiempo dedicada a hacer frente a este impacto (es decir, entre 10 y 20 personas-días)	Incumplimiento de pago a los contratistas del gobierno y/o de los subsidios, que tendrían consecuencias financieras y políticas derivadas de los atrasos en los pagos Demora en el pago al titular de un depósito o en la aplicación por fondos Imposibilidad de determinar el concepto de los ingresos Imposibilidad de emitir informes sobre operaciones y registro de los ingresos y formularios oficiales Imposibilidad de emitir certificados de de pagos recibidos para entregar a los contribuyentes Imposibilidad de abrir la bóveda que protege los formularios oficiales Informes incoherentes de las cuentas bancarias y sus transacciones y saldos

CUADRO 3. MÉXICO: MARCO DE CRITERIOS PARA DETERMINAR EL IMPACTO

Evaluación del impacto	Impacto reputacional	Impacto en el reporte (la declaración de datos) y los recursos	Impacto en las operaciones de la tesorería
Moderado	Mayor atención del gobierno mexicano La confianza del mercado no se ve afectada Cobertura mediática reducida o inexistente Considerable atención prestada dentro del ministerios de Hacienda La confianza de los depositantes y contribuyentes se ve moderadamente afectada	Declarados a la entidad responsable del monitoreo de la tesorería Cantidad moderada de tiempo dedicada a hacer frente a este impacto (es decir, entre 5 y 10 personas-días)	Incumplimiento de las transferencias de fondos a otras entidades del gobierno para gastos menores (fondos rotativos), y de obligaciones que podrían pagarse al siguiente día hábil
Secundario	Cierta atención por parte del gobierno Ninguna cobertura mediática Investigación interna del ministerio de Hacienda Atención de los contribuyentes	Incluidos en informes internos de tesorería Cierta cantidad de tiempo dedicada a hacer frente a este impacto (es decir, menos de 5 personas-días)	Retardo del mismo día en el envío de la disposición de pagos al banco central Solicitud oficial al banco central para ampliar los horarios de atención de los bancos Imposibilidad de colocar inversiones Imposibilidad de entregar informes puntuales a la oficina de contabilidad Entrega parcial de formularios oficiales y billetes Imposibilidad de acceso a la base de datos de los funcionarios autorizados para dar órdenes de desembolso, así como a las firmas autorizadas para el retiro de depósitos de terceros
Insignificante	Las relaciones del gobierno y mercado quedan intactas Ninguna cobertura mediática	No se necesitan informes Mínima cantidad de tiempo dedicada a hacer frente a este impacto (es decir, menos de 5 personas-días)	Imposibilidad de operar desde las oficinas principales, que causa una demora del horario de ejecución de pagos Errores en los archivos electrónicos de los ingresos enviados a los centros contables Retardo del mismo día en el pago a los depositantes Retardo del mismo día en la entrega de la orden de formularios oficiales

Este cuadro se basa en el marco elaborado por la Tesorería de la Federación de México. El autor agradece el esfuerzo del personal de la Tesorería, que ayudó a preparar el marco de criterios de impacto.

Para cada operación, proceso y sistema utilizados en el análisis de impacto en las operaciones, la tesorería asignará una probabilidad de que ocurra un incidente/evento y una calificación de impacto en el caso de que el incidente/evento se materialice. Las actividades a las que la tesorería les asigne calificaciones de 4 y 5 en el caso de un incidente se identifican en

el cuadro 4. Dependiendo de su nivel de tolerancia del riesgo, la tesorería podría incluir la calificación 3, particularmente cuando el impacto podría ser catastrófico en lo que se refiere a la reputación, la declaración de datos y los recursos, o cuando el impacto afecta a las operaciones de tesorería.

El último componente clave del análisis de impacto en las operaciones es la importancia crítica del momento en que se activa cada sistema y proceso en las distintas operaciones de tesorería. Para esto es necesario evaluar el tiempo máximo que la tesorería puede permanecer sin acceso al sistema o proceso antes de que las operaciones se vean afectadas sustancialmente en cualquier de las categorías antes indicadas. Es normal categorizar cada sistema o proceso utilizando períodos de tiempo tales como fin de la jornada, dentro de las 24 horas (o menos si es necesario), las 48 horas, las 72 horas, 5 días hábiles, o más de 5 días hábiles. Se puede usar el cuadro 1 para estos fines.

Es necesario formular una estrategia detallada de mitigación para los incidentes o eventos con calificaciones de 4 y 5 en el cuadro 4. Si el número de incidentes o eventos con estas calificaciones es alto, la matriz indicará claramente que se necesita un emplazamiento alternativo y un plan de recuperación en caso de catástrofe bien documentado. En tal caso, en el PCO/PRC se estipulará la siguiente información crítica 1) sistemas y procesos críticos; 2) lista de contacto de funcionarios y equipos clave; 3) procedimientos estandarizados para la activación de los planes; y 4) detalles de la infraestructura de recuperación, incluidos los equipos y documentación, que se almacenarán en la oficina de la tesorería (emplazamiento principal) y en el lugar donde se lleven a cabo las tareas de recuperación (emplazamiento alternativo).

Paso 3: Elaboración de un plan de continuidad de las operaciones y recuperación en caso de catástrofe

Una vez concluido el análisis de impacto en las operaciones, la tesorería debe formular estrategias que se centren en mejorar la capacidad de recuperación y en garantizar la adopción de técnicas de mitigación para los incidentes con calificaciones de 4 y 5 en el cuadro 4. Para estos aspectos la tesorería debe seleccionar la gestión del riesgo más adecuada y eficaz en función de los costos, utilizando una o más de las estrategias de respuesta descritas anteriormente. Posteriormente se le presenta a la alta gerencia un informe sobre el plan de continuidad de las operaciones en relación con los principales riesgos; las técnicas para mitigar, controlar o limitar los riesgos; las medidas recomendadas para hacer frente a las principales exposiciones, incluida la activación de un plan de recuperación en caso de catástrofe; y una estimación de los costos. La alta gerencia puede sopesar los costos y riesgos antes de tomar decisiones y de solicitar la aprobación del tesorero o de las autoridades máximas del ministerio de Hacienda.

Una parte integrante del plan de continuidad de las operaciones será el plan de recuperación en caso de catástrofe (PRC), en el que se documenta el componente de recuperación del plan de continuidad de las operaciones. El plan facilita i) la transición fluida a las operaciones de recuperación tras un incidente o evento importante (o catástrofe); ii) la jerarquización de las operaciones de recuperación en el caso de una perturbación prolongada; y iii) el retorno a las operaciones normales lo antes posible. Un aspecto importante del PRC es la estructura de los equipos de gestión de incidentes y recuperación y la administración de las funciones de

CUADRO 4. MATRIZ RIESGO/IMPACTO

		Nivel de impacto del riesgo				
		Insignificante	Secundario	Moderado	Importante	Catastrófico
Nivel de probabilidad del riesgo	Muy alto	3	4	4	5	5
	Alto	2	3	4	4	5
	Medio	2	2	3	4	4
	Bajo	1	2	2	3	4
	Muy bajo	1	1	2	2	3

apoyo de tecnología de la información. En el gráfico 5 se presenta un ejemplo de la estructura del centro de mando.

Paso 4: Ejecución del PCO/PRC

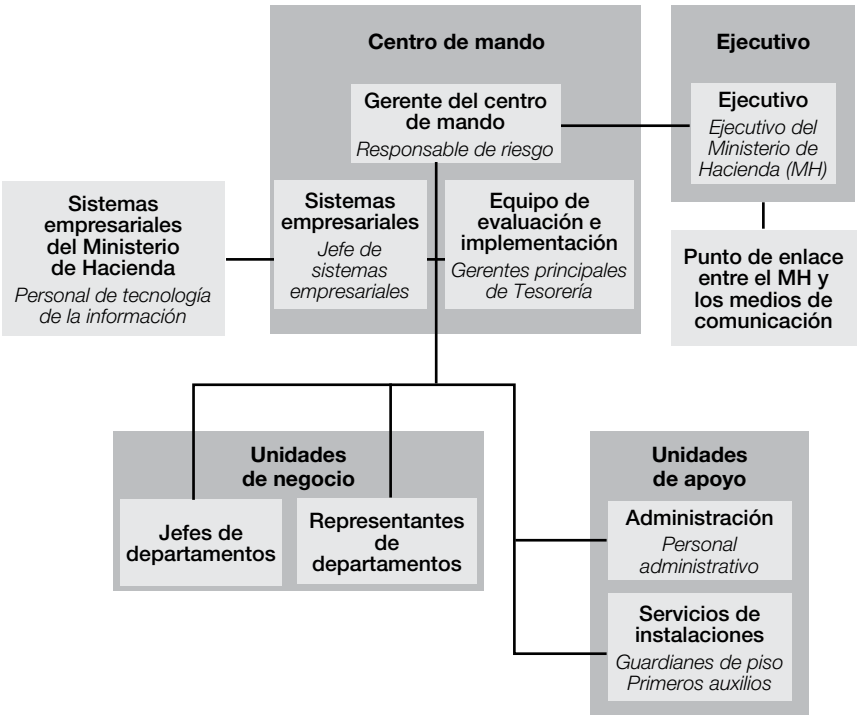
Una vez que el PCO/PRC haya sido aprobado, el responsable o la unidad de gestión del riesgo pueden supervisar su ejecución y su integración en las políticas y los procedimientos más generales de monitoreo y control de la gestión del riesgo operacional de la tesorería. Esto comprende concientizar a las partes externas para que estén cubiertas todas las actividades ajenas a la tesorería, pero que forman parte del marco del PCO/PRC y la gestión del riesgo operacional, de tal manera que comprendan sus respectivas funciones en lo que atañe a la continuidad de las operaciones y durante la etapa de activación cuando lo exija el PRC. El responsable o la unidad de gestión del riesgo se encargarán de efectuar y garantizar el cumplimiento de los requisitos estipulados en el PCO/PRC.

La tesorería también debe introducir el requisito de que los proveedores externos cuenten con un PCO/PRC y que dicho plan esté incluido en acuerdos de nivel de servicio o en un memorando de entendimiento. Entre esos proveedores estarían el banco central, los proveedores de servicios bancarios y de telecomunicaciones y los proveedores externos pertinentes de tecnología de la información. También sería útil que la tesorería integre su PCO/PRC con otros sistemas críticos, como el sistema integrado de información financiera (SIIF) del gobierno, el sistema de registro y gestión de la deuda y otros sistemas fundamentales del ministerio de Hacienda.

Paso 5: Capacitación

Los integrantes del personal de la tesorería deben comprender sus funciones y responsabilidades conforme a las políticas y los procedimientos del PCO/PRC y la gestión del riesgo operacional en sentido más general. Es posible que deban asumir responsabilidades adicionales con el fin de adoptar y mantener estrategias de reducción o mitigación de riesgos en sus respec-

Gráfico 5. Estructura del centro de mando del PRC



tivos ámbitos de responsabilidad. EL PCO/PRC debe incluir una sección sobre capacitación, con descripciones de ejercicios y escenarios de capacitación, e indicaciones de la frecuencia de la capacitación.

El responsable o la unidad de gestión del riesgo deben encargarse de la capacitación, que debe impartirse a todo el personal de la tesorería y debe abarcar lo siguiente:

- Presentaciones para concientizar a los empleados activos (también podrían incorporarse en el programa de orientación o iniciación para los nuevos empleados).
- Entrega de un manual de capacitación.
- Capacitación interactiva (Intranet).

Si la tesorería tiene un emplazamiento alternativo, este puede ser un lugar valioso para el suministro de capacitación, ya que las pruebas regulares en el emplazamiento alternativo pueden integrarse con el programa de capacitación. Por ejemplo, esto permitirá al personal de tesorería familiarizarse con el emplazamiento alternativo y con la manera en que se pueden llevar a cabo las operaciones de tesorería en el caso de que se produzcan un incidente o evento que den lugar a una reubicación. Si bien es normal recurrir al personal experimentado que se considera crítico para las operaciones de tesorería, este proceso puede ampliar los conocimientos de manera que se reduzca el "riesgo de persona clave". Además, es posible que el personal esencial no esté disponible cuando ocurran el incidente o evento, y esto permitirá recurrir a otro personal para obtener el respaldo necesario en esta situación. Algunas organizaciones tienen permanentemente personal en rotación en el emplazamiento alternativo. Esto

CUADRO 5. MARCO DE FRECUENCIA DE MANTENIMIENTO Y PRUEBAS DEL PCR	
Mantenimiento	**Frecuencia**
Examen y actualización de la documentación del PCO/PRC	Semestral
Pruebas de recuperación de la tecnología	Semestral
Pruebas de familiarización del personal	Anual
Pruebas de escenarios (hipótesis)	Anual
Prueba completa (simulacro de incidente)	Anual

garantiza la familiarización con los procedimientos y facilita un arranque rápido de los mismos. Además, permite la continuidad de las operaciones en el caso de destrucción total del emplazamiento primario.

Paso 6: Pruebas y actualizaciones regulares

Aunque el PCO/PRC pueda parecer muy bien diseñado y concebido, la experiencia internacional demuestra que muy rara vez funcionará en la práctica si no se realizan pruebas realistas y exigentes. Los sistemas y procesos críticos de tesorería deben someterse a pruebas anuales y el PCP/PRC debe actualizarse en función de los resultados de cada prueba y de la necesidad de efectuar mejoras continuas. Es importante que cada sistema y proceso sea sometido a pruebas individuales. Las pruebas pueden crear perturbaciones, ya que exigen el compromiso del personal para garantizar la disponibilidad de recursos suficientes. No se recomienda que el PCO/PRC se pruebe como un todo, ya que esto podría absorber demasiados recursos y afectar las operaciones normales, salvo que la prueba se realice en un fin de semana. Una opción sería un ejercicio de prueba basado en una situación hipotética (puede comprender un ensayo o la activación del PRC y una prueba del emplazamiento alternativo), pero se considera que la única manera de probar plenamente el PCR es mediante una prueba "en vivo". Las pruebas podrían realizarse conjuntamente con las pruebas de otros sistemas, como el Sistema Integrado de Información Financiera (SIIF) y el PRC del banco central. En el cuadro 5 se presenta un ejemplo de mantenimiento y prueba del PCO/PRC.

El mantenimiento del PCO/PRC implica un proceso permanente de monitoreo para evaluar su eficacia y para determinar si son coherentes con las políticas y los procedimientos más generales de la gestión del riesgo operacional. Esto se lograría mediante una combinación de actividades permanentes de monitoreo y pruebas periódicas, incluidas pruebas anuales del PRC. El monitoreo permanente se realiza en el curso normal de las operaciones de tesorería, y es responsabilidad en primera instancia de los gerentes de área, en tanto que la responsabilidad de coordinación recae sobre el responsable o la unidad de gestión del riesgo. Como ya se señaló, el PCO/PRC puede mejorarse con el tiempo a medida que se acumule experiencia, sobre todo si existe un historial sobre incidentes o eventos y sobre su impacto en la reputación, la declaración de datos y los recursos y las operaciones de tesorería. El proceso de seis pasos descrito anteriormente debe revisarse anualmente, aunque el primer paso puede consistir tan solo en una actualización de las operaciones, los procesos y los sistemas en función de los cambios derivados de la evaluación previa.

Todas las operaciones nuevas deben comunicarse al responsable o a la unidad de gestión del riesgo durante la etapa de planificación. Los cambios de los procedimientos y sistemas vigentes también se comunicarán al responsable o a la unidad de gestión del riesgo. Los estudios de las operaciones deben incluir una evaluación de los riesgos de continuidad de las operaciones, y los presupuestos de proyectos deben incluir una dotación suficiente para implementar medidas adecuadas de prevención y recuperación. No se debe poner en funcionamiento ningún sistema u operación nuevos hasta que se hayan implementado y probado los mecanismos adecuados de recuperación.

Activación del plan de recuperación en caso de catástrofe

Estructura del centro de mando

Si ocurren un incidente o evento que tengan un impacto en las actividades esenciales o críticas de tesorería y/o que exijan la reubicación del emplazamiento primario, se establecerá un proceso de gestión de incidentes en un centro de mando para administrar la reubicación y/o la recuperación. El gráfico 5 muestra las personas y equipos, y las interrelaciones entre las personas encargadas de gestionar una recuperación después de un incidente o evento. Ello garantiza que cuando ocurran un incidente o evento, existirá una estructura de gestión de incidentes bien definida para asegurar:

- El flujo eficiente de información.
- Un proceso de toma de decisiones coherente.
- Una comunicación eficaz de las decisiones.

En caso de producirse un incidente o evento, el personal designado previamente y que esté disponible se trasladará al emplazamiento alternativo para reanudar las operaciones. Ello simplificará la logística de planificación de la recuperación, reducirá la confusión entre el personal, y permitirá la preparación y el establecimiento de planes de desvío telefónico con los proveedores de telecomunicaciones con antelación. Es preciso un cierto grado de flexibilidad para adaptarse a los diferentes incidentes. No obstante, el número de emplazamientos de recuperación utilizados deberá mantenerse al mínimo para facilitar la comunicación con el personal y la gestión de emergencias.

En caso de producirse un incidente o evento que requieran la evacuación del edificio o impidan el acceso al edificio, deberá establecerse un centro de mando de emergencia en un emplazamiento alternativo (si existe) o en algún emplazamiento designado. Algunos incidentes o eventos tal vez no afecten a todas las unidades de operaciones o a todo el edificio. En este caso, tal vez sería más práctico trasladar al personal afectado a salas de reuniones o a otros espacios desocupados con la asistencia de proveedores de sistemas de operaciones y servicios de apoyo. La posibilidad de trabajar desde casa es una opción cada vez más viable y eficaz en algunos incidentes. Por ejemplo, con la pandemia de H1N1, los miembros del personal de la Tesorería de México que se vieron obligados a permanecer en sus casas pero que se sentían bien para trabajar recibieron el apoyo necesario para trabajar desde sus casas. Esta posibilidad es más viable si se dispone de sistemas habilitados para la web, buenos servicios de Internet, sistemas de cifrado y cortafuegos instalados con antelación.

La función primaria del centro de mando es la coordinación, el control y el intercambio de información dentro de la tesorería. El equipo del centro de mando pone en marcha el proceso de toma de decisiones cuando existen problemas e incidentes importantes que puedan requerir, o no, la reubicación de las operaciones. La gestión de crisis y las decisiones de carácter inmediato también forman parte de la responsabilidad del equipo. Estas funciones incluirán la gestión de las comunicaciones con partes externas, como los medios de comunicación y los principales grupos externos.

Los miembros del centro de mando y los grupos asociados comprenden los representantes siguientes:

- La alta gerencia del ministerio de Hacienda y el tesorero.
- Representante(s) de los sistemas operativos/informáticos.
- Representantes de los servicios de apoyo, como recursos humanos, administración y/o servicios diversos.

La responsabilidad de todos los miembros del centro de mando será reunirse en el emplazamiento del centro de mando de emergencia (en un emplazamiento alternativo, si está disponible, u otro emplazamiento específico) a fin de:

- Establecer un punto central de contacto para todas las cuestiones relacionadas con las operaciones de recuperación para el personal, los proveedores y los medios de comunicación.
- Facilitar la recopilación y verificación de la información relacionada con la situación de emergencia y los avances de la recuperación.
- Facilitar la distribución de instrucciones al personal, las contrapartes y otros terceros afectados.

Las responsabilidades del centro de mando comprenden las siguientes:

- Tomar rápidamente la decisión de poner en marcha las actividades de recuperación basándose en la información disponible.
- Coordinar las comunicaciones con el ministerio de Hacienda.
- Gestionar las comunicaciones con los medios de comunicación, directamente o a través de una persona de contacto con estos medios.
- Mantener el flujo de información con el personal, las contrapartes y otros principales interesados.
- Aprobar montos significativos de gasto relacionados con la recuperación.
- Monitorear los requisitos de cumplimiento a lo largo del proceso de recuperación.
- Garantizar el mantenimiento de una seguridad eficaz en los emplazamientos donde se pongan en marcha actividades de recuperación.
- Determinar el aumento gradual de las actividades de recuperación si se producen incidentes significativos.
- Planear y gestionar el restablecimiento y la nueva puesta en funcionamiento del emplazamiento primario de la tesorería.

Los sistemas de operaciones deberán abordar la recuperación de los sistemas y procesos esenciales/críticos de infraestructura informática. Algunos implicarán la participación de ter-

Recuadro 3. El caso de la Oficina de Gestión de Deuda del Reino Unido (UK DMO): Gestión de la Recuperación de las Operaciones

Objetivos

Además del plan de gestión de incidentes, se necesitan procedimientos adicionales para garantizar una recuperación eficaz y oportuna de las operaciones de la empresa. El Plan de Gestión de la Recuperación de las Operaciones presenta una guía de los pasos que se deben seguir.

El Plan de Gestión de la Recuperación de las Operaciones se utiliza conjuntamente con el componente de análisis de impacto del PCO. Mientras el Análisis de Impacto aporta un informe de situación sobre el impacto potencial de un incidente en ciertas funciones críticas, la Gestión de la Recuperación de las Operaciones se centra en la recuperación de las operaciones tras el incidente.

El Análisis de Impacto indica medidas y soluciones alternativas para procesos críticos específicos. La Gestión de la Recuperación de las Operaciones sirve para evaluar y determinar métodos para el restablecimiento de operaciones clave de las empresas.

Pasos de la recuperación de las operaciones

Paso 1: Evaluación de las operaciones (gerentes y/o jefes de equipo)

- Determinar la situación de cada actividad empresarial.
- Confirmar la disponibilidad del sistema y de los recursos de tecnología de la información para cada actividad empresarial.
- Evaluar las condiciones del mercado después de un incidente de alcance generalizado.
- Determinar la situación de las partes interesadas clave.

Paso 2: Informe de situación (gerentes y/o jefes de equipo)

Proporcionar informes de situación a la alta gerencia sobre cada actividad, con la siguiente información:

- Actividades de alta prioridad que deben completarse.
- Actividades que se suspenderán.
- Sistemas disponibles.
- Necesidades y disponibilidad de recursos.
- Comentarios de las partes interesadas.

ceros para poner en marcha el desvío de llamadas y ayudar en la asignación de otros servicios de comunicaciones alternativos. La tesorería garantizará que los acuerdos sobre el nivel de los servicios con los principales proveedores de información reflejen los requisitos de recuperación e incluyan disposiciones sobre la participación en los ejercicios de prueba.

Los sistemas de operaciones también abarcarán la gestión de los siguientes aspectos:

- El restablecimiento del correo electrónico, Internet y otros servicios esenciales de comunicación.
- El restablecimiento de los sistemas bancarios y de pago electrónico con el banco central y los bancos comerciales.

Paso 3: Establecimiento de prioridades

- La gerencia responsable de cada actividad empresarial debe determinar el orden de prioridades de cada área.
- Los gerentes principales deben confirmar el orden de prioridad de las operaciones empresariales clave y comunicar dicho orden a los gerentes y jefes de equipo.
- El departamento de tecnología de la información debe ser informado sobre las necesidades de los sistemas de acuerdo con las prioridades empresariales.

Paso 4: Toma de decisiones

- Todas las decisiones estratégicas deben referirse a los foros adecuados.
- Deben tomarse decisiones sobre si se realiza una suspensión o cancelación de cualquier operación específica.
- Las decisiones deben documentarse y comunicarse a las áreas empresariales pertinentes.

Paso 5: Implementación

- Cada equipo debe llevar a cabo las actividades acordadas utilizando las soluciones alternativas manuales indicadas en el análisis de impacto.
- El personal debe informar a la gerencia sobre el avance y la conclusión de actividades, para que se puedan realizar evaluaciones y priorizaciones posteriores.
- Toda declaración hecha ante las partes interesadas con respecto a cualquier actividad revisada o suspendida.

Paso 6: Retorno a la oficina principal

Una vez que el gerente de las instalaciones haya autorizado el retorno a la oficina principal y que la infraestructura de sistemas y telecomunicaciones esté restablecida, el proceso de retorno exigirá lo siguiente:

- Confirmación de que la infraestructura ha sido restablecida sobre la base de pruebas realizadas por las distintas áreas, bajo la coordinación de los jefes de equipos.
- Un plan detallado de migración elaborado por el equipo de gerencia de tecnología de la información, que incluya la sincronización y las pruebas de contracción (*cutting back*) de los sistemas y la reinstalación del emplazamiento de recuperación en caso de catástrofe; los detalles de este plan dependerán de la índole y el impacto del incidente original.
- El grupo de alta gerencia debe reunirse y acordar una estrategia de información que incluya un anuncio al mercado y la comunicación de la decisión de retorno (re-migrar) a los contactos clave.

- La recuperación de las copias de seguridad de datos y el restablecimiento de los datos para reanudar las funciones críticas en el emplazamiento de recuperación.
- La adquisición, configuración e instalación de terminales de trabajo adicionales, equipo periférico, redes y cableado, líneas telefónicas y teléfonos.
- La adquisición, configuración e instalación de servidores adicionales y servicios de telefonía, para respaldar la intensificación de las actividades de recuperación cuando la nueva puesta en funcionamiento del emplazamiento primario de la tesorería pueda llevar, por ejemplo, más de dos semanas.

- Punto de contacto con terceros para proporcionar apoyo a los usuarios.
- Gestión del proyecto sobre tecnología para el restablecimiento y la nueva puesta en funcionamiento del emplazamiento primario de la tesorería.
- Migración al funcionamiento normal de las operaciones y desmantelamiento de los servicios temporales.

Se prevé que los servicios de apoyo (el personal de recursos humanos, administración y servicios diversos) rendirán cuentas al equipo del centro de mando y proporcionarán asistencia según las indicaciones recibidas. Estas actividades podrán incluir las siguientes:

- Efectuar un seguimiento del paradero del personal y velar por su seguridad y bienestar.
- Responder a las llamadas de teléfono y transmitir mensajes.
- Ponerse en contacto con el personal para transmitir mensajes y confirmar disponibilidad.
- Organizar los servicios de restauración, alojamiento, asesoramiento en caso de trauma, pagos de emergencia, organización del cuidado de niños, rotación de personal, etc.
- Garantizar la seguridad en el emplazamiento del incidente y otros emplazamientos temporales de recuperación.
- Facilitar la tramitación de las solicitudes de rembolso relacionadas con seguros y las compras de emergencia.
- Redirigir el correo y los mensajeros.

Respuesta de emergencia

Después de producirse un incidente o evento, la respuesta de emergencia comprenderá las fases siguientes:

- **Evacuación y contención:** Incluye las acciones adoptadas por el personal de respuesta de emergencia para contener el incidente, garantizar la seguridad del personal, evitar nuevos daños o pérdidas y garantizar la seguridad del emplazamiento primario de la tesorería.
- **Evaluación de los daños:** Los miembros del centro de mando (incluidos los sistemas de operaciones y los servicios de apoyo) evaluarán la magnitud del incidente o evento y decidirán el plan de acción y/o recuperación.
- **Decisión sobre la recuperación:** Tomando como base la evaluación de los daños, se adoptará una decisión con respecto al proceso y al emplazamiento para recuperar las funciones esenciales/críticas de las operaciones. Si el incidente o evento puede aislarse y contenerse, se adoptarán medidas para restablecer las operaciones de tesorería utilizando políticas y procedimientos operativos estándar. Es importante que todo el personal sea consciente de su papel durante la operación de recuperación y que la información sobre la recuperación sea suministrada claramente y de manera regular al personal. Esto significará que el personal podrá permanecer en sus casas hasta que se les indique lo contrario, o trasladarse al emplazamiento alternativo.

El objetivo de la respuesta de emergencia es reducir al mínimo el riesgo al que pueden verse expuestas las actividades y operaciones de la tesorería en el emplazamiento primario. Esto se consigue reduciendo o, si es necesario, deteniendo las actividades hasta que se establezca la

infraestructura de recuperación, con el objetivo primordial de restablecer las actividades críticas en un plazo de 24 horas (o si es necesario para el final del día) y otras actividades esenciales en un plazo de 48-72 horas.

Cada funcionario recibirá una hoja de información y detalles de los contactos importantes (tesorería, ministerio de hacienda y banco central), incluidos los números de teléfono del domicilio y del móvil, los detalles de los contactos externos y los principales contactos en la tesorería. Esta información puede suministrarse en un formato que pueda almacenarse en los teléfonos móviles del personal de la tesorería, iPads, computadoras portátiles u otros medios, para facilitar el acceso y la recuperación de esta información.

Recuperación de las operaciones

Una vez decidido el plan de recuperación, las etapas del proceso de recuperación de las actividades serán las siguientes:

- **Activar la infraestructura de recuperación:** Se pondrá en marcha el plan de continuidad de las operaciones para las necesidades de infraestructura de sistemas y comunicaciones, desviando las llamadas entrantes y trasladando los principales sistemas de producción al emplazamiento alternativo. Para todas las aplicaciones esenciales o críticas, los datos serán accesibles en el emplazamiento alternativo tras el restablecimiento de los sistemas, o a través de un centro de datos, si es aplicable. En el caso de los servicios proporcionados por terceros como el banco central, el personal podrá trasladarse a las instalaciones de terceros para trabajar utilizando los sistemas designados.
- **Operaciones de nivel de supervivencia:** Inicialmente las operaciones en la tesorería o en el emplazamiento alternativo deberán limitarse a las actividades básicas. En el caso de funciones en las que el tiempo es un factor menos crítico, estas pueden interrumpirse temporalmente y/o dar instrucciones al personal para que trabajen desde sus casas.
- **Intensificación de las operaciones:** Si el incidente es tan grave que es necesario pasar un período prolongado fuera del emplazamiento primario (generalmente de más de dos semanas), pueden intensificarse las operaciones, dado que un período prolongado al nivel de supervivencia de las operaciones podría agravar los efectos del incidente, afectar a la capacidad de la tesorería de mantener las actividades, procesos y sistemas esenciales o críticos, y generar una tensión excesiva para el personal. En la medida de lo posible, pueden determinarse de antemano las prioridades con respecto a la intensificación de las operaciones estableciendo calendarios indicativos para la recuperación de cada operación o proceso.
- **Nueva puesta en funcionamiento del emplazamiento primario:** Comprende las medidas adoptadas para salvar, recuperar o remplazar la propiedad, las instalaciones y los servicios dañados o perdidos en el emplazamiento primario y el proceso de poner en marcha nuevamente las operaciones en el emplazamiento primario.

Evaluación ex post del incidente

Puede realizarse una evaluación exhaustiva para garantizar la actualización y el mejoramiento del plan de recuperación y de la infraestructura, tomando como base la experiencia del incidente. Concretamente, cada uno de los procesos de seis pasos puede ser examinado para

detectar las deficiencias y omisiones, y los resultados pueden usarse para revisar y actualizar el PCO/PRC. En esta fase esto puede provocar cambios en los procesos operativos y en la infraestructura básica, incluidos los sistemas y las instalaciones en el emplazamiento alternativo, así como mejoras de la capacitación y en las pruebas, entre otros cambios.

Conclusión

El establecimiento del marco de GRO, incluido el PCO/PRC, debería considerarse una prioridad para cualquier tesorería, dados los riesgos operacionales que afrontan estas instituciones y las funciones y actividades críticas que desempeñan. El desarrollo del PCO/PRC no debería considerarse un proyecto excepcional, sino que debería convertirse en parte integrante de las operaciones diarias de tesorería. El proceso de seis pasos para desarrollar, implementar, comprobar y mantener el PCO/PRC permitirá a la tesorería definir las medidas prácticas necesarias para asegurar que este proceso se lleve a cabo.

Referencias

Australian National Audit Office (2009), *Business Continuity Management: Building Resilience in Public Sector Entities*, Best Practice Guide, junio de 2009 [http://www.anao.gov.au/~/media/Uploads/documents/business_continuity_management_.pdf].

Banco Mundial (2010), *Guidance for Operational Risk Management in Government Debt Management*, Tomas Magnusson, Abha Prasad e Ian Storkey [http://siteresources.worldbank.org/INTDEBTDEPT/RelatedPapers/22491571/OperationalRiskManagement201003.pdf].

Banco de Pagos Internacionales (2003), *Sound Practices for the Management and Supervision of Operational Risk*, Comité de Basilea de Supervisión Bancaria [http://www.bis.org/bcbs/index.htm].

British Standards Institution (2006), Business Continuity Management: Code of Practice [http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/].

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2008), *Internal Control–Integrated Framework: Guidance on Monitoring Internal Control Systems, Volumes I, II and III* [http://www.coso.org].

Hakan Tokaç y Mike Williams (2011, de próxima publicación), *Government Debt Management and Operational Risk: A Risk Management Framework, and how it was applied in Turkey*, OCDE/UE.

Organización Internacional de Normalización (2011), *1SO-27031: Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity* [http://www.iso.org/iso/catalogue_detail?csnumber=44374].

TransConstellation (2007), *Best Practices in Qualitative Operational Risk Management: The ORM Reference Guide* [http://www.transconstellation.com].

TransConstellation (2007), *Roadmap to Operational Risk Management Success: The ORM Maturity Benchmark* [http://www.transconstellation.com].

Anexo: Listas de comprobación del PCO/PRC[7]

Para la elaboración de un PCO/PRC pueden utilizarse las listas de comprobación y las planillas siguientes.

LISTA DE COMPROBACIÓN 1: EJECUCIÓN DEL PCO		
Características de una práctica adecuada PCO/PRC en las operaciones de tesorería	**Concluido Sí/No**	**Nivel de ejecución (Básico/avanzado)**
Característica 1: Se ha establecido un marco de gestión del riesgo operacional (GRO), incluido el PCO/PRC.		
Característica 2: Se han llevado a cabo actividades de capacitación y concientización acerca del PCO/PRC.		
Característica 3: Se ha realizado una evaluación del riesgo.		
Característica 4: Se ha realizado un análisis del impacto en las operaciones.		
Característica 5: Se han aplicado controles preparatorios.		
Característica 6: La tesorería ha preparado informes y la alta gerencia ha aprobado el PCO/PRC.		
Característica 7: Se han realizado pruebas y ejercicios del PCO/PRC.		
Característica 8: Un responsable de la gestión del riesgo o una unidad de gestión del riesgo se encarga del monitoreo del PCO/PRC.		

LISTA DE COMPROBACIÓN 2: IDENTIFICAR LOS SISTEMAS Y PROCESOS OPERATIVOS CRÍTICOS	
Identificar los sistemas y procesos operativos críticos	**Concluido Sí/No**
Documentar y confirmar los objetivos y criterios de desempeño de la tesorería.	
Enumerar todos los sistemas y procesos operativos críticos que respaldan el logro de los objetivos.	
Clasificar los procesos y sistemas por orden de importancia para los objetivos de la tesorería y excluir aquellos procesos que no se consideren críticos para alcanzar los objetivos.	
Examinar el organigrama funcional, a fin de identificar ámbitos generales de responsabilidad operativa.	
Obtener la documentación de apoyo disponible que proveería un resumen de los sistemas y procesos operativos críticos.	
Entrevistar a los gerentes responsables de los sistemas y procesos operativos críticos, para confirmar su entendimiento de estos sistemas y procesos.	
Considerar las interdependencias existentes en el proceso: • Dentro de la tesorería y del ministerio de Hacienda. • Con terceros o partes externas.	

[7]Las listas de comprobación se basan en Australian National Audit Office (2009) y se han modificado a fin de incluir las operaciones de tesorería.

LISTA DE COMPROBACIÓN 2: IDENTIFICAR LOS SISTEMAS Y PROCESOS OPERATIVOS CRÍTICOS	
Identificar los sistemas y procesos operativos críticos	**Concluido Sí/No**
Determinar los requisitos mínimos necesarios para llevar a cabo cada proceso crítico. Considerar: • Actividades • Recursos • Personal ○ Instalaciones (incluidos los edificios y el equipo) ○ Tecnología (incluidos los sistemas y aplicaciones de TI) ○ Telecomunicaciones ○ Registros clave • Interdependencias • Otros	
Obtener la aprobación por la alta gerencia de la lista de prioridades en materia de procesos operativos críticos.	

PLANILLA: REQUISITOS NECESARIOS PARA APLICAR CADA SISTEMA O PROCESO CRÍTICO	
Sistema o proceso operativo crítico #< >:	**<escriba el nombre del proceso>**
Actividades	
Recursos	
Personal	
Instalaciones (incluidos los edificios y el equipo)	
Tecnología (incluidos los sistemas y aplicaciones de TI)	
Telecomunicaciones	
Registros clave (incluidos los datos en papel y electrónicos)	
Procesos interdependientes (incluidos los internos y externos)	
Otros	

Nota: Repetir para cada sistema o proceso crítico.

LISTA DE COMPROBACIÓN 3: REALIZAR UN ANÁLISIS DEL IMPACTO EN LAS OPERACIONES	
Realizar un análisis del impacto en las operaciones	**Concluido Sí/No**
Recopilar la información pertinente, como por ejemplo: • Escenarios de perturbación de las operaciones • Plan de gestión de la respuesta de emergencia • Plan de gestión de incidentes • Plan en caso de pandemia • Plan de recuperación en caso de catástrofe informática	
Consultar con el personal y las unidades de operaciones clave: • Cada unidad de negocios (operaciones) de tesorería, incluida la gestión del riesgo • Servicios informáticos, incluidos los del ministerio de Hacienda • Auditoría interna • Edificios e instalaciones • Alta gerencia del ministerio de Hacienda • Terceros o partes externas	
Evaluar el impacto de una pérdida de cada sistema o proceso crítico, utilizando los criterios del análisis del impacto en las operaciones de tesorería: • Reputación • Reporte (declaración) y recursos • Operaciones de tesorería	
Identificar técnicas de procedimientos provisionales (procesamiento alternativo o manual) que se adoptarán durante la fase de recuperación.	
Determinar el período máximo tolerable de perturbación para cada sistema o proceso crítico.	
Determinar las interdependencias internas y externas críticas.	
Identificar los registros clave (en papel y electrónicos).	
Determinar el tiempo de recuperación fijado como objetivo para cada proceso crítico y sistema o aplicación informática.	
Determinar el punto de objetivo de recuperación (*recovery point objective*) de los datos electrónicos.	
Estimar el tiempo que llevará superar el trabajo pendiente acumulado durante el incidente o evento de perturbación de las operaciones.	
Obtener la aprobación por la alta gerencia del análisis del impacto en las operaciones.	

LISTA DE COMPROBACIÓN 4: EXAMINAR LAS OPCIONES PARA MINIMIZAR LAS INTERRUPCIONES (PERTURBACIONES)	
Consideraciones para seleccionar actividades y recursos alternativos	**Considerado Sí/No**
Al seleccionar actividades y/o recursos alternativos, se examinarán las actividades siguientes: • Personal • Instalaciones (incluidos los edificios y el equipo) • Tecnología (incluidos los sistemas y aplicaciones de TI) • Telecomunicaciones • Registros clave • Interdependencias • Otros	
Preparar una breve descripción de cada opción para reducir los efectos de un evento de perturbación de las operaciones.	
Determinar otros recursos necesarios y el costo de cada opción (esto tal vez requerirá información de terceros).	
Comparar las opciones de recuperación, incluido el costo, teniendo en cuenta las prioridades de recuperación y el período máximo tolerable de perturbación.	

LISTA DE COMPROBACIÓN 5: CONSIDERACIONES SOBRE EL EMPLAZAMIENTO ALTERNATIVO	
Consideraciones sobre el emplazamiento alternativo (que será activado por el PRC)	**Considerado Sí/No**
Las características del emplazamiento alternativo indican una seguridad física adecuada y controles medioambientales adecuados.	
El perfil de riesgo del emplazamiento alternativo es diferente del emplazamiento de la tesorería, de manera que es poco probable que ambos emplazamientos se vean afectados por la misma perturbación. Por ejemplo, si existe una distancia suficiente con respecto del emplazamiento primario de la tesorería, una red de energía diferente y una central telefónica diferente.	
En los contratos se especifican claramente la disponibilidad del emplazamiento alternativo y los derechos de cada suscriptor en caso de múltiples declaraciones de catástrofe.	
Monto y naturaleza de los servicios de apoyo que se proporcionarán en el emplazamiento alternativo: • Asistencia en la implementación. • Apoyo para pruebas. • Apoyo logístico. • Apoyo fuera del horario de atención.	
Número de funcionarios de la tesorería necesarios en el emplazamiento alternativo y limitaciones en el número, si las hubiera, impuestas por la instalación.	
Las limitaciones impuestas en el uso del emplazamiento alternativo y si existe o no margen para ampliar/renovar el contrato en el caso de una perturbación prolongada importante y el uso de un emplazamiento alternativo.	
El plazo de tiempo y la disponibilidad para realizar pruebas en el emplazamiento alternativo.	
La tesorería tiene la capacidad para auditar periódicamente las instalaciones de los sistemas en el emplazamiento alternativo, para garantizar que se mantenga la configuración especificada.	

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