Continuidad de Negocio en los Sistemas de Pagos de Latinoamérica y el Caribe

Evaluación del estado actual

Banco de México

Septiembre, 2008

Agradecimientos

El Banco de México agradece a los Bancos Centrales de Argentina, Brasil, Colombia, Costa Rica, Guatemala y Trinidad y Tobago por compartir sus experiencias para la realización de este análisis. Las opiniones y apreciaciones reflejadas en esta presentación son responsabilidad exclusiva de Banco de México.

Asimismo, se agradece al Centro de Estudios Monetarios de Latinoamérica (CEMLA) por su apoyo.

Contenido

1. Introducción
2. Metodología empleada
3. Resultados cuantitativos
4. Resultados cualitativos
5. Análisis
6. Conclusiones

Introducción

- Los Bancos Centrales juegan dos roles muy importantes en los sistemas de pago: son reguladores y son operadores.

- En ambos casos, es de su interés conocer el grado de confiabilidad operativa de sus sistemas de pago.

- Por tal motivo, los integrantes de este Foro encomendaron al Banco de México hacer un primer análisis de la continuidad operativa de los sistemas de pago en la región.
  - En particular, se analiza la continuidad operativa del principal sistema de pagos de alto valor del país.

Contenido

Metodología empleada
Cuestionario de recomendaciones

- El Banco de México elaboró un documento que resume, basado en su experiencia, las recomendaciones del BIS y el Banco Central Europeo para Continuidad de Negocio en los sistemas de pago.

- Con el apoyo del Cemla, se distribuyó el documento y se solicitó a los Bancos Centrales de este grupo de trabajo que evaluaran el estado de continuidad de negocio de su principal sistema de pagos de alto valor.
  - 7 Bancos Centrales respondieron a esta solicitud.

- El documento presenta 8 recomendaciones, mismas que se enlistan a continuación.

Metodología empleada
Cuestionario de recomendaciones

I. Sobre las responsabilidades de los niveles jerárquicos más altos de una organización en la administración de la continuidad de negocio.

- La responsabilidad final de la administración de continuidad de negocio (ACN), así como de su efectividad, debe recaer en los niveles jerárquicos más altos de una institución. - 9 aspectos -

II. Sobre las interrupciones operativas graves.

- El Plan debe considerar aquellos escenarios de mayor gravedad y debe existir un sitio alterno de operación y respaldo. - 3 aspectos -

III. Sobre los objetivos de recuperación.

- Deben establecerse objetivos de recuperación para las operaciones críticas, que vayan de acuerdo con el riesgo que éstas representan para el sistema de pagos. - 5 aspectos -

Metodología empleada
Cuestionario de recomendaciones

IV. Sobre las comunicaciones.

- Deben existir procedimientos y protocolos de comunicación hacia dentro de la organización y hacia entidades externas. - 5 aspectos -

V. Sobre las comunicaciones transnacionales.

- Se debe evaluar si las posibles interrupciones operativas graves que sucedan a la organización pueden tener implicaciones en otros países. - 1 aspecto -

VI. Sobre las pruebas.

- Los planes de continuidad de negocio deben probarse, en su caso actualizarse, y su efectividad debe ser evaluada. - 7 aspectos -

Metodología empleada
Cuestionario de recomendaciones

VII. Sobre las revisiones de la administración de la continuidad de negocio que deben llevar a cabo las autoridades financieras.

- Las autoridades financieras deben revisar la ACN de los participantes de los sistemas de los cuales son responsables. - 4 aspectos -

VIII. Sobre la infraestructura.

- Debe existir al menos un sitio alterno de operación y uno de respaldo de información. - 3 aspectos -

Metodología empleada
Evaluación

1. Cada recomendación se desglosa en varios aspectos muy específicos los cuales son fáciles de evaluar en términos de "si se cumple" o "no se cumple".
   - Cada aspecto se califica con 1, si se cumple, y 0 si no se cumple.
2. Sumando los aspectos que si se cumplen, se determina el **grado de cumplimiento** de cada recomendación.
   - No todas las recomendaciones tienen el mismo número de aspectos
3. Se asigna un **peso** arbitrario, entre 1 y 4, a cada recomendación, considerando su relevancia.

	Recomendación	Peso	Porcentaje
I	Responsabilidades	3	12%
II	Interrupciones graves	4	15%
III	Objetivos de recuperación	4	15%
IV	Comunicaciones	4	15%
V	Comunicaciones transnacionales	1	4%
VI	Pruebas	4	15%
VII	Revisiones a participantes	2	8%
VIII	Infraestructura	4	15%
	Totales	**26**	**100%**

Metodología empleada
Evaluación

4. Se multiplica el **porcentaje** de la recomendación por su **grado de cumplimiento**.
   - Esto permite determinar en qué tanto, relativo al total, se cumple cada recomendación.
5. Finalmente, se suman las calificaciones ponderadas obtenidas en cada recomendación.
   - Esto determina un porcentaje de cumplimiento de los principios de continuidad de negocio.
   - El puntaje final será un número entre 0 y 100%.

Metodología empleada
Evaluación

- Sin embargo, como toda metodología cuantitativa, hay aspectos cualitativos que la calificación numérica podría no reflejar. Por esta razón se solicitó a cada evaluador dar una breve descripción justificando su calificación.
- Con las descripciones recabadas, Banco de México hizo un esfuerzo por identificar características sobresalientes y áreas de oportunidad.
  - Ejemplo: problemas que han tenido varios Bancos Centrales para cumplir algunas recomendaciones, o la forma en la que los han resuelto.
- Esto permite presentar, además de los resultados numéricos por país, un conjunto de resultados cualitativos para la región.

Contenido

Resultados Cuantitativos

PAIS	I									II			III					IV					V	VI							VII				VIII			CALIF
	1	2	3	4	5	6	7	8	9	1	2	3	1	2	3	4	5	1	2	3	4	5	1	1	2	3	4	5	6	7	1	2	3	4	1	2	3	
A	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	□	■	■	■	■	■	■	■	■	■	■	■	■	□	■	87.9
B	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	□	□	■	■	□	85.8
C	□	■	□	■	■	□	■	□	□	□	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	□	■	■	■	■	■	□	■	■	■	81.3
D	■	■	■	■	■	■	□	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	72.6
E	■	■	■	■	■	■	□	□	■	□	■	■	■	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	■	■	■	■	□	■	■	■	70.3
F	■	■	□	■	■	■	■	□	■	■	□	■	□	□	■	■	□	■	■	■	■	■	■	■	□	□	■	□	□	■	■	■	■	□	■	■	□	67.2
G	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	■	■	■	■	■	□	□	■	■	■	■	49.5

■ Si se cumple

□ No se cumple

■ 5%

■ 8%

■ 12%

■ 15%

Contenido

Resultados cualitativos
Fortalezas comunes

- Todos los países cumplen con la recomendación de poder recuperar su principal sistema de pagos el mismo día que suceda una caída operativa grave.
  - Dos países incluso reportaron objetivos de recuperación de 3 horas o menos, los cuales lucen semejantes a los objetivos buscados por estándares altamente exigentes, como el que el Banco Central Europeo establece para los sistemas participantes de Target2, que es de 2 horas.

- En casi todos los países (excepto País G) existen mecanismos de comunicación bien definidos que permiten informar al personal de eventos de contingencia y coordinar los planes de recuperación o movilización a sitios alternos.

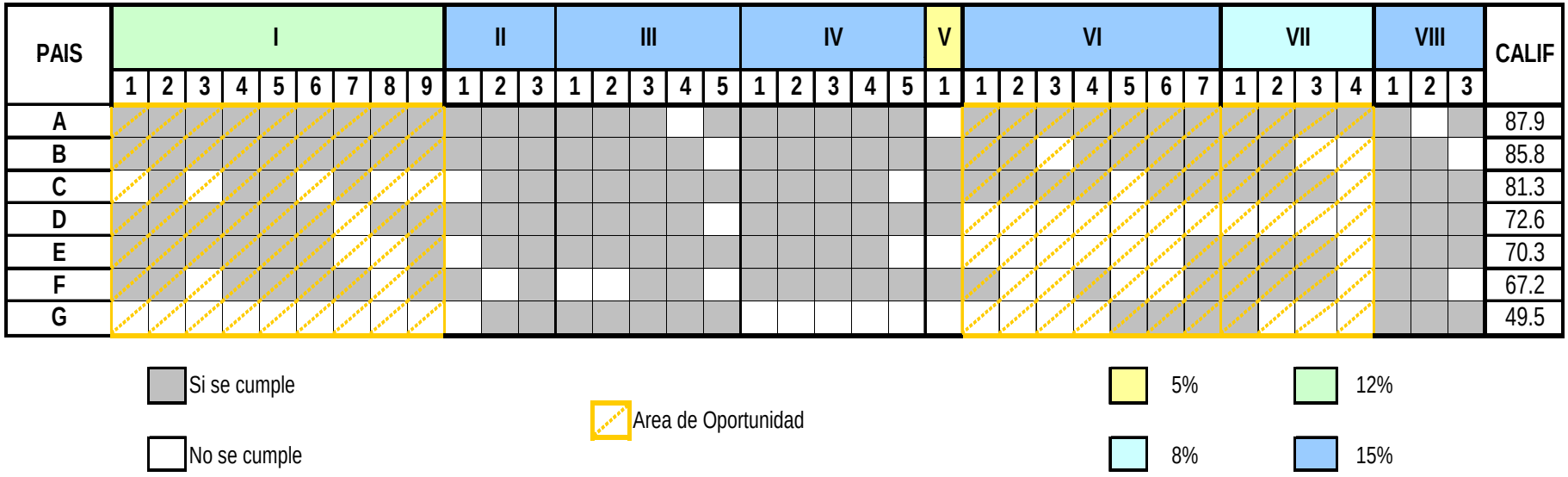
Resultados cualitativos
Fortalezas comunes

- Todos los países cuentan con sitios alternos de operación.
- Todos los sitios alternos son, o serán próximamente, administrados por los propios Bancos Centrales.
- De igual forma, todos los países cuentan con la infraestructura de equipo recomendada (respaldo de datos, replicación de operaciones, sitios alternos independientes, etc.).
- Lo anterior nos lleva a pensar que, en general, en la región se cuenta con los elementos físicos necesarios para una apropiada ACN, mostrando debilidad, sin embargo, en los aspectos de planeación y pruebas de los planes.

Resultados cualitativos
Fortalezas comunes

- Casi todos los países (5 de 7) consideran interrupciones operativas graves y escenarios extremos en sus sistemas. Esta es una de las recomendaciones más importantes, pues permite identificar los casos más graves que se deben resolver.
- A pesar de no ser parte del cuestionario, distintos países mencionaron su interés por seguir uno o varios estándares internacionales de continuidad de negocio o de seguridad de la información, buscando en algunos casos incluso la certificación (DRII, BS 25999, ISO 22399, etc.).
  - Sólo 2 países (C y D) no hacen referencia a ningún estándar.
  - Futuras versiones del cuestionario incluirán preguntas sobre los estándares.

Resultados cualitativos
Oportunidades de mejora



Resultados cualitativos
Oportunidades de mejora

- La participación de los niveles jerárquicos más altos en el diseño e implantación de planes de continuidad de negocio aún tiene aspectos que mejorar, en particular en lo referente a la formalización de roles, o la revisión periódica del plan.
  - Sólo 2 países (A y B) cumplen todos los aspectos de la recomendación.
- Pruebas. Algunos países aún no han hecho pruebas de sus planes (procesos e infraestructura) a nivel interno (D, E y G) o global, con los participantes (C, B y F).
  - Posiblemente, porque los planes dentro y/o fuera de los Bancos Centrales sean aún muy recientes.
- Revisión de la continuidad de negocio por parte de las autoridades financieras. Se detectó gran diversidad en cuanto a la revisión que los Bancos Centrales hacen de los planes de los principales participantes.
  - Desde muy detallada (A y F) hasta desconocimiento absoluto (D y G)

Contenido

Análisis
Observaciones

- Se manejan diferentes enfoques en la elaboración y administración del plan:
  - De arriba hacia abajo, es decir, el plan se diseña y administra a nivel institucional y las distintas áreas se apegan a los lineamientos definidos o,
  - De abajo hacia arriba, es decir, cada área define sus propios objetivos y planes, y las direcciones de los bancos incorporan todo esto en un plan institucional.
- Las compañías que manejan las telecomunicaciones y algunas que ofrecen servicios informáticos son jugadores importantes en los sistemas de pago.
  - Cuando estas compañías son monopolios en el país, los Bancos Centrales reportan poca cooperación con ellas.
  - En algunos lugares se han creado grupos de trabajo o comités de sistemas de pago que involucran a más jugadores, para atacar esta problemática.

Análisis
Observaciones

- Organismos internacionales como el BIS o el Cemla pueden ayudar a que las oportunidades de mejora identificadas sean atendidas a nivel regional.
- En la opinión de Banco de México, análisis como el que presentamos ayudarían a canalizar estos esfuerzos a áreas concretas.

Contenido

1. Introducción
2. Metodología empleada
3. Resultados cuantitativos
4. Resultados cualitativos
5. Análisis de resultados
6. Conclusiones

Conclusiones
Estado actual

- En general, el estado actual de la continuidad de negocio en la región es bueno.
  - Casi todos los países cumplen con más del 60% de las recomendaciones y están atendiendo el tema.
- En proceso de mejoras. Se observó que la mayoría de los Bancos Centrales está en proceso de afinar sus planes de continuidad y probar su efectividad.
  - Esto irá mejorando poco a poco sus planes, permitirá definir objetivos de mejora específicos y ayudará a incrementar las calificaciones del cuestionario.

Conclusiones
Retos

- Participantes. No todos los Bancos Centrales tienen facultades de supervisar la ACN de los participantes, sin embargo, podría buscarse, en coordinación con otras autoridades, mayor vigilancia de los principales participantes en los sistemas de pago.
- Los planes de continuidad aislados podrían no cubrir escenarios de fallas sistémicas, es importante considerar la continuidad de todo el sistema de pagos (participantes, proveedores, administradores, etc).
- Seguimiento. El proceso de mejora de la ACN debe ser permanente. El Banco de México ofrece a los integrantes del Foro dar seguimiento a las evaluaciones realizadas y generar versiones mejoradas del cuestionario.

Conclusiones

- Este Foro y este trabajo nos han permitido hacer una exploración inicial de la ACN de la región. Se detectaron logros importantes, así como áreas de oportunidad, en lo particular y en lo general.

- El Banco de México invita a los países que no enviaron sus cuestionarios a enviarnos sus evaluaciones. Esto nos permitirá enriquecer la experiencia y ampliar el panorama de soluciones y retos.

- Exhortamos a los Bancos Centrales integrantes de este Foro a que realicemos los esfuerzos necesarios para aumentar nuestras calificaciones.

¡ Gracias !

Anexos

Detalle del País A

- Obtuvo la calificación más alta.
- Los planes de continuidad son revisados por auditores internos, externos, empresas consultoras y autoridades financieras
- Su administración de continuidad de negocio está basada en el estándar internacional DRII

Detalle del País B

- Enfoque de arriba hacia abajo. Tienen un Comité de Sistemas de Pago
- Obtuvo una de las calificaciones más altas.
- Tiempos de recuperación muy adecuados
- El banco central no ejerce como entidad reguladora para revisar la continuidad de negocio de los participantes
- Algunos participantes todavía no pueden operar desde sus sitios alternos
- Cuenta con 2 sitios alternos localizados en ciudades diferentes
- Los planes de continuidad son revisados periódica y permanentemente por entidades externas

Detalle del País C

- Enfoque de abajo hacia arriba.
- Tiene planeadas mejoras importantes a su ACN
- No hay un plan integral que abarque todas las áreas
- Ha establecido tiempo de recuperación de 30 minutos para su principal sistema de pagos.
- Revisan la continuidad de negocio de los participantes.
- Realizan pruebas conjuntas con los proveedores de servicios.

Detalle del País D

- Enfoque de arriba hacia abajo.
- Etapa de pruebas en proceso. Al parecer su plan es muy nuevo y no han podido coordinar pruebas de los distintos escenarios plasmados en el plan.
- No revisa la continuidad de negocio de los participantes, pero está considerada para un futuro. Nuevamente, esto se puede deber a lo reciente que es su plan de continuidad.
- Los resultados de su auto evaluación muestran debilidades en los aspectos de pruebas y supervisión de los participantes.

Detalle del País E

- Enfoque de arriba hacia abajo
  - Planes muy bien definidos y estructurados, lo cual les dio una alta calificación.
  - Fallan en el aspecto de pruebas. Posiblemente esto esté en progreso y aún no han convencido a los participantes que se involucren.
- Sitio alterno altamente confiable, auditado y certificado por empresas especializadas.
- Alto apego a estándares y búsqueda de certificaciones.

Detalle del País F

- Enfoque abajo hacia arriba.
- Obtuvo una de las calificaciones más bajas, lo cual se debe, principalmente, a que falta documentar y formalizar planes de continuidad de negocio. En particular no cuenta con un análisis de impacto y los objetivos de recuperación.
- Las políticas de continuidad de negocio no son revisadas por entidades independientes.
  - Sin embargo, acaba de emitir nuevas normativas que atacan esta debilidad. Con esto, la calificación del país sería comparable a la de otros.

Detalle del País G

- Obtuvo una de las calificaciones más bajas.
- No cuenta con plan de continuidad de negocio, pero cuenta con un plan de contingencia.
- Se encuentra en proceso de formalizar su ACN y hacer mejoras substanciales que abarquen: pruebas, análisis de impacto, definición de responsabilidades, entre otros.

Anexos

- Estándares internacionales más comunes

Continuidad de Negocio
Estándar Internacional DRII (Disaster Recovery Institute International)

- Son un conjunto de prácticas profesionales para la Gestión de Continuidad de Negocio, cuyo objetivo principal es permitir a las operaciones comerciales seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias de gestión de riesgos.
- Este conjunto de prácticas abarca áreas como son: Iniciación y Gestión del proyecto; Evaluación y control de riesgo; Análisis de impacto del negocio; Estrategias de la Gestión de Continuidad del Negocio; Respuesta a emergencias y operaciones; Elaboración y Aplicación de planes de Continuidad de Negocio; Sensibilización y capacitación del personal; Ejercicio y mantenimiento de los planes de Continuidad del Negocio; Comunicaciones en las crisis y Coordinación con agencias externas.
- El plan de Administración de Continuidad del Negocio del Banco de Guatemala es una adaptación del estándar internacional DRII.

Continuidad de Negocio
Norma BS 25999

- Es una norma británica para la gestión de continuidad de negocio (Business Continuity Management) y abarca todo el ciclo de vida de la gestión de continuidad de negocio
- Comprende dos partes:
  - "El código de buenas prácticas" que proporciona recomendaciones de buenas prácticas en cuanto a la ACN y
  - "La especificación" que permite incorporar a la ACN procesos de mejora continua para incrementar la recuperación de la organización ante una contingencia o desastre, y cumplir con los requerimientos regulatorios de continuidad de negocio, reducir esfuerzos y costos derivados de la ejecución auditorias internas y de proveedores, justificar gastos de implantación y obtener la confianza de los directivos, clientes, accionistas en la "supervivencia" del negocio.
- El Sistema de Administración de la Continuidad del Negocio del Banco Central de Costa Rica, está basando en la norma BS 25999 empezando por el Sistema de Pagos.

Continuidad de Negocio
ISO 22399

- Presenta los principios y elementos generales para la preparación en caso de un incidente y tener continuidad operativa en la organización.
- Orienta a la organización para desarrollar sus propios criterios para el diseño adecuado de un Sistema de Gestión como son:
  - identificar objetivos;
  - comprender los obstáculos, los riesgos y perturbaciones que pueden obstaculizar los objetivos críticos;
  - evaluar el riesgo y la tolerancia para entender los resultados de los controles y las estrategias de mitigación;
  - alcanzar los objetivos en caso de que se produzca un incidente;
  - recuperación de procedimientos;
  - definir las funciones y responsabilidades, y recursos para responder a un incidente;
  - cumplir con las disposiciones legales y reglamentarias;
  - proporcionar asistencia de la comunidad;
  - establecer medios de comunicación y
  - promover un cambio cultural dentro de la organización.
- El **Banco Central de Costa Rica** también usa la ISO 22399

Seguridad de la Información
Norma ISO 27001

- ISO/IEC 27001 es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI).
- La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI
- El Sistema Nacional de Pagos de **Costa Rica** está certificado por la empresa Verizon, basadas en la norma ISO 27001 y el estandard TIA-942 para Centros de Datos.
- Las respuestas de **Colombia** sugieren que también sigue este estándar.