CONCHA BURGOS GARCÍA
Economista. Profesora del CEF

Extracto:

La recentísima aprobación por el Comité de Basilea de los *Principos de alto nivel para la continuidad del negocio financiero* ha venido a poner sobre la mesa de los presidentes de las entidades y mercados financieros el manual de una nueva disciplina, la «business continuity», que hace cinco años ni siquiera existía.

Las entidades financieras se caracterizan, entre otras cosas, porque su elevado apalancamiento se traduce en que el riesgo de crédito tenga un perfil mucho más significativo que en otro tipo de empresas. A la vez, el volumen, rotación y la velocidad de las transacciones electrónicas en los mercados financieros globalizados introducen el denominado riesgo sistémico, aquel que consiste en que la crisis de un actor principal del mercado se convierta en un virus letal que se contagie por todo el sistema. Este riesgo no es nada nuevo, desde luego, pero en los últimos tiempos hemos visto cómo los atentados terroristas de Nueva York en 2001, los apagones de Nueva York y Canadá en 2003, un terremoto en Kobe, el brote de SARS en Asia o la amenaza, este año, de una posible pandemia de gripe aviar han demostrado que acontecimientos externos sumamente graves pueden ser también el detonador de una crisis sistémica. De los medios para prevenir ese tipo de crisis y de la historia de cómo ha llegado a formarse la nueva disciplina es de lo que trata este artículo.

Sumario:

LA CONTINUIDAD DEL NEGOCIO FINANCIERO

Entre los elementos que distinguen a la empresa bancaria de otras actividades productivas o de servicios y a la vez conforman su estructura y modos de actuación está la alta proporción en que el riesgo y las técnicas para paliarlo entran a formar parte de la propia estructura de las organizaciones y de las decisiones de la gerencia.

Efectivamente, además del riesgo de insolvencia de clientes, común con otras empresas, las entidades financieras asumen riesgos específicos derivados de la naturaleza financiera de sus productos, como la evolución de los tipos de interés, de la volatilidad de los tipos de cambio o de las cotizaciones y rendimientos de los activos del balance. Pero eso no es todo: la complejidad de los mercados financieros, la alta rotación de los productos negociados y el gran volumen de transacciones negociadas diariamente en sistemas electrónicos exponen a las empresas al riesgo de ser víctimas de la insolvencia de otros actores del mercado. Este riesgo, denominado sistémico, se define por Junta de Gobernadores de la Reserva Federal (2003) como «el riesgo de que la imposibilidad de cumplir sus obligaciones por parte de uno de los participantes en un sistema de transferencias o en un mercado financiero cause problemas significativos de liquidez o de crédito amenazando a la estabilidad de los mercados financieros», definición consecuente, a su vez, con el concepto internacional de riesgo sistémico en los sistemas de compensación y pago contenido en el «Glosario de términos en sistemas de compensación y pago» del Commitee on Payment and Settlement Systems, Bank for International Settlements (2001).

El riesgo sistémico se actualiza y convierte en un problema real cuando algún acontecimiento extraordinario rompe el equilibrio del sistema. Mientras que tradicionalmente se venía considerando que dicho acontecimiento se originaría por la insolvencia de uno de los grandes actores del mercado, los atentados terroristas del 11 de septiembre de 2001 en Nueva York exhibieron la vulnerabilidad del sistema a un acontecimiento perturbador de gran magnitud que puede poner en peligro la solvencia del conjunto. Acontecimientos posteriores como el gigantesco apagón de Estados Unidos y Canadá en agosto de 2003, el brote del Síndrome de Insuficiencia Respiratoria Aguda SARS que afectó a

los mercados de valores de Hong Kong y Toronto en 2003, el terremoto de 6.8 grados que afectó a la región japonesa de Niigata en octubre de 2004, o los atentados terroristas en Madrid, Estambul y sobre todo en Londres el 7 de julio de 2005, así como la posibilidad, sentida muy de cerca este año, de que se produzca una pandemia con la gripe aviar más recientemente, han despertado el interés de la comunidad financiera internacional sobre la posibilidad de que estos acontecimientos externos y graves puedan disparar la crisis del sistema y afectar a la continuidad de los mercados.

Sin embargo, hace unos años este riesgo no contaba entre las preocupaciones de los reguladores bancarios nacionales ni de los organismos internacionales. Sin ir más lejos, el G-7 adoptó en su reunión de Colonia de 1999 una resolución titulada «Fortalecimiento de la Arquitectura Financiera Internacional» en la que se respalda el *Financial Stability Forum* y toda una serie de buenas prácticas relacionadas con la transparencia y la política monetaria, el gobierno corporativo y las obligaciones de información de las entidades financieras, pero en ningún momento se habla de la posibilidad de que acontecimientos extraordinarios puedan introducir riesgo sistémico [1]. Igualmente, el Comité de Sistemas de Pagos y Compensación del Bank For International Settlements publicó (2001) los *Core principles for systematically important payment systems*, pero entre los principios básicos no hay referencia alguna al riesgo de que ocurran acontecimientos externos suficientemente graves como para afectar a la estabilidad del sistema y, sin embargo, el 11 de septiembre de ese mismo año aprendimos dolorosamente la lección de cómo las empresas financieras son altamente interdependientes, y de que una interrupción de su funcionamiento puede crear riesgos para la compensación y liquidación y, consecuentemente, riesgos de crédito y liquidez.

En los escasos cinco años transcurridos desde 2001 hemos visto cómo se ha pasado desde una situación en que prácticamente se ignoraba este peligro a otra en que la continuidad del negocio se ha convertido en uno de los aspectos de mayor relevancia, incluyéndose dentro del marco de la política de gestión de riesgos de la empresa, y se ha situado al máximo nivel de responsabilidad: Consejo de Administración y Consejero Delegado.

De este modo, podemos decir que en el momento actual la *business continuity* y los planes de emergencia se han integrado en el marco de las decisiones estratégicas de las entidades financieras y, simultáneamente, se ha producido un importante movimiento multinacional entre los organismos reguladores para concienciar sobre el problema y extender las recomendaciones, cuya máxima expresión son los Principios de Alto nivel de la Continuidad del Negocio publicados por el Comité de Basilea en diciembre pasado (2005).

No obstante, antes de llegar a esta fase cuyas notas son la elevación del nivel a «gerencia para la continuidad» y la internacionalización y estandarización de las soluciones se pasó por una fase previa caracterizada porque las iniciativas eran de carácter nacional y no daban una relevancia tan crucial a los planes de emergencia. La fase de las autoridades nacionales comenzó, por motivos obvios, en Estados Unidos, donde la Reserva Federal (2003, 2006) publicó en 2002 guías de referencia, aunque a este movimiento pronto se sumaron otros países. Así, por ejemplo, la Asociación de Banqueros Británicos publicó su guía para gerencia de la continuidad del negocio en 2003, y la Auto-

[1] http://www.treasury.gov/press/releases/reports/cologne.pdf

ridad de Servicios Financieros del Reino Unido ha aprobado también una guía completa (2005). Tempranos fueron también los manuales de Hong Kong en 2002 y Singapore en 2003, y otras autoridades nacionales les han seguido, como Japón en 2003, Países Bajos en 2004, y Australia y Francia en 2005. Nuestro regulador nacional, según ha confirmado la Secretaría General del Banco de España, tiene planes de contingencia pero son reservados y no existen de momento intenciones de publicarlos. Tampoco parece que exista un proyecto de instrucciones para la gerencia para la continuidad dirigidas a las instituciones financieras. En lo tocante a los planes nacionales de otros países, la bibliografía que incorpora el documento de los Principios de Alto Nivel (2005) contiene una buena referencia para profundizar sobre los planes nacionales publicados.

La fase de internacionalización en la toma de conciencia sobre los riesgos y la necesidad de planificación llegó en 2004 y 2005, cuando algunos organismos internacionales propusieron soluciones que trascienden las fronteras nacionales, y así tenemos el documento sobre continuidad del negocio en los sistemas de pagos del Banco Central Europeo (2005) o el del propio Bank for International Settlements o Comité de Basilea: «High-level principles for business continuity» (2005).

Visto con la perspectiva de hoy, parece evidente que la intención de los terroristas en Nueva York era crear una crisis sistémica que afectara a Wall Street aunque, como veremos, poco faltó para conseguirlo, los mecanismos de seguridad de las empresas afectadas y de los sistemas de pago implicados sirvieron para conjurar el peligro de crisis del sistema, que de hecho funcionó bastante bien dada la magnitud de los acontecimientos y las pérdidas sufridas. Aunque no había experiencia de un atentado similar, parece que los planes de emergencia que se habían diseñado para el problema del año 2000 coadyuvaron a evitar la crisis sistémica. Sin embargo, la terrible experiencia ha llevado a un replanteamiento de la estrategia de seguridad, tanto para las compañías como para los sistemas de pagos.

La gerencia para la continuidad del negocio es hoy la respuesta contra el riesgo sistémico. El Comité de Basilea (2005) define la «continuidad» como el estado de operación continua e ininterrumpida del negocio y la «gerencia para la continuidad» como el enfoque global que incluye políticas, estándares y procedimientos para que las operaciones se reanuden puntualmente en la hipótesis de un acontecimiento externo con capacidad de interrumpir el negocio, con el objetivo de limitar las consecuencias negativas que ocurrirían en el plano operativo, legal, financiero y de la buena reputación de la empresa.

La gerencia para la continuidad como teoría se construye sobre la planificación para la continuidad, concepto que estaba ya definido, por ejemplo, por el Federal Financial Institutions Examination Council norteamericano (2003). Este manual se refiere a la *business continuity planning* como el proceso por el cual las instituciones financieras aseguran el mantenimiento y recuperación de las operaciones en la eventualidad de una interrupción. El elemento operativo de la *business continuity planning* son obviamente los planes de contingencias para garantizar que, cuando se enfrenten a acontecimientos como desastres naturales, fallos tecnológicos, error humano o terrorismo o, posiblemente, una pandemia como podría ser la de la gripe aviar, se cumplan los objetivos de continuidad.

El objetivo de los planes de contingencia será, por tanto, minimizar las pérdidas financieras para la institución financiera, continuar sirviendo a los participantes en el mercado, y mitigar los efectos negativos que las interrupciones pueden tener en los planes estratégicos de las instituciones, en su imagen pública, su operativa, liquidez, calificación crediticia, posición en el mercado y posibilidades de cumplir con sus requerimientos legales.

Los planes de continuidad del negocio no nacieron con el 11-S, sin embargo. En Estados Unidos, el manual de supervisión bancaria editado por el FFIEC o consejo que agrupa a las autoridades con competencia en supervisión bancaria en Estados Unidos tenía ya un capítulo sobre continuidad del negocio aunque antes trataba principalmente del fallo de los sistemas informáticos. Este capítulo se reescribió después para darle un ámbito mucho más amplio, porque ahora ya no se considera sólo el escenario del fallo informático sino de cualquier tipo catastrófico, y no se limita a una entidad dentro del sistema, sino que se contempla cómo el fallo de varias entidades en cadena puede afectar al propio sistema, así como la posibilidad de que se inutilicen infraestructuras vitales para la continuidad del negocio.

LA CRISIS DEL SISTEMA DE PAGOS DEL 11-S

De acuerdo con CUMMING (2002) los atentados terroristas neoyorquinos fueron la situación más crítica en que se haya visto el sistema de pagos, entendiendo por tal no sólo los dos sistemas principales de pagos de gran escala Fedwire y CHIPS, sino también dos grandes bancos de compensación, los bancos participantes, los sistemas de liquidación de valores bursátiles y las entidades financieras con cuota significativa del mercado.

Las torres gemelas albergaban varias agencias bursátiles de primer orden en volumen de negociación, y su servicio quedó interrumpido no sólo por la devastadora magnitud de los daños y las pérdidas humanas, sino por el colapso de las comunicaciones y de la infraestructura de transportes y de suministro eléctrico. Pese a los daños en las infraestructuras primarias, los dos sistemas principales de pagos, Fedwire y CHIPS, funcionaron ininterrumpidamente el día del ataque y los días siguientes, gracias sobre todo a los edificios de reserva situados fuera de Manhattan. Como luego veremos, este tipo de edificios que replican la actividad principal de la institución son la clave para la continuidad de los sistemas de pagos. Los sistemas de liquidación y compensación de valores corrieron peor suerte que los sistemas de pagos, quedaron efectivamente interrumpidos y sólo pudieron reestablecerse el día 13 de septiembre. Sin embargo, cuando el 17 de septiembre se reabrieron las bolsas, se pudieron liquidar y compensar adecuadamente las posiciones inmediatamente anteriores al ataque y el sistema funcionó sin solución de continuidad a pesar de la interrupción. De hecho, el 17 de septiembre marcó la fecha de mayor volumen de negociación en la historia de la bolsa neoyorquina. La clave para la supervivencia del sistema estuvo en la utilización en los sistemas de pagos con carácter casi exclusivo de medios electrónicos.

Sin embargo, dado que el sistema de pagos está ajustado por medios electrónicos para compensar posiciones en tiempo real, el desajuste de una parte del sistema supone una falta de liquidez

en el resto de operadores. En el 11-S se produjeron graves desajustes, sobre todo en la liquidación de operaciones de valores. Según CUMMING (2003), el valor de las transacciones del sistema federal Fedwire se redujo un 24 por 100, y durante el resto de la semana el volumen de transacciones bajó un 40 por 100 frente al nivel de agosto, debido a problemas de conectividad, y las empresas utilizaron sus reservas de liquidez o solicitaron crédito de sus bancos para poder saldar las posiciones.

Sin embargo, los desajustes fueron tan fuertes que no fue suficiente esta primera línea de contingencia y las empresas hubieron de recurrir a ayuda externa para mantener la liquidez. La reserva Federal inyectó enormes sumas de dinero mediante préstamos diarios en la ventanilla de descuento y mediante operaciones de mercado abierto. El 12 de septiembre, por ejemplo, inyectó 46.000 millones de dólares en la ventanilla de descuento y 38.000 millones mediante operaciones de mercado abierto, y además suspendió el recargo por descubierto en el mismo día y flexibilizó las normas que restringían el volumen que podía prestar al mercado. También, para hacer frente a la iliquidez de pagos en dólares en otros mercados no norteamericanos la Fed concluyó acuerdos con diversos bancos centrales como el europeo, el de Inglaterra o el de Canadá. El Banco Central Europeo recurrió a su línea de crédito recíproco en las jornadas posteriores al 11-S, habiendo llegado a un nivel de crédito de 19.000 millones de dólares. A medida que se normalizó la situación, la Reserva Federal fue reduciendo el volumen de liquidez y, el 21 de septiembre, las operaciones de ventanilla y de mercado abierto, habían vuelto a la normalidad.

REACCIONES POSTERIORES

Inmediatamente después de los atentados, en Estados Unidos empezaron a preocuparse por las medidas de seguridad del sistema para paliar el riesgo de que la crisis del 11-S pudiera repetirse y se interrumpiera el funcionamiento del sistema financiero. Tan sólo un mes después del ataque se reavivó el interés por la protección de la infraestructura informática contra el ciber-terrorismo, aunque en este caso, lógicamente, no limitado al sector financiero, y la Casa Blanca dictó la Orden Ejecutiva 13231 «Critical infrastructure Protection in the information Age», que en realidad era una actualización de una directiva ya publicada en 1998, como dice la GAO (2002).

En el caso concreto del sector financiero, las tres agencias federales con funciones supervisoras en Estados Unidos, es decir, el consejo de gobernadores de la Reserva Federal (Federal Reserve Board), la Oficina del Controlador de la Moneda (Office of the Comptroller of the Currency u OCC) y la Comisión del Mercado de Valores (Securities and Exchange Comisión o SEC), se pusieron enseguida a trabajar y crearon un grupo de trabajo conjunto para estudiar la capacidad del sistema financiero para soportar elementos perturbadores de gran magnitud. Tras unos meses de trabajo elaboraron un documento que publicaron en el Federal Register el 25 de septiembre de 2002 como borrador para comentarios [2].

El interés por la continuidad del negocio ante eventos extraordinarios se reavivó al año siguiente con los apagones de Nueva York, y en verano de 2004 el Foro para la Estabilidad Financiera y el Banco

[2] Federal Register 56835, September 5, 2002.

de Inglaterra organizaron conjuntamente un seminario sobre continuidad del negocio en el sector financiero. Como consecuencia del seminario, se requirió a los tres organismos reguladores transfronterizos en el sector financiero (Comité de Basilea de Supervisión Bancaria, la Asociación Internacional de Comisiones Nacionales de Valores IOSCO y la Asociación Internacional de Supervisores de Seguros IAIS) para que elaborasen principios de alto nivel para cada uno de sus ámbitos. En febrero de 2005 los tres cuerpos reguladores estuvieron de acuerdo en la conveniencia de emprender esa tarea, y el documento del Comité de Basilea se publicaba unos meses después, en diciembre de 2005.

PLANES DE CONTINUIDAD DEL NEGOCIO FINANCIERO

Entrando, así pues, en el análisis concreto de los planes de continuidad, seguiremos el orden cronológico, comenzando por los planes norteamericanos, para continuar con el plan del Banco Central Europeo, y terminaremos con los principios de alto nivel de Basilea.

LA PLANIFICACIÓN PARA LA CONTINUIDAD EN ESTADOS UNIDOS

Lo primero que se plantearon los supervisores financieros en Estados Unidos fue la definición de los objetivos de continuidad del negocio, así como las mejores prácticas para lograrlo. Para ello, tomaron como punto de partida la planificación de *business continuity* que a la sazón existía, sobre todo relacionada con el sistema informático y el problema del año 2000, y fijaron tres objetivos:

- La rápida recuperación y oportuna rehabilitación de las operaciones críticas después de un acontecimiento extraordinario.
- La rápida recuperación y oportuna rehabilitación de las operaciones aunque haya desaparecido personal clave en alguna de las ubicaciones de la empresa.
- El establecimiento de un alto nivel de confianza dentro de la empresa acerca de la seguridad de que las operaciones continuarán en una situación crítica.

Como luego veremos, el plan del Banco Central Europeo (2005) ha sido incluso más preciso en los objetivos de continuidad, distinguiendo entre los operadores que deben reanudar las operaciones dentro del mismo día y los que deben reanudarlas dentro de las primeras dos horas. También el documento inter-agencia norteamericano sobre la reanudación de operaciones se fijó en las prácticas seguras que deben adoptar los sistemas de pagos y las empresas participantes, para lo cual ha dividido el espectro de entidades afectadas en tres bloques:

- Mercados financieros críticos: son los que proveen de medios a los bancos y agencias de valores y otras instituciones financieras para ajustar sus posiciones de tesorería y de valores,

así como las de sus clientes, con el objetivo de gestionar la liquidez, el mercado y otros riesgos de sus organizaciones. Los mercados identificados como críticos son el de fondos federales, el de cambio de moneda extranjera, el de papel comercial, el de deuda pública y el de deuda privada.

- Organizaciones clave en la liquidación y compensación. Es un grupo de organizaciones que proveen servicios de liquidación y compensación y operan como operadores de transferencias de grandes importes. Existen dos subgrupos: los mediadores de mercado que trabajan para mercados críticos como los definidos en el punto anterior, o para otros pagos mayoristas de elevado importe, y las empresas privadas que proveen de dichos servicios dentro de uno de los mercados críticos.

- Las terceras son las instituciones financieras que desempeñan un papel crítico en su mercado financiero, esto es: aquellas que tienen un porcentaje del mercado tan alto que por sí mismas son susceptibles de crear riesgo sistémico, y que en el documento de 2003 se concreta en un 5 por 100.

Los objetivos de continuidad, definidos por orden de prioridad, son los siguientes:

1. Completar los pagos pendientes de elevado importe.
2. Liquidar y compensar las transacciones que materialmente estén pendientes.
3. Cumplir las obligaciones de pago y garantía definidas para el cierre de la jornada de manera que se consigan los dos objetivos anteriores.
4. Gestionar las posiciones de riesgo de la entidad y de sus clientes de la mejor manera para que se puedan cumplir los objetivos anteriores.
5. Comunicar las posiciones de la empresa y de sus clientes y reconciliar los registros del día, de modo que se puedan cumplir los objetivos anteriores, y
6. Desarrollar todas las actividades de apoyo y funciones accesorias para poder efectuar las operaciones anteriores.

La experiencia del 11-S muestra que hay que estar preparados, y para ello hay tres elementos que son clave: los planes para contingencias, los centros de reserva (*back-up facilities*), y la simulación de catástrofes.

La primera actividad, pues, es elaborar planes de emergencia, identificando las actividades de compensación y liquidación que son claves para que funcionen los mercados financieros críticos. A continuación, deben determinarse objetivos de recuperación y restablecimiento que sean realistas y operativos. Las empresas tienen que ponerse un objetivo temporal que sea razonable y consistente con otros operadores del mercado, teniendo en cuenta que no sólo puede tener dificultades dentro de su organización, sino también problemas de infraestructura. Las organizacio-

nes que desempeñan papeles clave en el mercado, sin embargo, deben marcarse objetivos más ambiciosos. Sus planes tienen que incluir recuperar los datos y reanudar las operaciones en el mismo día y, como su ausencia puede producir la crisis del sistema de pagos, debería poner en funcionamiento sus sistemas y consolidar las posiciones de los grandes operadores no sólo dentro del mismo día, sino dentro de las dos horas siguientes a la interrupción. Las entidades que desempeñan papel clave en un mercado por negociar más del 5 por 100 de su volumen tienen igualmente obligaciones de recuperación más exigentes que el resto de entidades financieras. Sin embargo, a éstas no se les exige que reanuden sus operaciones en dos horas, como a los mercados, sino en cuatro.

Por lo que atañe a la dispersión geográfica de los edificios e instalaciones críticas, las instrucciones de la Reserva Federal (2003) son disponer de centros de reserva o *back-up facilities* y dotar a la estructura de una adecuada dispersión geográfica. Los centros de reserva pueden ser de dos tipos, o bien aquellos asíncronos, que reciben la informacion de las transacciones una vez completadas, o los centros que duplican la actividad de la ubicación principal, siendo estos preferidos por ser mucho más operativos y rápidos. El problema con los centros de reserva es que los acontecimientos graves pueden afectar también al centro de reserva, por lo cual es preciso que unos y otros no compartan la misma infraestructura, ni de transportes, ni de suministro de energía, ni de comunicaciones. No existen estándares concretos sobre la dispersión geográfica, pero se entiende que han de estar suficientemente separados. El otro problema con los centros de reserva es que tienen que tener a su cargo a personal que sea capaz de asumir decisiones operativas importantes y rápidas. Además, en el 11-S se puso de relieve que la conectividad es un problema muy serio, porque antes de los atentados se habían hecho simulacros de concesión con otras entidades desde el centro de reserva, pero la experiencia del 11-S fue que había que conectar con otros centros de reserva, lo cual no se había comprobado antes.

El tercer pilar de la preparación es la realización sistemática de simulacros para asegurarse de que se van a recuperar la conectividad, la capacidad y la integridad de los datos transmitidos. El documento de la Reserva Federal de 2003 estableció también un calendario de implantación en el que, tras tomar en consideración consideraciones de coste y beneficio, decidió no convertir el *Interagency Paper* en legislación obligatoria, sino mantenerlo como guía orientativa, también en parte por consideraciones de seguridad y por la propia evolución dinámica de los mercados. Sin embargo, exigió a los principales actores del mercado objetivos temporales. A las organizaciones de compensación y liquidación les marcó un objetivo temporal de preparación para el 2004, que después fue ampliado hasta 2005 a la vista de la cantidad de trabajo y de inversiones que estas *guidelines* implicaban. A las empresas que desarrollan papeles clave en sus mercados se les pidió que estuvieran listas en 2006, y al resto de entidades del mercado financiero se les pidió que los objetivos de *business continuity* fueran incorporados en su planificación estratégica.

Con el fin de seguir la evolución de las directrices, la Ley de Prevención del Terrorismo [3] de 2004 encargó a las Agencias federales competentes que realizasen un estudio sobre el grado de preparación del sector financiero privado. Los resultados, publicados por la Reserva Federal en abril

[3] Intelligence Reform and Terrorism Prevention Act of 2004, sección 7803 (e).

de 2006, muestran que de todas las organizaciones de compensación y liquidación que estaban situadas en Manhattan, todas excepto una han construido o reformado los centros de reserva en ubicaciones muy distantes de Nueva York. Muchos sistemas de compensación y liquidación trabajan simultáneamente desde la ubicación principal y la de reserva, e incluso alteran ocasionalmente su lugar principal de operaciones para el mejor funcionamiento de los planes de emergencia. También los bancos y las entidades que desempeñan un papel significativo en los mercados tienen implantados sus sistemas de seguridad incluyendo las ubicaciones adicionales los planes de emergencia y la preparación y revisión sistemática de los planes, aunque a fecha de abril de 2005 todavía había cinco entidades que estaban trabajando para implementar sus planes de emergencia, pero como están trabajando en ello y las expectativas de que se completen son buenas, la comisión inter-agencia no ha recomendado que se adopten medidas legislativas o ejecutivas para acelerar sus procesos.

LA CONTINUIDAD DE LOS SISTEMAS DE PAGO DEL BANCO CENTRAL EUROPEO (2005)

En abril de 2004 se reunió a puerta cerrada el Eurosistema para abordar el tema de la continuidad del negocio a la luz de los antecedentes de atentados terroristas, apagón de Nueva York y epidemias en Asia, y decidió elaborar un manual de continuidad del negocio para el sistema europeo de pagos TARGET para que los bancos centrales del sistema, y las instituciones tuvieran unas líneas maestras a la hora de dirigir sus esfuerzos dictando regulaciones para la continuidad del negocio.

El trabajo del Banco Central Europeo continúa la línea de los planes implantados en Estados Unidos, centrando su atención en tres elementos clave:

- La concepción de la continuidad del negocio como una estrategia de la empresa.
- La planificación adecuada.
- La experimentación de los planes y sistemas con regularidad.

La gerencia para la continuidad es así un desarrollo del Principio Básico VII de los «Core principles for sistemically important payment systems» del Bank for International Settlements aprobados en 2001. El principio VII para sistemas de pagos importantes prescribe: «El sistema debería asegurar un alto nivel de seguridad y confianza operativa y debería incluir planes de contingencia para completar puntualmente el proceso diario de datos».

La primera recomendación del Banco Central Europeo es establecer una estrategia en términos de continuidad del negocio, que debe ir a cargo de personas de alto nivel dentro de la organización, y debe ser discutida regularmente en la Junta de Gobernadores de la misma. La segunda es identificar los elementos críticos para el funcionamiento del sistema. La tercera sería el establecimiento de

objetivos de recuperación del servicio dentro del mismo día y, en algunos casos, en dos horas. Además, debe definirse lo que se considera un mínimo nivel de servicio. Igual que en los planes de la Reserva Federal, los planes de emergencia deben contemplar una serie de escenarios de crisis alternativos basados en análisis de riesgos.

El segundo elemento son los edificios de reserva, que deben ser como mínimo uno y tener igualmente una separación geográfica adecuada, y depender en lo menos posible de las mismas infraestructuras de comunicación, transporte y suministro de energía. Además, el Banco Central Europeo recomienda la reserva sobre la ubicación de los edificios de reserva, para prevenir ataques coordinados a la central y a la reserva, así como el empleo de técnicas de *data mirroring* para reproducir los datos fundamentales del negocio.

Otro aspecto al que presta atención el Banco Central Europeo es al personal. El personal no debe estar reunido por completo en un mismo edificio nunca. Además, hay que promover sistemas de acceso remoto a los datos y automatizar la copia de ficheros de seguridad. También se definen obligaciones más estrictas para los agentes importantes en un mercado, que en este caso se definen no con un porcentaje fijo, como hemos visto en la Reserva Federal, sino marcando una franja de entre el 5 y el 20 por 100 de acuerdo con el mercado de que se trate.

Otro aspecto crítico es la estructura de comunicaciones. En Nueva York falló mucho la conectividad porque en las prácticas se había hecho siempre de la central a la ubicación de reserva y de la ubicación de reserva a otras centrales, pero nunca se había pensado en que tendrían que comunicarse entre centrales de reserva. Otro aspecto crítico es la definición de responsabilidades para que ante una crisis siempre haya personas que sean capaces de tomar decisiones. Por último, el Banco Central Europeo recomienda que se hagan simulacros y evaluaciones de los planes de seguridad por lo menos una vez al año, así como que se establezcan canales de comunicación sobre los planes de emergencia con otros participantes claves del negocio, con el debido nivel de confidencialidad.

LOS SIETE PRINCIPIOS DE ALTO NIVEL DE BASILEA

Aunque todavía con carácter provisional, porque el documento publicado está sometido a un proceso de crítica, el Comité de Basilea ha intentado generalizar lo más posible para que la continuidad del negocio sea una cuestión que preocupe igual a los mercados y a sus operadores y con el suficiente grado de generalidad para que sea universalmente válida. En consecuencia, los principios son bastante genéricos, y están concebidos como *guidelines* para que las autoridades de cada circunscripción tengan una directriz. Como veremos, también son bastante coherentes con los dos antecedentes que hemos señalado: la Fed y el Banco Central Europeo.

El primer principio de alto nivel es precisamente la generalidad. Esto significa que la gerencia para la continuidad se debe aplicar tanto a las autoridades financieras como a los participantes en los mercados. Además, este principio también indica que la responsabilidad de la gerencia para la continuidad reside en los directores y ejecutivos de mayor nivel.

El principio segundo determina que es necesario que los sujetos participantes y los mercados tengan planes de emergencia adecuados para la eventualidad de acontecimientos con capacidad de interrumpir el servicio y las operaciones.

El tercero afirma que los participantes de la industria deben definir objetivos concretos de recuperación que sean reflejo del riesgo que represente para el mercado su posición, lo que permite distinguir entre participantes críticos y otro tipo de participantes. Las autoridades financieras deben participar también en la definición de objetivos de recuperación.

El cuarto principio enfatiza la importancia de disponer de una estrategia de comunicación adecuada para la eventualidad de que las líneas habituales de comunicación queden afectadas. No sólo se refiere este principio a la comunicación de las entidades con el mundo exterior, sino también a la transmisión de instrucciones y directrices dentro de la propia organización.

El quinto principio subraya el caso especial de las comunicaciones transfronterizas, aconsejando a los mayores mercados y operadores que adopten protocolos de comunicación de emergencia.

El sexto principio enfatiza la necesidad de examinar periódicamente los planes de seguridad.

El último principio se aplica sólo a las autoridades de control, y se refiere a la necesidad de que entre las inspecciones de entidades se incluya una revisión de los planes de contingencia.

CONCLUSIÓN

La continuidad del negocio en los sistemas de pagos, en los bancos y agencias de valores es un aspecto crítico no sólo para la empresa bancaria, sino para la salud del sistema financiero en general y es la mejor prevención de que un elemento inesperado de gran magnitud no se transforme en una crisis sistémica. La gerencia para la continuidad y la planificación de escenarios de riesgo de interrupción del servicio son sus principales elementos, aunque en nuestro país parece que no han recibido hasta ahora la atención necesaria. Algunos consultores ofrecen servicios de planificación, pero se limitan a los aspectos de seguridad informática, como Peña (2005) o Campos (2006), donde hay estándares establecidos internacionalmente como el ISO 17799 o el CobIT de la Information Systems audit. and Control Association.

Una vez que los Principios de Alto Nivel de Basilea sean publicados con carácter definitivo, parece inexcusable que los reguladores nacionales, incluido el Banco de España, dicten instrucciones, al menos con carácter orientador, para que no se descuide un aspecto que puede resultar fundamental, como las experiencias nos han enseñado.

BIBLIOGRAFÍA

Bank for International Settlements. Committee on Payment and Settlement Systems [2001]: «Core principles for systematically important payment systems»; *http://www.bis.org/publ/cpss43.pdf.*

Basel Committee on Banking Supervision [2005]: «High-level principles for business continuity. Consultative document»; *http://www.bis.org/publ/joint14.pdf.*

Campos, María [2006]: «La continuidad del negocio en el sector financiero». *FinalcialTech Magazine*. Número 63.

Cumming, Christine M. [2002]: «El 11 de septiembre y el sistema de pagos». *Finanzas y desarrollo*. Marzo de 2002.

Department of the Treasury [1999]: «Joint report on progress strengthening the international financial architecture»; *http://www.treasury.gov/press/releases/reports/cologne.pdf.*

European Central Bank [2005]: «Payment Systems and Business Continuity»; *http://www.ecb.int/ecb/pdf/cons/paysysbusinesscontinuity/paysysbusinesscontinuity.pdf.*

Federal Financial Institution Examination Council: «Lessons learned from the Year 2000 Project»; *www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0005.htm.*

Federal Reserve Board [2003]: «Interagency paper to strengthen the resilience of the US financial system»; *http://www.federalreserve.gov/BoardDocs/Press/bcreg/2003/20030408/attachment.pdf.*

– [2006]: «Joint Report on efforts of the private sector to implement the *Interagency paper to strengthen the resilience of the US financial System»; http://www.sec.gov/news/press/studies/2006/soundpractices.pdf.*

Financial Institutions Examinations Council [2003]: «Business Continuity Planning»; *http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.*

Financial Services Authority [2005]: «Resilience Benchmarking Project: work done by the financial authorities to promote the resilience of the UK financial sector»; *http://www.fsc.gov.uk/upload/public/Files/9/Web%20-%20Res%20Bench%20Report%2020051214.pdf.*

Government Accountability Office –Gao– [2002]: «Critical Infrastructure Protection»; *http://www.gao.gov/new.items/d02474.pdf.*

Peña Ibarra, José [2005]: «Gobierno de TI y continuidad del negocio»; *http://www.borrmart.es.*