# PLAN
# Estrategias de contingencia

*Por Alicia Giorgetti*

**Las emergencias e imprevistos no avisan, pueden dejar fuera del mercado a una empresa por horas, días o para siempre. El tiempo depende de la existencia de planes de continuidad del negocio y de recuperación de desastres. Qué son, cómo se diseñan y cómo encararon sus estrategias Banco Itaú, Laboratorios Bagó, Officenet y Tetrapak.**

Problemas en servidores, vínculos de comunicaciones, redes, almacenamiento, aplicaciones o en el edificio, pueden generar pérdida de ingresos, clientes y demandas legales. Y peor: según Gartner, el 40 por ciento de las empresas que sufren un desastre sucumben en cinco años. En la Argentina, son pocas las compañías que tienen planes e infraestructura de contingencia, iniciativas más frecuentes en bancos o multinacionales que son auditadas y deben cumplir regulaciones, como Sarbanes-Oxley.

El Banco Itaú Buen Ayre trabaja en una infraestructura de contingencia desde 1998. Claudio Ercolessi, gerente de Tecnología y Procesamiento de datos de la entidad, dice que "es por supervivencia, ya que el negocio de un banco se basa en información y, si no está disponible, no soporta más de 24 horas. La pérdida en dinero sería incuantificable y, también, en imagen y clientes. Tenemos un sitio propio de contingencia a cinco kilómetros del site central, con plataforma AS/400, servidores virtualizados sobre VMware donde están replicadas todas las aplicaciones y varios enlaces de fibra oscura. Están duplicadas las comunicaciones y hay interconexión entre nuestros tres sites, además de redundancia de proveedores. Migrar la operación tarda menos dos horas. Usamos esta infraestructura 45 días en 2005 para soportar un rápido aumento de clientes. La decisión de tenerla es del holding y también lo obliga la resolución A4609 del Banco Central".

Según un estudio de KPMG y la revista Continuity Insights, el 88 por ciento de las firmas que crearon un plan de continuidad del negocio (BCP, por su sigla en inglés) lo hizo para darles persistencia a la operación y recuperación ante emergencias; el 43 por ciento lo hizo por cumplir regulaciones y el 30 por ciento por estándares de la industria.

El corte del servicio "downtime" tiene costos en ingresos, productividad, imagen, evaluaciones crediticias, demandas e infraestructura. Y el 46 por ciento de las empresas estadounidenses aseguró que una hora de "downtime" representa U$S 50.000 en pérdidas y, para el 28 por ciento, implica entre U$S 51.000 y U$S 250.000, según la consultora Eagle Rock Alliance.

## Equilibrio

¿Cómo asumir la inversión en algo que se implementa para no usar? La respuesta surge del equilibrio entre costo y riesgo. Juan José Cerezo, gerente de Ingeniería Informática de Laboratorios Bagó, afirma: "Hay que evaluar la tolerancia de cada área para saber cuánto invertir. Si a un área no le afecta estar tres días sin servicio, no necesita infraestructura de contingencia. Nuestra operación es administrativa y a la noche sincronizamos las bases de datos. No replicamos en tiempo real, porque sería muy caro poner enlaces de más velocidad. Buscamos equilibrio entre costo y riesgo".

En Bagó tienen cuatro centros de procesamiento que cumplen con la norma ISO 17799 en cuanto a procedimientos, seguridad física y prácticas, y prevén certificarlos en ISO 27000. "Un centro funciona al 15 por ciento dando servicio y puede soportar toda la operación desde hace dos años. Está a 250 metros del site central y tiene enlaces de datos, hardware y muchos elementos críticos redundantes y servicios amigos", detalla Cerezo. Y agrega: "Se desarrolló con personal propio. Cada cambio en centros de procesamiento se hizo de acuerdo con normas y eso no implicó más inversión. Con el tiempo, tenemos todo en orden y sin gastar de más". En Banco Itaú tampoco gastaron mucho. "Los costos se refieren a comunicaciones y equipos porque es un site desatendido. La decisión de no tercerizar surgió de 'benchmarks' que indicaron que era más barato hacerlo así", asegura Ercolessi.

Hay tres tipos de sitios de contingencia y su costo se relaciona con el nivel de riesgo: un "hot-site" está siempre online y es el más caro; un "warm-site" actualiza datos cada 48 horas y un "cold-site" semanalmente, además de no tener toda la infraestructura replicada. En el proveedor de productos de oficina Officenet tienen planes e infraestructura de contingencia, pero no en todos los sistemas. Federico Cavada, gerente de Tecnología de la firma, dice que "a los costos de infraestructura debimos sumarle un 30 por ciento, pero se hizo a medida que hubo recursos. Tenemos redundancia de enlaces por fibra para la salida a Internet y el acceso LAN-to-LAN hacia el data center externo: si se corta una salida de fibra, el usuario es redireccionado a la otra".

"Es importante que los proveedores cumplan los acuerdos de nivel de servicio (SLA) relacionados con redundancia —agrega—. Para conectividad interna, en cada rack hay un switch de back up y para el call center tenemos un doble tendido de multipares y equipos de back up. Para cada servidor crítico de producción hay uno de respaldo y un plan para migrar el servicio si hay problemas. Los back ups garantizan la recuperación de la información ante un desastre y usamos más de un medio (cinta y discos). Además, tenemos energía separada Clase A y Clase B para cada fuente de los servidores, y un generador eléctrico."

## Determinar el plan

Es como un seguro: hay que tenerlo y aspirar a no usarlo. El BCP es integral, revisa y prioriza los procesos, y decide cuáles no pueden caerse. Incluye al plan de recuperación de desastres (DRP), orientado a recuperar el centro de cómputos tras un desastre.

Para crear un BCP es útil un análisis de impacto del negocio (BIA), que mide los efectos del corte de un servicio en cada área e identifica riesgos y probabilidad de ocurrencia. Entonces, se escribe el BCP —documento con procedimientos a seguir en caso de desastre—, referido a telecomunicaciones, centro de cómputos, logística, capacitación del personal, responsables, DRP, políticas de back up, comité

**Claves para el CEO**

Evaluar los riesgos asociados de no tener una infraestructura de contingencia. Disponer de la inversión necesaria en dinero y recursos humanos para crear, mantener y actualizar la infraestructura de contingencia. Comprometer al responsable de la infraestructura de contingencia ante

Claves para el CEO: Evaluar los riesgos asociados a no tener una infraestructura de contingencia. Disponer de la inversión necesaria tanto de dinero como de recursos humanos para crear, mantener y actualizar la infraestructura de contingencia. Comprometer al responsable de la infraestructura de contingencia en todas las áreas del negocio. No es una tema del área de sistemas solamente asegurar que exista un plan de contingencia y que todas las áreas de la empresa sepan cómo actuar ante un desastre es vital para cualquier compañía. La responsabilidad va más allá de la de IT. (o sea, más allá del área de SI/TI )

**Claves para el CIO**

Es clave documentar el impacto de la caída del servicio en cada área y los riesgos potenciales que se enfrentan. Se deben definir los requerimientos de prevención y recuperación según la criticidad de los procesos y el riesgo aceptado. Probar y revisar el plan de continuidad del negocio (BCP) y crear equipos con responsabilidad sobre la contingencia son parte del trabajo que debe completarse con el ar-

Claves para el CEO: Es clave documentar el impacto de la caída del servicio en cada área y los riesgos potenciales que se enfrentan. Se deben definir los requerimientos de prevención y recuperación según la criticidad de los procesos y el riesgo aceptado.
Probar y revisar el **P**lan de **C**ontingencia del **N**egocio (**BCP**) y crear equipos con responsabilidad sobre la contingencia son parte del trabajo que debe completarse con el armado del un BCP entendible, concreto y sencillo.

del servicio. La ejecución puede hacerse duplicando o virtualizando servidores, o tercerizando servicios en la crisis".

En Laboratorios Bagó trabajan con clusters y virtualización. Cerezo explica que "tener recursos virtualizados hace innecesario duplicar todo. Tenemos duplicados los firewalls, los servicios de correo y las bases de datos, ya que en una contingencia la idea es mantener los servicios y no que la performance sea igual a la operativa. Identificamos dos riesgos, que son la seguridad física, porque siempre hay manifestaciones donde estamos, y la provisión de energía eléctrica, ya que un corte de luz en Buenos Aires implicaría dejar sin servicio a 23 centros de datos y 1.500 personas. Entonces, definimos tres niveles de seguridad para ingresar al centro de datos, relacionados con cerraduras

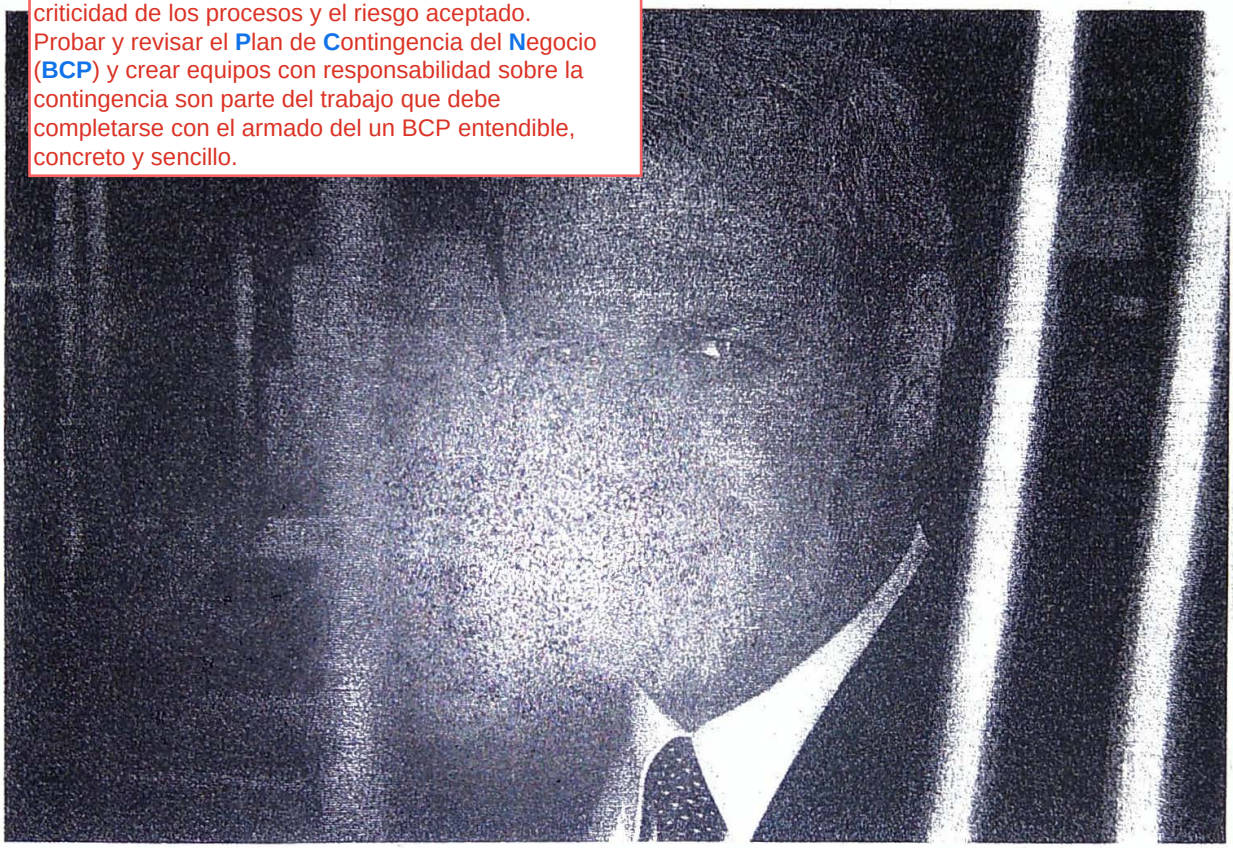


Foto: Gustavo Fernández

de crisis, sitio de contingencia, pruebas y actualización del plan.

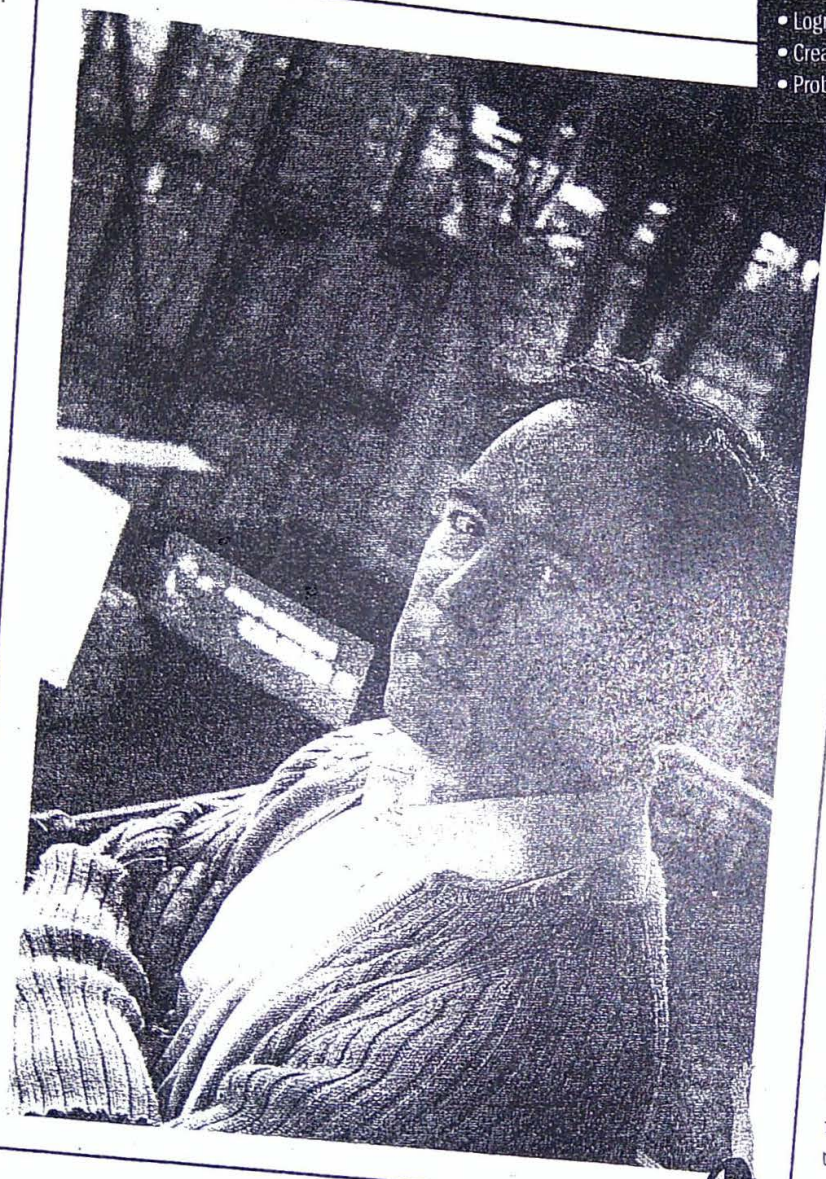
Hay dos entidades que crean certificaciones y "mejores prácticas": Business Continuity Institute (BCI), del Reino Unido, y Disaster Recovery Institute (DRI), de los Estados Unidos.

Cavada, de Officenet, cree que "la solución no es sólo duplicar, sino definir planes de contingencia y estar preparados. También hay que prevenir, porque el mantenimiento baja riesgos. Lo efectivo o no es el plan de contingencia: nuestra intención es cumplir con los clientes y su diseño se basa en la criticidad

**"El negocio de un banco se basa en información y, si no está disponible, no soporta más de 24 horas"**
**CLAUDIO ERCOLESSI,** gerente de Tecnología y Procesamiento de Datos de Banco Itaú Buen Ayre

inteligentes y controles de video, y compramos un grupo electrógeno".

En Tetrapak Argentina no tienen un DRP local, pero "hay planes de resguardo de datos y redundancia en algunos servicios locales. La información crítica está en un servidor en otro país y las sucursales se conectan con ese servidor, que tiene una infraestructura de contingencia con altas normas de seguridad. Con este esquema, la contingencia consiste en replicar los links internacionales y tenemos una conexión de topología estrella: las cuatro locaciones argentinas usan el link internacional a través de la oficina de Buenos Aires. Para tener disponibilidad inmediata deberíamos cuadruplicar el costo de las comunicaciones internacionales", manifiesta Marcelo Pagano, IT/IS Manager de la empresa.



**"A los costos de infraestructura debimos sumarle un 30 por ciento, pero se hizo a medida que tuvimos recursos"**
**FEDERICO CAVADA,**
gerente de Tecnología de Officenet

## Dinámica de la continuidad

Según un informe hecho por Dynamic Markets en 2007 para Symantec, aunque el 91 por ciento de las empresas revisan el BCP, la mitad de los ensayos falla porque la tecnología y/o las personas no están preparadas.

En Officenet los planes de contingencia surgen "de pensar los riesgos, de errores y de auditorías. La idea es hacer pruebas cada seis meses, pero priorizamos los servicios críticos. Hubo cortes y las infraestructuras de redundancia de telefonía y redes de datos funcionaron. También usamos los servidores de back up por la caída de un servicio crítico y en minutos volvimos a operar", cuenta Cavada. En Tetrapak, los planes de contingencia "se revisan anualmente y por auditoría externa, que marca mejoras que deben cubrirse inmediatamente", relata Pagano.

Bagó tiene "un equipo para mantener la infraestructura de contingencia aunque no exclusivamente, formado por gente de redes, base de datos, comunicaciones y seguridad informática. Al adherir a la ISO 17799 hay revisiones cuatrimestrales", explica Cerezo. En Banco Itaú Buen Ayre hay "un área de continuidad de negocios que fija el DRP y hace tres pruebas anuales: en 2007 operamos una semana con el sitio alternativo. Si no se hacen pruebas, en la crisis no se sabe qué hacer. Nosotros filmamos y documentamos todas las pruebas. Y hay un comité de crisis, con 15 personas a mi cargo, donde todos tienen un pen drive con indicaciones de cómo actuar", apunta Ercolessi. Y concluye con un consejo: "Un plan de contingencia es dinámico, no tiene fin". ■

### GUÍA PARA UN BCP EXITOSO

- Documentar el impacto de la caída del servicio en cada área y riesgos potenciales.
- Definir requerimientos de prevención y recuperación según la criticidad de los procesos y el riesgo aceptado.
- Lograr un BCP entendible, concreto y sencillo.
- Crear equipos con responsabilidad sobre la contingencia.
- Probar y revisar el BCP.