



BUSINESS CONTINUITY PLAN: **ES MOMENTO DE ASEGURAR LA CONTINUIDAD DEL NEGOCIO**

Por: Roberto Cabrera e Ignacio Martínez

Cuando las empresas dependen fuertemente de su infraestructura de tecnologías de la información, todos los riesgos y amenazas deben ser considerados. Un buen Plan de Continuidad de Negocios asegura que los datos y la infraestructura estén cubiertos contra cualquier contingencia.

Tabasco, noviembre 2007. Las intensas lluvias y el desbordamiento de varios ríos de la región ponen al estado en alerta máxima. Un millón de personas se ven afectadas. No sólo sus hogares se han inundado; sus centros de trabajo y negocios también. Ante una emergencia como ésta las primeras 72 horas son críticas para saber si el negocio se recuperará o perecerá. ¿Su empresa está preparada para una emergencia? Si es así, ¿cuáles serán las consecuencias? ¿Sabe qué hacer para que la contingencia no afecte a las operaciones diarias de su negocio?

Ha sido muy difícil concientizar a las empresas de tomar en serio el costo de perder una de sus joyas más preciadas: la información. Es debido a los atentados terroristas del 11 de septiembre en Estados Unidos que se ha logrado esta conceptualización o entendimiento.

Si bien ya existía el concepto de Plan de Recuperación en Caso de Desastres (Disaster Recovery Plan), es el Business Continuity Plan (BCP, por sus siglas en inglés) o Plan de Continuidad de Negocios el que se ha impuesto como una práctica preventiva en los corporativos.

¿Qué incidentes contempla un BCP? No sólo ataques terroristas, terremotos, inundaciones o incendios. También cosas tan comunes y de todos los días como fallas eléctricas, accidentes o, peor aún, ataques internos por empleados descontentos.

México vive su propio contexto político, social y de infraestructura, además de sus condiciones climáticas específicas. De ahí que deban considerarse cortes en la energía eléctrica, en el teléfono, y falta de acceso a las computadoras y a Internet. En algunos casos el aire acondicionado es un servicio infaltable.

Actualmente casi todas las compañías dependen de los avances tecnológicos y una interrupción en estos servicios no tiene que darse sólo a través de una explosión. Por ejemplo, los bloqueos de carreteras y avenidas que realizan algunos grupos inconformes pueden ocasionar severas pérdidas a las empresas.

Citemos el caso de una empresa de telecomunicaciones. El impacto de un incendio en su planta de manufactura de chips se volvió legendario. El fuego, ocurrido en marzo del 2000, inició en una lámpara y duró apenas 10 minutos, pero causó estragos en el "cuarto limpio" donde se fabrican los microprocesadores. La empresa reportó pérdidas por más de \$2,000 millones de dólares en su división de teléfonos celulares, un quebranto que los dejó muy lastimados en un sector donde habían sido líderes. La lección no fue haber perdido mercado ante la competencia, sino no tener a un proveedor global remoto.

Insistimos, para mitigar el impacto de estas contingencias es importante contar con un BCP porque resguarda uno de los activos más importantes de las empresas: la información.



Durante el año pasado ¿Su compañía resultó afectada por alguna de las siguientes interrupciones?

Falla en la electricidad	59.07%
Fallas en el hardware	51.04%
Desastres naturales	46.87%
Falla de telecomunicaciones	41.73%
Fallas en la red	40.61%
Fallas en el software	39.97%
Errores humanos	37.72%
Fusiones/adquisiciones	24.24%
Disputas laborales	6.90%
Terrorismo	4.98%
Guerra	2.41%

LA EMPRESA DEBE CONTINUAR

Un Business Continuity Plan debe ser considerado parte integral de la estrategia del negocio. Un buen plan revisa los procesos críticos de la operación en las empresas, los clasifica, prioriza y determina cuáles son los más sensibles y cuáles no pueden dejar de operar para que el negocio continúe su funcionamiento.

Si las empresas no cuidan ni manejan correctamente su información, en el momento en que padezcan una eventualidad no podrán atender asuntos prioritarios como: a quién le deben pagar, quién les debe, a quién le venden, a quién le deben otorgar un descuento, quién es meritorio de un crédito, entre otras variables vitales del negocio.

El hecho de no poder acceder a estos datos (no saber cómo operan, cuántas piezas producen, cuál era el pedido urgente, cuándo llega la materia prima para correr la programación de producción, entre otros) puede ocasionar importantes pérdidas al negocio.

En México muy pocas empresas tienen un plan BCP, el mayor número de empresas en México son medianas y pequeñas y en una gran proporción dependen de la tecnología y, sin embargo, carecen también de un BCP. Es, por mucho, más barato prevenir que corregir o reaccionar.

Desafortunadamente en nuestro país no está muy extendida la cultura de la prevención. La cultura de la planeación de desastres es poco común. Roberta J. Witty, Vicepresidenta de Investigación de la consultora Gartner, menciona que una de cada dos empresas en el mundo tiene la experiencia de algún tipo de eventualidad o desastre; 40% de los negocios desaparece inmediatamente o pocos años después del desastre.



1 de cada 2 empresas en el mundo ha tenido la experiencia de algún tipo de eventualidad o desastre; 40% de éstas desaparece inmediatamente o pocos años después del desastre

En un ejercicio de autoevaluación, Gartner ha invitado a diversas empresas a considerar y probar si sus sistemas podrían seguir operando a pesar de que un 30% del staff esté ausente de la oficina.

Recientemente, AXA, una aseguradora europea, encontró en un estudio que 46% de los medianos y pequeños negocios en Gran Bretaña no poseen un Plan de Continuidad de Negocios de ninguna especie, a pesar de haber sido alertados de los riesgos de una interrupción. Para algunas de estas empresas la tarea era demasiado desalentadora y los riesgos muy altos, pero estas compañías prefirieron asumir los costos de la suspensión.

El primer gran obstáculo que deben enfrentar las corporaciones que no han implantado un BCP es el desconocimiento. La segunda dificultad a vencer es el presupuesto. Dentro de las corporaciones debe dimensionarse al BCP como un seguro: hay que tenerlo para en ocasiones no usarlo, pero el día en que se requiera la empresa saldrá adelante.

¿Cuáles son las razones por las que su compañía decidió implantar un BCP?

Continuidad de las operaciones del negocio y recuperación en una emergencia	88.30%
Regulaciones gubernamentales	43.19%
Estándares de la industria	30.43%
Requerimiento de los clientes	25.11%
Ventaja competitiva única	16.81%

Fuente: A Review of the Factors Influencing Business Continuity Management Programs, KPMG y la revista Continuity Insights, 2007

El BCP debe dimensionarse como un seguro: hay que tenerlo y el día en que se requiera la empresa saldrá adelante

Un BCP es para todo tipo de industria. Los sectores en donde más se encuentran planes de continuidad o recuperación de desastres son los de comercio detallista, financiero, telecomunicaciones, manufacturero, industrial, de servicios y automotriz; sin embargo, son los primeros tres los que más han invertido en la prevención del cuidado de su información.

TECNOLOGÍA POR DOQUIER

Los orígenes del BCP se centran en el respaldo de la información en una computadora distinta a donde se lleva la operación del negocio. Hoy es un servicio conocido como centros de datos (data centers). Actualmente este servicio ha evolucionado y además de respaldar hardware, sistemas (software) y telecomunicaciones, se añadieron también los procesos. Es momento de ir más allá de los procesos: hay que estar disponible en el momento en que los clientes lo demanden y exceder sus expectativas.

Por ejemplo, en una cadena de tiendas, el cliente reporta en caja la escasez de un producto. La cadena de autoservicio podría enviarle al día siguiente un mensaje SMS (Short Message Service, por sus siglas en inglés) avisando que el artículo faltante ya está disponible en la tienda. O bien, que las aseguradoras pudieran terminar con la angustia del asegurado de no saber en qué momento llegará el ajustador. Podrían enviar cada cinco minutos mensajes al celular avisando en dónde se encuentra el ajustador y en qué tiempo estimado estará con ellos. Evidentemente un BCP tiene varios niveles y depende del sector en el que se desempeñe la empresa para que lo implante.

Las primeras 72 horas de interrupción en un negocio son críticas. Son vitales para saber si el negocio se recupera o muere. Morir no será un acto inmediato, sino que puede ser un proceso irreversible y lento porque no tuvieron respuestas inmediatas y los clientes eligieron a la competencia.

En dicho periodo la empresa debe tener las acciones bien planeadas, y debe conocer las consecuencias de la recuperación. Por ejemplo, es importante saber qué le ocurrirá a la compañía durante esas 72 horas y reaccionar con base en dicha prevención.

¿QUIÉN ADMINISTRA EL BCP?

El responsable del BCP es el Director de Administración en conjunto con el Director de Sistemas y, claro está, con el apoyo del Director General. Un BCP es un proyecto de toda la empresa. Para aplicar un BCP, antes hay que entender el funcionamiento de la compañía, y conocer los procesos. Y esto lo tienen que entender todos los empleados de la firma.

¿Quién es el principal impulsor del BCP en su empresa?

Director del programa de Business Continuity Management	21.91%
Coordinador del programa de Business Continuity Management	14.04%
Director del Departamento Específico	10.64%
Vicepresidente del programa de Business Continuity Management	9.79%
Director/Vicepresidente de Seguridad	5.74%
Director de Sistemas	5.32%
CEO/Presidente	4.04%
Director de Riesgos	3.62%
Director de Operaciones	3.40%
Director de Finanzas	1.49%
Otros	11.49%

Fuente: A Review of the Factors Influencing Business Continuity Management Programs, KPMG y la revista Continuity Insights, 2007

PASOS DE UN BCP

Las características de un BCP son que tiene que ser claro, entendible y concreto. Y para conseguirlo debe componerse de los siguientes pasos:

1. Entender los procesos del negocio
2. Identificar procesos vitales
3. Minimizar la toma de decisiones durante una crisis
4. Definir los beneficios

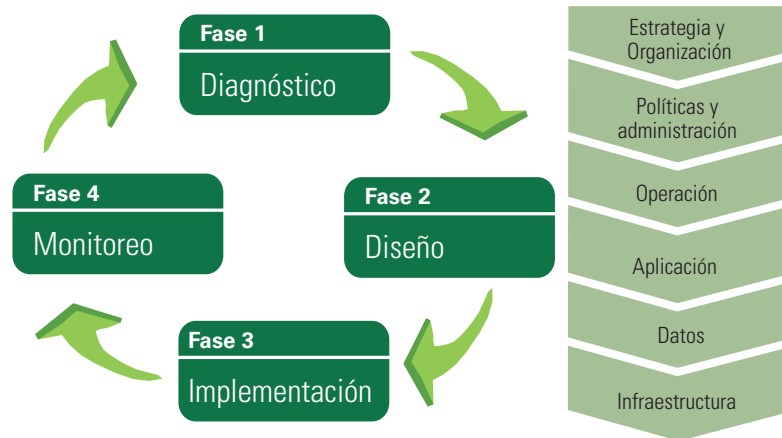
El beneficio más importante de un BCP es el conocimiento de la operación y de todos y cada uno de quienes participan en el negocio. Es importante reiterar que un BCP no es sólo para los directivos, es para todos los elementos de la corporación.

El BCP no sólo se refiere a infraestructura; el capital humano tiene un peso importantísimo en su exitosa aplicación porque es la gente quien lo va a operar. Si el personal no está capacitado y si no entiende su función, ni el mejor BCP conseguirá su objetivo.

Un gran beneficio de un BCP es que ayuda a reconocer qué procesos son los que deben mantenerse activos ante cualquier eventualidad y les da prioridad ante la contingencia

METODOLOGÍA KPMG

Es importante que cualquier BCP se desarrolle bajo una estrategia. El siguiente esquema resume la arquitectura de la metodología BCP:



Fuente: KPMG

Dada la profundidad y extensión de la metodología hay que mencionar de forma general sus fases y sus actividades:

Fase 1 - Diagnóstico

El objetivo de esta fase es partir del entendimiento de la organización, determinar el nivel de riesgo y la efectividad de los controles asociados a los componentes de un servicio, el impacto de una interrupción sobre los procesos del negocio y qué acciones a corto, mediano y largo plazo se deberían tomar para mitigar riesgos y mantener la disponibilidad en la prestación del servicio.

Las actividades que se realizarán en esta fase del proyecto son:

- Entender el negocio y el modelo de entrega del servicio
- Realizar el mapeo de interdependencias de procesos
- Evaluar la capacidad de recuperación y respuesta
- Realizar análisis de impacto (BIA, por sus siglas en inglés)
- Diagnóstico de la situación actual
- Elaborar el plan de acciones y recomendaciones

Fase 2 - Diseño

Basados en los resultados obtenidos en el análisis de riesgo e impacto se identifican las posibles estrategias de recuperación que apliquen a la entidad con el fin de seleccionar la que más se ajuste. Adicionalmente se elabora el plan de contingencia de TI.

La actividad que se realiza en esta fase del proyecto es:

- Diseñar estrategias de contingencia y/o continuidad

Fase 3 - Implantación

El objetivo de esta fase es acompañar a la empresa en la elaboración e implantación de las medidas de contingencia y el plan diseñado.

Nota importante: esta fase requiere que se hayan realizado las inversiones y acciones definidas en las fases anteriores.

- Elaboración del plan de contingencia de TI
- Acompañamiento en la implantación de las medidas de contingencia

En esta fase se inicia el proceso de ejecución e implantación de la arquitectura de la solución y del plan de contingencias de tecnología. La meta es proveer una estructura que facilite la administración de la implantación de las estrategias planteadas y los planes de transición, de forma tal que ayude a los implantadores a obtener resultados positivos.

Fase 4 - Monitoreo

Hay que validar el funcionamiento de la estrategia seleccionada y realizar los ajustes necesarios. Hoy las empresas deben ser más exigentes en la pruebas de un BCP, ya que un plan de continuidad no vale por lo que está impreso o escrito en el papel, sino por sus pruebas regulares. La intensidad y frecuencia de los simulacros dependen de las circunstancias y del negocio.

Un BCP es un plan vivo, de tal forma que hay que actualizarlo periódicamente. Se recomienda una revisión por lo menos cada año, aunque depende del tipo de negocio. Y para quienes ya tienen un plan de continuidad, es necesario revisar si es el adecuado y actualizarlo en dicha temporalidad.



NIVELES DE DISPONIBILIDAD

En nuestra experiencia creemos fervientemente -y así lo llevamos a la práctica- que si un BCP es llevado adecuadamente, encontrando un punto medio entre la previsión y la recuperación -combinando los factores de costo y tiempo-, no sólo mantendrá a la empresa a flote durante una crisis, sino que también puede mejorar la competitividad de la misma llevándola a un mejor entendimiento de todos los procesos de la organización.

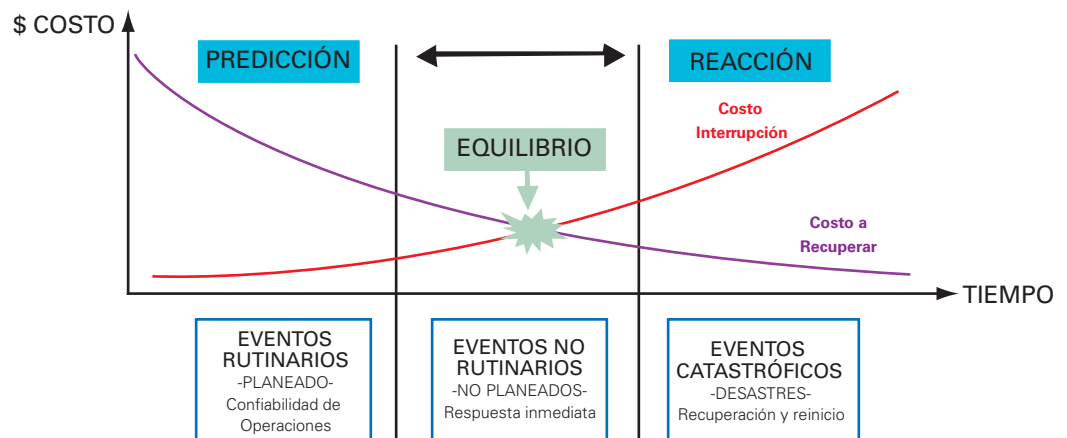
Un punto importante recae en la relación entre el costo y el tiempo en la reacción. Las empresas pueden contratar tres diferentes tipos de sitios:

Hot-site: Está todo el tiempo en línea. Si algo le pasa a la operación, el otro sistema entra simultáneamente. Evidentemente el costo es muy alto por la disponibilidad requerida.

Warm-site: Se actualizan los datos cada 48 horas.

Cold-site: Se recupera la información cada semana.

En México el que más se utiliza es el cold-site. Lo importante es tener un equilibrio entre la prevención y la reacción sobre el tiempo y el dinero.



En el libro llamado *La Empresa Resistente* de Yossi Sheffi, profesor de ingeniería en sistemas en el MIT, se ofrecen algunas guías a las empresas que aún no han calculado los riesgos. "Las interrupciones de gran escala rara vez aparecen sin una advertencia," dice Sheffi. Al monitorear y analizar cuidadosamente las fallas mínimas, las aerolíneas han evitado muchos accidentes. Aprender de los pequeños incidentes puede ayudar a las entidades a corregir las condiciones que propician las grandes catástrofes.



DESARROLLO DE UN BCP

Para entender mejor un BCP y/o desarrollar uno, deben considerarse cuatro aspectos: funciones, resultados, requerimientos y metodología.

1.- Un BCP debe tener ciertas funciones primordiales, tales como:

- Minimizar la necesidad de toma de decisiones durante una crisis
- Definición de alternativas para la continuidad de servicios críticos
- Definición de prioridades y marcos de referencia de tiempo

2.- Los beneficios que se esperan (si el plan no se usa):

- Prevención es mucho mejor en cuanto a costo-beneficio que la recuperación
- El entrenamiento administrativo y la concientización van aumentando conforme todos y cada uno de los participantes se involucran en el BCP

3.- Los requerimientos mínimos o puntos claves para tener éxito en el BCP son:

- Asegurarse que la administración esté consciente y de acuerdo con el esfuerzo total que es requerido para desarrollar y mantener el plan efectivo
- Obtener el compromiso apropiado en cuanto al soporte y participación del desarrollo del plan, así como a su implantación
- Definir requerimientos de recuperación focalizados en los procesos particulares del negocio
- Documentar el impacto de una pérdida extendida de la operación del centro de datos
- Desarrollar la capacidad de respuesta (self-sufficiency) para mantener eficientemente y probar con frecuencia los planes
- Definir apropiadamente la prevención de los desastres, la minimización de los impactos y la recuperación
- Seleccionar o definir equipos de trabajo con personal comprometido y experiencia funcional, así como de la industria o negocio de la empresa
- Desarrollar un BCP que sea entendible, fácil de usar y de darle mantenimiento
- Desarrollar un mecanismo para asegurar la plantación futura en el negocio de un desarrollo de procesos de sistemas considerando implicaciones de recuperación para asegurar la viabilidad de desarrollo de planes de continuidad

Los pilares del BCP

1. Disponibilidad: estar siempre cuando el cliente lo requiere y superar sus expectativas
2. Confiabilidad: que los datos sean fidedignos y fiables
3. Recuperación: respuesta y reacción pronta





UNIVERSIDAD PROTEGIDA

Hace casi cuatro años una universidad decidió establecer un BCP. La institución cuenta con 30 campus en la Ciudad de México, en la zona Metropolitana y en el interior de la República. Su población de alumnos es aproximadamente de 30 mil y su plantilla de profesores, administrativos, directivos y mantenimiento asciende a 4 mil.

Su operación diaria es mucho más complicada de lo que parece a simple vista debido al manejo de una gran cantidad de información. Los administrativos deben saber con certeza qué profesores llegaron a su clase y a qué hora, la cantidad de clases y alumnos registrados en ellas, si son profesores de tiempo completo o por asignatura, qué vida útil tienen los equipos de los laboratorios o el mantenimiento necesario, entre otras muchas cosas.

Sin duda alguna, para la escuela es importante saber también quiénes adeudan colegiaturas, las materias que han cursado y/o acreditado los alumnos. Así pues que con el BCP que poseen, la universidad ha protegido su información. Además, muy bien puede saber a quién y cuánto pagar por concepto de nómina, qué proveedores han cumplido, o más importante, a qué alumnos puede extenderles una constancia de estudios, en el caso de ocurrir cualquier eventualidad.

El mantenimiento que se le da a este documento es constante debido al crecimiento tanto en la plantilla de profesores como de alumnos e instalaciones. Tanto el personal como los alumnos y profesores saben qué hacer en caso de diferentes tipos de emergencias y están en constante capacitación gracias a los simulacros que se realizan.

Por fortuna, hasta este día la institución no ha tenido que hacer uso del BCP; sin embargo, la universidad se encuentra preparada para cuando así tenga que ser. En la decisión de contar con un BCP, participaron los gerentes de Sistemas, de Riesgos y de Finanzas. De hecho, la universidad cuenta con un Comité de Riesgos, responsable de ejecutar las medidas para prevenir eventualidades. Identificar y promover las medidas de riesgo es tarea del área de Finanzas.

Actualmente, la institución académica tiene la confianza de estar preparada ante cualquier eventualidad. De ahí que anualmente revisen su BCP para mantener la operación protegida y asegurar la continuidad de la universidad.

Conclusiones

Ante un panorama mundial de constantes cambios, las compañías se enfrentan a situaciones alarmantes como ataques terroristas, epidemias, virus, terremotos, inundaciones, huracanes, incendios, etc.

Los planes de contingencia en las empresas antes consistían en duplicar la infraestructura central de TI en caso de que los sistemas fallaran. Hoy, sin embargo, las compañías reconocen que no basta sólo con duplicar, también deben considerar otras amenazas potenciales que pueden interrumpir su operación.

Un Business Continuity Plan debe ser considerado parte integral de la estrategia del negocio. Y es que un buen BCP revisa los procesos críticos de la operación en las empresas, los clasifica, prioriza y determina cuáles son los más sensibles y cuáles no pueden dejar de operar para que el negocio continúe su funcionamiento.

Un BCP es para todo tipo de industria y tamaño de empresa. El beneficio más importante de un BCP es el conocimiento de la operación y de todos y cada uno de quienes participan en el negocio; no es sólo para los directivos, es para todos los elementos de la corporación.

Un BCP debe ser actualizado periódicamente de acuerdo al entorno de la organización. Se recomienda una revisión por lo menos cada año, y para quienes ya tienen un plan de continuidad, es necesario revisarlo y actualizarlo. Lo más importante es mantener el BCP como un plan vivo y dinámico.

Sobre los autores:



Roberto Cabrera

Roberto Cabrera es Socio a Cargo de la Práctica de Servicios de Asesoría en Riesgo de KPMG en México. Cuenta con más de 25 años de experiencia dando consultoría a importantes organizaciones nacionales e internacionales en sectores como: manufactura, comercio al detalle, servicios financieros, educación, salud, construcción, medios y entretenimiento, tecnología y telecomunicaciones, así como al gobierno. Antes de colaborar con KPMG, Roberto trabajó en Andersen Consulting y posteriormente inició su propia compañía de consultoría, Grupo Corporativo de Consultoría. En 1998, IBM adquirió su empresa y Roberto permaneció al mando de 1998 al 2002. Posteriormente, Roberto se integró a IBM, donde fue el Director de Business Integration Services. A partir del 2004 colaboró en PeopleSoft como Vicepresidente de Servicios para América Latina. Roberto tiene amplia experiencia en Mejora de Procesos, Business Intelligence e Implantación de aplicaciones empresariales.



Ignacio Martínez

Ignacio Martínez es Gerente de la Práctica de Servicios de Asesoría en Riesgos de KPMG en México. Cuenta con más de 18 años de experiencia dando consultoría a empresas de diferentes sectores, entre los que destacan: manufactura, construcción, tecnología, telecomunicaciones y servicios financieros. Ignacio se especializa en la selección e implementación de planificación de recursos empresariales (ERPs, por sus siglas en inglés), tales como JDEdwards, Solomon y Oracle. Ignacio tuvo a su cargo el desarrollo e implementación de productos bancarios de Banpaís mediante la domiciliación de éstos a través de Internet, así como del sistema de intercambio y venta de efectivo de la Cámara de Compensación Bancaria (Cecoban). En los últimos años se ha especializado en la consultoría de productos de seguridad, controlando y monitoreando las actividades de los usuarios en la red. En KPMG ha conducido, participado y colaborado activamente en la presentación, demostración y asesoría de proyectos de Seguridad (Security), Atestiguamiento SAS 70 (Attestation), Análisis de Procesos (Business Process Management), Análisis y Selección de Proveedores de IT (Sourcing Advisory) y Continuidad de Negocio (Business Continuity).

Si le interesa contactar a los autores de este artículo o desea información adicional, favor de dirigirse al 01 800 292 KPMG, o si lo desea escríbanos a asesoria@kpmg.com.mx.

Esta propuesta ha sido realizada por KPMG Cárdenas Dosal, S.C., la firma mexicana miembro de la red de firmas independientes afiliadas a KPMG International, cooperativa suiza, y está en todos los aspectos sujeta a la negociación, acuerdo y firma de una carta convenio o un contrato específico o la aprobación del destinatario de este documento. KPMG International no provee servicios a clientes. Ninguna firma miembro tiene autoridad para obligar o comprometer a KPMG International ni a ninguna otra firma miembro frente a terceros, ni KPMG International tiene autoridad alguna para obligar o comprometer a ninguna firma miembro.

"D.R." © 2008 KPMG Cárdenas Dosal, S.C. la firma Mexicana miembro de KPMG International, una cooperativa Suiza. Manuel Avila Camacho 176, México, 11650, D.F. Impreso en México. KPMG y el logotipo de KPMG son marcas registradas de KPMG International, una cooperativa suiza