

Riesgo Inteligente en la era de la incertidumbre global

Preparación sensata para un sinfín de amenazas



Índice

Prefacio	3
Gripe Aviar: ¿amenaza real o falsa alarma?	4
Impacto repentino	5
Preparación sensata y práctica	6
Velocidad del ataque	7
Recomendaciones	7
¿Cómo hacer una elección de Riesgo Inteligente?	8
Apéndice: Los siguientes pasos	10
Contactos	12

Prefacio

Esta publicación es el segundo folleto de nuestra Serie “Riesgo Inteligente”. Los conceptos y puntos de vista que se presentan aquí están basados en aquellos discutidos en el primer folleto informativo de la serie, *La Empresa de Riesgo Inteligente: Administración de Riesgos Empresariales (ERM) bien realizada*, el cual se puede obtener de manera gratuita en www.deloitte.com/RiskIntelligence.

Como se explicó en el folleto anterior, una de las características más importantes de la Empresa de Riesgo Inteligente™ es su “filosofía de administración de riesgos enfocada, no sólo a evitar riesgos, sino asumirlos como medio de creación de valor.”

Este punto es lo suficientemente importante para reiterarlo, aunque de forma breve, en este folleto. Pero los lectores observarán que el tema en cuestión—prepararse para sucesos de una variedad aparentemente infinita y que causan graves interrupciones – se presta para que el trabajo se centre más en mitigar y evitar riesgos que en asumirlos para obtener premios. El enfoque más estricto de este folleto no debe obscurecer el panorama general, ni representa un cambio de perspectiva de nuestra parte. Como indicamos en el primer folleto:

“Las organizaciones más eficaces y eficientes en la administración de riesgos para el mantenimiento de sus activos existentes y su crecimiento futuro, superarán, a largo plazo, aquéllas que no los son. En otras palabras, las compañías hacen dinero tomando riesgos y pierden dinero al no administrarlos.”

Riesgo Inteligente en la era de la incertidumbre global

Preparación sensata para un sinfín de amenazas

Al leer cuidadosamente las noticias uno llega a una conclusión inevitable: El mundo es un lugar extremadamente peligroso – y cada vez se vuelve más peligroso.

El sinfín de riesgos –reales y percibidos, nos asalta desde todos los ángulos: terrorismo y guerra; violaciones a la privacidad de información y seguridad de la TI; desastres naturales y provocados por el hombre; inestabilidad en el mercado y crisis monetarias; residuos peligrosos y accidentes industriales; demanda excesiva de energía eléctrica y escasez de combustibles; y así sucesivamente.

La manera en que, como personas, abordemos esta avalancha de preocupaciones es un asunto privado entre nosotros y nuestras deidades, psicólogos y/o seres amados. Pero, como gente de negocios, la manera en que percibimos, abordamos y administramos los riesgos no debe ser tomada a la ligera, ni dejada a la casualidad. Sencillamente, es mucho lo que está en juego.

Gripe Aviar: ¿Amenaza real o falsa alarma?

En las noticias aparecen constantemente informes sobre una posible pandemia de gripe aviar. El Banco Mundial estima que un brote grave del virus H5N1 entre los humanos costaría a la economía global cerca de 3.1 por ciento del producto interno bruto, alrededor de \$1.25 trillones de dólares. Este escenario de “caso grave”, preparado por el Grupo de Desarrollo de Prospectos Económicos del Banco, está basado en una tasa de mortalidad de 1%, lo que significa que 70 millones de personas fallecerán por el virus¹. Por supuesto, muchas más personas (hasta 40% ciento estimado de la fuerza laboral global²) podrían incapacitarse temporalmente a causa de la enfermedad. Claramente, el impacto humano, social y financiero de dicha calamidad sería devastador.

Aun cuando estas predicciones de una pandemia son serias, aquí tenemos un pensamiento en sentido contrario:

Las terribles advertencias sobre la gripe aviar son irrelevantes.

Esto no es por decir que el espectro de la virulenta enfermedad no es de gran preocupación. Sin embargo, en términos de negocio, no importa realmente si las desoladoras predicciones van a ocurrir, ya que si esta pandemia no les llega, con toda seguridad, algo más lo hará. La historia nos dice que en los siguientes años y décadas, todo tipo de hechos podrán causar interrupciones, y los negocios que no estén preparados van a sufrir. En la era de la incertidumbre global, lo único seguro es que a las buenas compañías les pasarán cosas malas.

Considere, por ejemplo, el efecto sobre los negocios si las entregas de petróleo a nivel mundial se redujeran drásticamente debido a guerra, terrorismo o desastre natural. Este escenario no es tan remoto como parece, tomando en cuenta que Estados Unidos mantiene únicamente una provisión de 59 días en la Reserva Estratégica de Petróleo³. Imagine, incluso, un paro laboral de larga duración que detenga embarques de componentes clave del inventario provenientes del extranjero. Visualice, también, un virus que ataque las computadoras y borre los datos de los servidores o las telecomunicaciones de las compañías por un período prolongado.

Afortunadamente, las compañías que entiendan y se preparen para una inevitable interrupción de negocios saldrán mejor librados de los problemas que aquéllas que adopten un enfoque tipo avestruz. La gripe aviar puede o no materializarse, pero sí da a las Empresas de Riesgo Inteligente motivación y oportunidad para abordar los problemas que surjan a partir de una interrupción de los negocios de gravedad extrema.

¹ “World Bank Outlines Economic Effects of Bird Flu” by Ahmed ElAmin, Food Production Daily, 7 July 2006. www.foodproductiondaily.com/news/ng.asp?n=69089-h-n-world-bank-avian

² National Strategy for Pandemic Influenza - Implementation Plan,” U.S. Dept. of Homeland Security Council, May 3, 2006. www.whitehouse.gov/homeland/nspi_implementation.pdf

³ <http://www.fe.doe.gov/programs/reserves/spr/spr-facts.html>

Más allá de dar una razón para actuar, las predicciones de una pandemia también ofrecen una oportunidad para ampliar nuestra propia percepción del riesgo. En un mundo interdependiente, es necesario ser perspicaz.

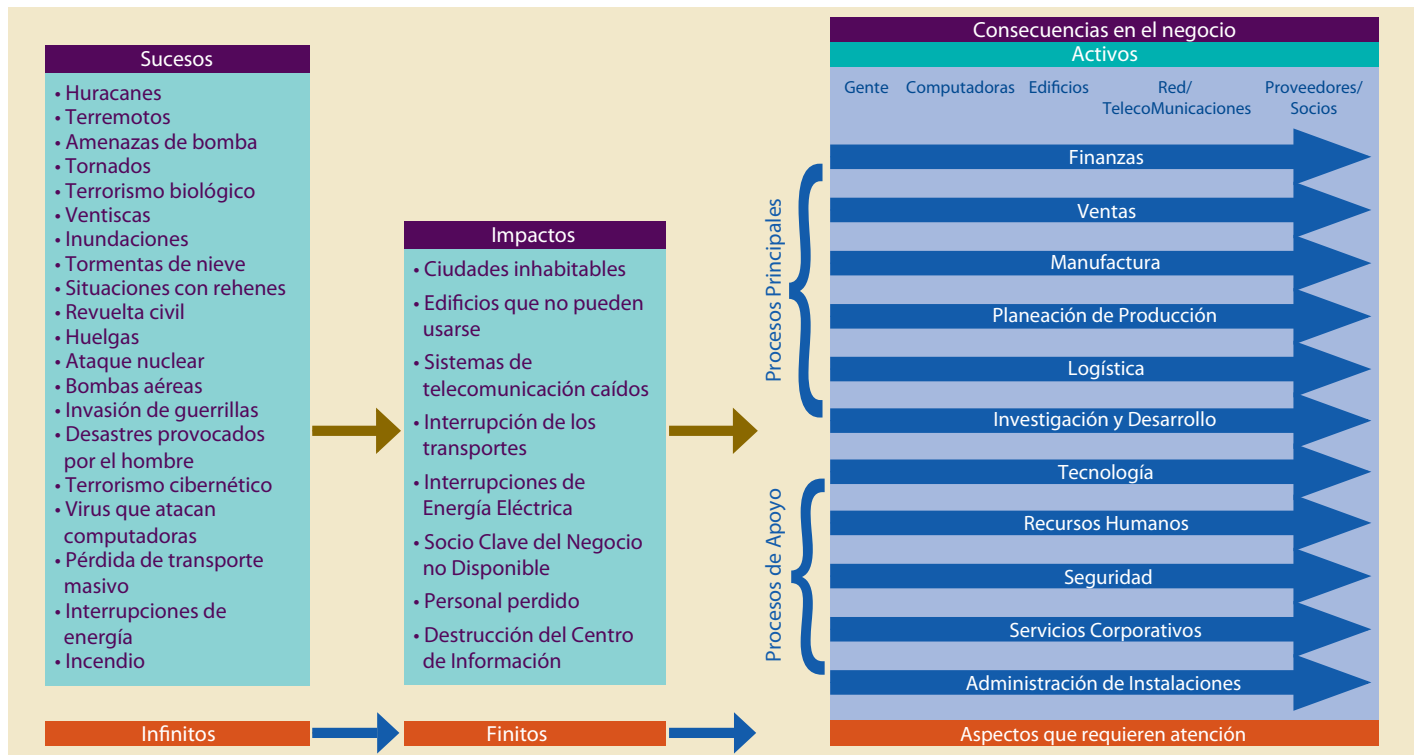
Actualmente, el probable impacto de una interrupción del negocio va más allá de sus muros: hacia arriba, en la cadena de suministros y hacia abajo, a los clientes. Las amenazas a los socios del negocio son amenazas a uno mismo y viceversa.

Asimismo, las compañías deben pensar más allá de su planeación de continuidad del negocio tradicional. Ya no es suficiente preguntar "¿Tengo un lugar externo para almacenar información?" o "¿Puedo cambiar la producción a otra instalación?". Ahora, las compañías también tienen que considerar qué sucedería si muchos lugares se tornan inoperables, o si la gente no puede asistir al trabajo por un periodo prolongado debido a una enfermedad, un edicto o una crisis energética.

Las compañías que tomen medidas para mejorar su resistencia a un impacto antes de que ocurra un acontecimiento, claramente tendrán una recuperación más fácil y rápida, así como una ventaja competitiva en el mercado. Incluso más importante es la resistencia de los negocios que forman nuestra infraestructura crítica — compañías financieras, de energía, de servicios públicos, de construcción y otras — que no sólo beneficia a la compañía, sino que puede ser de gran servicio al interés público.

Análisis del impacto en el negocio

Un conjunto de sucesos infinito puede impactar a un negocio en un número finito de maneras. Evítese el tedioso análisis de sucesos potenciales y en su lugar enfóquese en sus impactos y consecuencias en el negocio.



Impacto repentino

En nuestro primer folleto de la Serie *La Empresa de Riesgo Inteligente: Administración de Riesgos Empresariales (ERM) bien realizada* recomendamos que las compañías se dedican a planear escenarios para aumentar el modelo estadístico y ayudar a prepararse para sucesos específicos. La planeación de escenarios permite a los ejecutivos responder a las preguntas: "¿Qué podría interrumpir nuestros planes? y ¿Qué tan vulnerables seríamos ante esa eventualidad?".

Este proceso es valioso, pero una vez que las compañías hayan integrado la planeación de escenarios a su protocolo de administración de riesgos, es momento de iniciar una práctica complementaria: el análisis del impacto en el negocio. Este proceso llena un vacío crítico de conocimientos, porque aun cuando la probabilidad de la interrupción pueda ser cierta, las causas a menudo son impredecibles.

Un análisis del impacto en el negocio ayuda a ilustrar las maneras en que una compañía se puede ver afectada, independientemente de la causa, y permite identificar los principales impactos, incluyendo los de tipo financiero, humano, legal, accionaria, de reputación, salud y seguridad y en el medioambiente, derivados de un suceso o serie de sucesos.

Las empresas de Riesgo Inteligente implantarán planes de contingencia para que el trabajo pueda realizarse de manera remota, a fin de conservar la continuidad del negocio durante una ausencia prolongada de los trabajadores.

Si se hacen las siguientes preguntas: ¿Cuál sería la flexibilidad de la compañía para solucionar un descenso de crédito importante, boicot contra los productos de la empresa por accionistas, pérdida de las instalaciones principales por un período prolongado, crisis de reputación intensa? Los escenarios negativos posibles son casi ilimitados. El análisis de impacto en el negocio aborda este problema: simplemente, existen demasiadas variables para pronosticar cada suceso (o una serie de sucesos) adversos con los que la compañía tenga que lidiar.

¿Cuáles son algunos de los impactos posibles? Brevemente abordaremos tres de ellos:

Gente: Una característica distintiva de una pandemia es el impacto desproporcionado en la gente. Muchos otros tipos de interrupciones de negocios incluyen pérdidas importantes de propiedades e infraestructura — siendo el terrorismo y los huracanes los casos más recientes. Por otro lado, la pandemia (ocurra de forma natural o por terrorismo biológico) afecta principalmente al capital humano. Por ejemplo, las compañías pueden experimentar un alto nivel de ausentismo, desde los altos funcionarios hasta el personal operativo. Hay a quienes tal vez no les sea posible o no deseen reportarse al trabajo, no sólo por estar enfermos ellos mismos, sino tal vez por miedo, para cuidar a sus familiares enfermos, debido a un decreto gubernamental, o a problemas de transporte. Las empresas de Riesgo Inteligente deben establecer planes de contingencia para permitir que el trabajo se realice a distancia, para mantener la continuidad del negocio durante ausencias prolongadas de los trabajadores.

Cadena de suministros: La cadena de suministros de la compañía también puede ser vulnerable. Diversas interrupciones podrían dificultar la obtención de materia prima; los efectos negativos podrían tener consecuencias en la producción, el inventario y la distribución. La fuerte interdependencia con proveedores requiere vigilancia al estructurar y supervisar estas relaciones. Ciertamente, si no se hace esto con los proveedores más importantes, toda la planeación anticipada de su organización se irá por la borda, debido a la inevitable escasez.

Las compañías también pueden reconsiderar la dependencia de proveedores que sean la única fuente. Aun cuando la intención original de estas relaciones haya sido la reducción de costos, en el ambiente actual esas relaciones pueden llevar a una “concentración de riesgo” y a una posible vulnerabilidad a la interrupción.

La triste realidad es que las cadenas de suministros pueden ser eslabones débiles y socios mal preparados que pueden debilitar a las compañías fuertes.

Finanzas: Algunas veces se pasa por alto el impacto financiero de un suceso que cause interrupción. Si están caídos los sistemas financieros de los clientes y no pueden pagar oportunamente, ¿podrá sobrevivir una compañía a la contracción de los flujos de efectivo? Si fallaran los sistemas de transporte y distribución y no es posible que los productos de la compañía lleguen al mercado, ¿cómo afectaría eso a la capacidad de la empresa para cumplir sus obligaciones financieras? Al preparar planes de contingencia, se deben tomar en cuenta diversos asuntos, como líneas de crédito dedicadas y reservas de capital, así como la capacidad de la compañía para implantar con rapidez las reducciones de costos tácticas y la reasignación de los empleados conforme surja la necesidad.

Preparación Prudente y Práctica

Por supuesto, muchas variables entran en juego conforme se evalúan los posibles impactos, incluyendo factores de la industria, geografía, tamaño, estructura y otros. Pero en todos los casos, la situación requiere vigilancia constante y una preparación prudente y práctica.

Conforme la compañía evalúa la amplia gama de sucesos posibles e impactos en el negocio, también se debe considerar la continuidad de las acciones de preparación – de lo mínimo a lo máximo posible.

Desde luego, no es posible estar preparado para todo. Por lo tanto, el reto es determinar lo que es práctico y prudente. ¿Cómo obtener el máximo provecho del dinero que se invierte? ¿Cómo cubrir la gama más amplia de impactos en el negocio contra el mayor número de sucesos? ¿Cómo proteger la capacidad para conducir el negocio?

Nuevamente, cada situación es única y lo que puede ser adecuado para una compañía puede no serlo para otra. Cada organización debe tomar una decisión consciente, informada en cuanto a qué nivel de riesgo aceptar. Al final del día, los ejecutivos y directores deben poder decir a los consejos de administración y otros interesados (clientes, agencias reglamentarias, accionistas, analistas, comunidades, empleados, etc.) que hicieron todo lo que estaba razonablemente en sus manos para prepararse para una interrupción del negocio y responder a la misma.

Las experiencias adquiridas con Katrina

El Huracán Katrina, con todas las desgracias que trajo consigo, también aportó un buen número de prácticas excelentes de preparación para enfrentar riesgos. Por ejemplo, la disponibilidad de energía eléctrica es un requisito para que la mayor parte de las compañías reinicien sus actividades. Sabiendo esto, un detallista importante adaptó la parte trasera de cada tienda con una toma de corriente de alta capacidad, que les permitió tener un generador portátil y conectarlo. Un proveedor de productos médicos a nivel nacional transfirió sus provisiones médicas al perímetro de la zona azotada por el huracán. Una gran compañía de bebidas dejó de embotellar cerveza y empezó a embotellar agua.

Los ejecutivos deben preguntarse: ¿Cuáles son los riesgos que pueden prevenir, detectar y atender razonablemente? En muchos casos, lo más efectivo (pero no siempre lo más viable) es la prevención. El problema de los sistemas de cómputo del año 2000 es un ejemplo: Se dedicaron miles de dólares y de horas de trabajo para corregir una disfunción de los programas que amenazaba dejar a muchas computadoras sin capacidad de leer las fechas del siglo XXI. Y el proyecto masivo parece haber tenido éxito: muy pocas de las fallas de los sistemas de cómputo que se habían anticipado se materializaron. Sin embargo, al mismo tiempo, el que no se hayan presentado los problemas al cambiar el siglo llevaron a mucha gente a creer que el esfuerzo fue un desperdicio de tiempo y dinero. Desafortunadamente, es difícil demostrar que se evitó algo que nunca ocurrió.

Cuando un acontecimiento está fuera del control o capacidad para prevenirlo, entran en juego la detección, la respuesta y la recuperación. La detección requiere que se tengan sistemas establecidos que alerten con suficiente anticipación para poder dar una respuesta. Entre más temprana sea la detección, mayor será la capacidad de intervenir con éxito, ya sea reaccionando a un robo físico o a una violación a la seguridad cibernética. En el apéndice de ese folleto se dan a conocer las medidas prácticas que se pueden adoptar en estas áreas.

La planeación no necesariamente conlleva el desembolso de sumas de dinero considerables; se pueden realizar muchas actividades con poco o ningún costo. Por ejemplo, se puede obtener una ventaja importante teniendo equipos humanos de respuesta, identificados con anticipación, junto con sus responsabilidades y autoridad predeterminadas. Llevar a cabo juntas de los equipos en las que los empleados discutan las acciones posibles en caso de un desastre. Poner atención a las etapas fundamentales que a veces se pasan por alto, como es el caso de quién hará la declaración cuando ocurra un desastre y quién pondrá en marcha los planes de emergencia de la compañía.

Velocidad del Ataque

Entre los muchos argumentos para una preparación vigilante está el factor de la "velocidad del ataque". Aunque algunos riesgos se pueden presentar cuando se cuenta con las alertas oportunas, otros sucesos pueden ocurrir sin previo aviso y con una velocidad arrolladora. En esos casos, los planes bien formulados pueden representar la diferencia entre una recuperación rápida y una lenta.

En el caso del año 2000, la situación se veía venir. Desde unos años antes se conocía la vulnerabilidad y el posible impacto se documentó bien. A nadie tomó por sorpresa cuando los relojes marcaron las 12:00:01 a.m. del 1 de enero de 2000.

Pero otros sucesos de destrucción no telegrafían su llegada. Por ejemplo, la violación de la seguridad cibernética golpea sin avisar; por lo general, el suceso no se detecta sino hasta que el daño está hecho.

Aunque la publicidad en torno a una posible pandemia de gripe aviar raya en el exceso de cobertura en los medios, cumple un propósito importante: los niveles de conciencia son altos y nadie puede decir que no se le advirtió. Los ejecutivos Riesgote Riesgo Inteligente sacarán provecho del tiempo latente que tienen para reevaluar su estado de preparación.

Impacto en el negocio

- Un informe publicado en abril de 2004 por el US/Canada Power System Outage Task Force indicó que las pérdidas económicas, causadas por la interrupción en el sistema noreste de energía eléctrica de Estados Unidos y Canadá en agosto de 2003, fueron de entre US \$8 y 12 mil millones
- Dos terceras partes de las 129 compañías entrevistadas después del apagón de agosto de 2003 perdieron por lo menos un día completo de trabajo a causa de este suceso. La cuarta parte de los negocios entrevistados perdió más de US \$ \$50,000 por hora a causa de sistemas de cómputo inactivos, lo que significa, por lo menos, US \$400,000 por una jornada de 8 horas. El 4% de los negocios perdió más de US \$1 millón por cada hora de inactividad de los sistemas de cómputo
- En 2003, se estimó que el costo de los ataques cibernéticos contra compañías fue de US \$12.5 mil millones
- La caída del mercado del FTSE (Financial Times Stock Exchange) que siguió a los atentados con bombas terroristas en Madrid ocasionó pérdidas de US \$55 mil millones
- En 2003, las violaciones y virus que afectaron las redes de cómputo representaron costos de más de US \$1.5 billones para los negocios

Fuente: Deloitte Research – Prospering in the Secure Economy, September 2004 Reprinted with permission from the Deloitte & Touche /LLP publication, "Business Continuity Management: A Different Approach for a New World of Possibilities," Copyright 2005 Deloitte Development LP. All rights reserved.

Recomendaciones

Cuando la amenaza de la gripa pandémica se vea desde una perspectiva más amplia, la pregunta que predominará es "¿Ahora qué?" ¿Cómo pueden las compañías empezar a asumir el control de los problemas que genere una interrupción de negocios grave?

Un buen punto de arranque es nuestro primer folleto informativo de esta serie, *La Empresa Inteligente en Riesgos: La Administración de Riesgos Empresariales (ERM) bien realizada*. En el Apéndice se incluye una lista de medidas iniciales para introducir el Riesgo Inteligente en cualquier organización. (Visite www.deloitte.com/riskintelligence para ordenar o bajar una copia.

Aunque algunos riesgos se pueden presentar cuando se cuenta con las alertas/oportunidades, otros sucesos pueden ocurrir sin previo aviso y con una velocidad arrolladora.

Las amenazas pandémicas y de terrorismo biológico pueden tener un mayor impacto en la fuerza laboral que en el lugar de trabajo, por lo que es importante contar con la infraestructura y los procesos adecuados para que el personal pueda trabajar a distancia si es necesario.

A continuación se presentan algunos temas adicionales para reflexionar y actividades que pueden realizarse:

Creación de un caso práctico de negocios: En el pasado reciente, se dio poca atención a la administración de riesgos. En muchas ocasiones se llevaba a cabo una evaluación de riesgos, pero las recomendaciones se quedaban en el cajón (como fue el caso de preparación para el huracán de Nueva Orleans). En la actualidad, desde luego, una evaluación ya no puede ser un ejercicio menor: las medidas de seguimiento son de suma importancia. Una mayor concientización de los problemas de riesgo significa que los ejecutivos y otras personas responsables de la coordinación de administración de riesgos pueden presentar un caso más poderoso que nunca. Se puede subrayar que los costos de una administración de riesgos deficiente son relativos con respecto a una buena. El punto convincente puede ser que una mayor resistencia al impacto puede dar una ventaja competitiva y en esta era en que se enfatiza la buena ciudadanía corporativa, puede presentarse un argumento culminante: contar con un plan viable de Riesgo Inteligente para abordar diversas contingencias representa una elección socialmente responsable.

Evaluación de riesgos: Las compañías deben evaluar su exposición a riesgos, usando técnicas como la planeación de escenarios, análisis del impacto en el negocio, evaluaciones de vulnerabilidad, modelos estadísticos y otros métodos. Algunas preguntas que se deben contestar son las siguientes:

- ¿Cómo sería un suceso que causara la interrupción de actividades?
- ¿Cuáles serían los posibles impactos en el negocio?
- ¿Cuáles serían los impactos en cuanto a la competencia?
- ¿Cuáles serían los impactos ascendente y descendente en la cadena de valor de la compañía o de la industria?
- ¿Cuál es el nivel de preparación y resistencia de la compañía, así como el de sus proveedores, distribuidores y clientes?

Consideración del Impacto en la Gente: Como se señaló, las amenazas pandémicas y de terrorismo biológico pueden tener un mayor impacto en la fuerza laboral que en el lugar

de trabajo, por lo que es importante contar con la infraestructura y los procesos adecuados para que el personal pueda trabajar a distancia si es necesario. Muchas compañías están mejorando su capacidad para que los empleados trabajen a distancia, lo que implica dotarlos de *laptops*, teléfonos celulares y otros dispositivos móviles (con baterías reemplazables no recargables); también se les puede dar conectividad de banda ancha o de marcación directa, instalación de una red virtual privada (VPN) que permita el acceso seguro desde puntos remotos a los servidores de la compañía. En este sentido deberá probarse la capacidad de carga del sistema para asegurarse de que puede manejar la afluencia repentina de muchos usuarios.

Desde luego, la preparación no consiste únicamente en tener *laptops* y acceso a Internet. También deben tomarse en cuenta los procesos de la administración, ya que las actividades clave de las compañías deben alcanzar el mismo grado de calidad dondequiera que se lleven a cabo. Asimismo, debe prestarse atención a la capacitación y a la métrica del desempeño. La meta es lograr que el negocio funcione tan bien como antes de que se llevara a cabo la migración hacia el trabajo a distancia.

Sin embargo, no todos los negocios se prestan para trabajar a distancia. Si el personal debe tener acceso a maquinaria o equipo de gran tamaño, a espacios de trabajo limpios o secos u otros ambientes especializados, deben emplearse estrategias diferentes. En una situación de pandemia, las posibilidades incluyen tener múltiples turnos o emplear técnicas de distanciamiento social para minimizar el contacto directo entre las personas. Las compañías también podrían vigilar muy de cerca la salud del personal y tratar de utilizar trabajadores que se hayan recuperado de la enfermedad y haber desarrollado inmunidad a la misma.

Visión ampliada: Algunas amenazas pueden afectar un área geográfica mucho más grande que una simple planta o instalación. En tales casos, emplear una estrategia común, como trasladar las operaciones de una planta en la que se interrumpieron a otra. Puede ser poco viable.

La preparación ante ciertas categorías de interrupciones graves del negocio no debe limitarse a una sola ubicación, sino que deben abarcar las que sean críticas para la misión, sin importar el punto geográfico.

Observación del entorno fuera de los límites de la empresa: Muchas compañías deben buscar con una visión más amplia, que abarque a todas las entidades con las que operan, por ejemplo, los socios de la cadena de suministros, distribuidores, clientes, financieras y otras contrapartes.

La interconexión e interdependencia del mundo de los negocios actual significa que el trabajo en torno a la administración de riesgos debe ampliarse más allá de los límites físicos de la compañía. Cualquier vulnerabilidad en la cadena de suministros o los canales de distribución podría llevar a un escenario con “eslabones débiles”, que se traduzca en la suspensión gradual

de las operaciones del negocio. De ahí que sea importante exigir a proveedores y clientes que se sujeten a las mismas normas a las que se sujeta la empresa.

No bastan los compromisos verbales de los socios de la empresa. Un curso de acción más prudente sería que todos los socios importantes del negocio cuenten con evidencia verificable de sus planes de continuidad del negocio y de recuperación en caso de desastre.

Asimismo, si es posible, debe reducirse gradualmente la dependencia excesiva de un número limitado de proveedores. Las compañías deben tomar las medidas necesarias para ampliar su cadena de suministros antes de que ocurra una interrupción, en vez de tratar de hacerlo precipitadamente después del suceso.

Contar con un plan viable de Riesgo Inteligente para abordar diversas contingencias representa una elección socialmente responsable

Evaluación de Contratos de Servicios Externos (Outsourcing):

El *outsourcing* es una tendencia creciente. Las compañías dependen cada vez más de terceros para que presten servicios considerados críticos y, hasta hace poco, había razones de peso para hacerlo. Sin embargo, así como un eslabón débil de la cadena de suministros puede debilitar el estado de preparación, también puede ocurrir con el uso irrestricto de prestadores de servicios externos. Se puede aplicar el mismo enfoque: Un cuidadoso escrutinio de estas relaciones para asegurarse de que los prestadores de servicios cuenten con planes sólidos para prepararse y recuperarse en caso de desastre.

¿Cómo hacer una elección de Riesgo Inteligente?

Los sucesos pasados y actuales constituyen evidencias sólidas de que un evento importante que llegue a interrumpir las

actividades es, no sólo posible, sino inevitable. Si se acepta esta premisa, el no hacer nada es una pésima opción, incluso inaceptable.

La contingencia puede ser la gripe aviar u otra pandemia, o puede ser algo totalmente inesperado; sin embargo, el hecho de que suceda o no es menos esencial que reconocer que suceden cosas malas y que las compañías prudentes se preparan para encararlas.

La obligación de anticiparse, prepararse y responder a una crisis puede compartirse entre muchos (negocios, gobiernos, entidades no lucrativas y personas físicas). Sin embargo, en última instancia, sería el sector empresarial el que dirija las labores de recuperación. La historia reciente muestra que es posible que el gobierno no cuente con los recursos o la capacidad necesaria para asumir el control total durante acontecimientos que causen graves interrupciones. Los ciudadanos recurrirán a los negocios para asegurarse de que los servicios básicos sigan prestándose y esperan que las compañías trabajen arduamente para restablecer la vida a la normalidad, lo antes posible.

Las compañías también tendrán la oportunidad de ampliar o adaptar sus negocios para responder a una crisis. Si se hace debidamente la planeación y la preparación, las compañías podrán ayudar a los gobiernos, las comunidades y otras industrias vitales aportando experticia, bienes, servicios y/o voluntarios. Este aspecto "socialmente responsable" de planeación y respuesta puede mejorar mucho la imagen de una compañía, al tiempo que permite flujos de nuevos ingresos cuando se trata de negocios que son altamente susceptibles a ciertas crisis. En la medida en que una empresa responda con rapidez a una crisis y ayude a la recuperación (como lo hicieron tantas compañías después del huracán Katrina), podrá tener un impacto positivo de importancia, que alcance y trascienda el éxito económico, ambiental y social.

¿Su compañía es de Riesgo Inteligente?

Consulte nuestra serie completa de folletos informativos sobre Riesgo Inteligente, incluyendo los siguientes:

- No. 1: La Empresa de Riesgo Inteligente: La Administración de Riesgos Empresariales (ERM) bien realizada
- No. 2: Riesgo Inteligente en la Era de la Incertidumbre Global
- No. 3: La Empresa de Riesgo Inteligente: La Administración de Riesgos Empresariales (ERM) en la Industria de los Energéticos
- No. 4: La Empresa de Ciencias Biológicas con Riesgo Inteligente
- No. 5: El Director de Auditoría con Riesgo Inteligente

Visite www.deloittte.com/RiskIntelligence para bajar copias electrónicas o comuníquese con algún profesional de Deloitte para obtener copias impresas. Estos folletos se pueden obtener de manera gratuita.

Apéndice: Los siguientes pasos

Si el riesgo acecha a la vuelta de cada esquina, las consiguientes amenazas no se hacen esperar y, ante la sorpresa, los ejecutivos, así como los consejos de administración pueden quedarse inmóviles o juzgar que el problema es demasiado grande para manejarlo efectivamente y decidir ignorarlo.

Aunque es cierto que no es posible anticiparse ni prepararse para enfrentar todo riesgo concebible, se pueden tomar medidas metódicas para separar los riesgos creíbles y realistas de los riesgos imaginarios. Y en este proceso se puede crear un sólido caso para justificar que se comprometan recursos en los lugares más importantes. Los inversionistas, analistas, servicios de *rating* e incluso los jueces y jurados se inclinarán más a favor de una compañía que haya tomado medidas para mitigar su exposición al riesgo que a las que consideraron que el problema no podía manejarse.

Desde luego muchas compañías cuentan con estructuras y programas de administración de riesgos con distintos niveles de sofisticación. Los comentarios anteriores y los pasos siguientes no pretenden reemplazar o invalidar el trabajo que ya se haya hecho, sino que son consideraciones que deben ponderarse e incorporarse selectivamente a programas existentes, sean incipientes o bien establecidos.

Las actividades pueden separarse en tres etapas: (1) anticipación y preparación, (2) primera respuesta y (3) recuperación. A continuación se presentan algunos pasos que deben considerarse en cada etapa:

Anticipación y preparación

La observación resulta obvia, pero dada la falta de preparación de muchas compañías, vale la pena reiterar que el trabajo que se haga antes de una interrupción, servirá mucho más que tratar de improvisar al momento de una crisis.

- Asignar a una persona que dirija el trabajo de planeación de Riesgo Inteligente
- Nombrar un comité directivo de Riesgo Inteligente
- Determinar cuánto riesgo se quiere asumir
- Planear el impacto en el negocio; es decir, identificar los activos críticos (gente, procesos, sistemas, instalaciones y propiedad intelectual), así como determinar el tiempo máximo que es posible prescindir de ellos e incluir estos tiempos en la planeación

- Establecer las políticas que deban implantarse durante una interrupción
- Establecer procedimientos para respaldar las políticas
- Definir claramente roles y responsabilidades
- Comunicar los planes a los empleados antes de un suceso; asegurarse de haber capacitado adecuadamente a la gente.
- Establecer lineamientos de trabajo a distancia e identificar quién puede y quién no puede participar en el programa de trabajo a distancia
- Reconocer que los altos ejecutivos necesarios para la toma de decisiones estratégicas pueden estar incapacitados e implantar un plan de reemplazos
- Invertir en procesos y sistemas que den buenos resultados
- Establecer protocolos de comunicación de emergencia y rutas de información
- Determinar negocios críticos y establecer planes para reasignar a su personal.
- Determinar funciones críticas y establecer planes para reasignar a su personal.
- Considerar quienes son los clientes clave para prestarles servicios de la forma acostumbrada
- Solicitar a socios y proveedores planes de administración de riesgos
- Someter todo el plan a pruebas de esfuerzo, usando ejercicios de escritorio y simulacros reales

Primera respuesta

El principal objetivo de la etapa de primera Respuesta es contener el problema — proteger a la gente, instalaciones, comunidad, infraestructura crítica, etc.

- Asignar recursos para proteger a los empleados durante la interrupción inicial
- Iniciar el plan de comunicación de emergencia con los empleados
- Determinar la ubicación, condición y situación de los empleados
- Comunicarse y coordinarse con los socios externos
- Coordinarse con organizaciones externas y ayudar a las comunidades
- Vigilar sistemáticamente sucesos externos críticos a través de los medios de comunicación y otros medios disponibles
- Implantar planes para atender interrupciones de servicios
- Iniciar planes para prestar servicios a los clientes prioritarios
- Vigilar los sistemas y establecer detonadores para generar respuestas

Recuperación

La etapa de recuperación se refiere a la reanudación del negocio; es decir, regresar al “negocio de la forma acostumbrada” tan pronto sea posible. En esta etapa existen actividades a corto y largo plazo: las actividades de recuperación inmediata y las de reevaluación y ajuste posteriores a la recuperación.

- Continuar comunicando información crítica y oportuna a los empleados e interesados principales. No permitir que los medios de comunicación sean la única voz
- Considerar la reapertura escalonada o parcial de las instalaciones
- Implantar planes para reanudar primero las actividades críticas de la misión
- Comunicarse y coordinarse con terceros respecto de las necesidades de infraestructura críticas
- Trabajar con los medios de comunicación locales, regionales y nacionales para hacer publicidad de las mejores prácticas e historias de éxito
- Llevar a cabo una revisión oportuna posterior al suceso para identificar áreas débiles e iniciar mejoras para interrupciones futuras

Contactos

Gilberto Mercado
Tel. +52 (55) 5080 6770
gmercado@deloittemx.com

Walter Frascetto
Tel. +52 (55) 5080 6265
wfrascetto@deloittemx.com

Israel Zagal
Tel. +52 (55) 5080 6596
izagal@deloittemx.com

deloitte.com/mx

Deloitte presta servicios profesionales en auditoría, impuestos, consultoría y asesoría financiera a organizaciones públicas y privadas de diversas industrias. Con una red global de firmas miembro en 140 países, Deloitte brinda su experiencia y profesionalismo de clase mundial para ayudar a sus clientes a alcanzar el éxito desde cualquier lugar del mundo donde éstos operen. Los 150,000 profesionales de la firma están comprometidos con la visión de ser el modelo de excelencia.

Los profesionales de Deloitte están unidos por una cultura de cooperación basada en la integridad, el valor excepcional a clientes y mercados, el compromiso mutuo y la fortaleza de la diversidad. Disfrutan de un ambiente de aprendizaje continuo, experiencias desafiantes y oportunidades de lograr una carrera en Deloitte. Sus profesionales están dedicados al fortalecimiento de la responsabilidad empresarial, a la construcción de la confianza y al logro de un impacto positivo en sus comunidades.

Deloitte se refiere a Deloitte Touche Tohmatsu –asociación suiza– y a su red de firmas miembro, cada una como una entidad única e independiente. Conozca en www.deloitte.com/mx/conozcanos la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu y sus firmas miembro.

Limitación de responsabilidad

Este material y la información aquí incluida es proporcionada por Deloitte Touche Tohmatsu con el fin de mostrar un aspecto general sobre uno o varios temas en particular, y no son un tratamiento exhaustivo sobre el(los) mismo(s).

Por lo tanto, la información presentada no sustituye a la asesoría o a nuestros servicios profesionales en materia contable, fiscal, legal, financiera, de consultoría o de otro tipo. No es recomendable considerar esta información como la única base para cualquier resolución que pudiese afectarle a usted o a su negocio. Antes de tomar cualquier decisión o acción que pudiese afectar a sus finanzas personales o a su empresa debe consultar a un asesor profesional.

Este material y la información incluida se proporcionan sin interpretación alguna, Deloitte Touche Tohmatsu no hace ninguna declaración ni otorga garantía alguna, de manera expresa o implícita, sobre el mismo y la información proporcionada. Sin limitar lo anterior, Deloitte Touche Tohmatsu no garantiza que el material o el contenido estén libres de error o que cumplan con criterios particulares de desempeño o calidad. Deloitte Touche Tohmatsu renuncia expresamente a cualesquier garantías implícitas, incluidas de manera enunciativa mas no limitativa, garantías de comercialización, propiedad, adecuación para un propósito en particular, no infracción, compatibilidad, seguridad y exactitud.

Al utilizar este material y la información aquí incluida lo hace bajo su propio riesgo y asume completa responsabilidad sobre las consecuencias que pudieran derivar por el uso de los mismos. Deloitte Touche Tohmatsu no se responsabiliza por daños especiales, indirectos, incidentales, derivados, punitivos o cualesquier otros deterioros resultantes de una acción de contrato, estatuto, extracontractual (incluyendo, sin limitación, negligencia) o de otro tipo, relacionados con el uso de este material o de la información proporcionada.

Si alguna parte de lo anterior no es completamente ejecutoria, la parte remanente seguirá siendo aplicable.