t

Simulaciones de crisis

Un plan es tan sólo un plan hasta que se pone a prueba

La mayoría de las veces se sabe qué va a suceder una crisis, sin embargo, no se sabe cuándo ni dónde o que tan crítica será. Ante esta situación una empresa puede estar tranquila si tiene confianza en que su Plan de Gestión de Crisis funciona. La única manera de confiar, es con un programa de simulaciones eficaces y multidimensionales que ponen a prueba a su equipo completo y a la organización. Las respuestas a las siguientes preguntas determinarán la eficacia de dicho plan: ¿se toma en serio la situación de una crisis? Esa es una prueba para determinar eficacia. ¿Se aprende algo de esta experiencia?

Hay más de una manera de abordar una simulación. Aquellas simulaciones que realmente crean valor, van más allá del simple concepto de un "simulacro de incendio" que se enfoca sólo en una crisis a corto plazo. Una simulación de crisis eficaz pone realmente a prueba a la organización, sea cual sea el escenario. Exige que se hagan las preguntas y respuestas correctas, lleva un efecto dominó real en el que se tienen que tomar decisiones en distintos rubros y niveles de la organización, tanto internos como externos. Asimismo, deja a los implicados con una sensación de que realmente han aprendido algo al probar su habilidades y responsabilidades bajo circunstancias difíciles y retadoras que los someten a la incertidumbre, ambigüedad, información conflictiva e incompleta -en donde a menudo hay más factores desconocidos que conocidos- con el objetivo de que el escenario de crisis permee en todos los niveles de la organización.

La premisa de este enfoque es la preparación

El objetivo podría ser una exploración detallada de riesgo estratégico de mercado, una secuencia de escenarios dramáticos en los que se deben tomar acciones, o un escenario intermedio. El detonante podría implicar: una falla técnica, interrupción en el mercado, fenómenos naturales o malversación deliberada, etc. En cualquier caso, el esfuerzo que una organización pone en la planificación y personalización de su enfoque en una simulación de crisis reditúa al momento en que una crisis real llega, se debe buscar la preparación del personal, la mejora de procesos, la cohesión y confianza

del equipo. El resultado que esto trae es un equipo con mucha mayor confianza, preparado para manejar la crisis, con una rápida reacción y listo para obtener los recursos necesarios para una pronta recuperación.

¿Empezar con un escenario?

El primer error

Se debe comenzar con un propósito. ¿Para qué nos queremos preparar cuando una crisis ocurra? ¿En qué lugar queremos estar cuando ésta termine?

Únicamente cuando se tiene un objetivo claro es posible construir un escenario en el cual podrá lograrse dicho objetivo. Aunque la situación sea ficticia, los riesgos son reales. Una respuesta eficaz ante una crisis puede ayudar o destruir la reputación de una organización. La reputación puede representar incluso el 25% del valor de mercado de una organización. Una organización puede esperar en promedio un evento con el potencial de destruirla por lo menos una vez cada cinco años. Es importante entender que las simulaciones de crisis no son un lugar en el que se deban tomar atajos. Increíblemente, aún existen organizaciones que no utilizan simulaciones en lo absoluto, sin embargo cada vez son más aquellas que descubren los beneficios y ponen sus planes a prueba para tener una preparación que realmente haga una diferencia en la empresa.

Diseñar en múltiples dimensiones

Para proteger el valor de una organización, una simulación de crisis debe ser tan multidimensional como el mundo real en el que una crisis podría desarrollarse. Ya sea real o imaginaria, debe incluir factores externos, notificaciones realistas y diferentes escenarios entre las partes interesadas.

Las personas deberían interactuar como si lo hicieran en el mundo real. Deben considerar y cuestionar el impacto que cada decisión tendrá en las finanzas, los clientes, la estrategia y las operaciones, y estas decisiones deben tener consecuencias palpables.

Si los participantes superan fácilmente los límites de la simulación, esta no fue diseñada de forma suficientemente realista.

Un enfoque basado en la madurez

Dependiendo de la finalidad de la simulación, tanto el diseño de los escenarios y los recursos disponibles, así como el enfoque de la simulación variarán.
Por un lado, una simulación puede ser tan simple como una discusión de los posibles escenarios. El siguiente nivel es un ensayo donde los roles se ponen a prueba y se evalúan estrategias, flujos de información y comunicaciones en un entorno realista. Las simulaciones más robustas pueden competir con "juegos de estrategia" en cuanto al uso dinámico de los peores escenarios y situaciones críticas. Cuando los participantes toman decisiones, deben considerar las consecuencias que esas decisiones tendrán en días, semanas, e incluso meses después.

De igual manera, es importante que las decisiones se realicen en los niveles adecuados. Los directivos deben confiar en que otros desarrollarán las tácticas mientras que ellos se concentran en los accionistas, los resultados y las consecuencias futuras. Conseguir ventaja en el juego es crítico para ellos.

La simulación debe ayudar a los involucrados a visualizar distintas decisiones al tiempo que reciben información proveniente de diversas fuentes, entre más realista sea la experiencia, más confianza creará para la empresa y los equipos de trabajo. También es de vital importancia incluir a toda la organización, desde el Consejo de Administración y las direcciones hasta los niveles operativos, con la finalidad de evaluar la toma de decisiones a diversos niveles.

Un mundo de detonadores de crisis

Las crisis pueden ser resultado de accidentes, mala fe o ser completamente arbitrarias. La mayoría de las organizaciones son susceptibles a amenazas de más de uno de estos detonadores potenciales:

Detonadores de Crisis	Amenazas
Malicia cibernética	Ciberataques, robo de identidad o alteración de datos
Crimen financiero	Fraude y otras actividades criminales
Desorganización financiera	Fallas financieras que amenazan la existencia de una empresa
Tecnológica e industrial	Fallas complejas al sistema, ya sea por accidente, mal manejo o sabotaje
Confrontaciones	Conflictos legales, comerciales, geopolíticos, militares
Otras catástrofes	Desastres naturales o provocados que causen una quiebra importante

¿Cómo empezar?

En primer lugar, se deben decidir los objetivos. Se debe pensar como un productor de cine

Desarrollar una simulación de crisis no es tan distinto a producir una película. ¿Cuál es la historia?, ¿el escenario?, ¿cómo se convierten estos factores en un guion que determine quién va a decir qué, a quién se lo dirá y cuándo?

Este libreto se conoce como una lista maestra de eventos (LEM por sus siglas en inglés), esta lista debe ser algo más que un guion – ya que un guion tiene una narrativa inamovible y una lista maestra de eventos debe ser algo más, ya que contempla situaciones reales anticipando diversos puntos de decisión en la simulación, esto con el objetivo que la “película” sea realista de inicio a fin.

Cuando los participantes interactúan con la LEM utilizando datos reales en un escenario real, las lecciones aprendidas terminan siendo reales.

A continuación, definir el límite

Una simulación que no desafía, a las personas no les dejará ningún aprendizaje, las personas aprendemos por experiencias. Sin embargo, cuando las simulaciones sobrepasan el límite de los participantes, lo único que se logrará será humillación y una baja en la moral. Diseñar escenarios que ofrezcan lecciones útiles al final del ejercicio, es parte ciencia y parte arte. Y es la parte fácil. Cuando la película termina, el verdadero trabajo comienza. El verdadero valor se encuentra al recaudar las lecciones aprendidas y aplicarlas para fortalecer un Plan de Gestión de Crisis.

Simulaciones en acción

Medalla de oro a la confianza

El Comité Organizador de Juegos Olímpicos y Paralímpicos de Londres 2012 llevó a cabo más de 200 simulaciones de diversas crisis para preparar el evento. En un entorno de rápido crecimiento y de alta dependencia al gran número de socios comerciales, se desarrollaron protocolos de acción que permitieron a los organizadores estar preparados desde el primer día. Esta filosofía y mentalidad puso en acción diversas simulaciones y situaciones de crisis que fueron clave para el gran éxito de los Juegos.

Manteniendo el flujo de energía y recursos

La energía y los recursos son vitales para la sociedad. Cuando el flujo de cualquiera de éstos se ve amenazado o interrumpido, los efectos se ven reflejados en la economía, cultura y en los estilos de vida de la sociedad.

Los detonantes de una crisis abarcan un amplio espectro: infraestructura de tecnología, desastres naturales, amenazas cibernéticas, acción regulatoria, amenazas geopolíticas e incluso daño ambiental. Para enfrentar los peligros incluyendo daños permanentes a la reputación y el valor de una organización, debe haber preparación, vigilancia ante las amenazas y fortaleza en la recuperación.

Existe una diferencia entre las organizaciones que han superado una crisis y las que no. Todo empieza con la planeación, en la que se necesita cierta habilidad que no se puede obtener de la planeación de proyectos tradicionales. Es vital para las organizaciones construir planes robustos para enfrentar las crisis, darles seguimiento y actualizarlos continuamente. De esta manera, se puede mantener la

cadena de recursos intacta sin importar la gravedad de la crisis que se presente.

Las sorpresas se esconden en aquello que ya conocemos

Prepararse para una crisis significa identificar vectores que puedan afectar a la organización. Existen momentos en que las crisis más obvias disfrazan una crisis mucho más grave. Sobre todo una crisis que amenaza de manera directa a la empresa. Por ejemplo, un centro que maneja flujo de datos probablemente piensa que le afectan sólo las crisis relacionadas a las tecnologías de información. Sin embargo, el mismo evento puede llegar a convertirse en una crisis de personal.

Otro ejemplo, un accidente físico puede convertirse rápidamente en una crisis fiscal. El problema SCADA (por sus siglas en inglés Supervisory Control And Data Acquisition) percibido como un conflicto operacional, de igual manera, puede resultar ser una cuestión de seguridad. Cualquiera que sea una amenaza aparente puede ser que esté acompañada de una amenaza que no se había identificado anteriormente. Una situación como ésta puede provocar un cambio de planes que pone altamente en riesgo a la organización.

Anticípese, prepárese y piense a largo plazo

El mejor momento para conocer qué tan útil es el plan de manejo de crisis no es cuando se presenta el problema o la crisis. La organización debe de haber reunido previamente toda la confianza y conocimiento que solo puede venir del análisis, planeación de escenarios y simulaciones con una visión mucho más a futuro que ese momento. Esta es una manera de lograr la continuidad del negocio y tener una visión mucho más allá que una resistencia a largo plazo.

Las nuevas amenazas sobre las viejas

Para enfrentarse a una crisis de manera confiada, las organizaciones en la industria de la energía y recursos necesitan contemplar situaciones a largo plazo y en paralelo enfrentarse a las situaciones del presente. La industria tradicionalmente se ha enfocado en la cultura de la seguridad física, desde yacimientos petrolíferos, cuartos de control, y hasta las transmisiones de redes. Esto sigue siendo crítico. Sin embargo, ahora las barreras entre la información y la seguridad física se han desvanecido. Por ejemplo, las amenazas cibernéticas han logrado convertirse en amenazas de sistemas físicos de seguridad. Prepararse para una crisis hoy en día requiere tener un acercamiento a éstas con suficiente visión para cerciorarse de que la seguridad trascienda a todas las partes del negocio.

La industria de energía y recursos es global y está interconectada. Para llevar a cabo la estrategia de negocio, las obligaciones diarias con clientes y terceros relacionados, cada empresa debe de tomar cualquiera que sea el camino siempre y cuando sea con base en la continuidad y confiabilidad. Las interrupciones que afectan la producción y los mercados también afectan al ambiente, la salud pública y el orden social. Las organizaciones que operan en esta industria gastan una cantidad importante en cada una de las intersecciones entre los vectores de amenaza y efectos.

¿Cómo empezar?

Se debe empezar desde el inicio

El inicio es en donde terminan las crisis. Los Consejos de Administración y los directivos clave son los responsables de establecer el tono para la cultura de gestión de riesgos.

Algunos pueden ser complacientes con ello y aparentar indiferencia. Otros pueden crear tensión al tomar un rol altamente activo. Sin embargo, una persona previamente informada y con cualidades de líder es capaz de contemplar la gestión de riesgos dentro de los objetivos.

Hay que romper las barreras incluyendo las que rodean a toda la organización, las que existen entre la empresa y en las relaciones con partes relacionadas. Las relaciones externas son un elemento crítico para ambas operaciones y las amenazas potenciales.

Fracasar al ver el panorama general sólo aumenta las amenazas a la reputación de la organización, el valor y hasta su existencia. Se debe de aumentar la preparación y capacidad dentro y fuera de la empresa. Las crisis no respetan las barreras, por lo que el plan de manejo de crisis tampoco debería respetarlas.

Capacitar a las personas

Los procedimientos y medidas preventivas son los extremos para un plan de gestión de crisis. Las personas son el cerebro y

corazón. Si piensas “sobrevivir”, sobrevivir es a lo que más puedes aspirar. Si piensas “resurgir con más fuerza” del esfuerzo que se pone en la capacitación y sobre todo en la preparación, puede crearse una verdadera cultura de superación.

Un mundo de detonadores de crisis

Las crisis pueden ser maliciosas, accidentales o completamente al azar. La mayoría de las organizaciones son susceptibles a las amenazas de más de uno de estos detonadores potenciales.

Malicia y cibernética	Irregularidades y crímenes financieros	Daños financieros	Tecnología e industrial	Confrontaciones	Otras catástrofes
Ciber ataques, robo de identidad y alteración de productos	Fraudes y otras actividades criminales	Fraudes financieros que amenazan la existencia de la empresa	Fallas de sistemas complejos, ya sea por accidente, mal manejo o sabotaje	Legal, comercial, geopolítico y conflictos militares	Eventos destructivos ya sea por causa natural o por el hombre.

Gestión de crisis de energía y recursos en acción

Generando confianza

Ejecutivos de una gran empresa de energía con activos de generación nuclear piensan de manera anticipada acerca de cómo gestionar las crisis más importantes. A pesar de que la empresa tuvo un incidente en la gestión del plan para las diferentes unidades de negocio y no contaba con una estrategia, generó un acercamiento a nivel empresarial que comprometía a todos los ejecutivos. Por ello, consiguieron crear un modelo de gestión de crisis a nivel global-empresarial, un plan para satisfacer las necesidades de todos los terceros interesados, incluyendo líderes, empleados, Consejo de Administración, reguladores, accionistas, medios de comunicación y clientes. La empresa pudo definir la rendición de cuentas, roles, responsabilidades, procesos, gobierno y comunicaciones. Se hicieron varios simulacros y sesiones de prácticas durante varios años con el fin de poner a prueba el plan y mantener a los participantes siempre listos. Al mismo tiempo, se identificaron y cerraron brechas en la estructura y el desempeño.

El resultado final aumentó la confianza en toda la organización, particularmente en el nivel directivo; actuar de manera rápida y firme en la gestión de crisis. La empresa al día de hoy está completamente preparada para implementar el modelo de gestión de crisis sin retraso alguno y lo ha hecho de manera muy efectiva.

Construyendo un modelo de riesgos inteligente en la operación diaria

Una empresa de energía norteamericana reconoció que una crisis puede poner en riesgo al modelo de la operación de forma ascendente y descendente. Adelgazando márgenes financieros y disminuyendo la fortaleza en toda la industria, la empresa identificó que el proceso de ineficiencia no era un riesgo que se podía solventar, por lo que iniciaron en conjunto con otras empresas una iniciativa de excelencia operacional que contemplaba planes para potenciar la respuesta a la crisis y medidas para anticiparse a los eventos antes de que alcancen por completo el nivel de crisis.

El programa abarcaba seguridad y procesos de control, calidad en la información, gestión de expedientes, análisis de inteligencia de negocios y pruebas regulares de seguridad ambiental. La empresa logró potenciar el Enterprise Risk Group y estuvo acompañado de un pensamiento de concientización de riesgos en finanzas, recursos humanos, producción y otras áreas de operación. Como resultado, la empresa logró implementar completamente el régimen de excelencia operacional en donde estrictas métricas evaluaban continuamente las amenazas a la producción y riesgos en todas las áreas del negocio.

Conclusiones

Los ataques a la infraestructura crítica se han convertido en una importante preocupación para los gobiernos y proveedores de servicio privados de todo el mundo, ya sean ataques cometidos por criminales cibernéticos que buscan obtener ganancias financieras o por hackeos a actores políticos que buscan socavar la credibilidad de los gobiernos y las empresas.

La preocupación sobre estas amenazas está justificada, ya que la investigación demuestra que los ataques a la infraestructura crítica se ha vuelto más

común y sofisticada y continuará creciendo en el futuro inmediato. La gestión y el monitoreo de los sitios ha mejorado en las instalaciones de la infraestructura crítica gracias a que éstas se conectan más agresivamente cada vez a Internet. Sin embargo, la conveniencia de la conectividad ha convertido la superficie de ataques de algunas industrias en un campo fértil para los ataques cibernéticos. Debido a los efectos de alto perfil de los ataques a los sistemas de la infraestructura crítica, ciertas industrias se han convertido en blancos más atractivos para los criminales.

A medida que evoluciona el entorno de las amenazas cibernéticas, también debe desarrollarse la protección frente a dichas amenazas. Con la aparición de los ataques dirigidos y las amenazas persistentes, queda claro que es necesario utilizar un nuevo enfoque de seguridad cibernética. Las técnicas tradicionales simplemente ya no resultan adecuadas para proteger los datos frente a los ciberataques. Así, los riesgos cibernéticos y de reputación han pasado a ser preocupaciones fundamentales para todos los Consejos de Administración y las organizaciones, ya que cada organización en cualquier momento es un blanco potencial.

Para obtener más información, visite **www.deloitte.com/crisismanagement**

Mayor información

Daniel Aguiñaga
Socio Gobierno Corporativo
Tel: +52 (55) 5080-6000
daguinaga@deloittemx.com

Visite Deloitte México
www.deloitte.com/mx

Gobierno Corporativo
www.deloitte.com/mx/gobiernocorporativo

Aguascalientes
Universidad 1001, piso 12-1, Bosques del Prado
20127 Aguascalientes, Ags.
Tel: +52 (449) 910 8600, Fax: +52 (449) 910 8601

Cancún
Avenida Bonampak SM 6, M 1, lote 1, piso 10
77500 Cancún, Q. Roo
Tel: +52 (998) 872 9230, Fax: +52 (998) 892 3677

Chihuahua
Av. Valle Escondido 5500, Fracc. Des. El Saucito E-2, piso 1,
31125 Chihuahua, Chih.
Tel: +52 (614) 180 1100, Fax: +52 (614) 180 1110

Ciudad Juárez
Baudelio Pelayo No. 8450
Parque Industrial Antonio J. Bermúdez
32400 Ciudad Juárez, Chih.
Tel: +52 (656) 688 6500, Fax: +52 (656) 688 6536

Culiacán
Calz. Insurgentes 847 Sur, Local 103, Colonia Centro Sinaloa
80128 Culiacán, Sin.
Tel: +52 (667) 761 4339, Fax: +52 (667) 761 4338

Guadalajara
Avenida Américas 1685, piso 10, Colonia Jardines Providencia
44638 Guadalajara, Jal.
Tel: +52 (33) 3669 0404, Fax: +52 (33) 3669 0469

Hermosillo
Blvd. Francisco E. Kino 309-9, Colonia Country Club
83010 Hermosillo, Son.
Tel: +52 (662) 109 1400, Fax: +52 (662) 109 1414

León
Paseo de los Insurgentes 303, piso 1, Colonia Los Paraísos
37320 León, Gto.
Tel: +52 (477) 214 1400, Fax: +52 (477) 214 1405

Mazatlán
Avenida Camarón Sábalo 133, Fraccionamiento Lomas
de Mazatlán
82110 Mazatlán, Sin.
Tel: +52 (669) 989 2100, Fax: +52 (669) 989 2120

Mérida
Calle 56 B 485 Prol. Montejo Piso 2
Colonia Itzimna 97100 Mérida, Yuc.
Tel: +52 (999) 920 7916, Fax: +52 (999) 927 2895

Mexicali
Calzada Francisco López Montejano 1342, Piso 7 Torre Sur
Fraccionamiento esteban cantú
21320 Mexicali, B.C.
Tel: +52 (686) 905 5200, Fax: +52 (686) 905 5232

México, D.F.
Paseo de la Reforma 489, piso 6, Colonia Cuauhtémoc
06500 México, D.F.
Tel: +52 (55) 5080 6000, Fax: +52 (55) 5080 6001

Monclova
Blvd. Ejército Nacional 505, Colonia Los Pinos
25720 Monclova, Coah.
Tel: +52 (866) 635 0075, Fax: +52 (866) 635 1761

Monterrey
Lázaro Cárdenas 2321 Poniente, PB, Residencial San Agustín
66260 Garza García, N.L.
Tel: +52 (81) 8133 7300, Fax: +52 (81) 8133 7383

Carr. Nacional 85, 5000, local S-6 Colonia La Rioja
64988, monterrey, N.L.
Tel. +52 (631) 320 1673
Fax: +52 (631) 320 1673

Nogales
Apartado Postal 384-2
Sucursal de Correos “A”
84081 Nogales, Son.
Tel: +52 (631) 320 1673, Fax: +52 (631) 320 1673

Puebla
Edificio Deloitte, Vía Atlixcayotl 5506, piso 5, Zona Angelópolis
72190 Puebla, Pue.
Tel: +52 (222) 303 1000, Fax: +52 (222) 303 1001

Querétaro
Avenida Tecnológico 100-901, Colonia San Ángel
76030 Querétaro, Qro.
Tel: +52 (442) 238 2900, Fax: +52 (442) 238 2975, 238 2968

Reynosa
Carr. Monterrey-Reynosa 210-B, PA
Fracc. Portal San Miguel
88730 Reynosa, Tamps.
Tel: + 52 (899) 921 2460, Fax: +52 (899) 921 2462

San Luis Potosí
Av. Salvador Nava Martínez 3125, 3-A
Fracc. Colinas del Parque
78294 San Luis Potosí, S.L.P.
Tel: +52 (444) 1025300, Fax: +52 (444) 1025301

Tijuana
Misión de San Javier 10643, Piso 8,
Zona Urbana Rio Tijuana. Tijuana B.C., 22010
Tel: +52 (664) 622 7878, Fax: +52 (664) 681 7813

Torreón
Independencia 1819-B Oriente, Colonia San Isidro
27100 Torreón, Coah.
Tel: +52 (871) 747 4400, Fax: +52 (871) 747 4409

deloitte.com/mx