GUÍA DE GESTIÓN DE RIESGOS PARA LAS EMPRESAS

ICC MÉXICO

MEXICO
INTERNATIONAL
CHAMBER OF COMMERCE

The world business organization

Guía de Gestión de Riesgos ICC México para las Empresas

Elaborado por la
Comisión de Inteligencia Corporativa y Gestión de Riesgos
ICC México

AGRADECIMIENTOS

Agradecemos por su colaboración en la realización de esta Guía a:

Brian Weihs. **Kroll Inc.**
Alejandro Catalá Guerrero. **Basham, Ringe y Correa S.C.**
Ricardo A. Ramírez Molina. **PROSASEG Asesoría Integral, S.C.**
Alfredo Hernández Martínez. **PricewaterhouseCoopers, S.C.**
Francisco Villagrán Ballesteros. **Aguilar & Villagrán, S.C.**
Juan Carlos Simon Baqueiro. **PricewaterhouseCoopers, S.C.**

ICC MEXICO
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

CONTENIDO

INTRODUCCIÓN

En el escenario actual de negocios, los riesgos que enfrentan las organizaciones son cada vez más complejos y diversos. Desde riesgos operacionales, que se enfrentan diariamente, a riesgos estratégicos, que pueden poner en duda la continuidad de los negocios. El manejo de cada riesgo ya no corresponde únicamente a una función o a un área de la organización, si no que cada área y cada líder debe entender los riesgos que afecten a toda la organización.

En este contexto, es imprescindible tener una visión amplia de los varios riesgos que afectan a una empresa y las herramientas básicas para entender, monitorear y manejar esos riesgos. El manejo de riesgos no es una actividad aislada; es una actitud que corresponde a todos los miembros de la organización. La mayoría de los líderes son enfocados en buscar el éxito de su organización o negocio, pero en ocasiones falta la experiencia y el conocimiento para asegurar el manejo adecuado de los riesgos más importantes que les enfrentan.

En este sentido, la Comisión de Inteligencia de Negocios y de Gestión de Riesgos de la ICC México, consideró importante preparar una guía que pudiera poner al alcance rápido de cualquier líder los conceptos básicos y críticos para entender el manejo integral de riesgos.

La Guía de Gestión de Riesgos de la ICC, presenta de manera breve y sencilla los conceptos de análisis de riesgo y su manejo integral para organizaciones en México. Cada compañía enfrenta riesgos específicos, sin embargo con esta guía cualquier líder puede orientarse mejor para buscar otros documentos que le permitan profundizar su conocimiento en el tema, o bien, para entender qué tipo de apoyo especializado requiere de expertos.

Brian Weihs
Presidente de la Comisión de Inteligencia Corporativa y Gestión de Riesgos

OBJETIVOS

¿Por qué esta guía?

Es reconocido por todos, la relevancia del concepto de riesgo y la importancia de tomarlo en consideración en la administración de empresas y otras organizaciones. Sin embargo, para quienes no son expertos, dicho tema suele ser fuente de confusión. Como administrador de organización, ¿qué riesgos deben preocuparme? ¿Cómo los identifico? ¿Y qué hago una vez identificados? ¿Puedo eliminarlos o evitarlos? ¿Debo aceptarlos?

Si uno busca sobre el tema, se encuentra muchísima información. Una búsqueda en línea por "gestión de riesgos" arroja casi 50 millones de resultados. "Risk Management" otros 148 millones de resultados. Hay numerosos estándares diseñados como mejores prácticas en la identificación y administración de riesgos para organizaciones. Los estándares ISO 31000: 2009, OCEG "Red Book" 2.0: 2009, BS 31100: 2008 y COSO: 2004 son solo algunos de ellos. Cada uno tiene conceptos y metodologías en común, y diferencias. Algunos son obligatorios para ciertas empresas, por ejemplo empresas que cotizan en la bolsa de valores. ¿Cuál de los estándares sirve para mi organización? ¿Son útiles para México?

Con esta guía, la Comisión de Inteligencia Corporativa y Gestión de Riesgos de la ICC en México pretende ofrecer una herramienta que pueda guiar a los administradores de empresas y otras organizaciones a 1) entender la importancia que tiene el gestionar los riesgos para su organización, 2) explicar de manera clara y sencilla los conceptos más importantes para organizaciones de cualquier tamaño y complejidad, y 3) mostrar las actividades y actitudes necesarias para desarrollar la capacidad de gestionar y minimizar los riesgos para la organización. Además, la guía pretende ofrecer un recurso específicamente enfocado en los riesgos que enfrentan organizaciones en México.

¿Por qué gestionar riesgos?

En general, muchos de nosotros estamos acostumbrados a preocuparnos por ciertos tipos de riesgos en nuestras organizaciones. Las áreas jurídicas se preocupan por riesgos jurídicos, regulatorios, y varios otros riesgos que surgen de nuestras relaciones con otras empresas (nuestro personal y agencias del gobierno).

Las áreas financieras se preocupan por riesgos de crédito, cambiario, de costos y de manejo de recursos internos, entre otros. Cada área de la organización tiene un conjunto de riesgos relevantes e importantes. Sin embargo, una gestión eficaz y eficiente de los mayores riesgos para una

organización requiere una visión integral de éstos, así como una gestión integral.

Esa visión integral permite a los líderes de la organización asignar recursos a los riesgos de mayor importancia para la organización, y en muchos casos, permite implementar estrategias más eficaces que involucran varias de las funciones de la organización.

El primer concepto relevante que pretende demostrar esta guía es el de la importancia de gestionar riesgos de manera integral y como desarrollar la capacidad de llevar a cabo dicha gestión.

También estamos acostumbrados a confiar en ciertos expertos dentro de nuestra organización para administrar y disminuir riesgos. Estos expertos pueden ser directores de gestión de riesgo, de finanzas, de auditoría, del departamento jurídico, de compras, etc. Pero limitar la administración de riesgos a pocos individuos también nos limita en nuestra capacidad de reconocerlos y disminuirlos. Cada empleado y contratista de la organización tiene la oportunidad para contribuir a la identificación de riesgos y su mitigación.

El segundo concepto de importancia que pretende demostrar esta guía es que la gestión de riesgos es responsabilidad de cada miembro de una organización, y de cada miembro se contribuye a la mejora de la organización. Con este concepto, se pretende ofrecer las herramientas para asegurar que cada miembro de una organización tenga la capacidad, el conocimiento y el compromiso para cumplir su parte en la gestión de riesgos.

Con base en lo anteriormente expuesto, los objetivos específicos de esta guía son los siguientes:

- Explicar de manera sencilla y clara los conceptos clave necesarios para una gestión integral de riesgos de una organización, de cualquier tamaño y complejidad.
- Ofrecer una herramienta básica para que los líderes de la organización puedan:
  - Identificar, analizar y priorizar los riesgos de mayor importancia para la organización;
  - Diseñar e implementar estrategias para disminuir o evitar los riesgos de mayor importancia; e
  - Involucrar y coordinar a todos en su organización en la identificación y la mitigación de riesgos.
- Proporcionar referencias relevantes de material adicional sobre el tema para desarrollar la capacidad de gestión de riesgos en una empresa u otra organización.

Es el propósito de esta guía presentar información suficiente, reforzada con ejemplos concretos, para apoyar a cualquier líder o administrador en México en el desarrollo básico de la gestión de riesgos.

CONCEPTOS CLAVE

Además de los conceptos mencionados anteriormente –la importancia de analizar y gestionar los riesgos de manera integral y la importancia de involucrar a todos en la organización–, existen algunos conceptos clave para entender y gestionar los riesgos en una organización.

Riesgo, Probabilidad y Vulnerabilidad

Existen varias definiciones detalladas de riesgo, pero casi todas incluyen los elementos más básicos: la probabilidad que ocurra un evento negativo y el efecto o impacto negativo de tal evento. Así que la gravedad de un riesgo para una organización depende de la probabilidad de que ocurra y el impacto que tendría sobre la organización. Lo que determina estos dos factores es la amenaza (la fuente del peligro) y la vulnerabilidad de la organización a sus efectos.

Los dos factores que componen el riesgo son:

$$\text{Riesgo} = \text{probabilidad} \times \text{impacto}$$

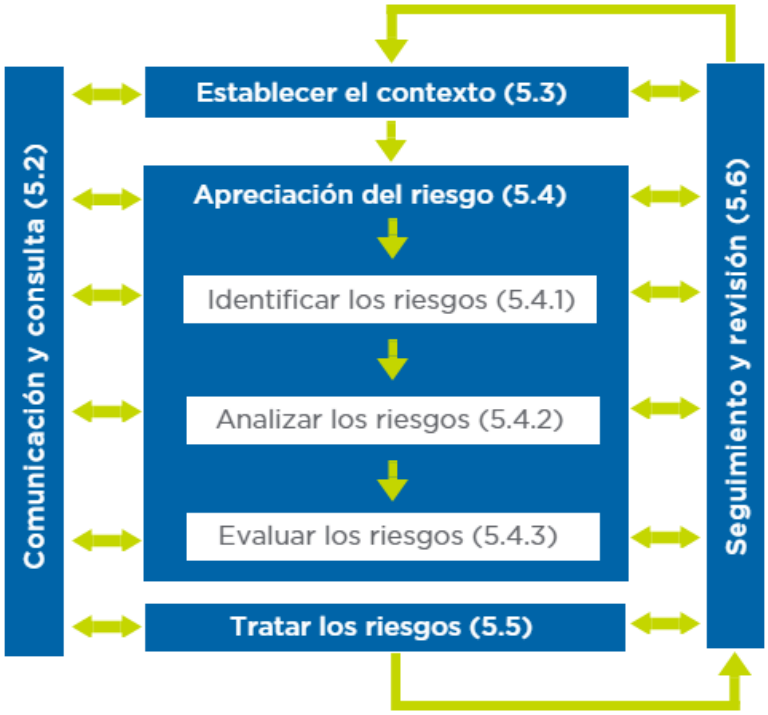
Así que, midiendo la probabilidad y el potencial de impacto, podemos medir la gravedad del riesgo para la organización, y podemos comparar la gravedad de un riesgo con otro. La buena noticia es que estos dos aspectos nos permiten disminuir el riesgo de dos maneras diferentes: minimizando la probabilidad de que ocurra el evento (prevención) y disminuyendo el potencial de efecto negativo del mismo, en el caso que ocurra (resiliencia).

Disminuir probabilidad
\+ Disminuir impacto
Disminuir riesgo

Más adelante, se analizarán más a detalle las actividades para evaluar riesgos y para disminuirlos.

Análisis e Implementación

En todas las metodologías y estándares para la gestión de riesgos, también existe un proceso que incluye varios pasos de análisis: del contexto en el cual existe la organización, de evaluación y tratamiento de los riesgos, y de monitoreo de resultados y condiciones de desempeño, lo cual es un ciclo constante para cualquier criterio de mejores prácticas. Un ejemplo de este ciclo es el que se usa en el ISO 31000:



Fuente: UNE-ISO 31000

Gobierno Corporativo

Finalmente, resulta pertinente introducir el concepto de gobierno corporativo (adoptado del *corporate governance*, en inglés). La gestión de riesgos para una organización implica prácticas de identificación y análisis de riesgo, además del seguimiento de una cierta disciplina en las conductas de la organización a todos niveles.

Esto requiere un nivel de vigilancia y de atención que no se presta para ser controlado o administrado exclusivamente por la gerencia de la organización, ni por un área especializada de gestión de riesgos. Requiere la participación coordinada de todos los miembros de la organización, y hasta terceros que contribuyen a las actividades de la organización.

La única manera de coordinar y asegurar este nivel de gestión es a través de un sistema de enseñanza, lineamientos, controles, responsabilidades, monitoreo y comunicación. Este sistema o estructura se conoce como gobierno corporativo, del cual el cumplimiento (de los lineamientos, políticas, etc.) es una parte integral.

Así pues, varias de las estrategias que son detalladas más adelante en esta guía, dependen del desarrollo de un eficaz gobierno corporativo – sea entre el dueño y los pocos empleados de una organización pequeña, o entre el consejo administrativo de una multinacional y sus varias operaciones locales alrededor del mundo–.

ADMINISTRACIÓN INTEGRAL DE RIESGOS

Las organizaciones se encuentran constantemente expuestas a riesgos de diferentes tipos y magnitudes, el emprender esfuerzos para intentar mantener todos ellos bajo control para contener su impacto pudiera no ser la mejor manera de invertir los recursos de una organización, toda vez que el costo pudiera resultar mayor que la materialización del propio riesgo.

Es por ello que una adecuada administración de riesgos es aquella que promueve la que permite a una organización crear, preservar, sostener y generar valor. Hoy en día los altos directivos buscan constantemente identificar los riesgos ante los cuales sus organizaciones son más susceptibles pero al mismo tiempo buscan obtener información relacionada a estos riesgos que les brinde la posibilidad de tomar decisiones estratégicas.

Apetito y Tolerancia

El apetito al riesgo lo podemos definir como el balance entre riesgo y oportunidad, en otras palabras el nivel de riesgo que la organización está dispuesta a aceptar en la persecución de sus objetivos.

Actualmente las organizaciones se han dado cuenta que el riesgo no es algo malo o que tenga que evitar y controlar, sino que en el ambiente de negocios actual para que la organización pueda desarrollarse tiene que entender y establecer cuánto del riesgo al que está expuesta está dispuesta a aceptar con la finalidad de lograr sus objetivos.

El apetito al riesgo debe ser definido por el órgano más alto de administración de la organización[1], el cual establece los umbrales de riesgos necesarios para dar forma y dirección a las estrategias de la organización. Al definir el apetito al riesgo la organización deberá considerar cuatro conceptos principales:

A) *Capacidad de riesgo:* Este es una evaluación del riesgo máximo que una organización podría soportar sin sufrir un deterioro grave en su capacidad de negocio. Proporciona un límite superior para el apetito de riesgo.

B) *Tolerancia al riesgo:* Se analizan las desviaciones aceptables e inaceptables de lo que se espera de cada riesgo al que la organización está expuesta como en su conjunto. Las percepciones de la tolerancia al riesgo tienen que ser consideradas en detalle para establecer el

[1] Típicamente en una organización grande, es el Consejo de Administración. En una pequeña se habla del o de los dueños administradores

equilibrio óptimo de un riesgo que ocurre frente a los costos y / o el valor de limitar ese riesgo.

C) *Perfil deseado de riesgo:* Es la descripción y cuantificación de los riesgos específicos que la organización planea gestionar. Se describe típicamente usando un modelo de categorización del riesgo y es una consecuencia directa de los componentes principales del apetito de riesgo. El perfil de riesgo objetivo vincula el apetito de riesgo del grupo para el rendimiento de la organización y es la base para el desarrollo de límites consistentes.

D) *Perfil actual de riesgo:* Se deriva de los riesgos a los que está expuesta la organización incluyendo su evaluación. La recopilación de estos datos se apoya en el proceso de administración de riesgos y los mecanismos de información.

Para ilustrar estos conceptos, imaginemos una empresa farmacéutica que está evaluando la posibilidad de expandir sus operaciones a Centroamérica. Después de un análisis de riesgos, el Consejo de Administración ha concluido que para no afectar la operación actual de la empresa se tiene una capacidad de riesgo del 25% del capital social de la compañía que equivale a poco más de 50 millones de dólares.

Para alinear a la organización a estos niveles el área de administración de riesgos detalló el perfil actual de riesgo identificando los eventos de riesgo y el grado de exposición a los que está expuesta así como los controles antes de realizar la expansión.

Posteriormente en la sesión del Consejo se estableció cuál debería ser el perfil de riesgo que la empresa perseguirá durante el programa de crecimiento. Previo a las actividades de expansión la Dirección General establece a su equipo que toda operación a realizar tendrá un límite de pérdida por cualquier evento que afecte la expansión de 15 millones de dólares.

Procesos Generales

Al adoptar una metodología de Administración Integral de Riesgos (ERM por sus siglas en inglés), las organizaciones deben establecer un proceso general para gestionar los riesgos y homologar los esfuerzos en toda la organización. En general el proceso de gestión de riesgos debe considerar las siguientes fases:

A) *Identificación:* Son las actividades que realiza la organización para identificar los eventos potenciales que, de ocurrir, afectarán el logro de

los objetivos de la organización o por el contrario representen una oportunidad.

Los eventos con impacto negativo representan un riesgo, éstos tienen que ser evaluados y definir una respuesta para ellos, entre los que se pueden encontrar conflictos de interés, incapacidad para ejecutar las estrategias o interrupciones prolongadas de los sistemas.

Los eventos con impacto positivo representan una oportunidad, que la organización reconoce y evalúa para incluirlos en la estrategia o dentro del proceso de fijación de objetivos, como por ejemplo evaluar la implementación de un sistema ERP para la organización.

B) *Evaluación:* Una vez identificado el universo de riesgos, la evaluación de riesgos le permite a la organización considerar la amplitud con que los eventos potenciales podrían impactarle en la consecución de sus objetivos.

Se deberán evaluar estos acontecimientos desde una doble perspectiva, probabilidad e impacto, y para ello debe utilizar una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben analizarse individualmente, por categoría y en toda la organización.

Es importante que cuando se realizan las actividades de evaluación se realicen con un doble enfoque: riesgo inherente y riesgo residual.

El riesgo inherente, siendo la probabilidad e impacto que tendrían los eventos de ocurrir sin que la organización realice actividad de control alguna, ejemplo de ello, la exposición que tiene una organización por el riesgo de perder personal clave; y el riesgo residual, siendo la exposición residual que tiene la organización posterior a la implementación de actividades de control del riesgo, en el mismo ejemplo, la exposición que tiene la organización a perder personal clave una vez definidos e implementados planes de sucesión.

Para ejemplificar estos conceptos podemos imaginar una empresa de telecomunicaciones en donde un ataque cibernético en sus bases de datos podría representar un riesgo inherente a su operación y éste ser evaluado con una probabilidad alta de ocurrir debido al sistema que utiliza y un impacto también alto, ya que de perderse o no tener control de la información podría crear problemas importantes desde en su operación como en su reputación. Mientras que el riesgo residual podemos evaluarlo como la probabilidad baja una vez que se implementan controles preventivos para evitar ataques cibernéticos.

C) *Respuesta:* Una vez evaluados los riesgos, se determinan las actividades para responder a ellos. Estas pueden tener una postura para evitar, reducir, transferir o aceptar el riesgo.
Siendo *evitar,* cuando la organización, decide no realizar la actividad en la que se identificó el evento de riesgo.

Reducir el riesgo cuando define planes de acción enfocados a la creación de políticas, procedimientos, procesos y controles que ayuden a los responsables del riesgo a mitigar y controlarlo.

Transfiere el riesgo cuando decide recurrir a un tercero como aseguradora, proveedor, consultor, etc., para minimizar la probabilidad o impacto de presentarse los eventos.

Y *acepta* el riesgo cuando por el costo, beneficio o estrategia de la organización comprende las consecuencias y decide no realizar alguna actividad para controlarlo.

Al considerar la respuesta, las organizaciones deberán evaluar el efecto sobre la probabilidad e impacto del riesgo, los costos y beneficios, así como seleccionar aquella que sitúe el riesgo residual dentro de las tolerancias al riesgo establecidas.

D) *Comunicación:* Se deberán definir los procesos, sistemas y estructuras necesarias para identificar la información relevante y comunicarla de forma estandarizada dentro de un marco de tiempo establecido que permita a las personas llevar a cabo sus responsabilidades.

Los sistemas de información de riesgos en la organización deben contar con datos generados internamente y de fuentes externas para asegurar la toma de decisiones informadas alineadas a los objetivos y al riesgo aceptado de la organización.

La comunicación de la información de riesgos debe ser eficaz y fluir en todas las áreas y unidades de negocio. Todo el personal debe recibir un mensaje claro de sus responsabilidades, las actividades que deberá realizar y la información suficiente para llevarlas a cabo, pero de igual forma el cómo sus actividades individuales se relacionan con el trabajo de los demás.

Cabe mencionar, se deben definir los medios y mecanismos necesarios para comunicar y reportar la información hacia arriba así como con clientes, proveedores, reguladores, accionistas, etc.

Principales Marcos y Estándares

Como respuesta a la creciente necesidad de las organizaciones en la adopción de una estructura robusta de administración de riesgos, el Committee of Sponsoring Organizations of the Treadway Commission

(COSO ERM), emite un marco de adopción con los principios de administración de riesgos que las organizaciones pueden implementar para gestionar los riesgos que puedan impedir la consecución de sus objetivos.

El marco COSO ERM consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la organización y cómo están integrados en el proceso de gestión.

La administración integral de riesgos no constituye estrictamente un proceso en serie, donde cada componente afecta solo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro.

Las empresas que cuentan o planean certificarse bajo la normatividad ISO, están sujetas a la adopción de la norma ISO 31000, estándar diseñado para que las organizaciones implementen un programa de administración de riesgos.

Aspectos Relevantes

Las organizaciones sin importar su tamaño, giro, industria o ubicación geográfica no están exentas de daños por impactos de riesgos. Para ello las organizaciones necesitan analizar y entender cómo le afecta su entorno externo e interno.

Entre algunos de los factores externos que las organizaciones deben analizar están los *cambios demográficos,* por ejemplo, los sistemas de salud a nivel global empiezan a sufrir cambios para cumplir con la demanda poblacional y para las organizaciones del sector salud esto podría representar un incremento adicional en las regulaciones. Este mismo factor externo, para otros tipos de organizaciones, podría representar un aumento en el riesgo de interrupción y sobre la continuidad de sus actividades.

Otro factor externo permite responder preguntas como, ¿cómo los cambios en las economías de China o Grecia impactan a mi organización?, los *cambios económicos* son factores que a menudo las organizaciones no analizan, pero factores como éstos podrían hacer que las organizaciones se enfrenten a cambios abruptos en la distribución de sus productos o tener que adecuarse a cambios excesivos en las regulaciones locales y propias de la industria, como ha sufrido la industria de la aviación aunado de los atentados terroristas en el mundo.

La *aceleración de la urbanización* que sufren las grandes ciudades puede tener un impacto importante en las organizaciones, aspectos como el cambio drástico en la demanda del mercado que incrementa el riesgo de cumplimiento para organizaciones como aseguradoras u hospitales en donde podría sobrepasar su capacidad de operaciones. De igual forma se ha

observado que ciudades altamente urbanizadas incrementan el uso de información y medios sociales que podrían llevar a vulnerabilidades de privacidad y seguridad en aspectos como propiedad intelectual e información sensible de los clientes.

Los *cambios climáticos*, a medida que incrementan, provocan cambios sociales en el comportamiento de los consumidores y aumentan la carga regulatoria a la que están sujetas las organizaciones. Ejemplo de estragos de cambios climáticos observamos en la industria automotriz en donde como consecuencia de un huracán, desaparecieron empresas proveedoras interrumpiendo la cadena de suministro de las armadoras y creando un desabasto en la demanda a nivel mundial.

Así como observamos diversos ejemplos de cómo factores externos podrían afectar a las organizaciones, éstas deben analizar e incluir en las actividades de administración integral de riesgos, actividades para analizar sus factores internos y ser capaces de responder preguntas como:

- ¿Qué riesgos podrían impedir alcanzar los objetivos en los próximos años?
- ¿Cuál es el riesgo que está dispuesta a aceptar la organización para alcanzar sus objetivos y cuáles no?
- ¿Cuántas de nuestras estrategias y nuestros proyectos han fracasado y qué impacto ha tenido en la organización?
- ¿Sabemos qué eventos podrían causar que la operación se interrumpiera?
- ¿Cuál es la probabilidad de presentarse un fraude en la organización, y estoy preparado para ello?
- ¿Tenemos la capacidad para reponernos rápidamente ante un evento de interrupción?
- ¿Se monitorea eficientemente el capital en riesgo de la organización?

El ambiente interno representa un reto para las organizaciones donde se tiene que estar preparado para afrontar distintas amenazas, ya que a diferencia de los factores externos generalmente la organización no cuenta con grandes cantidades de información para su análisis. De acuerdo con la Encuesta Global de CEOs de PwC en 2015, la percepción de los Directores Generales de las empresas considera un incremento en sus principales riesgos en comparación con los últimos tres años.

De la investigación de referencia se encontraron riesgos relevantes que preocupan a los Directores Generales a nivel global donde lo encabeza, con el 78% de los participantes en el estudio, la sobrerregulación de sus

organizaciones y relacionado con éste, el 72% consideró el déficit fiscal y el 70% los incrementos de los impuestos locales e internacionales, todos ellos como riesgos importantes que enfrentarán sus organizaciones.

Aun cuando las ciudades se están urbanizando y las economías trabajan cada vez más a un nivel global, el 73% de los Directores Generales a nivel mundial mostraron una preocupación en la falta de disponibilidad de personal con las capacidades y habilidades adecuadas, lo cual ha llevado a establecer estrategias y optimizar sus operaciones.

Los sistemas tecnológicos actualmente juegan un papel importante sobre el desarrollo de las organizaciones y mientras en 2013 no se consideraba como una amenaza, el estudio observó que el 61% de los Directores Generales actualmente considera el ciberataque como un riesgo crítico en la vulnerabilidad de la información, mientras que el 58% de los participantes mostraron gran preocupación en cómo la velocidad en los cambios tecnológicos podrían afectar, desde su operación, cambios en el mercado, hasta tener que cambiar su modelo de negocio.

La participación en el mercado es un punto fundamental dentro de toda organización y en donde el 60% de los participantes considera preocupante los cambios de comportamiento de sus clientes y cómo afectan estos cambios en sus modelos de negocio, así como desde el punto de vista competitivo el 54% de los Directores Generales consideró como un riesgo actual importante para sus organizaciones la entrada de nuevos competidores a sus mercados.

ADMINISTRACIÓN DE RIESGOS CLAVE

Riesgo Estratégico

Los riesgos estratégicos, usualmente son externos o afectan las decisiones más importantes de la alta dirección. Como tal, a menudo son omitidos en muchos inventarios de riesgos. La organización tiene la responsabilidad de asegurar que este tipo de riesgos sean incluidos en las discusiones estratégicas.

Algunos de los principales riesgos estratégicos a los que la organización se podría enfrentar son:

- Disminución en la demanda
- Retención de clientes
- Competidores
- Fijación de precios
- Factores macroeconómicos
- Reputación

- Desastres Naturales
- Pérdidas de socios comerciales

Riesgo Financiero

Los riesgos financieros forman parte de la rutina habitual de las discusiones de riesgo del Consejo, con un fuerte empuje proveniente de incrementos regulatorios, contabilidad y enfoque de la auditoría financiera. Como la información financiera es un elemento clave de la comunicación de los stakeholders, la medición del desempeño y la entrega de la estrategia, las conversaciones del Consejo dedicarán una gran parte de su tiempo a estos riesgos.

Algunos de los principales riesgos financieros a los que la organización se podría enfrentar son:

- Deuda y tasas de interés
- Tipo de cambio
- Préstamos
- Crédito y Cobranza
- Pérdida de activos

Riesgo Operativo

Los riesgos operativos típicamente son administrados desde el negocio y a menudo se enfocan en los asuntos de seguridad y salud que les son requeridos por las regulaciones y estándares. Estos riesgos conducidos internamente pueden afectar la capacidad de la organización para cumplir los objetivos estratégicos.

Algunos de los principales riesgos operativos a los que la organización se podría enfrentar son:

- Conflictos de Interés
- Retención de empleados
- Seguridad en las áreas de trabajo
- Controles operativos ineficientes
- Problemas en la cadena de suministros
- Regulaciones
- Asignación de precios de productos
- Fraude y corrupción

Riesgo Cibernético

Hoy en día, nuestros negocios dependen cada vez más del uso de datos digitales y de conexiones electrónicas. Desde comunicación por correo electrónico hasta integración de nuestras cadenas de logística y de producción, pues es casi imposible llevar a cabo negocios sin comunicarse electrónicamente con terceros -clientes, proveedores, empleados, contratistas, el público en general y las autoridades-.

En conjunto con la creciente conexión electrónica y con la dependencia de datos digitales, viene mayor riesgo de daño o pérdida de nuestros datos o nuestra información confidencial o crítica, y afectación a nuestros sistemas.

Los daños que pudieran sufrir nuestras empresas de una pérdida de nuestros datos pueden ser económicos, pérdida de ventaja competitiva, responsabilidad civil o regulatoria por daños a terceros afectados, pérdida de reputación, hasta incapacidad de operar.

Como varios de los riesgos, nuestra capacidad de prevenir pérdida de información y disminuir los daños de la misma empieza con una evaluación de los puntos más débiles o más sensibles - ¿cuál es la información que queremos proteger?- Las medidas de prevención y de preparación (porque es imposible prevenir este riesgo completamente) incluyen aspectos organizacionales (políticas empresariales, comunicaciones, estructuras corporativas de implementación), aspectos humanos (capacitación, actitud, vigilancia) y aspectos tecnológicos (protección de dispositivos y de sistemas, control de acceso electrónico y físico, y monitoreo).

Una discusión más completa de este riesgo y cómo disminuirlo, se encuentra en la Guía de Ciberseguridad publicada por la ICC[2].

Además de pensar en la prevención, es importante prepararse para responder en caso de una fuga de información. Eso implica el monitoreo constante de nuestras redes de informática, para detectar y analizar actividades sospechosas o posibles intentos de atacar.

También implica preparación para responder - investigación y detención de un ataque, comunicación de los efectos con interesados claves, y recuperación del ataque o de la pérdida. Igual como la prevención, la preparación necesita una combinación de tecnología adecuada y correctamente configurada, procesos de respuesta y personal preparada.

[2] International Chamber of Commerce. *Guía de Seguridad ICC para los Negocios*. Obtenido de: https://cdn.iccwbo.org/content/uploads/sites/3/2015/08/ICC-Cyber-Security-Guidelines-for-Business-Spanish-Cyber-Security-Guide-2.pdf

Fraude y Corrupción

Sin duda alguna, uno de los principales riesgos operativos de las empresas lo representa el fraude y la corrupción, ya que, lamentablemente, es común que los intereses económicos superen a los valores y a las prácticas éticas en los negocios.

Debido a lo anterior, la competencia económica, cada vez más intensa, pone en conflicto dos objetivos igual de importantes para el desarrollo y la sostenibilidad de los negocios: (a) la generación de utilidades; y (b) el cumplimiento y establecimiento y operación de controles adecuados. Es así como el fraude y la corrupción explota la tensión entre dichos objetivos, como campo fértil para un sinnúmero de delitos económicos.

Por una parte, el fraude puede llegar a causar grandes pérdidas y daños a los negocios; sin embargo, la corrupción es aquella que está siendo atacada en mayor medida por los reguladores, debido a que la misma es de naturaleza "sistémica", por lo que llega a corromper organizaciones y sociedades enteras desde sus raíces.

Pero, ¿de qué tamaño puede llegar a ser el impacto por fraude y corrupción? Según el Reporte a las Naciones 2014 (*"Report to the Nations"*) emitido por la Asociación de Examinadores Certificados de Fraude (*"ACFE"* por sus siglas en inglés o *"Association of Certified Fraud Examiners"*); se estima que una organización típica pierde hasta un equivalente al 5% de sus ingresos debido al fraude.

Por otra parte, la *"Encuesta 2014 Sobre Delitos Económicos"* publicada por PwC, reporta un índice de fraude y corrupción del 36% en México; es decir, más de una tercera parte de las organizaciones en México reportaron haber sufrido algún tipo de delito económico en los últimos 24 meses.

La Malversación de Activos, la Corrupción y el Soborno, y el Fraude en Adquisiciones son los tres tipos de delitos económicos más comunes en México, según dicha encuesta.

Sin embargo; más allá de lo económico, los daños totales se extienden a áreas que afectan el desempeño de los negocios, incluyendo daño a la moral de los empleados, en las relaciones comerciales, con reguladores, reputación de la marca, y precio de la acción, por mencionar algunos de los más importantes.

El fraude y la corrupción han sido tradicionalmente atacados de forma reactiva, más aún en México, en donde la cultura de prevención se ha ido desarrollando muy poco a poco.

No obstante lo anterior, cada vez más organizaciones se están percatando de los beneficios de establecer programas de prevención, los cuales, más allá de mitigar riesgos importantes de fraude y corrupción, pueden también aportar beneficios operacionales, amén de que actualmente y como se verá más adelante, se vuelve una "obligación" para las empresas el ejercer un debido control en sus administradores, representantes, directivos y empleados en general, al encontrarse vigente la "Responsabilidad Penal de las Personas Morales" por la comisión de delitos de estos últimos en nombre o bajo su amparo, por cuenta y en provecho o exclusivo beneficio de la empresa.

Incluso, las organizaciones transparentes dan mayor confianza a los accionistas, inversionistas, reguladores, y socios de negocios actuales o potenciales.

Uno de los pilares más importantes para un programa de prevención de fraude y corrupción (o de delitos en general) es, sin duda, contar con controles internos sólidos. El "Reporte Global Sobre Fraude 2015" publicado por Kroll encontró que, de los casos de fraude donde los responsables fueron identificados, 81% incluían al menos un defraudador dentro de la compañía.

Además, es importante que las organizaciones consideren iniciativas que ayuden a reforzar sus programas, sobre todo, aquellas relacionadas con el fortalecimiento de la cultura y ética corporativa, incluyendo un mensaje consistente y firme de la alta administración.

Desarrollar un conocimiento profundo de los riesgos específicos de fraude y corrupción a los que puede estar sujeta una organización, será el punto de partida para desarrollar iniciativas de prevención más eficientes, con enfoque a riesgos.

Responsabilidad Penal de las Personas Morales

Hoy en día, en el Código Penal para la Ciudad de México se tiene establecido que las personas morales o jurídicas pueden ser penalmente responsables por los delitos dolosos (inclusive en grado de tentativa) o culposos cometidos en su nombre, por su cuenta, en su provecho o exclusivo beneficio, por sus administradores (de hecho o de derecho) y/o representantes legales; asimismo, por aquellos cometidos por las "personas sometidas a la autoridad" de dichos administradores y/o representantes legales, por no haberse ejercido sobre ellas el debido control que corresponda al ámbito organizacional que deba atenderse.

Por su parte e igualmente en vigencia, el Código Nacional de Procedimientos Penales y el Código Penal Federal establecen, de manera similar a lo citado en el párrafo anterior, que las personas jurídicas serán penalmente responsables de los delitos (aquellos relacionados en el catálogo del artículo 11 Bis del Código Penal Federal) cometidos a su nombre o bajo su amparo,

por su cuenta, en su beneficio o a través de los medios que ellas proporcionen, cuando se haya determinado que además existió inobservancia del debido control en su organización.

Todo lo anterior con independencia de la responsabilidad penal en la que puedan incurrir sus representantes o administradores de hecho o de derecho.

La ley establece sanciones y consecuencias jurídicas accesorias para las personas morales que sean consideradas penalmente responsables.

Como sanciones y consecuencias jurídicas accesorias se contemplan: las pecuniarias (multa y reparación del daño); decomiso de instrumentos, objetos y productos del delito; suspensión o privación de derechos; publicación de sentencia; disolución; remoción; intervención; clausura; retiro de mobiliario urbano; custodia de folio real o mercantil; inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y gozar de beneficios e incentivos fiscales o sociales por un plazo hasta de 15 años.

Ante lo anterior, se vuelve de mayor relevancia para las empresas la implementación de un programa de cumplimiento y/o prevención de delitos, mismo que debiera contemplar, entre otros posibles aspectos:

- La adopción de medidas internas destinadas a asegurar su observancia
- La existencia de un código de conducta y/o ética dirigido a todos los empleados (y terceros tales como proveedores, intermediarios, clientes, etc.) y con firma de recibido
- La existencia de un responsable de cumplimiento normativo
- La existencia de un sistema de control de funciones y procedimientos con la vigilancia del responsable
- La existencia de un control documental
- La existencia de un programa de cumplimiento en materia penal entre compañías de un mismo grupo.

Responsabilidades Administrativas

Con la reciente entrada en vigor de la Ley General de Responsabilidades Administrativas, los particulares y las empresas podrán ser sujetos de procedimientos y sanciones administrativas por la comisión de denominadas “faltas graves” en sus relaciones con la administración pública.

En términos generales, se consideran faltas graves conforme a esta Ley: el soborno, la participación ilícita en procedimientos administrativos, el tráfico de influencias, la utilización de información falsa o alterada, la obstrucción de

facultades de investigación, la colusión, el uso indebido de recursos públicos y la contratación indebida de ex servidores públicos.

Para las empresas, las sanciones económicas contempladas incluyen:

- Hasta dos tantos de los beneficios obtenidos o hasta un millón quinientas mil veces el valor diario de la Unidad de Medida y Actualización ($113'235,000 para 2017).
- Inhabilitación temporal para participar en adquisiciones, arrendamientos, servicios u obras públicas por un periodo de entre 3 meses y 10 años.
- Indemnización por los daños y perjuicios ocasionados a la Hacienda Pública Federal, local o municipal, o al patrimonio de los entes públicos.
- La suspensión temporal de actividades por un periodo de entre tres meses y tres años si se acredita la participación de sus órganos de administración o el uso sistemático de la empresa para vincularse con faltas administrativas graves.
- Disolución de la sociedad si se acredita la participación de sus órganos de administración o el uso sistemático de la empresa para vincularse con faltas administrativas graves.

Conforme a la propia Ley se considerarán como atenuantes en la imposición de las sanciones, el que la empresa cuente con una política de integridad operante y efectiva, que haya formulado la denuncia correspondiente y colabore en las investigaciones, así como el efectuar el resarcimiento de los daños.

Por su parte será una agravante en la imposición de sanciones que las empresas conozcan de presuntos actos de corrupción de personas físicas que pertenecen a aquellas y que no los denuncien.

Riesgo Legal

Conforme al Diccionario de la Real Academia de la Lengua Española, riesgo es la contingencia o proximidad de un daño, o bien, cada una de las contingencias que pueden ser objeto de un contrato de seguro.

Para efectos de esta guía entendemos por riesgo aquella situación en la que está presente o se incrementa un acontecimiento de realización incierta y futura pero que es posible y probable que acontezca, y cuya actualización generará una o más **consecuencias dañosas**.

De esta manera resulta importante definir el "daño" y éste, desde el punto de vista estrictamente del derecho civil, debe entenderse como la pérdida o

menoscabo sufrido en el patrimonio por el incumplimiento de una obligación[3].

Este daño "civil" puede dividirse en daño material cuya definición antes se ha apuntado y el daño moral que es la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás[4].

Como lo recoge esta guía, existen distintos tipos de riesgos que las empresas asumen, evitan y administran en su operación, por lo que respecta al **riesgo legal**, no existe en el orden jurídico mexicano una definición, sin embargo, encontramos algunas disposiciones de carácter internacional que nos ayudan a conceptualizarlo, tal es el caso de lo que refiere el Comité de Supervisión Bancaria de Basilea[5] (Basel Committee on Banking Supervision, en inglés), que ha emitido diversos documentos en los que expresa lo que entiende por riesgo legal:

> Es el riesgo de pérdida debido a la exigibilidad de acuerdos contractuales, procesos legales o sentencias adversas (incluyendo procedimientos referentes a la insolvencia de una entidad de contrapartida). Tales pérdidas pueden provenir de errores, omisiones o defectos de forma en procedimientos legales, o de dificultades legales sustantivas o problemas legales que surjan del sistema legal de un país o grupo de países relevante para la operación[6].

El propio Comité ha precisado que cualquier empresa enfrenta **la posibilidad de ser sancionada**, y esto puede ir desde la imposición de una multa hasta el tener que cumplir con la obligación de pagar daños punitivos derivada del ejercicio de acciones supervisoras (auditorías) o incluso de incumplimientos de acuerdos entre particulares.

Por su parte, el Banco de México, **BANXICO**, en un estudio que emitió titulado "Riesgos de las Instituciones Financieras" expuso que por lo que corresponde a dichos entes, los riesgos son regulados (clasificados) en dos ordenamientos: la Circular Única de Bancos (**CUB**), emitida por la Comisión

---

[3] Artículo 2108 del Código Civil para el Distrito Federal.

[4] Artículo 1916 del Código Civil para el Distrito Federal.

[5] La organización mundial que concentra a diversas autoridades de supervisión bancaria y que tiene por objeto fortalecer los sistemas financieros.

[6] Banco Central Europeo. *La política Monetaria Única en la Tercera Etapa*. Obtenido de: http://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesBCE/PoliticaMonetaria/Fic/gendoc98es.pdf

Nacional Bancaria y de Valores, **CNBV**, y los requerimientos de capitalización emitidos por la Secretaría de Hacienda y Crédito Público.

La **CUB** precisa que existen: (i) Riesgos discrecionales, (ii) Riesgos no discrecionales y (iii) y riesgos no cuantificables.

Los riesgos legales, conforme a dicha Circular, **se encuentran en el rubro de riesgos no discrecionales, esto implica, que resultan a partir de la operación del ente**. El **riesgo legal** visto desde este ángulo, siguiendo la línea que ha marcado el citado *Comité*, implica una disminución o pérdida en el patrimonio que surge ya sea por el incumplimiento de normas tanto jurídicas como administrativas, por la obtención de resoluciones, judiciales o administrativas, que son desfavorables hacia los intereses de la corporación, o bien, por la aplicación de sanciones que resiente la institución, derivada de las actividades que lleva a cabo[7].

Aunada a las corrientes ya expuestas, existe otra que se distingue por tener un enfoque financiero y que precisa que hay dos formas de definir al riesgo legal:

a) De forma directa: Se refiere a la posibilidad de pérdidas en virtud del incumplimiento (o de la imperfección) de la normatividad que afecta a los contratos o, de plano, a la imposibilidad en cuanto a la exigibilidad del contrato.

b) De forma indirecta: La posibilidad de pérdidas ocurre en virtud de las reformas – en un sentido amplio- que puede sufrir la normatividad de manera que afecte negativamente a la empresa. En atención de las modificaciones que puede sufrir el marco jurídico lo que, por ejemplo, en un momento no era considerado una mala práctica, ahora lo puede ser, con las consecuencias que ello implica; otro ejemplo puede ser el de que una determinada actividad empresarial no estuviera regulada anteriormente y ahora ya lo sea o que, a pesar de que antes ya estaba sujeta a un marco regulatorio, ahora enfrente una "sobrerregulación".

Dicho lo anterior, lo que es importante considerar es que **el riesgo legal forma parte del riesgo operacional** pues supondrá una pérdida y daños para la empresa SIEMPRE como <u>consecuencia del incumplimiento de una norma jurídica</u> ya sea general o individualizada. Para mayor claridad se presenta el siguiente esquema:

Para la actualización del riesgo legal no es necesario siquiera que el incumplimiento resulte cierto y verdadero, puede llegar a causar daño tan

[7] Banco de México. Obtenido de: http://www.banxico.org.mx/sistema-financiero/material-educativo/basico/fichas/indicadores-financieros/%7B21F1ED23-A991-0977-ECD3-5555886B7F4D%7D.pdf

sólo si tiene el carácter de PRESUNTO. En cualquier caso, deriva normalmente en alguno de los siguientes procedimientos y/o procesos:

- De verificación en materia de lavado de dinero por parte de la Unidad de Inteligencia Financiera del SAT.
- De responsabilidades administrativas.
- De responsabilidades fiscales.
- De índole civil y/o mercantil.
- De una carpeta de investigación y/o de índole penal.

Dichos procesos concluirán con cualquiera de las siguientes RESPONSABILIDADES a cargo de la empresa, sus socios, accionistas, apoderados, representantes o empleados:

- En materia fiscal: imposición de créditos fiscales y en su caso, inicio de investigaciones de índole administrativa y/o penal.
- En materia de lavado de dinero: congelamiento de cuentas bancarias, imposición de multas, procedimientos administrativos sancionatorios y en su caso, inicio de investigaciones de índole penal.
- En materia de responsabilidades administrativas: multas, inhabilitación temporal, suspensión de actividades, indemnizaciones por daños y perjuicios e incluso la disolución de la sociedad.
- En materia penal: prisión y multa para las personas físicas que participen en la comisión del delito y para las empresas: multa y reparación del daño; decomiso de instrumentos, objetos y productos del delito; suspensión o privación de derechos; publicación de sentencia; disolución; remoción; intervención; clausura; retiro de mobiliario urbano; custodia de folio real o mercantil; inhabilitación para obtener subvenciones y ayudas públicas.

De tal manera que la gestión y administración de riesgos legales en las empresas siempre debe tener como objetivo el EVITAR, a través de Políticas de Compliance, Asesoría Legal Preventiva y Auditorías, los diversos INCUMPLIMIENTOS en los que puede caer la empresa de manera voluntaria o involuntaria.

Esta guía pretende, por lo que hace a este capítulo, concientizar a las organizaciones de la importancia de cumplir el marco jurídico aplicable, siendo esta práctica el mejor seguro contra posibles consecuencias legales que pueden poner en peligro la operación y la viabilidad de la misma empresa.

Evaluación de riesgo de Lavado de activo (LA) y financiamiento del terrorismo (FT)

La Guía para el Enfoque Basado en el Riesgo para el Sector Bancario, emitido por El Grupo de Acción Financiera Internacional (GAFI) respecto a la prevención del lavado de activos (ALA) y el estándar internacional sobre la lucha contra el financiamiento del terrorismo (CFT) sostiene lo siguiente:

> **(22)** La evaluación del riesgo de LA/FT implica que los países, autoridades competentes y bancos, deberán determinar cómo los afectarán las amenazas de LA/FT que han sido identificadas.
>
> Deben analizar la información obtenida con objeto de entender la probabilidad de que ocurran estos riesgos, y cuáles serían sus impactos en los bancos en lo individual, el sector bancario y, posiblemente, en la economía nacional de las instituciones financieras de importancia sistémica, en caso de ocurrir. Como resultado de la evaluación de riesgos, a menudo los riesgos de LA/FT son situados en categorías de bajo, medio y alto, y posibles combinaciones entre las diferentes categorías (medio-alto; medio-bajo, etc.).
>
> La clasificación pretende ser de ayuda para entender los riesgos de LA/FT y para ayudar a organizarlos de forma prioritaria. Por lo tanto, la evaluación de riesgos de LA/FT es mucho más que la mera recopilación de información cuantitativa y cualitativa: es la base para una mitigación eficaz del riesgo de LA/FT y debe mantenerse actualizado para no perder su relevancia.
>
> **(23)** La evaluación y comprensión de los riesgos significa que las autoridades competentes y los bancos deben contar con personal capacitado y de confianza que haya sido reclutado a partir de la aprobación de exámenes relativos adecuados. Lo anterior implica que deben contar con las herramientas técnicas necesarias para llevar a cabo este trabajo, dada la complejidad de las operaciones del banco[8]

CONTINUIDAD DE NEGOCIOS Y LA IMPORTANCIA DE SU ADOPCIÓN EN LAS EMPRESAS

Todas las empresas son susceptibles a interrupciones por causas internas o externas. La mayoría de los desastres no son previsibles, sin embargo, se puede estar preparado para enfrentarlos de la mejor manera y continuar en el negocio el día de mañana.

[8] Grupo de Acción Financiera Internacional. *Guía del Enfoque Basado en Riesgo para el Sector Bancario.* Obtenido de: http://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/GAFI_Risk-Based-Approach-Banking-Sector_%282014%29%20-ESP%20REV%20mayo8.v.pdf

Las tendencias actuales están cambiando al mundo: el poder económico, cambios demográficos, avances tecnológicos, urbanización y el cambio climático han puesto en escena un incremento en el número de amenazas y riesgos que anteriormente no se consideraban o simplemente no existían.

Asimismo, la creciente dependencia tecnológica y cadenas de suministros cada vez más robustas hacen reflexionar sobre la necesidad de estar preparados para afrontar las interrupciones a las que se puede enfrentar la operación de su organización y mantener el valor de la marca reduciendo sus impactos y aumentando su resiliencia.

Ninguna organización está exenta y todas pueden ser sorprendidas por las siguientes amenazas:

- Tecnológica – Daños en data centers, daños o fallas en software y hardware, incumplimiento de proveedores.
- Instalaciones – Sismos, incendios, inundaciones, fugas, cortes en servicios básicos (agua, luz, etc.), terrorismo, disturbios sociales y bloqueos.
- Gente – Contingencia sanitaria, amenaza de terrorismo, desastres naturales, huelgas.
- Proveedores clave – tecnológico, financiero, personal (outsourcing), transportación, insumos, cadena de suministro, proveedores y clientes críticos.

Considere los siguientes escenarios:

- *Un pronóstico del tiempo global predice un gran huracán con 30% de probabilidad de impacto en las costas de la ciudad, donde se localiza su manufacturera de mayor volumen de producción, logística y operación de proveedores.*

  Dentro de las próximas 48 horas, la probabilidad de impacto es una realidad, con una capacidad destructiva mayor a la predicha. Para hacer el escenario aún peor, el huracán tiene el potencial de impactar su call center subcontratado para su servicio de atención al cliente que soporta un volumen de 75% de las llamadas. Sumando a estas amenazas, actualmente existe una tensión política en el país.

  En las recientes elecciones, el partido que había gobernado por un largo tiempo fue vencido por la oposición y la mayoría de las funciones de gobierno están en medio de una transición. Bajo este entorno, ¿cuáles son sus opciones?

  ¿Va a tratar de capear el temporal y correr el riesgo de ver colapsar su estrategia de crecimiento global antes de obtener los beneficios prometidos? O;

¿Ha prevenido a su organización contra tales riesgos de interrupción del negocio mediante el establecimiento de un programa de gestión de continuidad de negocio que engloba el riesgo de sus proveedores mediante la incorporación de una mayor capacidad de recuperación?

- *Se ha informado en los medios de comunicación que una gripe pandémica ha alcanzado nuestro país. Las noticias de la Ciudad de México y las autoridades de salud pública han reportado altos niveles de enfermedad a lo largo y ancho de la ciudad. Por lo que han hecho la recomendación a las organizaciones a detener cualquier actividad laboral y evitar concentraciones de gente en lugares cerrados y públicos para evitar contagios y poner en riesgo la salud de las personas.*

  Para su organización el recurso humano es indispensable para seguir brindando productos y servicios, de lo contrario, habría un impacto económico para la Organización.

- *La operación de una organización tiene una alta dependencia de la cadena de suministro. Asimismo, esta organización, frecuentemente tiene cambios en la configuración y requerimientos de su cadena por la inclusión de nuevos productos o mejoras a los ya existentes.*

  Sin embargo, uno de los principales proveedores involucrados en la cadena de suministro está actualmente incapacitado para seguir suministrando sus productos y materias y primas por una inestabilidad social en el país de origen de los insumos, lo que ha provocado un cierre de fronteras en el mismo.

  Esta situación afectará sobremanera la entrega de productos al consumidor final ya que el insumo de este proveedor es clave para su proceso de producción.

- *Se ha registrado un ciberataque a una Organización, este ataque ha impactado en los principales sistemas tecnológicos incapacitando la operación crítica parcialmente.*

  La alta dependencia tecnológica de la compañía la ha colocado en un evento de interrupción de operaciones ya que la concentración de sus funciones críticas está basada en los sistemas atacados.

  De no recuperar los sistemas en un corto tiempo, impactará considerablemente en el servicio al cliente, provocando pérdidas importantes y un impacto reputacional de consideración.

Para hacer frente a las amenazas, las organizaciones adoptan estrategias de continuidad de negocios que les permita:

- Preservar valor y reputación de la Marca
- Salvaguardad la integridad física de las personas

- Identificar, priorizar y mitigar los principales riesgos con impacto en la continuidad del negocio y de los procesos críticos
- Reducir el impacto de las interrupciones del negocio
- Reducción de costos
- Certeza en la toma de decisiones durante un evento de crisis
- Ventaja competitiva necesaria para seguir entregando sus productos y servicios con la misma calidad y tiempo durante y después de una interrupción
- Comprender las capacidades de recuperación y resiliencia de sus proveedores críticos ante interrupciones como parte de los procesos de selección
- Establecer mecanismos que permitan anticipar y reaccionar a los requerimientos regulatorios
- Aumentar la resiliencia en la organización
- Identificar mejoras de procesos y estructura organizacionales

La continuidad de negocios es el desarrollo de estrategias, planes y acciones que proveen protección o modos alternativos de operación para aquellas actividades o procesos que si son interrumpidos pueden impactar negativamente a la organización derivando en potenciales pérdidas de consideración.

Una Gestión de Continuidad de Negocios (BCM por sus siglas en inglés), contribuye a que las organizaciones sean más resilientes a las amenazas potenciales, permitiendo a las entidades reanudar o continuar las operaciones en condiciones adversas o negativas, a través de estrategias y planes de continuidad de negocio que reduzcan el impacto derivado de la materialización de una amenaza o riesgo que no puede ser controlado.

Asimismo, proporciona un marco para fortalecer la resiliencia organizacional a través de un programa de respuesta que salvaguarde los intereses de los principales stakeholders, su reputación, marca y actividades que generan valor.

No importa el tamaño de la organización o industria, el BCM puede ser aplicado en todos los procesos del negocio.

El BCM se conforma principalmente de los siguientes elementos clave:

A. *Continuidad de Negocios (BCP):* Permite la recuperación y continuidad de las funciones críticas de negocio necesarias para mantener un nivel aceptable de operación en un periodo tiempo definido durante un evento de interrupción, con la finalidad de garantizar la continuidad operativa del negocio.

B. *Recuperación de Desastres (DRP):* Aborda la recuperación de activos críticos de tecnología, incluyendo sistemas, aplicaciones, telecomunicaciones, bases de datos, etc.

Relación entre Administración Integral de Riesgos y la Continuidad de Negocios (BCM)

La administración de riesgos busca identificar maneras de prepararse para tratar los riesgos inherentes a la operación y provocados por agentes internos o externos a la misma. Un impacto por la materialización de los riesgos puede afectar negativamente la capacidad de la organización para alcanzar sus objetivos de negocio. Por lo tanto, si una organización es incapaz de cumplir estos objetivos, es posible que la reputación de la organización quede dañada, derivando las amenazas en un riesgo reputacional.

Mirándolo desde este enfoque en el cual el logro de los objetivos se ve amenazado, es en donde se encuentra el punto de convergencia de la continuidad de negocios y el ERM, ya que ambos forman parte de una solución integral enfocada a la resiliencia organizacional que busque mitigar los distintos riesgos a la que está expuesta una organización, independientemente de la naturaleza de las amenazas. Asimismo, los resultados del análisis de riesgos y BIA pueden resultar como entradas clave para una iniciativa de ERM.

GESTIÓN DE CRISIS

*La Gestión de Crisis (CM) y Respuesta a Emergencias es la c*apacidad para reconocer y actuar estructuradamente frente a situaciones de crisis que pueden poner en riesgo a la operación e imagen de las organizaciones. Asimismo, consiste en desempeñar acciones de pronta respuesta en caso de detectar alguna situación que amenace el bienestar del personal en caso de ocurrir un incidente o evento mayor. La gestión de crisis se enfoca en estabilizar la situación adversa y prepararse para la recuperación de las operaciones.

Considere cualquiera de los siguientes escenarios:

- Un atentado o amenaza de bomba en corporativos, sucursales, tiendas, etc.
- Un incendio en las oficinas corporativas
- Inconformidad y quejas de consumidores en redes sociales
- Desastres naturales
- Accidentes en el lugar de trabajo
- Productos defectuosos
- Derrames de sustancias químicas

Debe considerar que, como organización, en primer lugar, tiene que ser capaz de alertar rápidamente a los empleados de la ocurrencia de un incidente; en segundo lugar debe de mantenerlos actualizados e informados sobre la evolución de la situación, así ellos no dependerán de la información de fuentes externas, como internet, redes sociales o la televisión. Sin embargo, los empleados son sólo una de las audiencias que necesitan estar consideradas en una crisis.

También es necesario comunicarse con los clientes, informarles proactivamente de la situación con la finalidad de evitar que se enteren por otros medios que pueden mal informar o manipular la situación. Asimismo, disipar las dudas con relación a la capacidad de seguir brindando bienes y/o servicios.

Por último, y por ello no menos importante, se debe notificar a los principales proveedores, socios y otros grupos de interés que deben ser informados de cualquier incidente y su probable impacto.

En la actualidad los planes de gestión de crisis son un elemento esencial del programa de continuidad de negocio y por ello deben estar alineados, ya que ambos buscan esencialmente salvaguardar la integridad física de las personas y la reputación del negocio desde distintos flancos: la continuidad del negocio en la parte operativa y la gestión de crisis en la respuesta a emergencias, toma de decisiones y la comunicación hacia sus grupos de interés, previo, durante y posterior a un evento de crisis.

Con el apoyo de plataformas masivas de tecnología como son las redes sociales es posible responder rápida y oportunamente ante situaciones de crisis.

En casos de respuesta a emergencia, es posible contactar o enviar un mensaje de auxilio a los servicios de emergencia, esto apoya en la coordinación con estas entidades públicas; de la misma forma para dar actualizaciones de la situación de crisis a entidades regulatorias, medios de comunicación o grupos de interés, evitando información distorsionada y versiones alternas o negativas que aumenten el estado de alerta de la organización, sabiendo que llegará a un gran porcentaje de la audiencia meta (medios de comunicación, entidades regulatorias, autoridades públicas, público en general).

Es importante mencionar que antes de pensar en utilizar las redes sociales como una herramienta para responder a eventos de crisis, se deben revisar las estrategias de comunicación y plataformas tecnológicas de la organización para verificar si es posible utilizarlas para comunicarse con sus grupos de interés, y en dado caso que se recurra a éstas, deberán probarse periódicamente para medir su efectividad.

Asimismo, deberán analizar los escenarios de desastre o indisponibilidad del negocio más probable y evaluar la factibilidad de implementar el uso de las plataformas sociales como herramientas que faciliten abordar situaciones de crisis, ya que una mala planeación y utilización de dicho recurso puede derivar en otra fuente de crisis en lugar de ser una solución.

Es imperativo que las empresas comiencen a reflexionar y preguntarse ¿qué tan resiliente es su empresa? y si esta resiliencia les dará certeza para el logro de sus objetivos en su horizonte de riesgos actual.

La Continuidad de Negocios no puede seguir siendo vista como un commodity, un BCM le brindará a las organizaciones la capacidad para salir adelante y responder a las interrupciones con menores costos de recuperación y a su vez, nos generará un impacto directamente en logro de los objetivos de la empresa y el futuro sostenible de la misma.

También nos ayudará a entender, planificar y ejecutar una mejor respuesta ante los retos y riesgos que surjan del constante cambio climático y global, brindándonos así una efectiva resiliencia organizacional.

OTRAS REFERENCIAS

- ALARM (The National Forum for Risk Management in the Public Sector)
- Association of Certified Fraud Examiners (ACFE) – Report to the Nations: http://www.acfe.com/rttn2016.aspx
- Chartered Institute of Internal Auditors. Standards for managing risk Auditors: https://www.iia.org.uk/resources/risk-management/standards-for-managing-risk/
- Código Nacional de Procedimientos Penales de México. http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf
- Código Penal Federal de México. http://www.diputados.gob.mx/LeyesBiblio/pdf/9_260617.pdf
- Documentos Basilea II, Basilea 2.5 y Basilea III - Sitio del Comité de Basilea para la Supervisión Bancaria. http://www.bis.org/bcbs/basel3/compilation.htm
- Enterprise Risk Management - Integrated Framework COSO, (the Committee of Sponsoring Organisations of the Treadway Commission): https://www.coso.org
- European Federation of Risk Management Associations (FERMA)
- Grupo de Acción Financiera de Latinoamérica. http://www.gafilat.org/content/quienes/

- Institute of Risk Management (www.theirm.org)
- ISO 31000 – Risk Management:2009
  https://www.iso.org/iso-31000-risk-management.html
- Kroll Global Fraud & Risk Report.
  http://www.kroll.com/en-us/intelligence-center/reports/global-fraud-risk-report
- OCEG Red Book 3 on Governance, Risk & Compliance (GRC)
  http://www.oceg.org/resources/red-book-3/
- The Association of Insurance and Risk Managers (AIRMIC)

AVISO DE DERECHOS DE AUTOR

*** *** ***