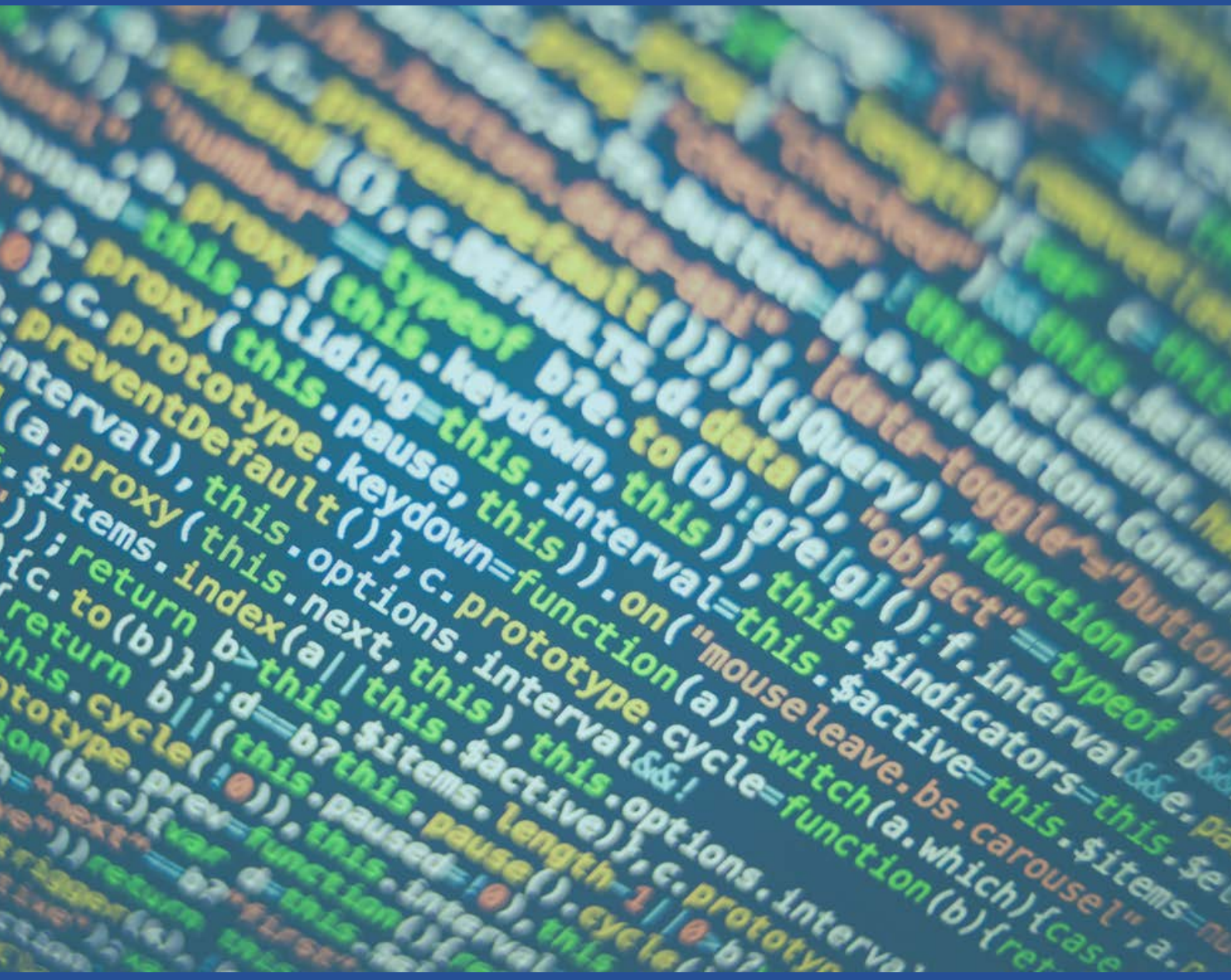
ICC MEXICO

PAUTA

Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio A.C.



ECONOMÍA DIGITAL Y GESTIÓN DE RIESGOS

No. 83
Noviembre 2017

PAUTA 83

Economía Digital y Gestión de Riesgos

No. 83 Noviembre 2017

ICC México PAUTA
Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio, A.C.

Pauta Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio.- Es una publicación de análisis educativo, social, comercial, financiero, económico e internacional, exclusivo para socios del Capítulo Mexicano de la Cámara Internacional de Comercio. Las ideas expuestas por nuestros colaboradores no corresponden necesariamente al pensamiento de ICC México. Su distribución es exclusivamente para socios activos de ICC México.

Título de la publicación: «ICC México PAUTA Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio A.C.»
Editor Responsable: Lic. Rosa Laura Altamirano López
Número de certificado de reserva otorgado por el Instituto Nacional del Derecho de Autor: 04-2016 -122015041500 - 106
Número de Certificado de Licitud de Título: 11518
Número de Certificado de Licitud de Contenido: 8105
Domicilio de la publicación y del distribuidor: Indiana 260 Piso 5 Oficina 508 Colonia Ciudad de los Deportes, C.P. 03810, México D.F.
Teléfonos: (52) 5687 2203, 5687 2207, 5687 2321 5687 2507, 5687 2601.
Renovación de Reserva de Derechos al uso exclusivo
Número 04-2016 -122015041500 -106
Título. ICC MEXICO PAUTA BOLETIN INFORMATIVO DEL CAPITULO MEXICANO DE LA CAMARA INTERNACIONAL DE COMERCIO A.C.
Género: Difusiones Periódicas
Especie: Difusión vía red de computo
web: www.iccmex.mx
e-mail: ygonzalez@iccmex.org.mx; laltamirano@iccmex.org.mx

PAUTA 83

ÍNDICE

1 Ciberseguridad y el factor humano

Manuel Ballester

4 La Corrupción: uno de los mayores riesgos que afrontan las empresas más allá del aspecto regulatorio

Alfredo Hernández

9 La innovación como motor de la economía digital

Sebastián Spósito

14 Las Nuevas Sociedades por Acción Simplificadas

Marcelo Estrada

20 Las Casas de Bolsa y la contratación por medio de firma electrónica

Margarita Ríos-Farjat

40 Tipos de Riesgo y su adecuada gestión

Samuel Rivero Pardo

48 Gestión de Riesgos y oportunidades

Manuel Ballester

52 Guía de ICC México para la Gestión de Riesgos para las Empresas

Carta del Presidente

Estimados socios:

La aceleración de las tecnologías digitales en cada vez más ámbitos de nuestras vidas está cambiando radicalmente el panorama de las empresas, reconfigurando la naturaleza del trabajo y redibujando las fronteras, los riesgos y las responsabilidades de las empresas. Estas tendencias van más allá de la innovación tecnológica.

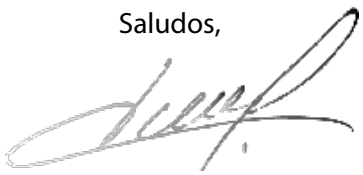
Sin importar el sector o el nivel de desarrollo de las economías, las empresas son las primeras en sentir los efectos de las políticas públicas del área de Tecnologías de Información y Comunicaciones, Internet y flujos de datos. Con las políticas adecuadas en su lugar, los avances tecnológicos y la conectividad digital pueden impulsar la innovación en los modelos de negocio, las redes empresariales globales y la transmisión de conocimiento, mientras que facilitan también el acceso a los mercados internacionales.

Por otra parte, las tecnologías y medios digitales también han traído riesgos un sinnúmero de riesgos para las empresas y estos se tienen que gestionar de una manera integral, junto con los otros tipos de riesgos. Una adecuada administración de riesgos permite a las empresas crear, preservar, generar y sostener su valor. Hoy en día los altos directivos buscan constantemente identificar los riesgos ante los cuales sus organizaciones son más susceptibles para poder evaluarlos y responder estratégicamente ante ellos.

Por esta razón, dedicamos este número de Pauta No. 83 a que nuestros socios compartieran su análisis y reflexión sobre distintos temas de economía digital y gestión de riesgos.

Esperamos que encuentren los artículos de nuestros socios de gran valor e interés para mejorar sus prácticas empresariales y apostarle cada vez más a generar valor a través de plataformas digitales y se protejan de los múltiples riesgos que éstas abren para la seguridad de las empresas. De esta manera, las empresas continuarás siendo una fuente de nuevas oportunidades para el crecimiento y la prosperidad global.

Saludos,



María Fernanda Garza Merodio
Presidente

Ciberseguridad y el factor humano

Manuel Ballester

Doctor Ingeniero Industrial, CISA, CISM, CGEIT, COBIT Trainer, cuenta con 35 años de experiencia en empresas privadas, así como en universidades públicas y privadas en las áreas de informática, seguridad, gobierno de TI, telecomunicaciones y eficiencia energética. Director de la Cátedra de Buen Gobierno y del Postgrado de Buen Gobierno en Universidad de Deusto, ostenta el cargo de Vicepresidente General de la Academia Mexicana de Ciencia de Sistemas y es catedrático en la Universidad Inttelmex, es Socio Director de la firma TEMANOVA en México.

Resumen

El avance de la tecnología conlleva riesgos de seguridad asociados a su uso. La razón principal es porque existen atacantes que buscan sacar provecho sobre las organizaciones y los usuarios. En este contexto, la mayoría de las amenazas a los equipos digitales actuales tiene como propósito generar un beneficio económico.

Introducción

Las organizaciones operan de manera compleja e incierta, debido a los cambios tecnológicos, y con poca comprensión del nivel de conciencia de seguridad de sus sistemas y sin la concienciación y capacitación de los empleados. Los medios de comunicación social, la informática móvil y los servicios en la nube cambiaron la forma de hacer negocios. A medida que las organizaciones aprovechan estas nuevas tecnologías, los sistemas nacen sin la protección adecuada y los riesgos no se mitigan. El factor clave más importante, el humano, suele quedar en el olvido.

Los técnicos avanzados que en un inicio buscaban modificar el comportamiento de los sistemas para que operaran de una manera en la que no habían sido diseñados, con el paso de los años se han transformado en la industria de los ciberdelitos, pasando de hackers entusiastas y curiosos a crackers que buscan lucrarse con sus habilidades. En muchos casos se comenten actos no tipificados en la legislación utilizando las nuevas

tecnologías. Y en caso de que estos actos causen un perjuicio, hacemos referencia a ciberdelincuentes.

La formación de los profesionales de la seguridad juega un papel preponderante en el contexto de la ciberseguridad. Pero al mismo tiempo lo hace la formación de quienes usan los sistemas de información, que deberían tener como base unos principios y valores que determinan el actuar de las personas.

La delgada línea entre lo lícito y lo ilícito

En el panorama actual, la ciberseguridad y la seguridad de la información, así como sus tendencias, nos muestran la necesidad de contar con profesionales muy preparados y actualizados, encargados de proteger los activos más importantes dentro de cualquier tipo de organización y sus usuarios. Pero, según la demanda actual, se detecta una escasez de personal cualificado en un futuro cercano.

Las habilidades técnicas, conocimientos y aptitudes que posean los profesionales de seguridad resultan fundamentales para tal propósito, aunque no se debe dejar de lado la formación que considera también el factor humano.

Una persona que posee los conocimientos suficientes para vulnerar un sistema y acceder a la información privilegiada se encuentra frente a una delgada línea que puede traspasar fácilmente para obtener un beneficio, al tiempo que puede comprometer la seguridad de organizaciones, usuarios y la sociedad. Solamente su formación ética en ciberseguridad le permitiría discernir entre lo que puede ser considerado como lícito e ilícito, y por supuesto, lo que es legal o no.

El famoso caso de Edward Snowden: él era un usuario con permisos para acceder a una gran cantidad de sistemas confidenciales, y ninguna organización es capaz de mantener la confidencialidad si un usuario en el que confía decide violarla. Aunque Edward Snowden tenga un aptitud, conocimientos profesionales, fue la ética la que le impulsó a desvelar la vigilancia a que estaban sometidos varias personalidades.

Debemos considerar otros aspectos, como la personalidad misma. Esta responde a un sinnúmero de estímulos, tanto internos como externos, donde pueden incluirse los intereses, ideologías, creencias, escalas de valores, motivaciones, experiencias, la

formación desde el hogar o la escuela. Por lo tanto, la personalidad se determina a través del carácter (innato) y el temperamento (experiencias y educación) que también es fundamental en el ejercicio profesional.

En el ámbito de las organizaciones, a la hora de seleccionar profesionales, pueden haber personas bien intencionadas y otras no tanto, por lo que a veces la elección se limita a conocer lo mejor posible la voluntad y las intenciones de la persona, y si está realmente interesada en el hacking ético o tendrá siempre un aspecto que puede generar dudas.

Muchos de los que hoy son expertos en seguridad informática, han experimentado y aprendido con el hacking en su juventud y primeros años en el mundo informático, pero en cada caso hay matices que separan, por ejemplo, a quien usó una vez un gusano simple para molestar a sus amigos, de quien desarrolló un malware destructivo, administró una botnet, robó información personal o confidencial o lucró a costa de engañar a otros usuarios. Este es un debate de nunca acabar en este sector profesional de la seguridad informática.

Por lo tanto, una tarea en la que debemos prestar atención y prriorizarla es en la formación de profesionales de seguridad con las habilidades técnicas necesarias para la protección, pero al mismo tiempo con sentido de responsabilidad y ética para el ejercicio de sus actividades.

Moral, ética, leyes y su propósito principal

En un contexto mayor, una condición ideal consistiría en la alineación y concordancia entre la moral, la ética y las leyes que emanan de los distintos países; sin embargo, en ocasiones esto no es posible. Además, estos elementos varían de una sociedad a otra, y cambian con el tiempo.

El fin principal que deberíamos alcanzar dentro del contexto de los responsables de la ciberseguridad y la seguridad de la información es actuar y tomar decisiones sin afectar a otros. Esto determinaría un comportamiento ético y profesional, una tarea sin duda aún pendiente y que significa un gran esfuerzo con implicaciones no solo laborales sino también sociales.

La Corrupción: uno de los mayores riesgos que afrontan las empresas más allá del aspecto regulatorio

Alfredo Hernández Martínez

Socio de Servicios Forenses de PwC México.

Puede enviar sus comentarios al correo:
alfredo.hernandez@mx.pwc.com

Sin duda, los delitos económicos relacionados con un evento específico, como la malversación de activos, pueden causar pérdidas importantes a las organizaciones. Sin embargo, los delitos de tipo sistémico, como la corrupción y el soborno, son los que más daño causan debido a que erosionan las estructuras más básicas de las sociedades y de sus instituciones, mientras que en las empresas degradan la integridad de los empleados y debilitan las estructuras de control interno, aumentando así el riesgo de pérdidas económicas, multas y daños reputacionales, entre otros efectos negativos.

En el caso particular de México, diversas encuestas especializadas señalan al país como una nación de alto riesgo en esta materia. El Índice de Percepción de la Corrupción de Transparencia Internacional 2016 ubica a México en el puesto 123 del ranking, con una puntuación de 30 sobre 100, siendo "cero" una situación extremadamente preocupante y "100" la ideal.

Por otro lado, diversas encuestas realizadas por PwC en este ámbito arrojan resultados poco alentadores sobre la percepción del ambiente de corrupción en el ámbito local. Tal es el caso del Suplemento México de la Encuesta de Delitos Económicos 2016, en el que se destaca que una de cada cinco organizaciones mexicanas fue víctima de este delito en los últimos dos años. Además, el 90% de los directores generales encuestados, considera que la corrupción y el soborno son las principales amenazas para su negocio, según datos de la 7ª Encuesta de CEO en México de PwC.

Más aún, un estudio efectuado por PwC sobre los casos sancionados por la ley de Estados Unidos contra Prácticas Corruptas en el Extranjero (FCPA, por sus siglas en inglés), aplicables a transacciones originadas en Latinoamérica de 2000 a 2016, muestra que México estuvo a la cabeza en casos sancionados,

evidenciando el porqué es considerado un país de muy alto riesgo en temas de corrupción.

Lo anterior son sólo algunos factores que están concienciando a las empresas mexicanas sobre la importancia del combate a la corrupción, y sobre el rol estratégico que debe darse a los programas de cumplimiento anticorrupción, por lo que las empresas están diseñándolos e implementándolos con diferentes enfoques y objetivos.

Los programas de cumplimiento anticorrupción bajo el nuevo marco legal en México

Un enfoque básico es contar con un programa de cumplimiento que cubra los requerimientos mínimos indispensables que marca la ley en México para utilizarlo como medio de defensa ante posibles actos de corrupción que enfrenten las empresas. En este sentido, vale la pena destacar que en mayo de 2015 se emitieron las reformas constitucionales que crearon el Sistema Nacional Anticorrupción (SNA), y en julio de 2016 se promulgaron y reformaron diversas leyes para la prevención y combate a la corrupción, entre las que se encuentra la nueva Ley General de Responsabilidades Administrativas (LGRA) que establece, entre otras disposiciones, las responsabilidades y obligaciones de los servidores públicos, así como las faltas administrativas graves y las sanciones para servidores públicos y particulares.

Los actos que sancionan la LGRA incluyen: i) el soborno a servidores públicos; ii) la participación ilícita en actos administrativos; iii) el tráfico de influencias; iv) la utilización de información falsa en procedimientos administrativos; v) la obstrucción de investigaciones relacionadas a faltas administrativas; vi) la colusión en contrataciones públicas; vii) el uso indebido de recursos públicos, viii) la contratación indebida de ex servidores públicos.

Es importante destacar que la LGRA no sólo establece sanciones sobre los actos descritos, sino que también dicha ley valorará si las personas morales cuentan con una "Política de Integridad" para la determinación de su responsabilidad en actos de corrupción. Es decir, la Política de Integridad representa los requerimientos mínimos indispensables que se evaluarán sobre los programas de cumplimiento anticorrupción establecidos por las personas morales para, en su caso, considerarlos como atenuantes en la responsabilidad de las mismas.

La Política de Integridad requiere que se cuente con, al menos, los siguientes elementos preventivos para actos de corrupción: i) manual de organización y procedimientos que delimiten las funciones y responsabilidades de cada área, cadena de mando y liderazgo; ii) código de conducta debidamente publicado e informado al personal; iii) sistemas adecuados y eficaces de control, monitoreo y auditoría sobre el cumplimiento de los estándares de integridad en toda la organización, iv) sistemas adecuados de denuncia, tanto al interior de la organización como hacia las autoridades competentes, así como procesos disciplinarios y consecuencias concretas respecto de quienes actúen en forma contraria a las normas internas o a la legislación mexicana; v) sistemas adecuados de entrenamiento y capacitación; vi) políticas de recursos humanos que eviten la incorporación de personas que puedan generar un riesgo a la integridad de la corporación, y vi) mecanismos que aseguren la transparencia y publicidad de sus intereses.

Un programa de cumplimiento que cubra adecuadamente los aspectos descritos puede servir como medio de defensa bajo el nuevo marco legal mexicano; sin embargo, es importante preguntarse si estos componentes pueden ser suficientes para también satisfacer las necesidades de otros actores con quienes las empresas interactúan, como socios de negocios actuales o potenciales, proveedores de financiamiento, y otros. Lo anterior implica que las organizaciones deberán de definir el objetivo, propósito y bases para establecer un programa de cumplimiento, incluyendo la adopción de mejores prácticas internacionales que vayan más allá de lo requerido por la regulación local.

Los programas de cumplimiento bajo mejores prácticas, y como medio para aumentar la ventaja competitiva de las empresas

Ante el panorama actual y los crecientes esfuerzos globales por combatir la corrupción, no es suficiente cumplir la regulación, lo ideal es adoptar estrategias más robustas que ayuden a prevenir este delito, lo cual también es de gran valor en las interacciones que efectúan las empresas con terceros que pueden tener muy diversos intereses, más allá de las leyes locales. Este es el ejemplo de las empresas que tienen como socios de negocios a otras corporaciones internacionales, que pueden estar sujetas a leyes y marcos anticorrupción más estrictos que los que actualmente tenemos en el país.

Debido en parte a lo anterior, y antes de la entrada en vigor del SNA, en 2015, y las disposiciones secundarias de 2016, pocas empresas mexicanas, y más extranjeras con operaciones en México, habían ya adoptado programas de

cumplimiento anticorrupción con base en estándares internacionales, incluyendo la FCPA y la Ley Antisoborno del Reino Unido (UK *"Bribery Act"*).

Es por esto que contar con programas de cumplimiento efectivos cobra aún mayor relevancia en México, en donde el riesgo de corrupción es muy alto y se encuentra latente en todos los sectores de la economía, situación que requiere a las empresas extranjeras a tomar las precauciones necesarias al hacer negocios en nuestro país.

Para la construcción de un programa de cumplimiento efectivo, las organizaciones deben conocer las tendencias y esquemas de corrupción en el país, su industria y su ámbito específico de operaciones, para desarrollar e instaurar los controles adecuados que mitiguen los riesgos de este tipo, como pueden ser: los pagos directos, o más aún, indirectos a través de socios comerciales o agentes, los regalos, donativos, hospitalidad u otros beneficios o dádivas con propósitos indebidos, entre otros. Un punto central de los programas anticorrupción es establecer mecanismos robustos de monitoreo enfocados en cada área de riesgo, siendo una de las más importantes, la evaluación y monitoreo de terceros, desde una perspectiva de integridad. Cabe mencionar que una gran parte de los esquemas de corrupción, el 67%, involucra pagos a través de terceros, según la publicación de PwC *"Mexico Energy Reform – How to Mitigate Corruption Risks in Mexico"*.

Estos programas se deben diseñar a la medida de cada empresa, pero de manera general consideran puntos como: el compromiso de la alta dirección contra la corrupción, evaluación de riesgos, programas de gestión de relaciones con terceros, sistemas de denuncia, investigación y sanciones, entre otros.

En definitiva, el mensaje debe comenzar por los niveles más altos de las organizaciones y llegar a toda la organización y terceros involucrados. Fomentar comportamientos éticos y ser congruente con las acciones, estar alineado y enfocado a riesgos y contar con los recursos necesarios, así como poseer las herramientas y procesos de detección y prevención, son algunos puntos clave de un programa efectivo. Adicionalmente, es recomendable establecer funciones y roles claros para diseñar, implementar, monitorear y hacer que se cumpla el programa, incluyendo su difusión y alineación con la estrategia y compromiso en la organización.

Sin duda alguna, México ha dado un paso importante hacia una etapa de autorregulación de las empresas. Aquellas organizaciones que adopten y fortalezcan sus programas de cumplimiento anticorrupción como parte de su estrategia de negocios, con base en las mejores prácticas internacionales más

estrictas, y más allá de los requerimientos regulatorios, habrán de posicionarse con una mayor ventaja competitiva en los sectores en que operen.

La innovación como motor de la economía digital

Sebastián Spósito

Analista Senior en el equipo de Políticas Públicas y Relaciones con el Gobierno de Google en México. Nacido en Buenos Aires, Argentina, graduado como Licenciado en Economía y en Ciencia Política por la Universidad de Buenos Aires, se mudó a México para sumarse al equipo de Políticas Públicas hace dos años.

El desarrollo tecnológico de estos tiempos derrama en todas las facetas de nuestra vida. Hoy por hoy pensar la idea de economía digital como una subespecie de la economía comienza a tener un sutil dejo de anacronismo. Desde la postal de una persona usando su correo electrónico a la omnipresencia de "la nube", todo indica que el diálogo entre nuestras actividades cotidianas y el mundo digital es el signo de nuestros tiempos.

Palabras como creatividad e innovación comienzan a estar a la orden del día en sectores otrora impensados. La idea de empoderamiento condensa el inédito poder transformador que la revolución digital pone en manos de las personas. Internet, y la tecnología en general, son herramientas que nos permiten llevar adelante nuestros proyectos, materializar nuestras ideas. Sin embargo, como tales, requieren de la destreza de quienes las usan y de un escenario que contenga y potencie esa interacción para liberar su potencial innovador ¿Cómo podemos poner estas herramientas al servicio del crecimiento y el desarrollo?

En primer lugar cabe una reflexión acerca de la idea de innovación. Lo primero que se viene a la mente ante este concepto es la idea de lo novedoso, de lo que nadie hizo antes. Esto sin duda condensa en parte el significado del término, pero dista de abarcar su verdadero potencial transformador, el cual se complementa con la idea de disrupción. Esta idea apunta al quiebre de una continuidad, de una expectativa, en nombre de una manera más eficiente de hacer las cosas. Innovar es, desde esta óptica, la capacidad de aportar ideas novedosas a problemas tradicionales. El poder de transformar el potencial de las herramientas digitales a mano en soluciones tangibles y cotidianas. La innovación es la savia de la economía digital, mas no se puede forzar. Sin embargo, se puede crear un ambiente en el que se permita y se fomente. ¿Qué necesitamos para lograrlo?

Un aspecto fundamental es disminuir la brecha digital. La misma refiere a las diferentes condiciones de acceso a Internet que un grupo puede tener en comparación a otro, como así también a la diferencia en las capacidades de utilización eficaz de tecnologías de información y comunicación por parte de un grupo frente a otro. En su primera acepción, la fórmula para moderarla emana de su propia definición: aumentando la conectividad y condiciones de acceso lograremos mejorar el escenario general. Ahora bien, es la segunda de sus acepciones la que no presenta soluciones de un efecto tan inmediato y se presta a un mayor diálogo con un entorno a priori no necesariamente digital como es la educación. Cerrar esta brecha digital a través de dotar al grueso de la población de las habilidades básicas para poder hacer un uso eficaz y eficiente de las tecnologías disponibles es sin dudas un imperativo ineludible en los tiempos que corren, pero el cierre de esta idea de brecha no es más que acercarse a un punto de partida. Hoy por hoy pensar a la educación por fuera del mundo digital no es solamente un despropósito, sino un gran obstáculo. La tecnología es el prisma a través del cual todos, y sobre todo las generaciones más jóvenes, interactúan con el mundo que los rodea. Es en la sinergia entre la educación y el aprovechamiento de las tecnologías disponibles donde radica el potencial de conocimiento y desarrollo inédito de nuestra era.

Otro pilar central de este ambiente innovador es el marco normativo. Los mayores polos de innovación se encuentran en los países que sostienen la idea de "permissionless innovation" (innovación sin pedir permiso), la cual impulsa que la experimentación con las nuevas tecnologías y modelos de negocio pueda fluir libremente sin ser sometida a trabas, como pueden ser permisos o autorizaciones previas, a menos que existan razones serias para justificarlas. Este tipo de escenarios han permitido desarrollos inéditos hasta el momento, nutridos del emprendedorismo y la iniciativa privada enmarcada en un escenario de competencia global. Este tipo de políticas se nutren de las posibilidades que Internet abre en tanto canal de comunicación e interacción, como así también se hace eco de la ubicuidad y la naturaleza de este.

Un marco normativo que busque apalancarse en esta dinámica debe habilitar el libre flujo transfronterizo de datos, el pilar fundamental de la economía digital, reconociendo que es en ese fluir donde se condensa la nueva dinámica de mercado inherente a la economía misma. Este flujo debe darse de manera informada para los usuarios y con medidas de seguridad que generen confianza. Esta idea de la confianza es crucial dado que es otro de los pilares de la economía digital, en particular en lo que hace al comercio en línea. Desde esta óptica también es crucial evitar los requerimientos de localización forzada de datos, los cuales no solo contravienen la naturaleza misma de Internet sino que coartan la

posibilidad de acceder libremente y de manera competitiva a servicios, soluciones y herramientas que se desprenden de y eficientizan con la utilización de "la nube", desde la analítica de datos hasta el aprendizaje computarizado. Esto a su vez genera un aumento considerable en los costos y atenta muchas veces contra la sustentabilidad misma de emprendimientos que solo asoman sustentables bajo la dinámica de apertura que ha sabido cobijar el gran desarrollo de la economía digital de estos últimos años. Otro aspecto importante de un escenario con libertad para la innovación es la capacidad de garantizar esquemas de certeza jurídica para las plataformas de servicio en línea, condición necesaria para que las mismas puedan operar como plataformas abiertas para el comercio y la comunicación, particularmente en el caso de nuevos emprendimientos.

A la luz de esto, queda claro que el aporte esencialmente multifacético de Internet a la economía es difícil de medir en su totalidad aunque está a la vista de todos. La economía digital va mucho más allá de las empresas de Internet. Internet empodera a usuarios, a pequeñas y medianas empresas (PyMEs), y a nuevos emprendedores. En esta economía, las plataformas de internet juegan un rol habilitador, permitiendo a aquellos que deciden adoptar las herramientas a disposición en el mundo en línea generar nuevos emprendimientos, llegar a nuevos mercados y aumentar su productividad. Las plataformas digitales proveen a cualquier empresa, de manera accesible, de herramientas de diseño, desarrollo y distribución de productos y servicios a escala mundial a un costo mucho menor del que podía esperarse hace solamente una década. Los individuos y las empresas crecen y se desarrollan en el mercado mundial gracias a la oferta de herramientas de relacionamiento y networking de fácil implementación y costo-efectivas.

En este contexto, las pymes, potenciales micro-multinacionales, tienen la posibilidad de operar a nivel global de manera eficiente y económica y así escalar rápidamente. Este concepto de micro-multinacional viene a desterrar la idea de que para operar en muchos países a la vez es necesaria una gran estructura y planta. Internet ofrece herramientas para la exportación que permiten a los negocios volverse globales sin importar su origen o tamaño. Esta situación representa una oportunidad de desarrollo muy particular en el caso de Latinoamérica y el mundo hispano-parlante. Con más de 400 millones de personas que tienen el español como lengua nativa, y más de 280 millones de ellos conectados a internet en la actualidad, el idioma deviene un denominador común con un potencial de explotación inédita gracias a las nuevas tecnologías, más aún considerando que América Latina todavía tiene un gran camino por recorrer en materia de penetración de internet, a lo que se suma España e incluso la comunidad hispana de los Estados Unidos.

Sumados a los aspectos normativos y de cierre de la brecha digital, la consolidación de un ámbito innovador requiere del afianzamiento de una cultura emprendedora y creativa en línea con las dinámicas de la economía digital. Ésta debe ser abierta, transparente e inclusiva, promover un enfoque pragmático, es decir, de resolución de problemas, y fomentar el pensamiento crítico como así también desterrar la idea de que el fracaso es algo intrínsecamente negativo. Esta desfetichización del fracaso es uno de los pilares fundamentales de la nueva cultura emprendedora de la innovación. El riesgo es un ingrediente irremplazable en la búsqueda de soluciones novedosas, por lo que, siendo la posibilidad del fracaso una parte integral del mismo, no debería verse como algo malo sino, muy por el contrario, como una experiencia necesaria y formativa de cara a un objetivo. Estos valores deberían insertarse en la currícula de las escuelas y universidades para poder capitalizar de la mejor manera el gran manejo de las herramientas que ya de por si tienen las generaciones más jóvenes. La denominada generación Z, los nativos digitales, es global, social, visual y tecnológica y en tanto tal, aprende de otra manera. Es crucial que los valores de la innovación y el emprendedorismo sean parte de ese nuevo paradigma educativo de cara al fortalecimiento de la economía.

Las mejores ideas surgen cuando a las personas se les da la libertad de crear, de ser originales, de caer y volver a levantarse. Es momento de capitalizar la unión entre el mundialmente reconocido talento latinoamericano y las herramientas digitales a mano. El aprovechamiento de esta oportunidad que la economía digital representa para América Latina depende de nuestra capacidad de constituir un escenario económico, político, social y cultural alineado con los valores de la innovación, la creatividad y la competencia.

Las Nuevas Sociedades por Acción Simplificadas

Marcelo Alejandro Estrada Navarro

Licenciado en Derecho y Ciencias Sociales, Corredor Público 31 del Estado de Nuevo León, Especialista en Valuación de Bienes Muebles e Inmuebles, Perito Valuador y Perito Traductor del Tribunal Superior de Justicia de Nuevo León y Tribunal Federal de Justicia Administrativa, Miembro del Colegio de Corredores Públicos de Nuevo León.

Resumen

A partir de septiembre de 2016 entraron en vigor reformas en la Ley General de Sociedades Mercantiles relacionadas con las especies de sociedades mercantiles que reconoce agregando un nuevo tipo de sociedad mercantil que se denomina Sociedad por Acciones Simplificada o SAS por su abreviatura. Las SAS son de creación gratuita a través de Internet y se pueden crear desde un solo socio.

¿Qué son las SAS?

A partir del mes de septiembre de 2016 entraron en vigor importantes reformas en la Ley General de Sociedades Mercantiles relacionadas con las especies de sociedades mercantiles que reconoce dicha ley en su artículo primero. Con esta reforma se agrega un nuevo tipo de sociedad mercantil en la fracción séptima del artículo primero de la mencionada ley que se denomina Sociedad por Acciones Simplificada o SAS por su abreviatura. [1]

Este nuevo tipo social se encuentra establecido y regulado en el Capítulo XIV de la Ley General de Sociedades Mercantiles del artículo 260 al 273.[2]

La Ley General de Sociedades Mercantiles las define como "Artículo 260.- La sociedad por acciones simplificada es aquella que se constituye con una o más personas físicas que solamente están obligadas al pago de sus aportaciones representadas en acciones. En ningún caso las personas físicas podrán ser simultáneamente accionistas de otro tipo de sociedad mercantil a que se refieren las fracciones I a VII, del artículo 1o. de esta Ley, si su participación en dichas sociedades mercantiles les permite tener el control de la sociedad o de su administración, en términos del artículo 2, fracción III de la Ley del Mercado de Valores." [3]

Del análisis del Artículo 262 de la Ley General de Sociedades Mercantiles podemos conocer los requisitos para la constitución de una sociedad por acciones simplificada que son los siguientes: I. Que haya uno o más accionistas personas físicas solamente; II. Que el o los accionistas externen su consentimiento para constituir una sociedad por acciones simplificada bajo los estatutos sociales que la Secretaría de Economía ponga a disposición mediante el sistema electrónico de constitución; III. Que alguno de los accionistas cuente con la autorización para el uso de denominación emitida por la Secretaría de Economía, y IV. Que todos los accionistas cuenten con certificado de firma electrónica avanzada (FIEL) vigente emitida por el SAT. En ningún caso se exigirá el requisito de escritura pública, póliza o cualquier otra formalidad adicional, para la constitución de la sociedad por acciones simplificada. [4]

Como principales características podemos mencionar las siguientes: Es una sociedad creada en línea, puede crearse desde un solo socio, contempla una administración sencilla, sin capital mínimo y protege el patrimonio personal del socio.

Este tipo de sociedades tienen sus orígenes en Colombia y México tomando ese modelo lo implementó en nuestra legislación mercantil Mexicana. A mi parecer fue muy acertado el legislador con la creación de este nuevo tipo social debido a que mi experiencia como Corredor Público me ha enseñado que ciertas sociedades mercantiles que se crean en el país son sociedades unipersonales que por fuerza y debido a la obligatoriedad de un mínimo de dos socios que establece el artículo 89 fracción primera de la Ley General de Sociedades Mercantiles tienen a otro socio como invitado con una participación mínima solo por cumplir con el requisito. Sobra decir que este socio mayoritario es quien tiene la administración única y todas las facultades para administrar, manejar y obligar a la sociedad. En pocas palabras, es una sociedad de un solo socio real y un invitado que no aporta ni realiza actividad alguna más que firmar el acta constitutiva e identificarse ante el fedatario público que la constituye.

Ahora con esta reforma y la creación de las nuevas Sociedades por Acciones Simplificadas ya es posible llevar a la realidad las sociedades como anteriormente se creaban sin la necesidad de simular una sociedad de dos personas. Ahora, desde la comodidad de su casa u oficina todos los emprendedores que deseen crear una persona moral lo pueden hacer mediante las Sociedades por Acciones Simplificadas. Solo necesitan su firma electrónica expedida por el SAT, conexión a Internet y su PC.

Para crear una SAS es necesario ingresar a una nueva plataforma electrónica a cargo de la Secretaría de Economía Federal ubicada en el dominio www.gob.mx/tuempresa en la cual podrán ingresar como ciudadano para solicitar

primero la autorización del nombre de la nueva sociedad. Una vez autorizado el nombre el usuario podrán proceder a completar todos los puntos importantes que se deben de incluir en los estatutos que ya vienen cargados en el sistema como lo son: Denominación; nombre de los accionistas; domicilio de los accionistas; Registro Federal de Contribuyentes de los accionistas; correo electrónico de cada uno de los accionistas; domicilio de la sociedad; duración de la sociedad; la forma y términos en que los accionistas se obliguen a suscribir y pagar sus acciones; el número, valor nominal y naturaleza de las acciones en que se divide el capital social; el número de votos que tendrá cada uno de los accionistas en virtud de sus acciones; el objeto de la sociedad, y la forma de administración de la sociedad. Una vez que el socio único o los socios en caso de haber más de uno estén de acuerdo en el contenido de los estatutos los mismos procederán a firmarlos mediante su firma electrónica. [5]

Al finalizar el proceso el usuario obtendrá los estatutos de la sociedad, la boleta de inscripción de la sociedad ante el Registro Público de Comercio, Registro Federal de Causantes de la sociedad y próximamente la firma electrónica de la SAS y el alta patronal ante el IMSS de la persona moral creada. [6]

Cabe hacer mención que todos los documentos de la SAS creada expedidos por el sistema vienen firmados electrónicamente por la autoridad por lo que son totalmente válidos ante cualquier autoridad o entidad privada. Tan es así que el artículo 262 en su último párrafo establece que "En ningún caso se exigirá el requisito de escritura pública, póliza o cualquier otra formalidad adicional, para la constitución de la sociedad por acciones simplificada." [7] Desafortunadamente en la práctica es común ver batallar a los emprendedores que una vez creada su SAS desean aperturar una cuenta bancaria se topan con criterios absurdos en ciertas instituciones de crédito en las que les llegan a solicitar que vengan sellos de Corredor Público o Notario Público para aceptar los documentos o en el peor de los casos negar completamente el servicio debido a que la institución bancaria desconoce o no confía en este nuevo tipo de sociedades mercantiles. Todas estas situaciones son bastante lamentables ya que desvirtúan la naturaleza de estas sociedades en pro de la creación e inicio de operaciones rápidas de empresas.

Obligaciones y responsabilidades de las SAS

Los ingresos totales anuales de una sociedad por acciones simplificada no podrán rebasar de 5 millones de pesos. En caso de rebasar el monto respectivo, la sociedad por acciones simplificada deberá transformarse en otro régimen societario contemplado en la Ley General de Sociedades Mercantiles como la

Sociedad Anónima. En caso que el o los accionistas no lleven a cabo la transformación de la sociedad responderán frente a terceros, subsidiaria, solidaria e ilimitadamente, sin perjuicio de cualquier otra responsabilidad en que hubieren incurrido. [8]

La Asamblea de Accionistas será convocada por el administrador de la sociedad, mediante la publicación de un aviso en el sistema electrónico establecido por la Secretaría de Economía denominado PSM con una antelación mínima de cinco días hábiles. En la convocatoria se insertará el orden del día con los asuntos que se someterán a consideración de la Asamblea de Accionistas, así como los documentos que correspondan. [9]

Obligaciones y responsabilidades de los accionistas

Las obligaciones y responsabilidades que tienen los accionistas que forman parte de una SAS consisten en que el o los accionistas son subsidiaria o solidariamente responsables, según corresponda, con la sociedad, por la comisión de conductas sancionadas como delitos. En pocas palabras, tratándose de materia penal la responsabilidad de los accionistas va más allá de la obligación de los accionistas del pago de sus aportaciones como el caso de la materia mercantil.

Los accionistas que soliciten la constitución de una sociedad por acciones simplificada serán también responsables de la existencia y veracidad de la información proporcionada en el sistema de la Secretaría de Economía donde se crean. De lo contrario responden por los daños y perjuicios que se pudieran originar, sin perjuicio de las sanciones administrativas o penales a que hubiere lugar. [10]

Al momento de crear la sociedad por acciones simplificada el sistema de la Secretaría de Economía proporciona la opción a los accionistas de pagar las acciones en el momento o posteriormente a su constitución. Las acciones deberán pagarse dentro del término máximo de un año contado desde la fecha en que la sociedad quede inscrita en el Registro Público de Comercio. Cuando se haya suscrito y pagado la totalidad del capital social, la sociedad deberá publicar un aviso en el sistema electrónico establecido por la Secretaría de Economía PSM. [11]

Los contratos celebrados entre el accionista único y la sociedad deberán inscribirse por la sociedad en el sistema electrónico establecido por la Secretaría de Economía PSM conforme a lo dispuesto en el artículo 50 Bis del Código de Comercio que indica "Las publicaciones que deban realizarse conforme a las leyes mercantiles se realizarán a través del sistema electrónico que para tal propósito establezca la Secretaría de Economía, y surtirán efectos a partir del día siguiente de su publicación." [12] El portal creado es el Portal de Sociedades Mercantiles

conocido como el PSM y se localiza en el sitio https://psm.economia.gob.mx/PSM en el cual se pueden hacer las publicaciones de los contratos celebrados entre el accionista único y la sociedad como puede ser el caso de otorgamiento en arrendamiento de un local comercial propiedad del accionista que lo da en arrendamiento a su propia sociedad por acciones simplificada, por dar un ejemplo. [13]

Restricciones SAS

En ningún caso las personas físicas podrán ser simultáneamente accionistas de otro tipo de sociedad mercantil a que se refieren las fracciones I a VII, del artículo 1o. de la Ley General de Sociedades Mercantiles cito "I.- Sociedad en nombre colectivo; II.- Sociedad en comandita simple; III.- Sociedad de responsabilidad limitada; IV.- Sociedad anónima; V. Sociedad en comandita por acciones; VI. Sociedad cooperativa, y VII. Sociedad por acciones simplificada"[14], si su participación en dichas sociedades mercantiles les permite tener el control de la sociedad o de su administración, en términos del artículo 2, fracción III de la Ley del Mercado de Valores que dice "Control, la capacidad de una persona o grupo de personas, de llevar a cabo cualquiera de los actos siguientes: a) Imponer, directa o indirectamente, decisiones en las asambleas generales de accionistas, de socios u órganos equivalentes, o nombrar o destituir a la mayoría de los consejeros, administradores o sus equivalentes, de una persona moral. b) Mantener la titularidad de derechos que permitan, directa o indirectamente, ejercer el voto respecto de más del cincuenta por ciento del capital social de una persona moral. c) Dirigir, directa o indirectamente, la administración, la estrategia o las principales políticas de una persona moral, ya sea a través de la propiedad de valores, por contrato o de cualquier otra forma." [15]

Además, los ingresos totales anuales de una sociedad por acciones simplificada no podrán rebasar de 5 millones de pesos. En caso de rebasar el monto respectivo, la sociedad por acciones simplificada deberá transformarse en otro régimen societario contemplado en la Ley General de Sociedades Mercantiles, en los términos en que se establezcan la misma Ley. El monto establecido en este párrafo se actualizará anualmente el primero de enero de cada año, considerando el factor de actualización correspondiente al periodo comprendido desde el mes de diciembre del penúltimo año hasta el mes de diciembre inmediato anterior a aquel por el que se efectúa la actualización, misma que se obtendrá de conformidad con lo establecido en el Código Fiscal de la Federación. La Secretaría

de Economía publicará el factor de actualización en el Diario Oficial de la Federación durante el mes de diciembre de cada año. [16]

Las SAS en números

Conforme a las última actualizaciones que nos otorgó la Secretaría de Economía Federal tenemos la siguiente información: El promedio de crecimiento mensual de las Sociedades por Acciones Simplificadas es del 146%; de octubre de 2016 hasta la primer quincena de octubre de 2017 se han creado 7,342 Sociedades por Acciones Simplificadas, de las cuales el 76% tienen un solo socio; en todas las Sociedades por Acciones Simplificadas creadas participan 10,913 socios de los cuales el 75% son hombres y el 25% mujeres; el promedio de constitución de una Sociedades por Acciones Simplificadas es de una hora con veintitrés minutos; y cada 50 minutos nace una Sociedad por Acciones Simplificada las 24 horas del día los 365 días de año. [17]

Con esta estadística podemos inferir que esta nueva especie de sociedad mercantil definitivamente está siendo aceptada por todos los emprendedores en México y se está logrando que los emprendedores que actualmente desarrollan sus actividades comerciales como personas físicas den el gran salto a pasar a constituirse como persona moral gracias a las bondades y facilidades que otorga la figura de las Sociedades por Acciones Simplificadas.

NOTAS BIBLIOGRÁFICAS

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14] Ley General de Sociedades Mercantiles - México, Cámara de Diputados. Diario Oficial de la Federación del 14-03-2016.

[11] Reglas de carácter General para el funcionamiento y operación del Sistema Electrónico de Sociedades por Acciones Simplificadas - México, Secretaría de Economía. Diario Oficial de la Federación del 14-09-2016.

[12] Código de Comercio - México, Cámara de Diputados. Diario Oficial de la Federación del 02-05-2017.

[15] Ley del Mercado de Valores- México, Cámara de Diputados. Diario Oficial de la Federación del 10-01-2014.

[16] Secretaría de Economía. Sesión "Sistema Electrónico de Sociedades por Acciones Simplificadas" 27-10-2017 Ciudad de México.

Las Casas de Bolsa y la contratación por medio de firma electrónica

Margarita Ríos-Farjat

Abogada en Nuevo Léon, con estudios avalados por el Consejo de la Judicatura Federal, una maestría en derecho fiscal y doctorado en política pública. Profesora de la Facultad Libre de Derecho de Monterrey, columnista de El Norte e integrante de la Coalición Anticorrupción (Nuevo León). Abogada externa de Vector Casa de Bolsa, S.A. de C.V., para este y otros temas.

Resumen

Hay pequeñas grandes cosas que podrán hacerse para lograr el crecimiento del sector bursátil. La adopción de una firma electrónica avanzada para celebrar contratos de intermediación con personas que estén geográficamente lejos de las casas de bolsa, por ejemplo. Crecería el sector y crecería la cultura financiera. Pero la normatividad resulta tan confusa que constituye el primer obstáculo.

Introducción

Una narrativa a grandes rasgos diría que la firma electrónica evolucionó a la firma electrónica *avanzada* (también conocida como "Fiel"), que ha sido el instrumento de seguridad diseñado para identificar de manera única y segura a cada contribuyente ante las instancias recaudatorias. Después surgió la firma electrónica certificada del Poder Judicial de la Federación (conocida como "Firel"), que permite a su titular promover juicios de amparo, consultar expedientes electrónicos y recibir notificaciones a través del Portal de Servicios en Línea de dicho Poder. Otras dependencias públicas también desarrollaron sus propias firmas tomando como base la "fiel", y ésta siguió desarrollándose con más elementos de seguridad hasta llegar a la "E.Firma", que es ahora la requerida por el Servicio de Administración Tributaria (SAT). Sobre ésta, en la página de internet del SAT se lee que, por sus características, es segura y garantiza la identidad, porque *"la información es incorporada y protegida en las bases de datos del SAT, a fin de darle*

seguridad a tus trámites fiscales y evitar que otra persona suplante tu identidad e intente realizar algún fraude fiscal". La evolución tecnológica continúa y ahora incluso se cuenta con la "E.Firma Portable" para dispositivos móviles.

La tendencia es clara, y las casas de bolsa podrían beneficiarse de esa herramienta para ampliar su base de clientes porque tradicionalmente las contrataciones de servicios bursátiles son presenciales, requiriéndose firma autógrafa y entrevista personal. Podríamos decir entonces que la geografía se convierte en una gran limitante para ampliar el potencial de este tipo de inversiones financieras. Esta limitante no solo afecta a las casas de bolsa sino también a los mexicanos en general porque estos no logran su inclusión financiera[1] a una mayor variedad de servicios (como los bursátiles). Por cierto, en un reporte de 2015, el Instituto Mexicano de la Competitividad (IMCO) identificó como una de las brechas de acceso que impiden la inclusión financiera de los mexicanos el hecho de que seis de cada diez cuentas de casas de bolsa están solo en tres lugares: Ciudad de México, Monterrey y Guadalajara, y ello coincide con el domicilio de las propias casas de bolsa[2].

Si bien este nexo entre inclusión financiera y firma electrónica no es directo porque depende también de otras variables (como la capacidad de ahorro de los clientes, su cultura en finanzas y sus deseos de invertir a largo plazo), las casas de bolsa podrían diseñar estrategias de promoción y de educación financiera sin el freno que les representan la geografía o la presencia física, creándose entonces una especie de espiral de crecimiento, donde el sector bursátil amplía su base de clientes, aumenta entonces el interés por sus servicios y llegan así más clientes, crece la cultura financiera y así sucesivamente, lográndose contar con las casas de bolsa como entidades importantes para esta inclusión.

Las casas de bolsa pertenecen al sector financiero, que está especialmente regulado por ser muy sensible a cierto tipo de delitos, y la contratación directa o presencial ha sido uno de los mecanismos para salvaguardar la seguridad de las transacciones. Esto explica por qué "llegan tarde" al beneficio generalizado que presuponen las firmas electrónicas. Sin embargo, la tendencia del propio gobierno es ampliar el uso de la firma electrónica en todos los rubros, y esto no es una apreciación subjetiva sino una declaración contenida en el documento que contiene diversas iniciativas de reforma en materia fiscal

para 2017: "*Reconociendo la eficiencia que ha tenido esta herramienta tecnológica en los últimos años, se han impulsado reformas con la finalidad de que la firma electrónica avanzada se utilice no solo en el cumplimiento de obligaciones fiscales, sino también para la realización de determinados trámites ante las entidades públicas*"[3]. Esta iniciativa devino en una reforma al artículo 17-F del Código Fiscal de la Federación (CFF) que se menciona más adelante.

La normatividad del sector bursátil ha empezado a revisarse a la luz de todo lo anterior. Si bien algunas provisiones parecen claras, la estricta regulación del ramo requiere un entramado legal sin lugar a dudas porque de lo contrario se genera una comprensible incertidumbre jurídica que impide a las casas de bolsa atreverse a utilizar la firma electrónica como un mecanismo para celebrar contratos a distancia. Es cierto que el sector bursátil utiliza con normalidad los medios electrónicos de intercambio de datos, el punto en cuestión es que ello sucede *una vez celebrado* el contrato inicial, y por eso se plantea la posibilidad de que se celebre a través de firma electrónica pues ello permitiría ampliar la base de usuarios de este tipo de servicios aprovechando el espacio virtual.

Este artículo se ocupa precisamente de este tema. Para ello, primero se revisa el marco jurídico general de esas contrataciones, después se analiza la modificación regulatoria que permite el uso de la firma electrónica y las confusiones que esa modificación provoca, finalmente se refiere el otro obstáculo para la celebración a distancia de los contratos, proponiéndose algunas soluciones al respecto. El artículo surgió de forma natural al estar asesorando a una casa de bolsa cuyo interés en la inclusión financiera en general y en este tema en particular nos permitió encontrar inquietudes similares en otras casas de bolsa y asociaciones financieras.

Cabe aclarar que este artículo solo pretende aportar elementos de análisis y hacer un llamado a fortalecer la certidumbre para las empresas del ramo, sobre las que al final del día recaen las responsabilidades. No se pretende desincentivar alguna idea para ampliar sus servicios ni complicar los escenarios con interpretaciones jurídicas extremas. La certidumbre siempre debe ser clara, y si hay interpretaciones encontradas esto solo significa que la regulación no posee la claridad suficiente.

Marco general de la contratación bursátil

El marco legal que regula la celebración de los contratos de intermediación bursátil deriva de la Ley del Mercado de Valores (LMV), concretamente del primer párrafo del artículo 199:

> **Artículo 199.-** *Las operaciones que las casas de bolsa celebren con su clientela inversionista y por cuenta de la misma, se regirán por las previsiones contenidas en los contratos de intermediación bursátil que al efecto celebren por escrito, salvo que, como consecuencia de lo dispuesto en ésta u otras leyes, se establezca una forma de contratación distinta.*

El requerimiento de que el contrato sea por escrito significa que no puede ser verbal, pero no arroja luz a si puede ser celebrado por vía electrónica o debe ser presencial4. Sobre el uso de medios electrónicos encontramos una disposición expresa en la fracción V del artículo 200 de la LMV, sin embargo, esta aplica a *posteriori* (ya que es "*a consecuencia del contrato*"):

> **Artículo 200.- Como consecuencia del contrato de intermediación bursátil:**
>
> **[…]**
>
> *V. En caso de que las partes convengan el uso de medios electrónicos, de cómputo o de telecomunicaciones para el envío, intercambio y en su caso confirmación de las órdenes y demás avisos que deban darse, incluyendo la recepción de estados de cuenta, habrán de precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización.*
>
> *Las claves de identificación que se convenga utilizar conforme a este artículo sustituirán a la firma autógrafa, por lo que las constancias documentales o técnicas en donde aparezcan, producirán los mismos efectos que las leyes otorguen a los documentos suscritos por las partes y, en consecuencia, tendrán igual valor probatorio.*

Esta fracción V del artículo 200 deja a las partes en libertad de elegir qué tipo de claves de identificación utilizarán entre ellas para sustituir a la firma autógrafa, sin embargo, eso es algo que se pacta en el contrato porque sucede "a consecuencia" de su celebración. Dado que esta modalidad es algo que sucede "a consecuencia", el contrato mismo no se puede celebrar así. Esto no significa que no se puedan formalizar contratos por medios electrónicos, sino solo que este artículo 200 no serviría de base para ello. La LMV no contiene ninguna disposición que señale con toda claridad que el contrato de intermediación bursátil pueda ser celebrado por medio de firma electrónica, pero tampoco ninguna que lo prohíba. Es más, el propio artículo 199 deja abierta la puerta a lo electrónico (y a otras formas de contratación) al disponer que estos contratos se pueden celebrar de otra forma si otras leyes así lo disponen.

Debajo de la LMV hay una extensa normativa que incide en las formas de contratación, como es el caso de las Disposiciones de Carácter General Aplicables a las Casas de Bolsa (conocida como la 'Circular Única'), que contiene una disposición expresa sobre los contratos de intermediación bursátil en su artículo 120 Bis 2 (que hasta junio de 2017 señalaba lo siguiente):

Artículo 120 Bis 2.- *Las casas de bolsa podrán pactar con sus clientes la realización de operaciones o servicios a través de medios electrónicos, siempre que en los contratos respectivos se establezca de manera clara y precisa, las bases para determinar:*

I. […]

II. […]

III. […]

IV. […]

Las casas de bolsa solo podrán permitir a sus clientes la utilización de medios electrónicos, cuando cuenten con el consentimiento expreso y por escrito de éstos, otorgado mediante firma autógrafa, previo al uso que por primera ocasión hagan de dichos medios.

Las casas de bolsa deberán comunicar a los usuarios los riesgos inherentes a la utilización de los medios electrónicos y las recomendaciones para prevenir la realización de operaciones irregulares o ilegales.

Esta Circular Única cerraba el círculo, por decirlo así. Se podían usar medios electrónicos siempre y cuando se contara con consentimiento previo y otorgado en firma autógrafa5.

Modificación que incorpora la firma electrónica

Hasta de junio de 2017 se contenía la redacción con la que cerramos el apartado anterior. Ahí se remarcaba con toda claridad que se podían utilizar medios electrónicos siempre y cuando existiera un consentimiento expreso y "*previo al uso*". Esto excluía al contrato mismo, es decir, éste no podría ser suscrito por medios electrónicos, y entonces el requisito de "*por escrito*" debía entenderse en su fórmula tradicional, es decir, firmarse presencialmente.

Sin embargo, el 23 de junio de 2017 se publicó en el Diario Oficial de la Federación (DOF) una reforma a este artículo 120 Bis 2 de esta Circular Única, y es una modificación de gran importancia porque abre la posibilidad de que los contratos de intermediación bursátil se suscriban electrónicamente, con la idea de eliminar así los obstáculos y cargas que provoca una firma presencial:

Artículo 120 Bis 2.- *[…]*

I. […]

II. […]

III. […]

IV. […]

Las casas de bolsa solo podrán permitir a sus clientes, previa identificación de estos, la utilización de medios electrónicos, cuando cuenten con el consentimiento expreso y por escrito, otorgado mediante firma autógrafa, o bien mediante firma electrónica avanzada o fiable de sus clientes, previo al uso que por primera ocasión hagan de dichos medios, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio para estos efectos.

[…].

Si bien esta reforma lleva implícita la intención de ir eliminando brechas de acceso al mercado bursátil mediante el uso adecuado de la tecnología, resultó lejos de ser práctica porque el uso de la firma electrónica prevista en el Código de Comercio no está extendido, en contraste con la firma electrónica prevista en el CFF.

Considerando que el CFF contiene regulación propia sobre la firma electrónica y el Código de Comercio también, que no coinciden en todo y, especialmente, considerando que la legislación fiscal del CFF no es supletoria la bursátil (LMV) como sí lo es el Código de Comercio, comienzan aquí las complejidades de interpretación legislativa. Aunque se desee utilizar la firma prevista en el CFF, la regulación bursátil se refiere expresamente a la del Código de Comercio.

Es natural que surja la pregunta ¿cuántas firmas electrónicas puede tener una persona? Debiera ser una sola porque es una sola la firma autógrafa. Sin embargo, dado que por seguridad jurídica en la confección de las firmas electrónicas se involucran certificados digitales de autenticación, en México parecieran existir varias formas de certificar o varios tipos de firmas electrónicas según la finalidad o materia donde aplicaría esa firma. Más que firma electrónica pareciera más bien existir una variedad de 'llaves de acceso electrónicas'. Por ejemplo, para trámites ante el Instituto Mexicano del Seguro Social (IMSS) existe una firma digital *ad hoc* para el intercambio de información entre las empresas y el IMSS, y se integra por un certificado digital (como toda firma electrónica) pero también por el número patronal de identificación electrónica6; también la Secretaría de la Función Pública emite certificados digitales para empresas interesadas en participar en procesos de contratación pública (a través del sistema CompraNet), y así pudiéramos encontrar muchos casos. La "Firel" del Poder Judicial es otro ejemplo.

A pesar de la variedad, es probable que las tres modalidades más importantes de firma electrónica sean (desde el punto de vista jurídico):

a) la del Código de Comercio;
b) la del CFF, y
c) la de la Ley de Firma Electrónica Avanzada (LFEA).

El uso de la tecnología en las transacciones cotidianas permeó en la legislación mexicana pero de modo fragmentado e inarmónico. Quizá tardío. Lo ideal hubiera

sido contar primero con una ley marco de firma electrónica, donde alguna modalidad variara (si fuera necesario) dependiendo de su uso o finalidad, pero esto sucedió al revés. Primero se adoptó esta firma para actos mercantiles en 20037, luego para efectos fiscales en 20048, y casi una década más tarde apareció la LFEA9, que debía haberse creado primero, y que a pesar de que su objeto es *"la homologación de la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas por otros ordenamientos"* (artículo 1), se precisó que no sería aplicable a las materias fiscal, aduanera y financiera10, con lo que la pretendida homologación quedó trunca. Quizá algún día se eliminen todas las provisiones sobre firma electrónica diseminadas en muchas leyes, y se centre todo tipo de modalidades en la LFEA, ello facilitaría las transacciones del futuro, daría certidumbre y promovería su uso.

Volviendo al tema, la preocupación original es que una casa de bolsa pueda celebrar contratos de intermediación bursátil con una persona que se encuentre fuera de su radio geográfico, y para eso es necesario que ese cliente potencial cuente con una firma electrónica. Si la obtención de esa firma resulta gravosa, el requisito será un desincentivo para contratar electrónicamente, por ello lo ideal es que el cliente ya cuente con ella (por utilizarla para otros asuntos, como los fiscales) o no le resulte una carga tramitarla.

El atractivo de la firma electrónica prevista en el CFF es que se trata de una firma de uso relativamente generalizado. Si bien no es obligatoria para todo el universo de contribuyentes, sí lo es para un amplio sector, por ejemplo, para aquellos que acuerden su uso como medio de autenticación o firmado de documentos digitales, para quienes deben presentar declaraciones periódicas o estén obligados a expedir comprobantes fiscales, o tengan saldos a favor por encima de los catorce mil pesos (2017), entre otros supuestos.

Lo anterior hace que la firma electrónica para efectos fiscales sea de uso común, y que el SAT tenga un papel relevante en el otorgamiento o en el proceso de la certificación, lo cual abona en la percepción de seguridad y certeza. Por estas razones, esa firma resulta atractiva para utilizarse en los contratos de intermediación bursátil. Sin embargo, el fiscal y el financiero son dos sectores muy distintos, y el CFF no es de aplicación supletoria a la LMV.

Ya mencionamos que en virtud de que los contratos de intermediación bursátil son financieros y esa es una materia excluida en la LFEA, entonces esa legislación no aplicable al ramo; y el CFF tampoco lo es, porque no es supletorio a la LMV.

El supletorio es el Código de Comercio11. Lo anterior no obstante que en el CFF se incorporó una disposición en noviembre de 2016 que quizá pretende tener el carácter de general12 (y que es a la que nos referimos en la introducción de este ensayo):

> Artículo 17-F.- *[…]*
>
> *Los particulares que acuerden el uso de la firma electrónica avanzada como medio de autenticación o firmado de documentos digitales, podrán solicitar al Servicio de Administración Tributaria que preste el servicio de verificación y autenticación de los certificados de firmas electrónicas avanzadas. Los requisitos para otorgar la prestación de dicho servicio se establecerán mediante reglas de carácter general que emita dicho órgano administrativo desconcentrado.*

Esta provisión podría permitir la firma electrónica del CFF para el mercado bursátil, pero como el CFF no es supletorio de la LMV, sus reglas y disposiciones no entran al sector. Esto solo pudiera suceder si la propia LMV o la regulación bursátil hicieran, por decirlo así, 'un llamado directo' al CFF. No es el CFF el que debe decir 'soy general para todas las materias' (que de todos modos no lo dice) sino que cada materia debe señalar expresamente qué es lo que toma de las otras. Esta es la congruencia del sistema jurídico y un principio de armonía legislativa. El punto adquiere mayor importancia cuando la legislación mercantil, que sí es supletoria a la bursátil, contiene una regulación determinada sobre el mismo tema. No hay en la regulación bursátil ningún indicativo explícito que permita recurrir a la fiscal. Además, si bien este 17-F habla en términos generales, no debe perderse de vista que éstos se constriñen a la materia fiscal (autenticación de documentos *fiscales*, firmado de documentos digitales *fiscales*).

Las dudas

Si consideramos que la firma electrónica 'fiscal' es una firma electrónica avanzada y está avalada por autoridades, pareciera que no debe haber problema para utilizarla en el sector bursátil. Pero tanto el CFF como el Código de Comercio regulan sobre firma electrónica, y no es optativo qué ley aplica. En el sector bursátil es la LMV y su supletoria (el Código de Comercio), no el CFF.

Si la firma prevista en el CFF estuviera autorizada según el Código de Comercio (supongamos), entonces sí podría utilizarse en el sector financiero. Pero esto requeriría que el Código de Comercio la considerara viable, así se incorporaría al sector aunque esté en la legislación fiscal. La pregunta será entonces ¿el Código de Comercio considera viable la firma electrónica que se usa para trámites fiscales? Es decir, ¿puede utilizarse?

Comenzamos la revisión al Código de Comercio observando que éste contiene una provisión en el sentido de interpretar las disposiciones del Código de manera que "*no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una firma electrónica*"13, esto parecería una invitación a considerar que este Código avala o adopta todo tipo de firmas, tanto la prevista en el CFF como la del IMSS o la "Firel", por ejemplo, pero ello no sería admisible para firmar un contrato de intermediación bursátil. ¿A qué se refiere entonces este precepto? ¿Solamente a que puedan subsistir diferentes modalidades de firmas electrónicas en el mundo jurídico por el hecho de que han sido creadas con métodos válidos (mismos ejemplos: la del IMSS o la "Firel")? Este Código tiene su propia manera de crear una firma electrónica, pero advierte que no por eso las demás firmas creadas por otras leyes pierden validez para sus respectivas finalidades.

No perdamos de vista que si estamos revisando el Código de Comercio no es solo porque sea supletorio a la LMV, sino por la disposición expresa del 120 bis 2 de la Circular Única. Citamos de nuevo:

> *Las casas de bolsa solo podrán permitir a sus clientes, previa identificación de estos, la utilización de medios electrónicos, cuando cuenten con el consentimiento expreso y por escrito, otorgado mediante firma autógrafa, o bien mediante firma electrónica avanzada o fiable de sus clientes, previo al uso que por primera ocasión hagan de dichos medios, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio para estos efectos.*

Lo anterior puede significar que la firma electrónica que se utilice en los contratos de intermediación bursátil 'debe sujetarse' a lo establecido en el Código de Comercio (ojo, no en el CFF). Ese 'deber sujetarse' no es solo que una firma subsista porque se le reconoce creada conforme a otras normas, sino porque fue creada conforme a este Código.

En este punto ya podemos distinguir los dos enfoques interpretativos que chocan entre sí:

1. Que la firma del CFF puede utilizarse para celebrar contratos de intermediación bursátil porque es una firma electrónica válida y por lo tanto no está restringida por el Código de Comercio, así que está conforme a éste;

2. Que la firma del CFF no puede utilizarse porque si bien la legislación mercantil reconoce que existen otras firmas electrónicas válidas en el mundo jurídico, tiene *su propio mecanismo* para crear una firma electrónica y eso es lo que le interesa a la regulación bursátil: el contar con una firma *creada* con el Código de Comercio, no solo reconocida como válida para otros fines.

Es poco afortunado que la duda sea tan técnica, y que se requiera de una exégesis minuciosa para algo que debería estar absolutamente claro. Si no fuera porque se trata de lo que pudiera significar una importante apertura de las casas de bolsa en su base de clientes, el tema parecería ocioso, así que es comprensible la frustración que provoca tanto para clientes como para casas de bolsa e incluso para funcionarios esta especie de limbo. Al final del día lo que todas las partes quieren es una absoluta seguridad jurídica porque se trata de la celebración misma del contrato. Una firma inválida nulifica todos los efectos. Para tratar de dilucidar cuál de esas dos posturas es válida, recurrimos de nuevo al Código de Comercio, que señala que la firma electrónica se considerará avanzada o fiable si cumple con cuatro requisitos mínimos[14], que prácticamente se cumplen en cualquier tipo de firma electrónica porque son parte de los requerimientos tradicionales. Estos requisitos son a grandes rasgos los mismos para una firma electrónica con efectos fiscales que para una firma electrónica para efectos mercantiles, donde aparecen las diferencias es en los certificados.

Veamos si la firma electrónica prevista en el CFF cumple con los requisitos para asimilarse al Código de Comercio. Una firma electrónica creada conforme éste parte de lo siguiente:

Artículo 100.- *Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:*

I. Los notarios públicos y corredores públicos;

II. Las personas morales de carácter privado, y

III. Las instituciones públicas, conforme a las leyes que les son aplicables.

[…]

Podría pensarse que la firma electrónica prevista por el CFF es emitida por una institución pública y que por lo tanto está incluida en la fracción III de este artículo 100, sin embargo, el certificado de la 'firma fiscal' puede ser expedido por el SAT pero también por un prestador de servicios certificación autorizado por el Banco de México[15], en este último caso, deja de tratarse de una "*institución pública*" para efectos de la fracción III. Además, aunque el propio SAT o el Banco de México otorgaran la certificación (como instituciones públicas), se necesitaría que estuvieran acreditadas para hacerlo ante la Secretaría de Economía. Por extravagante que esto pueda parecer, se trata de una exigencia y como tal no puede obviarse. Toda institución pública que conforme a las leyes aplicables expida un certificado para firma electrónica que se pretenda válido según la legislación mercantil, debe estar *previamente acreditada en la Secretaría de Economía* para ello. Respecto de los prestadores de servicios de certificación autorizados por el Banco de México para el ramo fiscal, se necesitaría que también estuvieran registrados en la Secretaría de Economía para efectos de cumplir con este artículo 100, y es improbable que lo estén ya que para expedir certificados de acuerdo a la legislación fiscal no requieren este registro sino solo la autorización del Banco de México.

Por otra parte, en cuanto a los certificados de firma electrónica, para ser considerados válidos el Código de Comercio dispone lo siguiente:

Artículo 108.- *Los Certificados, para ser considerados válidos, deberán contener:*

I. La indicación de que se expiden como tales;

II. El código de identificación único del Certificado;

III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su nombre de dominio de

Internet, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;

IV. Nombre del titular del Certificado;

V. Periodo de vigencia del Certificado;

VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;

VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

En términos generales, hay provisiones similares o idénticas en el CFF, pero también existen diferencias en algunos puntos. Por ejemplo, sobre el periodo de vigencia del certificado, el Código de Comercio dispone que no podrá ser superior a dos años (artículo 109), mientras que el CFF los expide con una vigencia hasta de cuatro años (artículo 17-D). Si revisáramos a detalle ambas legislaciones encontraríamos más sutilezas que prueban dos tratamientos distintos en cuanto a las certificaciones de las firmas electrónicas. En estricto sentido, la firma del CFF no es la misma a la que se refiere el Código de Comercio.

Podría considerarse que basta con que la firma electrónica sea válida bajo otra legislación para que se entienda validada por el Código de Comercio, pero también podría interpretarse lo contrario porque este Código prevé *su propia manera* de certificar las firmas. ¿A qué nos remite entonces la Circular Única? ¿A tomar el Código de Comercio como una puerta abierta para que a través de este pueda usarse cualquier firma electrónica (incluyendo, por ejemplo, la del IMSS, la del CompraNet o la "Firel")? ¿O a tomar en cuenta las certificaciones de firmas creadas conforme a ese Código?

¿Consultar a la autoridad?

Las preguntas reflejan dos posturas contrarias en la forma de interpretar. Pero como se trata de un elemento constitutivo de contrato y no un tema discrecional o administrativo, no es algo que la autoridad burocrática del ramo pueda determinar a través de una consulta. La propia LMV dispone que la Secretaría de Hacienda y Crédito Público (SHCP)

podrá interpretar los preceptos de la misma *pero solo para efectos administrativos*, y los elementos constitutivos de un contrato no son administrativos sino legales. Solamente un juez podría fijar una interpretación pero no es deseable llegar hasta esa instancia para lograr la certidumbre jurídica.

Cabe comentar como anécdota que durante esta investigación, alguna autoridad de la CNBV comentó que sí se puede utilizar la firma del CFF para los contratos de intermediación bursátil "porque también se usa para el programa 'CetesDirecto'[16], de la SHCP", y que para el caso era lo mismo. Sin embargo, ese contrato que con sus clientes celebra Nacional Financiera, S.N.C. (Nafinsa), al amparo de este programa, es de comisión mercantil y depósito bancario, y si en su Cláusula Decimosegunda establece cualquier firma electrónica entre las partes[17] es porque así se lo permite el artículo 52 de la Ley de Instituciones de Crédito. Esta legislación sí es aplicable a Nafinsa pero de ninguna forma a las casas de bolsa.

> Artículo 52.- *Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases…*
>
> *[…]*
>
> *El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.*

Las casas de bolsa operan con una regulación distinta no con la de instituciones de crédito, y si bien una regla así les serviría mucho, esta no existe con esa claridad en el sector bursátil. Aquí nos topamos con la omisión de la LMV y con la referencia que la Circular Única hace expresamente a la firma electrónica del Código de Comercio. Por lo tanto, la opción segura de las casas de bolsa es seguir los lineamientos de certificación del Código de Comercio, a pesar de que ello implique una carga para el cliente, quien

tendría que obtener su firma electrónica certificada conforme a ese código aunque cuente su firma electrónica fiscal.

Si se insiste en realizar alguna consulta a la autoridad para allanar de cierta forma el camino, esta no puede ser de mucho alcance, si acaso para que informe cuáles son las certificadoras acreditadas por la Secretaría de Economía, a fin de informárselas a los clientes potenciales para que tramiten la firma que se requiere para los contratos de intermediación bursátil.

Conclusiones, ¿Qué se puede hacer?

La autoridad tiene la posibilidad de contribuir a que esta apertura hacia la firma electrónica realmente signifique un cambio importante, y lo puede hacer de varias formas. Lo idóneo sería que la propia LMV (artículo 199) sea mucho más clara respecto a la firma de los contratos de intermediación bursátil permitiendo que pueda usarse la firma electrónica certificada, ya sea otorgada conforme al Código de Comercio o al CFF. Si el propio SAT es el certificador, la salvaguarda de la seguridad e identidad debe ser de un parámetro acorde a las certificaciones de la Secretaría de Economía. Si no es posible modificar la LMV, al menos sería importante ajustar el artículo 120 Bis 2 de la Circular Única con la finalidad de permitir con claridad el uso de la firma electrónica prevista en el CFF adicionalmente a la ya mencionada del Código de Comercio.

Por supuesto que otra alternativa es que las casas de bolsa sigan la interpretación más amplia y favorable para ellas sobre el uso de la firma electrónica, asumiendo que el Código de Comercio reconocería a la firma otorgada conforme al CFF como una firma electrónica válida; pero sin olvidar que existe una interpretación opuesta. Como adoptar el esquema de la firma electrónica les implica gastos y rediseños institucionales y en su documentación, se podría reservar el uso de la firma electrónica solo para contratos de menor cuantía, de suerte que las pérdidas no sean graves en caso de que una autoridad judicial considere que la regulación bursátil es estricta y anule el contrato por no estar celebrado con la firma electrónica pertinente.

Una alternativa más sería que la Secretaría de Economía acreditara como prestadores de servicios de certificación al SAT y al Banco de México (si es que no los tiene acreditados), y convenir con el Banco de México en que las empresas que a su vez

éste autoriza para certificar en términos de la legislación fiscal, también sean autorizados conforme a la legislación mercantil y para efectos del Código de Comercio. Esto podría dar mayor seguridad al uso de la 'firma fiscal' para los contratos de intermediación bursátil porque entonces las firmas certificadas por el SAT o el Banco de México también estarán acreditadas ante la Secretaría de Economía, y se cumpliría así ese requisito de instituciones públicas acreditadas (artículo 100 del Código de Comercio, arriba transcrito).

Finalmente, las casas de bolsa también pudieran ser acreditadas por la Secretaría de Economía para otorgar certificados de firma electrónica y ello cumpliría con el artículo 100 del Código de Comercio, aunque implicara expedir una regulación especial para el sector en este rubro.

Adenda. Otro tema urgente: las reglas para la prevención del lavado de dinero

La adopción de una firma electrónica que resulte conveniente y atractiva como para celebrar de esta forma contratos de intermediación bursátil es apenas un primer paso para lograr superar la barrera geográfica como obstáculo, porque hay disposiciones para la prevención del lavado de dinero que requieren de entrevistas personalizadas antes de contratar con el cliente. Tales reglas se conocen como "Reglas para la Prevención del Lavado de Dinero" o "Reglas PLD" y constituyen un conjunto de disposiciones de carácter general derivadas del artículo 212 de la LMV, que se refiere a las medidas que deben adoptar las casas de bolsa para prevenir y detectar el lavado de dinero. Una de tales medidas es la siguiente:

> ***6ª.-*** *Antes de que una Casa de Bolsa establezca o inicie una relación comercial con un Cliente, aquella deberá celebrar una entrevista personal con este o su apoderado, a fin de que recabe los datos y documentos de identificación respectivos y asentará de forma escrita o electrónica los resultados de dicha entrevista.*

Ciertamente si se logra adoptar una firma electrónica avanzada para la celebración de contratos bursátiles se hace necesario revisar y replantear las medidas de las Reglas del

PLD, porque provisiones como la transcrita (y otras más, como la integración de expedientes sobre cada cliente) vuelven nugatorios los alcances de la firma electrónica. De poco serviría adoptar una firma electrónica si de todas maneras es necesaria una entrevista personal con el cliente antes de celebrar el contrato.

¿Qué se puede hacer?

El tema de las Reglas del PLD excede el interés primordial de este ensayo, que es analizar el enredo legislativo en materia de firma electrónica para las casas bolsa. Sin embargo, podríamos aportar un par de ideas para cuando la atención se centre en revisar las Reglas del PLD. Quizá una solución sería que esa entrevista personal sucediera, si acaso, dentro de un rango de tiempo una vez de celebrado el contrato por firma electrónica, a fin de dar oportunidad a que más clientes de la misma región contraten sin que ello implique viajes constantes de los empleados de las casas de bolsa a fin de cumplir con estas entrevistas, sino que puedan optimizar sus recursos y aprovechar los beneficios de una firma electrónica. Otra solución podría ser restringir el tipo o monto de operaciones que puedan celebrarse a través de los contratos que se apertura con firma electrónica y respecto a los cuales no haya constancia de entrevista personal.

Se insiste en que este es un tema posterior pero que es necesario ir considerando para efectos de la firma electrónica que se adopte. Permitir la firma del CFF, si bien no necesariamente brinda elementos al SAT para rastrear contribuyentes que sean clientes de las casas de bolsa, podría contribuir a generar mejores mecanismos electrónicos para prevenir el lavado de dinero, y en este sentido es una razón más para su procurar su adopción expresa como firma electrónica autorizada para celebrar contratos de intermediación bursátil.

NOTAS BIBLIOGRÁFICAS

[1] La inclusión financiera es prioridad según el Banco Mundial, ya que la identifica como un pilar para el desarrollo sostenible de un país, y al mismo tiempo un factor clave para reducir la pobreza

extrema y promover la prosperidad compartida. http://www.bancomundial.org/es/topic/financialinclusion/overview

[2] IMCO, *Acciones para democratizar el acceso al Mercado bursátil*, 2015. Para el IMCO, el principal problema es de acceso, y señala que la escasa inclusión bursátil limita la riqueza de los mexicanos y el crecimiento económico del país. Para ese instituto, las causas de esa falta de acceso son variadas: existen pocas empresas medianas y grandes que cotizan en el mercado bursátil, el tamaño y la profundidad del mercado accionario mexicano son bajos (comparados con otros países), el mercado está significativamente concentrado en un número reducido de empresas, las brechas de acceso son un problema, y México sigue siendo un país donde el ahorro es informal, que no aprovecha el mercado bursátil y donde falta educación financiera. http://imco.org.mx/banner_es/acciones-para-democratizar-el-acceso-al-mercado-bursatil/

[3] Véanse las págs. 43 y 44 de la Iniciativa de Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley del Impuesto sobre la Renta, de la Ley del Impuesto al Valor Agregado y del Código Fiscal de la Federación (paquete fiscal para 2017), de noviembre de 2016: http://www.diputados.gob.mx/PEF_2017/2017/work/models/PPEF2017/paquete/ingresos/LISR_LIVA_CFF.pdf

Esta política sigue siendo impulsada, según puede constatarse en la Cuarta Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2017 (DOF, 10 de octubre de 2017), cuya regla 2.2.12 se refiere expresamente a que el SAT prestará los servicios de verificación y autentificación de los certificados de firmas electrónicas avanzadas a los contribuyentes que así lo soliciten. Si bien aún falta establecer los lineamientos para echar a andar este proceso, queda claro que el SAT contará con la infraestructura para otorgar este tipo de servicios.

[4] En alguna consulta administrativa la Comisión Nacional Bancaria y de Valores señaló que *"se considerará como firma autógrafa cuando provenga del puño y letra del autor, con independencia de la forma en que dicha firma quede plasmada o suscrita, ya sea en papel o en algún otro equipo tecnológico"* (Oficio Núm. 313-17300/2017), sin embargo, este tema es difícilmente materia de una consulta administrativa. Además es cuestionable esa conclusión. Por ejemplo, la Ley de Instituciones de Crédito, cuando se refiere a las firmas autógrafa y a la expresada a través de medios electrónicos lo hace utilizando una "o" disyuntiva, como cosas distintas; y además existe jurisprudencia, si bien no directa sí en el sentido de que "autógrafo" es del puño y letra, y también desestimando que una firma facsimilar sea de puño y letra (aplicaría la misma interpretación si la firma es ahora sobre una tableta). Si se acepta como "de puño y letra" una firma sobre una tableta, se podrían otorgar testamentos por ese medio, por ejemplo. Por eso tradicionalmente la firma de "puño y letra" implica un rasgo biométrico, es decir, biológico. Por estas y más consideraciones similares, una consulta administrativa no puede fijar los alcances jurídicos de lo que debe entenderse como una firma "de puño y letra".

[5] Esta frase es otra prueba del error del oficio referido en la nota al pie que antecede: se autoriza el uso de medios electrónicos después de firma autógrafa. ¿Una firma otorgada en tableta no es haciendo ya uso de medios electrónicos? Aquí ya estamos dentro de la normativa del ramo, no en ámbito jurídico en general.

[6] Por cierto, el IMSS está migrando a la firma prevista en el CFF, véase su portal de internet: http://idse.imss.gob.mx/imss/

[7] El 29 de agosto de 2003 se publicó en el DOF el *Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de firma electrónica*, para efectos puramente mercantiles.

[8] El 5 de enero de 2004 se publicó en el DOF el *Decreto por el por el que se reforman, adicionan y derogan diversas disposiciones del Código Fiscal de la Federación*, que implicó una reforma muy amplia para incorporar las modalidades de firma y documentos electrónicos para efectos exclusivamente fiscales.

[9] DOF, 11 de enero de 2012.

[10] **Artículo 4:** *Las disposiciones de esta Ley no serán aplicables a los actos en que no sea factible el uso de la firma electrónica avanzada por disposición de ley o aquéllos en que exista previo dictamen de la Secretaría. Tampoco serán aplicables a las materias fiscal, aduanera y financiera.*

[11] **Artículo 5:** *La legislación mercantil, los usos bursátiles y mercantiles y la legislación civil federal, en el orden citado, serán supletorios de la presente Ley.*

[12] DOF, 30 de noviembre de 2016.

[13] **Artículo 96.**

[14] **Artículo 97:** *Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.*

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;

II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;

III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

[15] Artículo 17-D del CFF: *Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario Oficial de la Federación la*

denominación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente.

[16] Incluso se ha desarrollado una norma oficial para regular con más detalle y uniformidad la "*digitalización de documentos y la conservación de mensajes de datos cuando estos sean utilizados por los comerciantes en actos de comercio que estén relacionados con sus negocios*", según dice la introducción de la propia Norma Oficial Mexicana NOM-151-SCFI-2002, *Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos*, publicada en el DOF el 30 de marzo de 2017.

Cabe agregar que esta NOM no podría servir de base para celebrar un contrato de intermediación bursátil a través el uso de firma electrónica, porque ni está orientada a celebrar contratos (solo a conservar la información digitalizada) ni este tipo de contratos serían celebrados entre 'comerciantes' (sino entre la casa de bolsa y sus clientes, ninguno firmando con calidad de comerciante).

[17] *SERVICIO DE BANCA ELECTRÓNICA DÉCIMA SEGUNDA.- Las partes acuerdan que podrán suscribir este contrato a través del uso de una firma electrónica ("Firma Electrónica") en sustitución de firma autógrafa, las cual obligará y producirá los mismos efectos que la ley otorga a los documentos que contienen firma autógrafa y en consecuencia, tendrá el mismo valor probatorio,* ***conforme a lo dispuesto en el artículo 52 de la Ley de Instituciones de Crédito*** *y demás* ***disposiciones aplicables****, por lo que las partes asumen totalmente y desde este momento todas las obligaciones y responsabilidades inherentes o que resulten por el uso de las mismas. Las partes acuerdan que la Firma Electrónica podrá consistir de cualquiera de las siguientes opciones:*

i) Firma electrónica avanzada ("FIEL"), es aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97 del Código de Comercio.

ii) Firma electrónica simple, consiste en los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

iii) ***Cualquier otra que establezca NAFIN*** *para la identificación y/o autenticación del CLIENTE, incluyendo de manera enunciativa y no limitativa usuario, contraseña, combinación numérica de Tarjeta de Seguridad.* […]

Tipos de Riesgos y su adecuada gestión

Samuel Uziel Rivero Prado

Samuel Rivero es Asociado Senior de Financiero en BGBG Abogados. Es egresado de la Universidad La Salle y maestría en Derecho del Comercio Internacional de la Universidad de Nottingham. Cuenta con más de 15 años de experiencia en materia de derecho financiero, banca y mercados globales, con sólidos conocimientos en las áreas de Gobierno Corporativo, Cumplimiento Normativo, Prevención de Lavado de Dinero, Financiamiento de Proyectos y Comercio Internacional, con amplia experiencia en trabajo con equipos multidisciplinarios, implementación de proyectos y en el manejo de relaciones con Alta Dirección, autoridades y reguladores.

Puede enviar sus comentarios al correo: suirivero@bgbg.mx

1. Tipos de Riesgos

Las entidades existen con el fin último de generar valor para sus grupos de interés. En su camino cotidiano se enfrentan con la falta de certeza en diversos ámbitos, por lo que el reto de toda organización consiste en determinar cuanta incertidumbre se puede y se desea aceptar mientras se genera valor.

Ahora bien, ¿a qué riesgos se enfrenta una empresa?

- *Riesgo de crédito: Posibilidad de que la contraparte incumpla sus obligaciones contractuales.*
- *Riesgo de liquidez: Imposibilidad de poder deshacer una posición con la suficiente rapidez y a un precio de mercado competitivo. O bien, imposibilidad de asumir un pago por falta de liquidez. Es un riesgo difícilmente cuantificable desde fuera de la propia empresa.*
- *Riesgo operacional: Riesgo asociado a la realización de las transacciones (calidad de los sistemas informáticos de gestión y control, nivel de formación, complejidad de los productos, etc.). Es decir, posibilidad de que ocurra una contingencia en la empresa.*

- *Riesgo legal: Proviene fundamentalmente de las carencias legislativas en relación con la continua innovación financiera, pero también de la falta de rigor al analizar las posibles limitaciones legales de actuación de las distintas contrapartidas.*

- *Riesgo estratégico: Riesgo asociado a la elección de una estrategia inadecuada para permanecer y competir en el negocio.*

- *Riesgo reputacional: Consecuencia de un hecho adverso para la entidad. Proviene fundamentalmente de la pérdida de confianza de los clientes. Lo que puede sacar a una empresa del negocio.*

- *Riesgo de mercado: Posibilidad para una posición o cartera de incurrir en pérdidas ante movimientos desfavorables de los precios en el mercado. Este riesgo tiene, a su vez, otros muchos tipos de sub-riesgo:*

- *Riesgo de tipos de cambio.*

- *Riesgo de tipos de interés.*

- *Riesgo de acciones.*

- *Riesgo de volatilidad.*

- *Etc.*

2. Definición de gestión de riesgos corporativos

El Informe COSO (Committee of Sponsoring Organizations of the Treadway Commission) define a la gestión de riesgos corporativos de la siguiente manera:

> *"…es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos".*

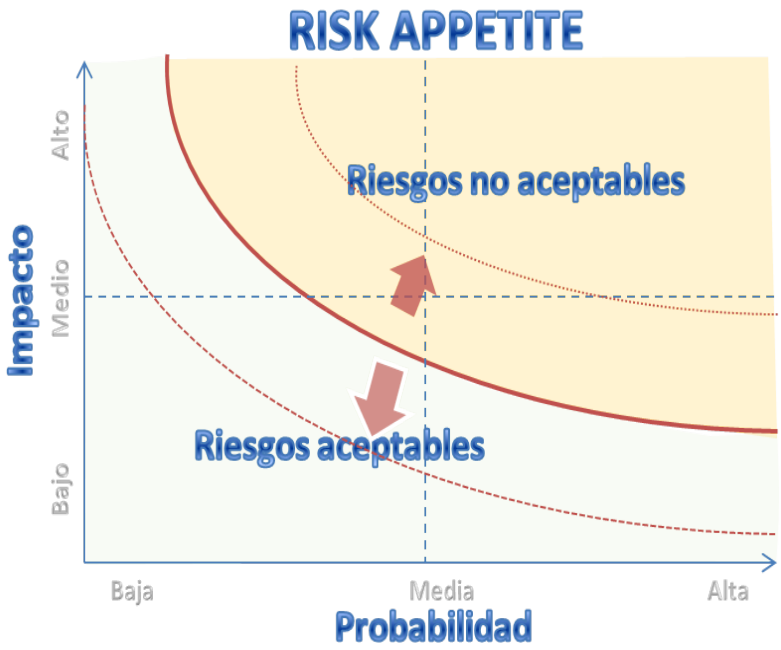
La definición enunciada nos permite identificar las siguientes características de la gestión de riesgos corporativos:

- Es un proceso continuo y de ninguna manera una tarea que se realiza en un único momento determinado o con una periodicidad preestablecida – es un instrumento para un fin y no un fin en sí mismo.
- Es realizado por el personal de todos los niveles de la organización, y no únicamente por un departamento de riesgos ó área similar – no es la mera conjunción de políticas, encuestas y formularios, sino que involucra gente de los distintos niveles de la organización;
- Está directamente relacionado con el establecimiento y el seguimiento de la estrategia corporativa;
- Se aplica en toda la entidad, y de alguna manera se incluye adoptar una perspectiva del riesgo a nivel integral de la entidad, dejando de lado estrategias parciales;
- Está diseñado para identificar eventos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel de riesgo aceptado;
- Su fin último es proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad;
- Está orientada al logro de objetivos de la organización dentro de unas categorías diferenciadas, aunque susceptibles de enlazarse.

3. Apetito de Riesgo

Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar.

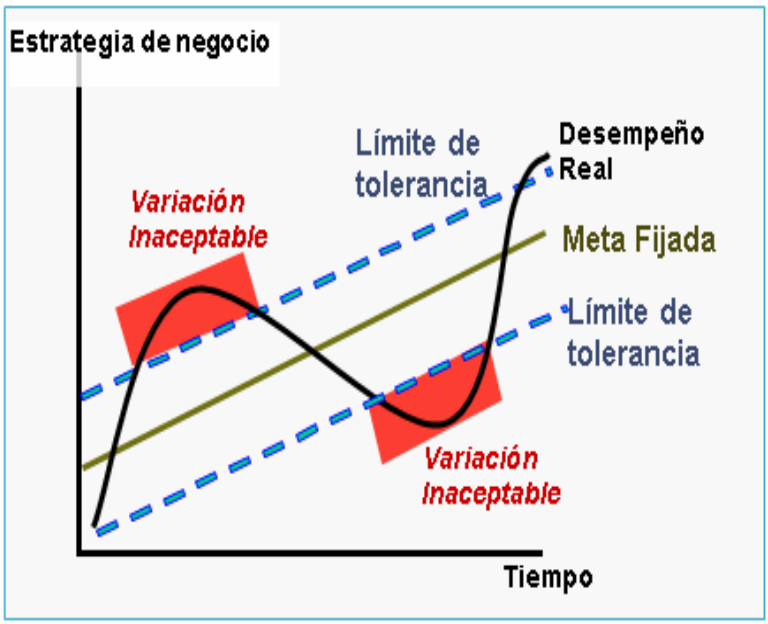
- Es una guía en el establecimiento de la estrategia.
- La gerencia lo expresa como un balance entre: crecimiento, riesgo y retorno.
- Dirige la asignación de recursos.
- Alinea la organización, personal, procesos e infraestructura.



4. Tolerancia al riesgo

Son los niveles aceptables de variación de las metas fijadas.

La tolerancia al riesgo se puede medir preferiblemente en las mismas unidades que los objetivos relacionados.



5. Riesgos y Oportunidades

La gestión de riesgos corporativos se ocupa de los riesgos y oportunidades que afectan a la creación de valor o su preservación.

RIESGOS: Tienen un impacto negativo que puede impedir la creación de valor o erosionar el valor existente.

OPORTUNIDADES: Los eventos con impacto positivo pueden compensar los impactos negativos o representar oportunidades, que derivan de la posibilidad de que ocurra un acontecimiento que afecte positivamente al logro de los objetivos, ayudando a la creación de valor o a su conservación.

6. Objetivos de las entidades

La idea subyacente de la gestión de riesgos corporativos, es proporcionar una seguridad razonable sobre el logro de los objetivos organizacionales. Los mismos suelen dividirse en cuatro categorías:

- Estrategia: objetivos a alto nivel, alineados con la misión de la entidad;
- Operaciones: objetivos vinculados al uso eficaz y eficiente de recursos;
- Información: objetivos de fiabilidad de la información suministrada;
- Cumplimiento: objetivos relativos al cumplimiento de leyes y normas aplicables.

Con respecto a las dos últimas categorías de objetivos (**información y cumplimiento**), es en donde la **gestión de riesgos corporativos facilita directamente su consecución**, puesto que son categorías "internas". En cambio, en relación a las dos categorías restantes (**estrategia y operaciones**), **la gestión de riesgos sólo puede proporcionar una seguridad razonable de que la dirección está adecuadamente informada sobre el progreso de su consecución**, pero la misma no puede asegurar su logro, puesto que existen factores externos que no se encuentran bajo el control de la entidad.

7. Componentes de la gestión de riesgos

De acuerdo al marco definido en el informe COSO, la gestión de riesgos corporativos está conformada por ocho componentes relacionados entre sí, los cuales se describen brevemente a continuación:

- Ambiente interno

  Abarca el talante de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía para su gestión, el riesgo aceptado, la integridad y valores éticos y el entorno en que se actúa.

- Establecimiento de objetivos

  Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución. La gestión de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

- Identificación de eventos

  Los acontecimientos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

- Evaluación de riesgos

  Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual.

- Respuesta al riesgo

  La dirección selecciona las posibles respuestas -evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

- Actividades de control

  Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.

- Información y comunicación

  La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas direcciones dentro de la entidad.

- Supervisión

  La totalidad de la gestión de riesgos corporativos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez.

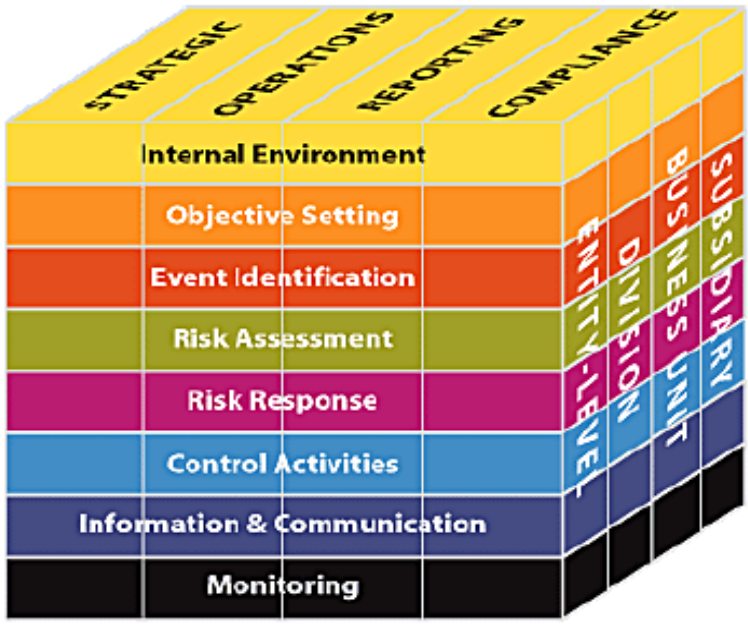
8. Relación entre objetivos y componentes

La relación entre los diferentes conceptos hasta aquí enunciados puede graficarse como un cubo, tal como se muestra en la figura 1, en donde las cuatro categorías de objetivos están representadas por las columnas verticales, los ocho componentes de la gestión de riesgos corporativos por las filas horizontales y los diferentes niveles organizacionales por la tercera dimensión del cubo.

Esta matriz tridimensional refleja la capacidad de centrarse sobre la totalidad de la administración de riesgos de una entidad o bien por categoría de

objetivos, por componente, por unidad de negocio o por cualquier subconjunto de ellos.

FIGURA 1



9. La eficacia de la gestión de riesgos

Cuando se determine que la gestión de riesgos corporativos es eficaz para cada una de las cuatro categorías de objetivos, lo que se intenta decir es que:

- La dirección tiene la seguridad razonable de que conoce el grado de consecución de los objetivos estratégicos;
- La dirección también conoce el nivel de logro de los objetivos operativos, siempre con un grado de seguridad razonable;
- La información generada por la entidad es fiable;
- Se cumple con las leyes y las normas aplicables.

Es importante destacar que siempre hablamos de un grado de "seguridad razonable" debido a que la gestión de riesgos corporativos, si bien proporciona

grandes ventajas, también posee algunas limitaciones, como el juicio humano, la connivencia, o la posibilidad de fallas por error humano. Estas limitaciones son las que impiden que la dirección tenga un grado de seguridad absoluta.

Gestión de Riesgos y Oportunidades

José Manuel Ballester Fernández

Doctor Ingeniero Industrial, CISA, CISM, CGEIT, COBIT Trainer, cuenta con 35 años de experiencia en empresas privadas, así como en universidades públicas y privadas en las áreas de informática, seguridad, gobierno de TI, telecomunicaciones y eficiencia energética. Director de la Cátedra de Buen Gobierno y del Postgrado de Buen Gobierno en Universidad de Deusto, ostenta el cargo de Vicepresidente General de la Academia Mexicana de Ciencia de Sistemas y es catedrático en la Universidad Inttelmex y es Socio Director de la firma TEMANOVA en México.

La gerencia de riesgos es una disciplina que se está desarrollando muy rápidamente y existe un sinfín de puntos de vista y descripciones de lo más variado sobre lo que implica, cómo se debe llevar a cabo y para qué sirve. Se necesita por ello algún tipo de reglas o estándares para establecer:

- *El significado del vocabulario utilizado.*
- *El proceso a través del cual se puede llevar a cabo la gerencia de riesgos.*
- *La estructura organizativa para desarrollar la gerencia de riesgos.*
- *Los objetivos de la gerencia de riesgos.*

Es importante que los estándares reconozcan que los riesgos presentan un lado positivo y otro negativo.

La gerencia de riesgos no está destinada sólo a las multinacionales y empresas que cotizan en bolsa, sino a cualquier actividad, ya sea de corto o de largo plazo. Las ventajas y oportunidades se deben considerar no sólo en el marco de la actividad empresarial en sí misma, sino también en relación con todos los

interesados en la empresa ("stakeholders"), numerosos y variados, a los que pueda afectar.

Hay muchos modos de conseguir los objetivos de la gerencia de riesgos y resultaría imposible intentar recogerlos todos en un solo documento. Por ello, no se ha pretendido crear una norma imperativa que pudiera desembocar en un enfoque rígido ni tampoco establecer un proceso certificable. Al cumplir las diferentes partes que componen estos estándares, aunque sea de maneras diferentes, las empresas estarán en condiciones de afirmar que se conforman a los mismos.

Los estándares representan la mejor práctica con la que las empresas pueden autoevaluarse. En la medida de lo posible, los estándares han usado la terminología de gerencia de riesgos, establecida por la Organización Internacional de Normalización (ISO) en su reciente documento Guía ISO/CEI 73 Gestión de riesgos - Terminología - Líneas directrices para el uso en las normas.

El riesgo se puede definir como la combinación de la probabilidad de un suceso y sus consecuencias (Guía ISO/CEI 73).

En todos los tipos de empresa existe un potencial de sucesos y consecuencias que constituyen oportunidades para conseguir beneficios (lado positivo) o amenazas para el éxito (lado negativo).

Se reconoce cada vez más que la gestión de riesgos trata tanto los aspectos positivos como los negativos de los riesgos. Por lo tanto, los presentes estándares consideran el riesgo desde ambas perspectivas.

En el campo de la seguridad, se suele admitir que las consecuencias son sólo negativas, por lo que la gestión de riesgos de seguridad se centra en la prevención y en la mitigación del daño.

La gestión de riesgos es una parte esencial de la gestión estratégica de cualquier empresa. Es el proceso por el que las empresas tratan los riesgos

relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el conjunto de todas las actividades.

Una gestión de riesgos eficaz se centra en la identificación y tratamiento de estos riesgos. Su objetivo es añadir el máximo valor sostenible a todas las actividades de la empresa. Introduce una visión común del lado positivo y del lado negativo potenciales de aquellos factores que pueden afectar a la empresa. Aumenta la probabilidad de éxito y reduce tanto la probabilidad de fallo como la incertidumbre acerca de la consecución de los objetivos generales de la empresa.

La gestión de riesgos tiene que ser un proceso continuo y en constante desarrollo que se lleve a cabo en toda la estrategia de la empresa y en la aplicación de esa estrategia. Debe tratar metódicamente todos los riesgos que rodeen a las actividades pasadas, presentes y, sobre todo, futuras de la empresa.

Debe estar integrada en la cultura de la empresa con una política eficaz y un programa dirigidos por la alta dirección. Tiene que convertir la estrategia en objetivos tácticos y operacionales, asignando responsabilidades en toda la empresa, siendo cada gestor y cada empleado responsable de la gestión de riesgos como parte de la descripción de su trabajo. Respalda la responsabilidad, la medida y la recompensa del rendimiento, promoviendo así la eficiencia operacional a todos los niveles.

Los riesgos clave en las organizaciones pueden verse afectados por factores internos y externos y Se pueden clasificar en diferentes categorías de riesgo tales como: de azar, financieros, operacionales, estratégicos, etc.

La gestión de riesgos protege y añade valor a la empresa y sus interesados ("stakeholders") mediante el apoyo a los objetivos de la organización a través de:

- *Proveer una estructura que permite que las actividades futuras se desarrollen de forma consistente y controlada.*

- *Mejorar la toma de decisiones, la planificación y el establecimiento de prioridades mediante una visión integrada y estructurada del negocio, su volatilidad y las oportunidades y amenazas del proyecto.*
- *Contribuir a una asignación más eficiente del capital y los recursos dentro de la organización.*
- *Reducir la volatilidad en las áreas no esenciales del negocio.*
- *Proteger y mejorar los activos y la imagen de la organización.*
- *Desarrollar y apoyar a los empleados y la base del conocimiento de la organización.*
- *Optimizar la eficiencia operacional.*

La política de gestión de riesgos de una empresa debe definir su enfoque y apetito del riesgo, así como su enfoque de la gestión de riesgos. La política también debe establecer las responsabilidades de la gestión de riesgos en toda la organización.

Además, debe referirse a cualquier requerimiento legal para los principios de la política, por ejemplo, en el campo de la salud y la seguridad. Vinculado al proceso de gestión de riesgos, debe existir un conjunto integrado de herramientas y técnicas para usar en las diferentes fases del proceso empresarial.

Para trabajar de forma efectiva, el proceso de gestión de riesgos requiere:

- *El compromiso por parte del presidente y los altos ejecutivos de la empresa.*
- *La asignación de responsabilidades dentro de la empresa.*
- *La asignación de los recursos apropiados para la formación y el desarrollo de una conciencia de riesgos mejorada por parte de todos los interesados.*

El consejo de administración tiene la responsabilidad de determinar la dirección estratégica de la empresa y de crear el entorno y las estructuras necesarias para que la gestión de riesgos opere de forma eficaz.

Esta tarea se puede realizar a través de una dirección ejecutiva, una comisión no ejecutiva, un comité de auditoría o cualquier otra función que se ajuste al modo de operar de la organización y que sea capaz de actuar como "promotor" de la gestión de riesgos.

Al evaluar su sistema de control interno, el consejo debe, como mínimo, tener en cuenta:

- *La naturaleza y extensión de los riesgos negativos aceptables por la compañía que puede absorberlos en su negocio particular.*
- *La probabilidad de que esos riesgos se conviertan en realidad.*
- *Cómo deben tratarse los riesgos inaceptables.*
- *La habilidad de la compañía para minimizar la probabilidad y el impacto en el negocio.*
- *Los costes y beneficios del riesgo y la actividad de control llevada a cabo.*
- *La efectividad del proceso de gestión de riesgos.*
- *La implicación en los riesgos de las decisiones del consejo de administración.*

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 3

Objetivos 4

¿Por qué esta guía? 4

¿Por qué gestionar riesgos? 4

Conceptos clave 6

Riesgo, Probabilidad y Vulnerabilidad 6

Análisis e Implementación 6

Gobierno Corporativo 7

Administración Integral de Riesgos 8

Apetito y Tolerancia 8

Procesos Generales 9

Principales marcos y Estándares 11

Aspectos Relevantes 12

Administración de riesgos clave 14

Riesgo Estratégico 14

Riesgo Financiero 15

Riesgo Operativo 15

Riesgo Cibernético 16

Fraude y Corrupción 17

Responsabilidad Penal de las Personas Morales 18

Responsabilidades Administrativas 19

Riesgo Legal 20

Continuidad de Negocios y la Importancia de su Adopción en las Empresas 24

Relación entre Administración Integral de Riesgos y la Continuidad de Negocios 28

Gestión de Crisis 28

Otras Referencias 30

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:

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

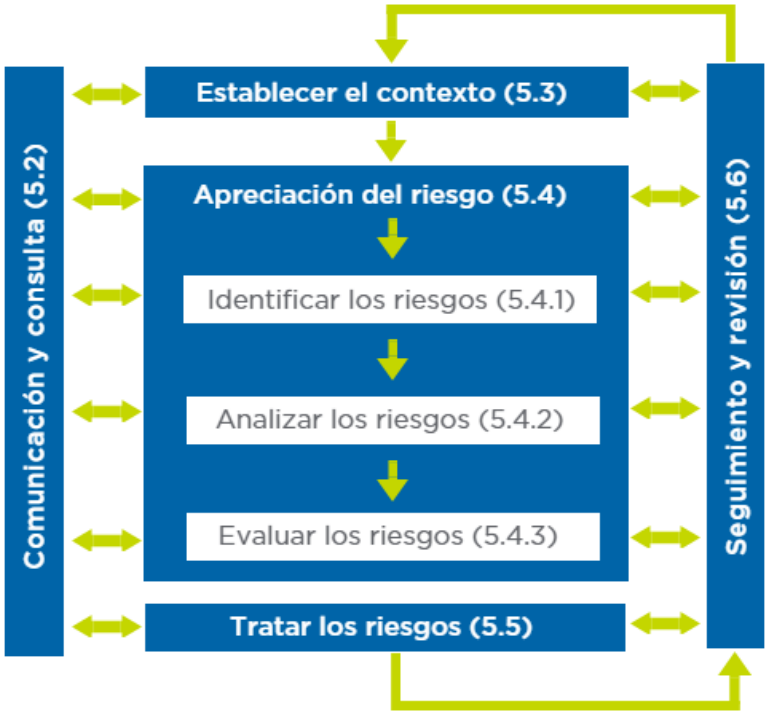
Así que, midiendo la probabilidad y el potencial de impacto, podemos medir la gravedad del riesgo para la organización, y podemos comparar la gravedad de un riesgo con otro. La buena noticia es que estos dos aspectos nos permiten disminuir el riesgo de dos maneras diferentes: minimizando la probabilidad 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

*** *** ***