6

Importancia de medir la delincuencia contra el sector privado para diseñar políticas públicas que prevengan y combatan este fenómeno: algunas de las mejores prácticas

Michael Levi, Stuart Hyde

En este capítulo se analizan las experiencias actuales y concretas en el uso de la información recopilada sobre la delincuencia contra el sector privado, para desarrollar políticas públicas dirigidas a prevenir y limitar el impacto económico que la delincuencia organizada tiene en la comunidad empresarial. Se sugiere adoptar una visión amplia respecto al impacto de la delincuencia en las empresas, incluidos los delitos cometidos fuera del contexto empresarial que afectan tanto a los empleados de todos los niveles como a los clientes. También se examinan las ventajas, los retos y las oportunidades de un enfoque colaborativo para la prevención de la delincuencia empresarial, basándose principalmente en los esfuerzos del Reino Unido y de otros países europeos dentro de una variedad de contextos, como el fraude y la explotación infantil en internet. Se sostiene que la participación del sector privado como verdadero socio trae consigo resultados imprevistos y a veces sorprendentes; sin embargo, tales resultados con frecuencia se ponen en riesgo por la desconfianza mutua —esté o no fundamentada— y la superación de esta desconfianza entre los sectores público y privado representa un proyecto a mediano y largo plazo, cuya referencia más común se encuentra en los países de América Latina.

INEGI. Medición y análisis de la delincuencia contra el sector privado: Experiencias internacionales y el caso mexicano. 2014.

6. Importancia de medir la delincuencia contra el sector privado para diseñar políticas públicas que prevengan y combatan este fenómeno: algunas de las mejores prácticas

Michael Levi,[111] *Stuart Hyde*[112]

6.1 Introducción

En este capítulo se analizan las experiencias actuales y concretas en el uso de la información recopilada sobre la delincuencia contra el sector privado, para desarrollar políticas públicas dirigidas a prevenir y limitar el impacto económico que la delincuencia organizada tiene en la comunidad empresarial. Es un cliché hablar del "problema de la delincuencia", aunque la palabra *delincuencia* como sustantivo colectivo representa una imagen que incluye muchos componentes individuales que pueden estar interconectados, pero que se desglosan de forma útil para combatirlos más efectivamente, al tiempo que se deben tener en cuenta las interrelaciones entre estos componentes. Por este motivo, a menudo se empleará el término *delitos* (plural) en vez de *delincuencia* (singular). Tanto la delincuencia como el miedo de las empresas/sociedad a los delitos son obstáculos importantes para el comercio y la armonía social.

Los enfoques tradicionales sobre la participación del sector privado en el combate al delito y la delincuencia en ocasiones implican estrategias descendentes dirigidas por el gobierno, en las que las empresas privadas se consideran fuentes de recursos alternativos o adicionales, o son vistas como un complemento opcional más que como un socio en condiciones de equidad. En una era de austeridad global, el sector privado puede representar una fuente generosa para el financiamiento de la aplicación de la ley, aunque sus objetivos formales sólo consisten en maximizar las ganancias para sus accionistas clave, lo que en ocasiones puede considerarse un acto antisocial y falta de compromiso con la comunidad.

Se argumenta que, independientemente de que estén dirigidos o no en particular contra el sector empresarial, gran parte de los delitos tienen *impactos* en el sector privado, y que las creencias tradicionales sobre la delincuencia contra el sector privado se centran sobre todo en los ataques depredadores directos que se realizan contra las empresas —lo cual es en sí un problema importante— y deberían enfocarse también al entorno contextual más amplio que afecta las operaciones de las empresas y su rentabilidad. Como se ha demostrado en los capítulos anteriores, estos delitos incluyen el robo, el fraude, el allanamiento y, en años más

111 Profesor de Criminología, Cardiff University (Reino Unido).
112 Jefe de Policía Interino, Comandancia de Policía de Cumbria (Reino Unido).

recientes, los delitos no convencionales, como la extorsión, el soborno y corrupción, y la usura (en los países que la penalizan). Sin embargo, también se incluyen los delitos digitales más modernos que se cometen mediante el uso de la tecnología y cuya escala y velocidad de explotación cambia las dimensiones del riesgo, especialmente desde fuera del país, como en el caso del robo[113] de propiedad intelectual de las empresas, así como el fraude. El aumento de los ataques cibernéticos directos contra las organizaciones financieras y el mal uso de identidades para obtener ganancias financieras de las empresas e individuos ilustran la perspectiva más estrecha de la delincuencia contra el sector privado. Empero, el impacto de los "delitos personales" no puede ser ignorado. Los ejemplos incluyen: un gerente que es asaltado de camino al trabajo; un ingeniero que es víctima de allanamiento de morada; un encargado de limpieza que es arrestado por vender drogas; demostrar una conducta antisocial fuera de un centro comercial; todas estas conductas causan estragos en el lugar de trabajo y tienen un impacto en la actividad empresarial del sector privado. Asimismo, el robo de equipos técnicos o el riesgo de que se haga mal uso de ellos, como el hurto de teléfonos inteligentes o *laptops* de los automóviles de los empleados, amenaza la seguridad digital de una organización. Los capos de la droga que provocan caos en los vecindarios ahuyentan a los clientes y trabajadores por igual. Cualquier delito que ocurra en cualquier lugar afecta el desarrollo y el crecimiento del sector privado. Por tanto, es legítimo, y ciertamente esencial, que las empresas participen en esquemas más generales de reducción de la delincuencia más allá de la periferia de sus empresas, aunque haya límites respecto a lo que pueden lograr por sí mismas.

Se aborda, con cierto grado de incertidumbre, este proceso de transferencia cultural de prevención de la delincuencia contra las empresas. La agenda respaldada en la evidencia (si no es que dirigida) "de lo que funciona" es atractiva, pero las transferencias de la política pública que no toman en cuenta las condiciones variables en principio quizá fallen al aplicarlas, independientemente de que se trate de políticas contra el lavado de dinero, fraude o narcotráfico/delincuencia organizada. Para lograr el cambio, es preciso desarrollar estrategias para contextos particulares, las cuales también deben analizarse cuidadosamente para determinar si podrán funcionar.

Históricamente, los enfoques referentes a la delincuencia organizada en México se han centrado en el narcotráfico y la guerra entre los diferentes cárteles. Se han invertido enormes sumas de dinero para combatir la delincuencia armada organizada, particularmente por parte de Es-

113 El término *robo* no es fácil de definir. Por lo general, si alguien roba un bien, la víctima lo pierde y el autor del robo se queda con él. Sin embargo, en el robo de propiedad intelectual, el ladrón obtiene una ventaja ilícita pero la propiedad sigue estando en manos de la víctima, en tanto que en el caso de los secretos empresariales, el valor del bien disminuye, lo mismo que en el caso del robo de identidad. Por tal motivo, Levi (2013) prefiere emplear el término *reproducción* en vez de *robo*. No obstante, por motivos de simplicidad, aquí se ha utilizado el término *robo*.

tados Unidos, en un afán de proteger su frontera (Ferragut, 2012). Con algunas excepciones, como la ciudad de Monterrey (*The Economist*, 2013), la participación del sector privado se ha visto como un esfuerzo aislado y dirigido a brindar ayuda complementaria en lugar de considerarse como un compromiso total (UNODC, 2010, p. 107).

En muchas investigaciones se ha identificado la dinámica cultural de la corrupción (Morris, 2012), así como su impacto en la estabilidad a largo plazo que puede requerir una legitimidad más amplia mediante la acción contra las élites que ostentan impunidad (Levi, de próxima aparición). Como se muestra en Brasil, China e India, es posible que haya un alto nivel de crecimiento económico junto con un importante nivel de corrupción, pero parece que la fuerte desconfianza en los funcionarios públicos y la aceptación tácita de una gran economía informal mina la capacidad que el sector privado tiene para desarrollarse, lo cual convoca a la aplicación de un enfoque nuevo. Hoy es necesario un mayor entendimiento mutuo entre las organizaciones de los sectores público y privado. Al contar con un enfoque más comprometido habrá riesgos considerables, aunque también grandes beneficios potenciales. El enfoque tradicional de aplicación de la ley para reducir la delincuencia debe evolucionar para incluir la colaboración y el establecimiento de relaciones. Al participar con el sector privado en el control de la delincuencia será posible contar con un enfoque más efectivo que combata el delito y la delincuencia.

En los temas en los que el sector privado ha mostrado tener iniciativa, ha sido en ocasiones a través de políticas públicas alternativas o complementarias. Las empresas de seguridad privada están asumiendo *de facto* el papel de cuerpos policiales en los lugares donde no existen fuerzas policiacas efectivas. Cambiar este modelo implica cierto trabajo. Desarrollar un enfoque más actual para la prevención de la delincuencia requiere que haya más confianza entre las organizaciones de los sectores público y privado, certidumbre que necesita construirse, ya que no puede simplemente asumirse mediante "la importación de políticas públicas" de otros países. Al realizar la transición hacia papeles bien definidos, asistencia mutua y compartir información, en conjunto con un enfoque sensible, se creará un mejor entorno para combatir la delincuencia.

Las empresas del sector privado están obligadas a desarrollar su propia comprensión sobre la forma en que la delincuencia afecta su actividad empresarial, de manera directa e indirecta. Al maximizar las oportunidades para ampliar la comprensión del sector privado respecto a las capacidades y limitaciones de la acción pública será posible crear un entorno de confianza. El enfoque supone un cambio de paradigma: de la separación en igualdad de condiciones a la integración y el compromiso reales; dicho enfoque se ha arraigado en la apreciación común, integral y firme del impacto real de la delincuencia en todos los niveles. En el presente documento se describirá cómo un análisis cuidadoso y la acción basada en este análisis llevan a mejorar el combate de algunas formas de delincuencia contra el sector privado.

Al examinar tres iniciativas en particular —Prevención del Fraude con Tarjetas de Débito y Otras Formas de Fraude, ActionFraud y el Centro de Protección contra la Explotación de Menores en Internet (CEOP, por sus siglas en inglés)— se proporcionarán algunos ejemplos del enfoque empleado en el Reino Unido para incluir al sector privado en la clasificación de prevención de la delincuencia, aunque la última de estas iniciativas está destinada más bien a reducir el daño social en general con la ayuda de las empresas, en lugar de abordar la delincuencia contra las empresas de forma directa. Estas iniciativas identifican las áreas de beneficio mutuo sin poner en riesgo la independencia del esfuerzo de aplicación ni comprometer la sensibilidad comercial. Existen otros proyectos, como los de la Industria de la Extracción y demás iniciativas anticorrupción, que pueden reducir las pérdidas corporativas de las empresas que pagan sobornos mediante la corrupción pública y del sector privado, aunque estas iniciativas no son lo suficientemente conocidas como para tratarlas en este documento.

Se han llevado a cabo esfuerzos más contundentes para tratar de supervisar y reducir la corrupción en el sector público, especialmente en las áreas vulnerables, como la de adquisiciones. Tales esfuerzos incluyen los estudios sobre las inversiones realizadas por la Mafia (http://www.investimentioc.it/); sobre la vulnerabilidad de sectores particulares en Italia, como el de la construcción (Savona, 2010) y las energías verdes (Caneppele *et al.*, 2013); acerca de los sectores de la construcción y de valores en Canadá (Gabor *et al.*, 2012, Hicks *et al.*, 2013); estudios del Barrio Rojo de Amsterdam y otros sectores (Nelen, 2010), y sobre la corrupción de los funcionarios públicos en Suecia (Korsell y Skinnari, 2010). Se han elegido estos estudios, de entre otros, debido a que tienen un impacto particular en las empresas, dejando fuera lo legítimo e incluyendo a las pequeñas y medianas empresas desmoralizadas.

Las iniciativas de ActionFraud y CEOP fueron promovidas desde el principio como sociedades compuestas por el sector industrial y el gobierno, y han elaborado un enfoque que contribuye a la realización de transacciones financieras más seguras y para que los niños cuenten con una mayor seguridad en internet. En ambos casos ha habido desafíos, aunque el poder colectivo conformado por los especialistas de los sectores privado y no lucrativo (de asistencia social) de aplicación de la ley ha facilitado ciertas transformaciones. Las iniciativas de prevención del fraude con tarjetas de débito comenzaron mucho antes (a finales de la década de 1980), y ofrecen un modelo un poco diferente al de las sociedades intraindustriales y, posteriormente, entre las sociedades público-privadas.

Este artículo considera los beneficios, retos y oportunidades de un enfoque de colaboración para la prevención de la delincuencia. Se argumenta que la participación del sector privado como un verdadero socio genera resultados imprevistos y en ocasiones sorprendentes, aunque existe el riesgo de que no haya confianza mutua, independientemente de que esta incertidumbre esté o no fundamentada.

6.2 ¿Qué tipos de delito afectan al sector empresarial en las economías avanzadas, medidos por su gravedad e impacto?

6.2.1 Introducción

En principio, el problema de las empresas y la inseguridad derivada de la delincuencia puede representarse de diferentes maneras. En primer lugar, en términos de las amenazas enfrentadas por las empresas, básicamente:

- diferentes tipos de delito contra la propiedad (robo y fraude cometido por personas externas, robo y fraude cometido por personas internas —quizá en colaboración—, robo de propiedad intelectual y daño delictivo), y
- delitos contra la propiedad y violencia (por ejemplo, el robo que es experimentado como un delito violento, pero cuyo propósito fundamental es económico; y extorsión, incluyendo los "secuestros tigre" de personas).

En segundo, en función del impacto que esto tiene en las empresas y la comunidad, por ejemplo, las decisiones que afectan dónde ubicar a las empresas, lo cual comprende el desplazamiento del centro de la ciudad y de las zonas inmobiliarias dañadas, que tiene efectos tanto en las oportunidades de empleo como en las de compra (y en las de cometer delitos).

En tercer lugar, en cuanto a la preocupación manifestada por las personas en los diferentes estratos de la organización empresarial, desde los empleados de cuello azul hasta la alta gerencia: sus riesgos y temores pueden ser distintos, relacionados con sus intereses económicos o con su capacidad de contar con seguridad adquisitiva. En realidad, el término *temor* debe utilizarse con cautela cuando se trata con una cadena de mando en la burocracia: los empleados de primera línea y el personal de seguridad de las zonas difíciles pueden tener un enfoque cognitivo muy diferente acerca de los lugares peligrosos en comparación con los gerentes de finanzas/gerentes de riesgo que son transportados por choferes con capacitación antisecuestro, quienes se trasladan a las oficinas corporativas desde sus hogares en zonas más tranquilas.

En cuarto, los delitos provocados por la empresa y los efectos que estos delitos tienen, por ejemplo, en cuanto al fraude cometido por los clientes, daños al medio ambiente, y la salud y seguridad en el trabajo; todos estos factores afectan la legitimidad percibida de la empresa en la sociedad, tanto para las personas externas como para los empleados (Tyler, 2006, 2009; Levi, de próxima aparición).

Por último, existen problemas conceptuales respecto al significado de este tema en relación con los riesgos electrónicos que ocurren durante el comercio electrónico en vez de suceder

durante las ventas personales. Por tanto, como mejoró la protección de las cajas fuertes, los delincuentes deben reconsiderar el robo de transeúntes a mano armada, el hurto en comercios o la reducción del "botín" esperado y concentrarse ahora en las camionetas y camiones que distribuyen productos a los clientes o establecimientos de ventas al menudeo/mayoreo. Estas actividades pueden surgir en los puntos cercanos a los hogares de los clientes, aunque también se presentan cerca de los lugares de distribución, cuando las cargas de mercancía están en su nivel máximo.

Respecto al volumen, en el sector de comercio al menudeo, la delincuencia es dominada por los robos pequeños cometidos por el personal y personas externas aunque, en términos de valor, el fraude cometido por la alta gerencia, incluidos los directores, es más significativo. Algunos de estos delitos pueden realizarse "en beneficio de la empresa", al manipular los datos de desempeño para que la compañía continúe con sus actividades o para evadir impuestos, pero a veces sólo son excusas para los actos que también benefician a la gerencia personalmente. De igual manera, el fraude y el lavado de dinero derivados de otros delitos son actividades que pueden ser facilitadas por los sectores de servicios profesionales y financieros, ya sea a través de despachos nacionales o internacionales.

Los efectos que el temor tiene en las empresas y los daños colaterales que esto implica para la población urbana aún no se han investigado con suficiencia, ya sea de manera empírica o conceptual, pero cabe destacar que en un estudio sobre las actitudes ante la delincuencia y la vigilancia policiaca en una zona de la fuerza policial del norte y el sur realizado a principios de la década de 1980, Jones y Levi (1983) pidieron a las personas que clasificaran las prioridades de vigilancia policiaca en su jurisdicción. Uno de los encuestados, una persona de bajos recursos del centro de la ciudad, clasificó el allanamiento de las empresas como la mayor prioridad para la policía, y se le siguieron planteando preguntas bajo el supuesto de que se había confundido respecto a la escala de uno a cinco y se equivocó al contestar. Sin embargo, explicó que debido al alto riesgo de allanamiento, nadie estaba dispuesto a abrir comercios en su zona, lo cual reducía tanto las oportunidades de empleo como las de compra a nivel local.

En su análisis sobre la delincuencia contra el sector privado en América Latina, Mugellini (2012) sugiere dos tipos de delito: los que afectan a las empresas y los que afectan a los individuos como resultado de trabajar en estas empresas. Sin embargo, en la práctica, los problemas no son tan nítidos como lo sugiere esta tipología. Por ejemplo, un empleado puede ser asaltado a punta de pistola para quitarle objetos de valor que no tengan ninguna relación con la empresa donde trabaja. No obstante, el impacto de la delincuencia, en términos de una menor productividad, temor o pérdida de ingresos, puede ser considerable.

La delincuencia contra las empresas a menudo se define en función del delito económico cometido contra empresas individuales (véase Sjögren y Skogh, 2004, pp. 1-2). No obstante, la delincuencia que afecta a las empresas implica una categoría mucho más amplia que ésta. Por

ejemplo, se considera una situación en la que un empleado es asaltado para quitarle una *laptop* de la empresa, implicando daños al empleado y la pérdida de un equipo. La *laptop* es simplemente un artículo comercializable y su contenido digital podría tener poco o ningún valor adicional (a menos que tuviera información de propiedad intelectual o datos personales que se pudieran convertir en dinero *para el delincuente y su red de contactos*). Sin embargo, esta situación podría representar una pérdida de productividad para la empresa, causar alteraciones al entorno laboral y un trauma para la víctima. Una interpretación más completa del problema podría incluir todos los impactos causados por la delincuencia, por ejemplo, daños físicos a la propiedad, así como el costo implícito por la interrupción de la actividad empresarial. Se tendría que abordar tanto la victimización como el impacto en el personal. Por último, debe ponerse atención en los costos incrementados para contar con seguridad adicional.

Los índices de victimización sólo cuentan una parte de la historia. Se esperaría que la probabilidad de que una empresa se convierta en víctima de la delincuencia sea mucho mayor en comparación con las personas, ya que las empresas —a menos de que sean muy pequeñas— son mucho más grandes que las personas, hogares o automóviles, y representan objetivos deseables para los delincuentes. Éste es, de hecho, el caso de países como México (Mugellini, 2012, y datos del Banco Mundial, http://www.enterprisesurveys.org/Data/ExploreEconomies/2010/mexico#crime). Los estudios, incluyendo el de Mugellini (2012) y la ENVE, demuestran que aproximadamente una cuarta parte de las empresas son víctimas de algún tipo de delitio una vez al año, mientras que el índice de victimización de personas es de aproximadamente uno entre 15 para el país en su totalidad; como en todo el mundo, los riesgos para las personas varían considerablemente dependiendo de su ubicación geográfica.

Analicemos un caso hipotético obtenido de uno real. Tubeflus es una unidad industrial pequeña ficticia donde se fabrican tubos de polietileno para la industria automotriz. Cuenta con 20 empleados y los suministros se entregan por la mañana, mientras que los productos para automóviles salen de la fábrica por la tarde. Los suministros se entregan "justo a tiempo" por lo que se conserva un pequeño inventario en la unidad. Cierta tarde, el supervisor de piso y encargado de las llaves de esta unidad estuvo en algunos bares y fue lesionado cuando ocurrió un tiroteo. Después de ser llevado al hospital, siguió inconsciente y no llevaba consigo ningún documento de identificación. A las siete de la mañana el personal de piso llegó a trabajar pero el lugar estaba cerrado. Mientras tanto, se realizó una búsqueda para encontrar al supervisor. A las ocho de la mañana, la entrega diaria llegó pero no se pudo descargar el material en la unidad, perdiendo así los suministros de un día y haciéndose acreedor a una sanción por parte del proveedor. Al mediodía se encontró un juego adicional de llaves y fue posible abrir la unidad, pero la productividad llevaba un retraso y uno de los empleados tuvo que darse a la tarea de localizar al supervisor. Desafortunadamente, el supervisor había perdido las llaves. El turno vespertino fue cubierto mediante el pago de horas extra al personal y se incurrió en un cargo por entrega extemporánea por los productos que salieron de la unidad a las 7 p.m. y no a las 4 p.m. Los costos para la empresa por concepto de la delincuencia se pueden resumir de la siguiente manera:

- Ausencia del supervisor durante cuatro semanas.
- Cargo por penalización de aceptación tardía de la entrega.
- Cargo por penalización de entrega tardía del producto.
- Costo de mandar hacer llaves nuevas y controles de alarma.
- Costo de horas extra para cumplir con el programa de entrega.

Aunque podrían incluirse en una encuesta de victimización individual o quizá en un reporte policiaco de delito, ninguno de éstos aparecería como parte del costo de la delincuencia cometida contra la empresa. Esto podría ser correcto en términos analíticos, pero lo que implica es que la empresa tiene un interés directo en las actividades de prevención de la delincuencia que afectan a la comunidad (por supuesto, la comunidad no es responsable de la comisión de estos delitos).

Algunos ejemplos similares ilustran este punto:

- Una persona que trabaja en un bar es víctima de violencia doméstica debido a un ataque perpetrado por su pareja en casa. Este empleado no puede ir a trabajar ni avisar con anticipación, lo que genera costos adicionales para buscar a alguien que lo sustituya. El empleado tiene un justificante de ausencia por enfermedad durante cuatro semanas y se ha convertido en una persona muy introvertida que requiere apoyo en el trabajo.
- Un empleado de un establecimiento comercial es arrestado por delitos relacionados con las drogas, lo que provoca que se lleve a cabo una búsqueda en el casillero de este empleado en el trabajo. Esto, a su vez, ocasiona una interrupción y desvío respecto a la actividad principal del establecimiento. El empleado ha estado distribuyendo cocaína entre sus compañeros, poniendo en riesgo su estado de alerta mientras trabajan con equipos.
- A un empleado del área de servicios financieros le robaron una *laptop* durante un allanamiento a su hogar. Los datos de la *laptop* se perdieron, y estos incluían datos personales de los clientes. Como consecuencia de esto, varios clientes se cambiaron a una empresa de la competencia.
- Un empleado de una fábrica fue agredido sexualmente por un compañero de trabajo, lo que provocó el arresto del agresor en el lugar de los hechos y la hospitalización de la víctima.

Ninguno de los ejemplos anteriores cuenta como delincuencia contra las empresas, aunque su comisión implicaría costos y el uso de recursos para las empresas involucradas. Invertir en elementos de protección del personal fuera del lugar de trabajo obviamente puede ayudar a reducir la vulnerabilidad de las personas y de las empresas.

La mayoría de los sistemas de registro de delitos (por ejemplo, los que se utilizan en el Reino Unido) identifican a la víctima y al delincuente. Sin embargo, no identifican el *impacto* colateral que se presenta en el establecimiento comercial (en los demás tipos de víctima). En ocasiones,

el simple uso de palabras clave o *hashtags* en los sistemas de registro puede ayudar a identificar el impacto que se tiene en los grupos homogéneos, como los de estudiantes. Estos datos se han utilizado para estudiar la vulnerabilidad e identificar las estrategias específicas de la delincuencia basada en estudiantes. Sin embargo, estos datos sólo abarcan la consecuencia directa y no el impacto secundario. En un contexto empresarial, es necesario realizar trabajo adicional para abordar el impacto indirecto que la delincuencia tiene en el lugar de trabajo. Puede resultar útil en este sentido tomar en consideración el patrón de la delincuencia en una empresa. Aunque es relativamente fácil identificar ciertos robos en un establecimiento comercial —por ejemplo, el número de ladrones atrapados—, habrá un nivel de robos no identificados debido a la colaboración de los empleados con el robo o a la negligencia. Los bienes faltantes se pueden denominar de manera eufemista como "merma de inventarios", y esto se relaciona con los daños o pérdidas. La merma de inventarios por lo general corresponde a 2% y 3% (Bamfield, 2010). Si bien la proporción de pérdidas derivadas de los "robos" internos es un tanto diferente dependiendo del país y continente, el principio básico sigue siendo el mismo. El personal es responsable de una proporción bastante significativa del robo/merma de inventarios (y de peculado, casi por definición). Aunque se debe ser escéptico respecto a los costos del robo de propiedad intelectual que surgen debido a las actividades de *hackers* externos (Detica, 2012) en comparación con la corrupción interna, en la medida que las economías mejoran, generan más valor agregado a partir de la propiedad intelectual durante el proceso de producción, y esta corrupción interna en materia de propiedad intelectual y actividades de *hackers* externos para extraer propiedad intelectual son relevantes en México, a pesar de que no se trate de un objetivo de alto perfil en comparación con los países industrializados tecnológicamente avanzados de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

La delincuencia contra las empresas representada por el robo interno tiene menos probabilidades de ser denunciada a las autoridades ya sea por la falta de confianza o por la falta de motivación de la empresa. Puede ser más rápido simplemente despedir al empleado sospechoso y seguir con las actividades comerciales que denunciarlo formalmente por el delito de robo. Se sabe que la probabilidad de que el robo interno sea procesado penalmente es baja. Para hacer frente a estos tipos de amenaza por parte del personal interno, las empresas deben desarrollar estrategias para abordar la prevención, proporcionar capacitación para el personal y considerar la posibilidad de contar con vigilancia electrónica. También pueden —sujeto a las reglas de protección de datos— conservar bases de datos del personal que sea despedido o a quien se le prohíba seguir trabajando para la empresa por demostrar su falta de honradez, siempre y cuando estas bases de datos no se conviertan en una "lista negra" para los empleados que insistan en conservar sus derechos. (El Servicio de Prevención de Fraudes del Reino Unido [CIFAS, por sus siglas en inglés,y que se tratará más adelante] conserva una base de datos de "fraude cometido por empleados", teniendo en cuenta la premisa aprobada por el Comisionado de Información del Reino Unido.) Bajo un modelo público/privado de políticas que funcione con más eficiencia, la organización se puede beneficiar de dos fuentes de información: el Estado y las demás empresas.

Las empresas del sector privado se enfrentan a una variedad de amenazas delictivas, lo cual incluye a su personal y a personas externas, así como a los ataques directos y los efectos indirectos contra terceros y empleados/directores mientras se encuentran fuera del lugar de trabajo. En el cuadro 6.1 se presenta las relaciones mediante ejemplos sencillos.

Cuadro 6.1

Relación de las amenazas directas e indirectas contra el sector privado

AMENAZAS DE LA DELINCUENCIA CONTRA EL SECTOR PRIVADO	INTERNAS	EXTERNAS
DIRECTAS	El empleado es el delincuente y el empleador es la víctima. Por ejemplo: robo de bienes cometido por un empleado, como el robo de efectivo de la caja, herramientas de oficina, o la transferencia fraudulenta de fondos.	El empleado/empleador puede ser la víctima de un delincuente externo. Por ejemplo: robo a una tienda, allanamiento de un edificio de oficinas, o daños criminales a las instalaciones de una empresa.
INDIRECTAS	El empleado es el delincuente y el empleador no es la víctima. Por ejemplo: pelea entre empleados provocando una agresión, o empleado que es sorprendido comerciando drogas y que es detenido por la policía.	El empleador es la víctima principal del delincuente externo. Por ejemplo: el empleado no puede trabajar por estar lesionado después de un atraco en un bar. La violación de un empleado que se dirigía al trabajo. La respuesta de la policía a un tiroteo a unas cuadras de la empresa evita el acceso físico a ésta.

Fuente: Stuart Hyde (Análisis propio 2013).

El presente documento analizará estos conceptos en el contexto mexicano.

6.2.2 Percepciones de la delincuencia en América Latina

Los estudios realizados por Di Tella *et al.* (2010) y el Latinobarómetro (2012 y años anteriores) indican el importante sitio que la delincuencia ocupa en América Latina en comparación con otras regiones del mundo, así como el bajo nivel de confianza que la población latinoamericana en general tiene en la policía de su localidad (aunque no se sabe si esto aplica respecto a los empresarios). Según los sondeos de opinión levantados por el Latinobarómetro (2012), la seguridad pública es la principal preocupación de la población o bien la segunda más importante después del desempleo (véase gráfica 6.1).

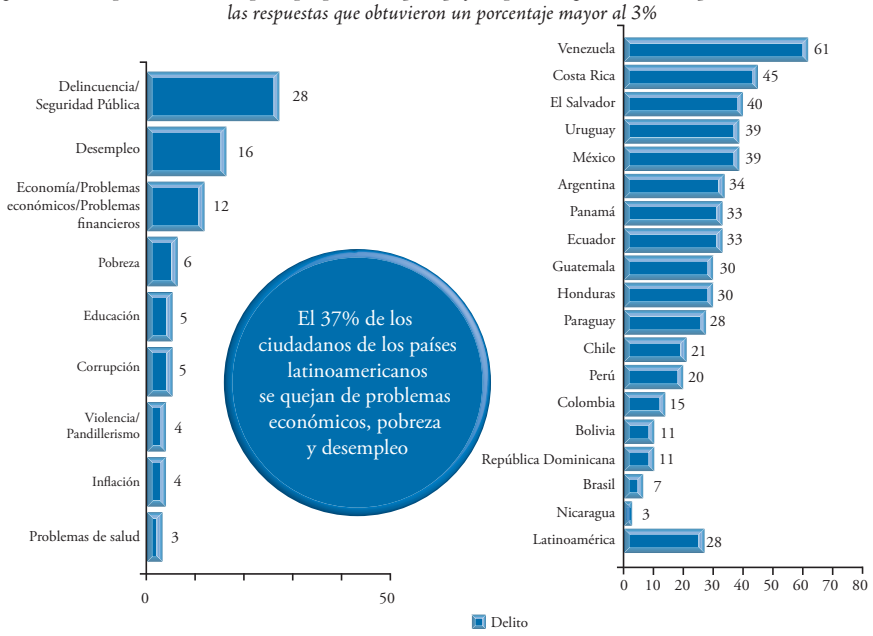
Gráfica 6.1

Importancia relativa de los problemas socioeconómicos a los que se enfrentan los países de América del Sur

Principal problema del país

Totales de Latinoamérica 2011 - Totales por país 2011 con respecto al delito

Pregunta: En su opinión, ¿cuál es el principal problema que aqueja al país? Pregunta abierta: aquí se muestran únicamente las respuestas que obtuvieron un porcentaje mayor al 3%



Fuente: Informe 2011 de Latinobarómetro (2012), Santiago de Chile, Corporación Latinobarómetro

El impacto que la delincuencia tiene en la economía es tan grande que se estima que el PIB sería hasta 25% mayor si el índice delictivo en América Latina fuera el mismo que el de otras regiones. Existen tres canales mediante los cuales la delincuencia puede generar pobreza: reducir las inversiones, presentar pérdidas de bienes, y reducir el valor de los bienes que siguen bajo el control de los hogares. Al usar datos sobre la variación de secuestros que tienen como objetivo a los gerentes de las empresas en diferentes regiones de Colombia, Pshisva y Suárez (2010) se encontraron que las empresas realizan menos inversiones cuando los secuestros están dirigidos directamente a estas empresas, y que no hay efecto alguno cuando existen otros tipos de delito violentos que no están dirigidos expresamente a las empresas como homicidios, ataques por parte de la guerrilla y secuestros en general. El efecto estimado en una empresa es mayor en el caso de los secuestros experimentados por otras empresas de la misma industria. La inversión en las empresas donde el capital extranjero es considerable es particularmente sensible al secuestro de los gerentes y propietarios extranjeros.

El papel de la delincuencia y el temor asociado a ella es un fenómeno complejo. Innes (2004) ha desarrollado un modelo de "manifestaciones delictivas" que se refieren a los delitos particu-

lares que ejercen un efecto importante en la pobación ya que tocan una parte simbólica. Las percepciones públicas de lo que el Latinobarómetro (2012) considera como tareas pendientes para la democracia, incluyen la reducción de la corrupción (48%), garantizar la justicia social (33%), incrementar la participación ciudadana (31%) y aumentar la transparencia del Estado (31%). En Colombia, Argentina, Perú y Paraguay, cerca de 60% identifican la reducción de la corrupción como una tarea pendiente, mientras que en El Salvador esta cifra sólo llega a 29%. En 2011, la confianza interpersonal aumentó en dos puntos porcentuales para ubicarse en 22%, volviendo así al nivel que tenía en 2006. Por otro lado, en los países de Europa, este indicador alcanza casi 70%, lo que marca una de las diferencias principales entre estos países y los latinoamericanos. La confianza esta conformada por dos componentes: la confianza en las personas y la confianza en las instituciones.

Respecto a la confianza en las instituciones, ésta es particularmente baja en América Latina, un hecho que obstaculiza seriamente el trabajo en conjunto entre el sector público y el privado. Debe notarse el ligero incremento respecto a la confianza en los bancos (aunque sigue siendo de sólo 43%; representa un enorme incremento si se considera que en 2003 era de 29%), y la ligera disminución respecto a la confianza en las empresas privadas y la policía.

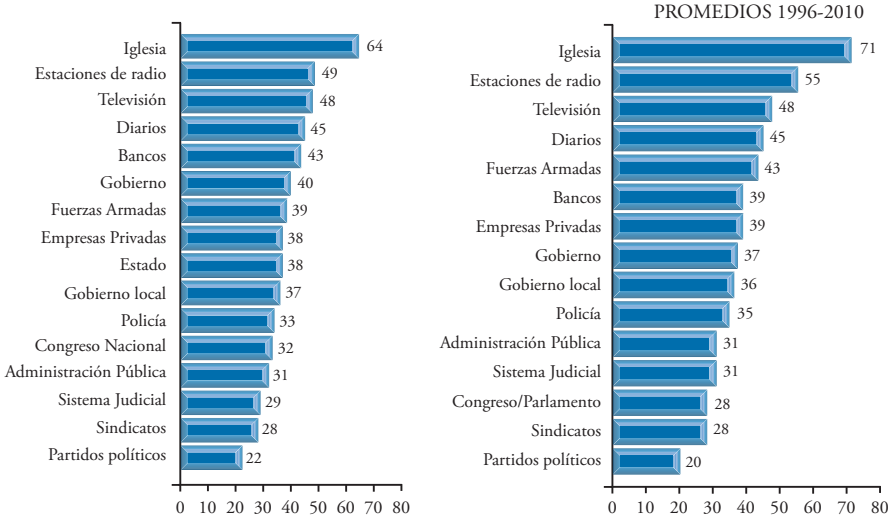
Gráfica 6.2

Confianza en los grupos e instituciones nacionales en América del Sur

Confianza en...

Total en Latinoamérica 2011

Favor de revisar esta tarjeta y dígame, ¿qué tanta confianza tiene en cada uno de los siguientes grupos/instituciones? ¿Diría usted que tiene mucha, algo, poca o nada de confianza? Sólo se incluyen las respuestas "mucha" y "algo" en esta gráfica.



Fuente: Informe 2011 de Latinobarómetro (2012), Santiago de Chile, Corporación Latinobarómetro

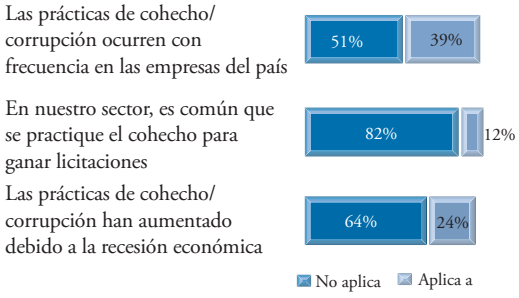
Es interesante que la confianza en las empresas privadas sea mayor que la confianza en la policía. Esta información puede tener un valor real al justificar que el sector privado desempeñe un papel mayor para abordar la delincuencia. Es posible que la población tenga más probabilidades de confiar en la participación del sector privado que en la de otros interesados, como la policía.

6.2.3 Comparaciones internacionales de la delincuencia corporativa en el contexto de América Latina

En años recientes, se ha presentado un crecimiento en el número de encuestas internacionales de victimización de empresas, las cuales abordan los delitos cometidos por las empresas y contra ellas. Cuando están bien diseñadas, aunque muchas no lo están (para un estudio de este tema véase Levi *et al.*, 2007), son útiles en términos de comparación. No siempre es claro en las encuestas si las respuestas tratan sobre victimizaciones reales o sentencias; hay más ambigüedad inherente sobre la interpretación, lo que hace que los datos sean más inciertos en comparación a la victimización en los hogares y en la vía pública. Además, el conocimiento ejecutivo varía dependiendo del tiempo y el lugar. Ernst & Young (2013) contribuye con el siguiente estudio de altos ejecutivos (N = 176 en América Latina) cuyas percepciones se combinan con la experiencia (gráfica 6.3).

Gráfica 6.3

Comparación del cohecho y corrupción en varios países



	% aplica a					
	Brasil	China	República Checa	Indonesia	México	Turquía
Las prácticas de cohecho/ corrupción ocurren con frecuencia en las empresas del país	84	14	80	72	60	52
En nuestro sector, es común que se practique el cohecho para ganar licitaciones	18	8	12	36	38	6
Las prácticas de cohecho/ corrupción han aumentado debido a la recesión económica	20	26	8	52	44	56

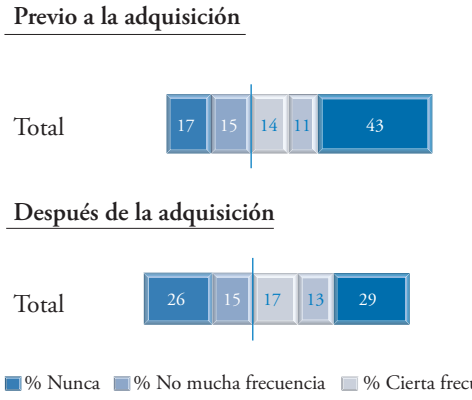
Pregunta: En el caso de cada uno de los siguientes elementos, ¿podría decirme si usted cree que aplica o no aplica a su país/industria, o si es que no sabe?
Base: Todos los encuestados (1,758)
Los porcentajes correspondientes a ¨no sabe¨ o ¨se negó a responder¨ fueron omitidos para permitir una mejor comparación entre las respuestas dadas. Los resultados de China incluyen a Hong Kong.

Fuente: Ernst & Young (2013). "Growing Beyond: a place for integrity", XII Encuesta Global sobre el Fraude, Londres, Ernst & Young.

Las empresas mexicanas se ubicaron en la segunda posición, sólo después de las empresas estadounidenses, por su debida diligencia en los riesgos de fraude y corrupción, antes y después de hacer adquisiciones (gráfica 6.4).

Gráfica 6.4

Frecuencia de la implementación de la debida diligencia en los riesgos de fraude y corrupción



% de mucha frecuencia / siempre

	Previo a la adquisición	Después de la adquisición
China	32	29
República Checa	9	8
Japón	33	11
México	56	51
Nigeria	9	8
EU	84	59

Pregunta: ¿Con qué frecuencia su empresa ha llevado a cabo la debida diligencia con respecto a los riesgos de fraude y/o corrupción antes de adquirir un nuevo negocio en los últimos dos años?
Pregunta: ¿Con qué frecuencia su empresa ha llevado a cabo la debida diligencia con respecto a los riesgos de fraude y/o corrupción después de adquirir un nuevo negocio en los últimos dos años?
Base: Todos los encuestados indicaron haber adquirido algún negocio (975)

Fuente: Ernst & Young (2013). "Growing Beyond: a place for integrity", XII Encuesta Global sobre el Fraude, Londres, Ernst & Young.

Casi las tres cuartas partes de los encuestados creyeron que las juntas directivas de las empresas debían comprender mejor a la empresa para poder protegerla contra el fraude, un porcentaje que fue menor en comparación a otros países encuestados con excepción del Reino Unido; y casi la misma cantidad apoyan los esquemas de compensación para la denuncia de irregularidades. Estas opiniones pueden reflejar una actitud severa hacia los riesgos a los cuales se enfrentan las empresas.

El Informe Global sobre Fraude de 2011-2012 (Kroll, 2013) detectó que, como sucedió en el resto del mundo, en México se redujo la prevalencia del fraude, aunque este patrón está cambiando, ya que 26% de las empresas fueron víctimas de robo, pérdida o ataque hacia sus datos, lo cual está por encima del promedio mundial de 21%; 19% fueron víctimas de fraude por parte

de los proveedores o vendedores; 19%, experimentaron el robo de bienes o productos físicos, y 15%, víctimas de corrupción o cohecho (lo que representó una disminución considerable de 37% respecto al año anterior). Colombia presentó cifras idénticas en el caso del fraude en adquisiciones y robo de bienes. Por tanto, en términos generales, Colombia y México tuvieron las cifras más altas en cuanto a este tipo de delitos, que quizá reflejen los elevados riesgos implicados en los sectores del petróleo y la minería. En Brasil, el patrón fue distinto: en este caso "el conflicto de intereses administrativos" (es decir, la autocontratación) obtuvo el mayor porcentaje, que fue de 23%; el robo de bienes o productos físicos alcanzó 17%, mientras que el robo, pérdida o ataque hacia los datos obtuvo 14%. En general, en América Latina, más de la mitad de las empresas habían sido víctimas de por lo menos un episodio de fraude el año anterior (lo que representó una disminución de tres cuartas partes en relación con el periodo 2010-2011). Casi una de cada cinco empresas fueron afectadas por el robo físico, y una de cada seis por incumplimiento en la entrega de datos y por el fraude en las adquisiciones. En el sector de los recursos naturales, se identificó que casi 1% de los ingresos se perdieron por el delito de fraude. En Brasil, 87% de las empresas manufactureras fueron afectadas por el fraude, y se detectó que 1.9% de los ingresos de estas empresas se perdieron debido al fraude.

6.2.4 La delincuencia en México

Todo debate sobre la delincuencia en México tendría que hacer una referencia previa a la guerra contra el narcotráfico. Cruzando una enorme frontera internacional, México tiene al norte el mercado de drogas más grande del mundo, lo que significa márgenes de utilidades provenientes del narcotráfico que superan por mucho los márgenes disponibles en negocios legítimos. Vinculados con una gama de factores sociales (Liu y Taylor, 2012), la participación en la distribución de drogas se convierte en una opción de empleo y un modo de vida para muchas personas a falta de alternativas atractivas y viables. Los delitos que facilitan el transporte y el consumo de drogas pueden llegar a "desplazar" las oportunidades para que las empresas legítimas crezcan y prosperen.

Los índices delictivos relacionados con el narcotráfico que han sido reportados y registrados en México tienen el potencial de causar estragos en las empresas legítimas y crear terceras víctimas. Se recurre a servicios públicos limitados y al uso de financiamiento público para combatir el narcotráfico. El impacto resultante es la reducción de la efectividad del sector privado.

En lo que respecta a la ciudadanía, las prioridades para México, que se mencionan constantemente, son la economía y la inseguridad. Ambos aspectos afectan a las empresas. Se considera que el tema de la pobreza es parte esencial del problema relacionado con la corrupción y la participación en el narcotráfico. La creación de un entorno en el cual las empresas puedan crecer es una estrategia clave para combatir la pobreza y la guerra contra el narcotráfico. A pesar de ser la decimosegunda economía del mundo, su PIB ocupa la posición número 62. Muchos factores demuestran la existencia de una economía que crece, pero que enfrenta problemas sociales. Los

estándares eductivos y la asistencia en educación están mejorando, aunque todavía no alcanzan los niveles que se presentan en una economía equivalente (OCDE, 2012).

Aunque este estudio se realizó hace 10 años y es posible que la información no esté actualizada, Moloeznik (2003) subrayó una variedad de problemas respecto a la competitividad de la economía mexicana, entre los que se incluyen:

- falta de cumplimiento de la ley
- deficiencias en los sistemas financiero y fiscal
- baja calidad de la educación técnica
- inseguridad pública

Se han hecho grandes avances desde 2003 y la prioridad del gobierno actual se ha centrado en la prevención de la delincuencia. Esto último no se debe pasar por alto. Si no se cuenta con un sistema eficaz de registro de delitos en el que confíen las personas y que refleje los niveles delictivos actuales, las estrategias de prevención de la delincuencia no podrán ser evaluadas ni efectivas. Es importante generar cifras que sean válidas a nivel local, y la credibilidad general de las estadísticas de la delincuencia es un asunto preocupante independientemente de la calidad objetiva de la investigación. Éste es un asunto que corresponde a la Autoridad de Estadística del Reino Unido, del que el autor principal es miembro independiente, y parece ser un asunto que también deben abordar México y los demás países latinoamericanos. El gobierno del Reino Unido esta preocupado por la falta de credibilidad de la población en los datos policiales y de las encuestas de victimización que indican una disminución en la delincuencia.

El nivel de inseguridad existente sugiere que un desafío efectivo contra la criminalidad, esto es, que sume y entregue resultados a la población mexicana, tendría un impacto desproporcionado. Sin embargo, debido a que 60% de los mexicanos declaran que la gente no respeta la ley y que casi 50% no desea intervenir en la prevención de la delincuencia, parece que el camino por recorrer es largo. Al afianzar las fortalezas del sector privado, la participación local puede ayudar a crear una solución más completa (Moloeznik, 2003).

Generar confianza en la policía es un reto igualmente importante para la participación en la prevención de la delincuencia. La Encuesta Mundial de Valores (2000) y las encuestas subsecuentes de Latinobarómetro indican que la confianza que los mexicanos tienen en sus fuerzas policiacas está por debajo del nivel de confianza que tienen en los medios y el gobierno. Las empresas y la población pueden compartir la falta de confianza en la policía. Para asegurar la participación del sector privado, las partes interesadas en el sector empresarial deben tener un mayor nivel de confianza en la aplicación de la ley.

El Instituto Nacional de Estadística y Geografía (INEGI) publicó los resultados de su Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2012, que

indica un índice de falta de denuncia de 92%, debido principalmente a la falta de confianza en la policía y los tribunales. Es importante conocer los niveles delictivos reales para desarrollar estrategias efectivas de reducción de la delincuencia. Con base en los datos actuales sobre la delincuencia, se estimó que 20 millones de delitos no son denunciados (INEGI, 2012). Para facilitar y mejorar el índice de denuncia, los centros de registro externos no gubernamentales pueden ofrecer una alternativa eficaz. Los centros externos alientan a la ciudadanía a denunciar los delitos de una forma independiente a la policía, y esto es algo que debe llevarse a cabo incluso si no se cuenta con un seguro a manera de incentivo para denunciar. Es esencial contar con normas de registro precisas y completas para crear la base de conocimientos necesarios para elaborar estrategias eficaces de reducción de la delincuencia. Existe una oportunidad clara para que el sector privado ejerza un papel como organismo para registrar y transferir los datos a nombre de las autoridades encargadas de la aplicación de la ley.

La encuesta del INEGI incluyó las respuestas a los delitos e identifica las estrategias de respuesta que se emplean con mayor frecuencia para la prevención de la delincuencia. Estas estrategias son: un mayor patrullaje por parte de la policía, mejoras en la iluminación, dirección de operaciones, combate al narcotráfico, circuitos cerrados de televisión (CCTV) y programas de carácter informativo. El análisis de los datos sin procesar de la encuesta identifica un alto nivel delictivo contra las empresas y el sector privado. El porcentaje de delitos que ocurren en la ubicación de las empresas del sector privado es alto (62%), en los casos en los que fue especificado. Una proporción pequeña se relaciona con los delitos que ocurren antes o después de una entrega hecha en la unidad empresarial. Esto indica que si el sector privado fuera capaz de informar directamente, sería mucho más fácil establecer un sistema de registro de delitos más sólido. Es importante resaltar que el sistema debería estar diseñado para ser dinámico, dando a las empresas del sector privado la oportunidad de observar lo que sucede ya sea en la localidad o en el sector donde se ubican. Una iniciativa precisa de denuncia contribuirá a crear estrategias de reducción y prevención de la delincuencia.

El INEGI y la UNODC han creado una hoja de ruta para la creación de un plan más estricto a fin de mejorar la calidad y cantidad de las estadísticas sobre la delincuencia en los niveles nacional e internacional (UNSC, 2013). Contar con una clasificación común ayuda a generar el conocimiento y entendimiento para crear estrategias de prevención efectivas. Esto también conduce al registro congruente y a los datos en los que las personas pueden confiar. Los datos referentes a la victimización de empresas —sean registrados por la policía u obtenidos mediante encuestas— podrían clasificarse por sector, dependiendo de qué tan similares o diferentes sean los riesgos a los que se enfrentan, y podrían desglosarse aún más de acuerdo con áreas de delito que sean útiles para las intervenciones (Levi *et al.*, 2007).

Ferragut (2012) describe la rentabilidad del lavado de dinero que procede de los mercados del narcotráfico. En lugar de que la propia delincuencia sea quien controle las drogas, o cualquier otro producto ilícito, el autor demuestra el valor que representa el que una empresa, que

de otra manera sería legítima, administre el dinero resultante de las transacciones. Por otro lado, las empresas que no están dispuestas a colaborar pueden ser víctimas de mecanismos menos discrecionales, como las amenazas o la extorsión (Ferragut, 2012). Las organizaciones legítimas del sector privado pueden ocultar el crecimiento deficiente o las caídas en las ventas al inyectar las ganancias en efectivo provenientes de la venta de drogas (aunque los sindicatos criminales deben tener cuidado de que las empresas no sean tan poco rentables que quiebren y, en consecuencia, los delincuentes pierdan su dinero). El trabajo de Ferragut (2012) describe el porcentaje probable de rentas obtenidas al ocultar dinero mediante un negocio. Aunque gran parte del sector privado en México está conformado por empresas que son propiedad de familias, es posible crear una ventaja competitiva al producir márgenes mucho mayores mediante el uso de pequeñas cantidades de dinero que está casi libre de riesgos. En México, el papel del sector privado en el combate contra los problemas de narcotráfico implica tanto ventajas como desventajas. La participación de este sector en las estrategias antidelito puede provocar que estas empresas llamen la atención de los cárteles, o hacerlas vulnerables a la tentación de recibir inyecciones de efectivo de los cárteles como parte del proceso de lavado de dinero, ya sea como socios silenciosos o simplemente como parte del proceso de colocación y diversificación.

La gobernanza de la banca y las ganancias del sector financiero proporcionan cierta protección pero, como lo indica HSBC, Wachovia y los escándalos anteriores de Citibank durante el sexenio de Salinas, éstas no son suficientes por sí mismas para prevenir los delitos financieros como el lavado de dinero. Se han abordado muchos de los impedimentos referentes a la inversión interna en México, incluyendo un conjunto de reformas fiscales y empresariales (Servicios de Riesgo Político, 2012). El gobierno de México ha trabajado arduamente para atraer inversiones. El incremento en el número de tratados comerciales puede preparar el camino de oportunidades para que el sector privado tenga un mayor peso en el enfoque a la delincuencia cometida contra las empresas. A pesar de la sólida agenda de inversión interna y crecimiento, la corrupción se sigue percibiendo. La Encuesta de Empresas 2010 del Banco Mundial (2010) reportó que casi una tercera parte de las personas declararon haber pagado un soborno o una dádiva para ganar una licitación del gobierno. Aunque algunos de los sobornos son pagados para obtener una ventaja sobre la competencia en lugar de hacerlo a través de la extorsión, si cada una de estas transacciones fuese registrada como un delito, el índice oficial de la delincuencia aumentaría en 30 millones. Es indudable que todavía hay muchos retos que deben resolverse, y se requiere congruencia económica para que el sector privado prospere eficientemente. El ofrecimiento de sobornos o el otorgamiento de dádivas para facilitar incluso la más pequeña de las transacciones interrumpen el flujo de trabajo y en cierta medida distorsionan los mercados financieros. A través de sus representantes, las organizaciones del sector privado trabajan para contrarrestar el entorno del soborno, aun cuando algunas también sean infractoras. Actualmente, en Italia existen ciertas iniciativas que no sólamente revisan todos los contratos mediante la verificación de los antecedentes, sino que también exigen que todos los pagos se realicen en forma electrónica e incluyan códigos especiales para demostrar que tales pagos provienen de contratos con el gobierno, y se requiere que las transferencias adicionales sean etiquetadas electrónicamente

para evitar que los miembros de la delincuencia organizada se beneficien y luego laven el dinero. Es muy pronto para poder evaluar la efectividad de esta estrategia, pero su finalidad es alentar a que los contratos se entreguen a empresarios legítimos.

El Informe de Servicios de Riesgo Político (2012) resume los factores que influyen en los niveles de inversión concretamente en México, incluyendo los que son propiedad del Estado o de la iniciativa privada. Es probable que quienes invierten de otros países con un enfoque más integral para la prevención de la delincuencia y la aplicación de la ley tengan una influencia en México. Un modelo moderno que podría involucrar con éxito a las empresas del sector privado como socios atendería de una mejor manera los objetivos e intereses del país. El presente estudio esta sustentado en la experiencia y conocimiento que el autor tiene respecto a las mejores prácticas. Sin embargo, la exploración de las iniciativas locales sirve para enriquecer el desarrollo de una solución específica para México. Vilalta (2013) evaluó la manera en que la población de Ciudad Juárez se enfrentó a la delincuencia a través de la intervención y colaboración de la comunidad. Siendo la segunda ciudad fronteriza más grande de México, Juárez ha experimentado altos niveles de asesinatos que se relacionan directamente con el narcotráfico y los conflictos derivados del pandillerismo. Entre las respuestas al creciente índice de homicidio, más de la mitad de la comunidad estructuró una forma de seguridad privada, quizá por falta de una respuesta de política pública, tratando de evitar acudir a la delincuencia organizada, lo que significaría imponer la autoridad de ésta última. La conclusión de que 11% de los ciudadanos decidieron actuar de manera conjunta con sus vecinos indica su disponibilidad para colaborar a nivel comunitario, por lo menos entre sus grupos de referencia. Sin embargo, no existe evidencia alguna del papel que desempeña el sector privado en la respuesta de la comunidad, y esta información tampoco se encuentra en el análisis hecho por Di Tella (2010). *The Economist* (2013) también ha informado sobre cierta cooperación entre el sector público y privado (iniciada por el privado) en el municipio de San Pedro Garza en Nuevo León, la que hasta la fecha ha resultado efectiva para reducir el número de homicidios y otros riesgos.

Helgesson (2011) analiza el objetivo de crear un entorno donde la participación del Estado y del sector privado sea esencial para combatir el lavado de dinero. Mientras que el artículo examina el modelo sueco de sociedades público-privadas, los principios y las prácticas reflejan su relevancia a nivel global. Las reglas actuales contra el lavado de dinero implementadas en Suecia, y en todos los países desarrollados y en casi todos los países en vías de desarrollo, dependen de una interacción considerable entre las organizaciones del sector privado y las instituciones gubernamentales y financieras, como ocurre en México. Para reducir las oportunidades de lavado de dinero y prevenir o investigar estos asuntos, el Estado requiere que las empresas del sector privado se encarguen de estas actividades, ya sea registrando o dando aviso sobre las actividades potencialmente delictivas.

Debido a que las empresas del sector privado están comprometidas en este nivel para abordar el riesgo y la amenaza evidente para el Estado, las instituciones financieras buscan obtener

algún incentivo por los costos adicionales que se generan al mantener los mercados financieros relativamente limpios, por lo menos antes de que las enormes multas impuestas a los bancos en 2011-2013 las hicieran conscientes de lo que los riesgos financieros y otros riesgos podían causar por hacerse de la vista gorda. El incentivo podría ser el derecho a exigir una posición en el desarrollo de iniciativas de prevención de la delincuencia, aunque esta reforma bajo amenaza de sanción no podría implementarse de inmediato en otras zonas de comercio en las que no existe esta amenaza.

En resumen, existen muchas formas de delito que afectan directa o indirectamente a las empresas en México y en otros países latinoamericanos. La situación es dinámica: el establecimiento de la paz en Colombia no sólo ha promovido la seguridad para las industrias a nivel internacional, sino que también implica menos amenazas a las empresas. Por otro lado, si se copia la estrategia que Irlanda del Norte aplicó después del Acuerdo de Paz, podría reemplazar las amenazas terroristas con delitos organizados menos violentos provenientes de las mismas personas, por lo menos a corto plazo. También existe un problema con la "normalización" de los datos de victimización corporativa en las encuestas. Es sorprendente que haya empresas que no son víctimas de fraude o robo de bienes, ni de infracciones respecto a sus datos, sean o no intencionales. Se requiere mucha concentración y capacitación para *nunca* incurrir en pérdidas de datos, o para que un sistema informático jamás sea atacado por los *hackers*. Lo que puede ser importante es no considerar los delitos contra las empresas como un daño binario (víctima/no víctima), sino más bien reducir la amenaza de que aumente la gravedad e incidencia de los delitos mediante la vigilancia: reducir los riesgos a niveles que sean "aceptables", lo que puede variar dentro y entre sectores y países, ya sea en América Latina o en cualquier otra parte.

6.3 Buenas prácticas en la prevención de la delincuencia en el sector privado

Se realizará una revisión bibliográfica y un análisis de las buenas prácticas en los países socios del G8 y otros países con el fin de identificar ejemplos y opciones que sean específicos del sector privado en la prevención de la delincuencia (incluyendo empresas grandes y PyME). El estudio examinará el origen, organización y eficacia de los centros específicos, como ActionFraude en el Reino Unido, y las iniciativas de control de delitos cibernéticos que suponen la aplicación de la ley tanto en los ámbitos público y privado como en los proveedores y clientes, para individuos y empresas. Se hace una comparación de las probables barreras y oportunidades identificadas en México.

La prevención de la delincuencia puede tener una definición amplia o estricta. En su forma más amplia, incluye un conjunto de factores sociales que pueden ayudar a reducir el impacto de la actividad delictiva, y van desde la educación en el aula para combatir la corrupción (Kenney y Godson, 2002), hasta los enfoques éticos basados en la religión transmitidos a la sociedad e in-

cluso los mensajes subliminales presentados en los programas de televisión. Una interpretación más estricta podría incluir enfoques específicos para evitar el acceso a un inmueble (candados, cerrojos y barretas).

El enfoque contra el fraude del Reino Unido es un ejemplo en el que las empresas han compartido sus datos con el Estado y han utilizado una vigilancia más elaborada en conjunto con los delitos denunciados. ActionFraud fue desarrollado después de la fuerte crítica que se dio en torno al enfoque incompatible y desarticulado respecto al registro e investigación del fraude en las 43 fuerzas policiales del Reino Unido. Para abordar estos retos, las instituciones financieras acordaron combinar sus datos referentes al fraude en un centro de inteligencia nuevo. El Buró Nacional de Inteligencia en Materia de Fraudes es administrado por la policía de Londres. Mediante software comercial y una base de datos segura, el centro obtiene datos de los sectores de la industria de servicios financieros y elabora un reporte directo a través del centro de atención telefónica de ActionFraud o de una herramienta en línea. El resultado neto es que todas las denuncias de fraude son estandarizadas y luego se comparan con los datos existentes conservados por la industria como efecto de su acción no competitiva basada en el intercambio de datos bajo el principio de que "el fraude no es un asunto de competencia" (Levi *et al.*, 1991). La estrategia de prevención del fraude está ligada al enfoque de ActionFraud. El alcance de la estrategia se ha ampliado para que incluya el registro de los delitos en línea. El personal de seguridad del sector privado, representativo de los organismos industriales colectivos, trabaja en conjunto con la policía para proporcionar datos y usar los datos agregados a fin de priorizar los esfuerzos colectivos de prevención. Los datos en tiempo real que indican una "acción delictiva" pueden —en la medida en que los recursos lo permitan— llevar a la detección y arresto de los delincuentes (véase Doig y Levi, 2013).

Reducir las oportunidades para la comisión del fraude es conveniente para todos: gobierno, industria y consumidor. Al unir los elementos, el enfoque puede crear soluciones para las nuevas actividades fraudulentas antes de que éstas sean un problema mayor. La superación de la falta de confianza y las barreras jurídicas implicadas en su creación requirió negociaciones delicadas entre todas las partes involucradas, lo que se analizará posteriormente en este documento.

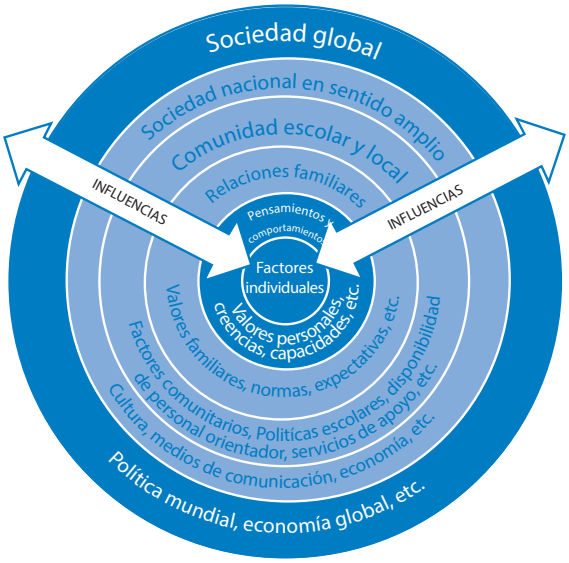
De manera histórica, los enfoques incompatibles usados para contrarrestar el fraude resultan ineficaces. Una de las diferencias clave que caracteriza el enfoque de ActionFraud es el compromiso para involucrar a la industria como un socio implicado en términos de equidad. La participación de la industria se ve como algo más que un simple patrocinio comercial, es un elemento operativo clave. Se trata de un cambio abismal en el enfoque para combatir el fraude.

En esta sección se comparan varios enfoques de las Estrategias de Prevención de la Delincuencia a nivel nacional en el Reino Unido, y se busca identificar los problemas que tienen una relevancia específica para el sector privado en México. El debate inicial se centra en el Manual de

las Directrices para la Prevención de la Delincuencia (de las Naciones Unidas), que se publicó en 2010. Este manual es un recuento integral de un conjunto de enfoques en todo el mundo, incluyendo tanto a países desarrollados como en vías de desarrollo. Su argumento central es el valor de invertir de manera proactiva en la prevención de la delincuencia en lugar de invertir en recursos de justicia penal reactiva. El lineamiento está dirigido a los gobiernos centrales y a los países donantes o a las instituciones que ofrecen apoyo a otros, en particular a los países en vías de desarrollo. El análisis presentado en el Manual de las Naciones Unidas sugiere un conjunto de iniciativas y de mejores prácticas. No obstante, la descripción de la relación entre un "conjunto de factores influyentes" sobre la prevención de la delincuencia no incluye el impacto sobre las organizaciones del sector privado (véase diagrama 6.1).

Diagrama 6.1

Factores que influyen en la delincuencia



Fuente: UNODC (2010). Crime Prevention Handbook on the crime prevention guidelines: Making them work, Viena, ONU.

De acuerdo con el enfoque de situaciones, el Manual de la ONU describe las estrategias que pueden tener un impacto en la reducción de la delincuencia mediante una de cinco opciones, que incluyen las estrategias que, con base en el modelo Británico de Reducción de la Delincuencia, fueron desarrolladas por Ron Clarke y otros en el Ministerio del Interior:

- aumentar los esfuerzos de los delincuentes
- aumentar los riesgos para los delincuentes

- reducir los incentivos de los delincuentes
- reducir la motivación para delinquir
- eliminar las excusas para delinquir

Cada uno de estos enfoques puede aplicarse a los delitos que tienen un impacto directo en el sector privado y se pueden emplear para dirigir las acciones para combatir las amenazas futuras de la delincuencia.

Al igual que muchas guías para la prevención de la delincuencia, y a pesar del estrecho vínculo con los modelos de prevención de la delincuencia basados en situaciones, el sector privado parece casi un elemento adicional. Esto se evidencia en su lista de instituciones, donde se prioriza el papel desempeñado por los gobiernos, se crea un enfoque basado en el conocimiento, se considera la necesidad de contar con una planeación estratégica, monitoreo y evaluación. Se sugiere la necesidad de cohesión entre los socios y la necesidad de hacer participar a las comunidades y a la sociedad civil. Se incluye al sector privado sin hacer referencia a su importancia respecto al impacto que tiene en las estrategias.

El contenido del Manual de la ONU recomiendan la capacitación de universidades, funcionarios, comunidades; así como del sector educativo y profesional y el desarrollo de capacidades profesionales. No se incluye el rol específico del sector privado en la capacitación y educación. Desde 2010, han prosperado en algunos países, como el Reino Unido, los avances en la formación de sociedades entre los sectores público y privado. Los investigadores y los expertos hoy en día identifican el valor de asociarse con el sector privado en formas significativas. El sector privado puede contribuir sustancialmente a ampliar las políticas de seguridad comunitaria y pública de manera positiva, por ejemplo:

- Al contribuir con los programas sociales a nivel local que contrarrestan los factores de causalidad.
- Al ayudar a reducir las oportunidades e incentivos para delinquir a través de los cambios de situaciones y del entorno, incluyendo el diseño de productos que disminuyan las oportunidades de robar.
- Al contribuir a la revitalización de las áreas y espacios públicos o semipúblicos.
- A través de la participación en los proyectos de renovación urbana.
- Al ayudar a evitar la delincuencia y la reincidencia a través del desarrollo de programas de aprendizaje y capacitación de habilidades laborales y al proporcionar oportunidades de trabajo.

Siguiendo el Manual de Prevención de la Delincuencia de la ONU, se ayudará a enfocar la atención hacia un conjunto de medidas preventivas, pero se sostiene que un enfoque "descendente dirigido por el gobierno" depende en gran medida de un sistema eficaz de registro de delitos que no existe en muchos países, incluyendo a México y otros países latinoamericanos.

Es necesario recurrir al sector privado para asegurar un sistema de registro de delitos que sea eficaz, equitativo y accesible. El desarrollo de un sistema en el que la población y las industrias puedan confiar es un primer paso importante.

Capobianco (2005) identificó un conjunto de semejanzas y diferencias entre los enfoques de los sectores privado y público. Al examinar el enfoque del sector privado, analizó la manera en que se presenta un crecimiento de sociedades, se hizo evidente el estímulo del sector público para la participación del sector privado, la necesidad de una mayor demanda de éste para que se le vea como una prioridad, así como su proliferación, al mismo tiempo que se da el ascenso de la responsabilidad social corporativa. Desde la publicación de esta investigación, el surgimiento del periodista ciudadano en los medios sociales muestra la capacidad de los consumidores para cuestionar la falta de contribución de las empresas legítimas a fin de reducir la delincuencia y exponer el impacto creado por sus servicios contra la delincuencia. Los medios sociales han eregido el perfil de responsabilidad social y, por tanto, otorgan funciones al sector privado para responder a este nuevo fenómeno.

6.3.1 Fraude en solicitudes y fraude crediticio relacionado

El fraude en solicitudes se da cuando una persona presenta información incorrecta o engañosa, conscientemente, en su solicitud, y es una vía importante para el fraude, al igual que el fraude de identidad y la apropiación fraudulenta de cuentas (Levi, 2013; CIFAS, 2013). El Servicio de Prevención de Fraudes del Reino Unido (CIFAS) cuenta con la membresía de 270 organizaciones en los ámbitos de la banca, tarjetas de crédito, financiación de activos, crédito minorista, pedidos por correo, seguros, administración de inversiones, telecomunicaciones, factoraje y compraventa de valores y —en menor medida— , algunas partes del sector público. Los miembros comparten información sobre los fraudes identificados en la lucha para prevenir el fraude, al utilizar una exención de la Ley de Protección de Datos, la cual permite compartir la información por motivos de prevención de la delincuencia. El CIFAS fue el primer esquema para compartir datos en el mundo, y comenzó antes de la publicación del informe de Levi *et al.* (1991). Otros esquemas basados en el CIFAS se han puesto en marcha en Sudáfrica y Alemania, aunque las leyes de protección de datos y las tradiciones intraindustriales para compartir datos son distintas. El punto clave es que se debe establecer una situación de confianza con el paso del tiempo, por lo que ha sido más difícil establecer bases de datos relacionadas con el fraude cometido por empleados debido a la ambigüedad en los motivos de despido/renuncia, y al riesgo de difamación cuando es necesario divulgar los registros como resultado de las solicitudes de Libertad de Información.

La Base de Datos Nacional sobre el Fraude de CIFAS contiene registros de los fraudes confirmados que han sido cometidos (o que se han intentado cometer) contra las organizaciones que son miembros de CIFAS. Para registrarse en la base de datos de CIFAS, cada caso debe

satisfacer una norma de prueba. Esto significa que debe haber evidencia suficiente para que el caso sea presentado ante la policía, aunque no es un requisito obligatorio. CIFAS audita los registros de sus miembros para garantizar que cumplan con las normas de la industria. El informe Fraudscape 2012 (CIFAS, 2013) muestra que casi dos terceras partes de todos los fraudes se relacionaron con el uso indebido de datos (con vínculos evidentes con el *hackeo* de datos y cuando se ponen en riesgo los datos internos por parte del personal que fue cómplice o fue el objetivo abordado por los delincuentes).

Una de las áreas que han sido blanco de la delincuencia organizada/redes de delincuentes en las instituciones financieras —especialmente en el Reino Unido y Estados Unidos— es el sector de préstamos hipotecarios. De hecho, el fraude en las hipotecas de alto riesgo y en las Obligaciones de Deuda Garantizadas y otras que se basan en éstas fueron el factor clave que impulsó la crisis financiera global. Si se hubieran implementado mejores medidas de control, esto jamás habría sucedido. Algunos ejemplos del fraude en solicitudes en el sector hipotecario son los siguientes:

- exagerar los ingresos del prestatario para que se le otorgue un enganche mayor;
- solicitar una hipoteca como propietario-ocupante para un inmueble (o inmuebles) cuando se tiene la única intención de rentarla a otros.

Los miembros del Consejo de Prestamistas Hipotecarios pasan por varias revisiones detalladas durante la etapa de solicitud con el fin de identificar fraudes potenciales. Si la solicitud fue presentada por un intermediario, las demás solicitudes presentadas por la misma empresa también son verificadas para identificar inconsistencias o patrones.

Una vez que concluye la verificación del intermediario, los detalles del solicitante son sometidos a revisiones pormenorizadas que incluyen:

- información crediticia de los tres organismos de referencia crediticia (Experian, Equifax y CallCredit) para verificar los particulares y antecedentes del solicitante;
- verificación de la coherencia de la solicitud mediante el sistema National Hunter, que fue desarrollado en 1993 por los organismos de referencia crediticia al emplear información aportada por la CML, y muchos prestamistas participan en este sistema;
- una verificación de la credibilidad de ingresos; y
- el prestamista también puede llevar a cabo revisiones adicionales procedentes de su análisis o sistemas, como la búsqueda de cualquier tipo de patrón en las solicitudes.

Un gran número de prestamistas cuentan con equipos que se dedican a la investigación de solicitudes para examinar, de manera sistemática, las solicitudes marcadas como sospechosas e investigar los casos de posible fraude. También se les motiva a remitir los casos investigados al regulador o a la policía.

6.3.2 Fraude con tarjetas de débito y seguros

Existe una relación interactiva entre las medidas de control y los índices de fraude. Es normal que los altos ejecutivos soliciten pruebas del crecimiento alarmante del fraude antes de invertir recursos para establecer modificaciones, en particular (según dijeron los entrevistados) si esta inversión implica gastos significativos a corto plazo y los beneficios se consolidarán hasta años después, una vez que estos ejecutivos ya no estén al mando. Es posible que esta hipótesis no sea general, y supone un cuestionamiento a la teoría de la empresa en la economía convencional: se esperaría ver un mayor grado de disponibilidad para invertir en la prevención de fraudes en las situaciones en las que los altos ejecutivos han ocupado un puesto por más tiempo y que los inversionistas estuvieran más orientados a los intereses de largo plazo de las empresas (Levi, 2003). Enseguida se presenta un historial del fraude con tarjetas de débito en el Reino Unido y las medidas de control (datos proporcionados por bancos del Reino Unido, que se publican anualmente):

1988 (pérdida por fraude de £69.3 millones). La apertura de bancos ante la competencia creciente llevó a una lucha por la participación del mercado y esto redujo los ingresos significativamente, implicando también costos más elevados. Lo anterior dio como resultado que la industria de tarjetas de débito incursionara en el crecimiento empresarial, sin una consideración adecuada de los riesgos de fraude.

1990. Se llevó a cabo un estudio sobre la prevención del fraude con cheques y tarjetas de débito, que fue implementado por el Ministerio del Interior en cooperación con la industria y la policía (Levi *et al.*, 1991).

1990/1992 (pérdida por fraude en 1992, registrada entonces por £165 millones). El Ministerio del Interior ejerció presión en la industria de tarjetas al hacer uso del informe realizado por Levi *et al.* (1991), que centró su atención en la industria sobre las medidas de cooperación y para compartir datos, rechazando como una solución rentable/no rentable, la noción entonces popular de que las fotografías en las tarjetas serían la mejor manera de eliminar el delito con tarjetas. Las recomendaciones también estuvieron dirigidas a la policía y a los comerciantes, así como a los esquemas de tarjetas, con el fin de vigilar a los comerciantes fraudulentos. La industria de tarjetas del Reino Unido estableció el Foro para la Prevención de Fraude con Plásticos para compartir datos y experiencias sobre el riesgo de fraude entre los miembros de la industria.

1992/1995 (pérdida por fraude en 1995 por £83.3 millones, equivalente a la mitad de la cifra presentada en 1992). Un esfuerzo concertado por la industria de tarjetas se dirigió a la aplicación de soluciones a corto y largo plazo. Los esfuerzos a corto plazo requerían, entre otras cosas, el establecimiento de sociedades con los comerciantes (a expensas de la industria de tarjetas, ya que esto tenía un impacto en los comerciantes), y la introducción de medidas dirigidas a los casos en los que "la tarjeta no fue recibida" (por el titular); algunos componentes estuvieron

dirigidos al robo de la correspondencia, en colaboración con la Oficina de Correos, para rastrear los puntos de riesgo. Estas medidas provocaron la reducción del fraude, lo que es aún más significativo en el contexto de los volúmenes crecientes del uso de tarjetas.

1995/1999. Se observaron pequeños incrementos en las pérdidas hasta 1999, año en que se presentó un incremento más agudo de 40%. En una revisión llevada a cabo por el Ministerio del Interior en colaboración con la industria, Levi y Handley (1998) demandaban acciones adicionales, incluyendo la acción contra los fraudes "sin presencia física de tarjeta" (CNP). Los datos en conjunto provenientes de los emisores de tarjetas del Reino Unido revelaron un cambio de la situación de tarjetas extraviadas y robadas a una situación más organizada de delitos con tarjetas de débito, principalmente la falsificación y el fraude CNP. La tendencia del fraude a principios de la década de 1990 requirió un enfoque de reducción de la delincuencia dirigido al ladrón/estafador que había robado una tarjeta de crédito (o, con menos frecuencia en aquellas fechas, una tarjeta de débito), aunque la tendencia cambió hacia una mayor sofisticación tecnológica y una red más amplia para sacar provecho de la "clonación", es decir, el copiado de los datos de la cinta magnética a otras tarjetas, ya sea grabadas o simplemente en "tarjetas blancas" que se pueden usar en terminales remotas.

En la prevención de la delincuencia, en general se supone que existe una racionalidad calculada en las medidas que se implementan, incluso se considera el aspecto de inevitabilidad. Sin embargo, como en los casos del *chip* y el *NIP*, el cambio a menudo debe ser impulsado a través del compromiso entusiasta por parte de individuos clave, sin el que la "racionalidad" no se concretará y ni se apoyará. Habiendo ganado en principio el acuerdo para comenzar a enfrentar la amenaza que crecía rápidamente de la falsificación/clonación —para la cual el sistema de la banca no contaba con una respuesta tecnológica— la prueba de ensayo de tres meses con *chips* y *NIP* comenzó en Northampton en mayo de 2003. Esta zona fue seleccionada en parte debido a que representa demográficamente al Reino Unido y en parte porque era la sede de Barclaycard, el principal emisor de tarjetas del Reino Unido y uno de los organismos que impulsaron este cambio. Para reproducir la activación gradual del despliegue a nivel nacional, algunos establecimientos comerciales no fueron sometidos a la actualización y muchos clientes siguieron usando sus firmas. Al contar con el apoyo de la industria bancaria, el esquema recibió gran publicidad que destacó sus aspectos de reducción de fraudes con tarjeta.

Después del éxito de la prueba, la implementación de *chips* y *NIP* a nivel nacional comenzó en octubre de 2003. ¿Cómo fue posible lograrlo? Esto se debió en gran medida (tras darse argumentos internos importantes) debido a que la industria de tarjetas acordó pagar los gastos de implementación en el ámbito de comercio al menudeo. Los minoristas, quienes agradecieron el hecho de que la industria de tarjetas ya había invertido sumas enormes, se dieron cuenta que se encontraban en una fuerte posición de negociación: si la industria de tarjetas se negaba a pagar por los costos de los minoristas, esta inversión se desperdiciaría en gran medida. El resultado era claro: menores pérdidas en el fraude actual con tarjetas, ya que el total

de pérdidas por fraude con tarjetas disminuyó de £439.4 millones en 2005 a £341 millones en 2011; esta disminución constante del fraude cometido con tarjetas extraviadas y robadas puede apreciarse en el cuadro 6.2.

Cuadro 6.2

Pérdidas anuales con respecto a tarjetas expedidas en el Reino Unido durante el periodo 2001-2011
Todas las cifras se expresan en millones de libras (£)

Tipo de fraude	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	+/- cambio 10/11
Sin presencia de tarjeta	95.7	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	226.9	220.9	-3%
Tarjeta falsificada	160.4	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1	-24%
Extra-viada/ robada	114.0	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	50.1	+13%
Robo de identidad	14.6	20.6	30.2	36.9	30.5	31.9	34.1	47.4	38.2	38.1	22.5	-41%
No recibida por correo	26.8	37.1	45.1	72.9	40.0	15.4	10.2	10.2	6.9	8.4	11.3	+34%
TOTAL	**411.5**	**424.6**	**420.4**	**504.8**	**439.4**	**427.0**	**535.2**	**609.9**	**440.0**	**365.4**	**341.0**	-7%
Contenido en este total/desglose por ubicación												
Reino Unido	273.0	294.4	316.3	412.3	356.6	309.9	327.6	379.7	317.4	271.5	261.0	-4%
Fraude en el extranjero	138.4	130.2	104.1	92.5	82.8	117.1	207.6	230.1	122.6	93.9	80.0	-15%

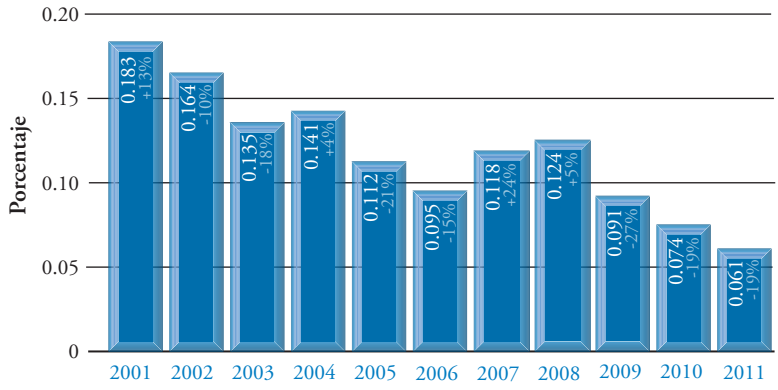
Fuente: Informe de Acción contra el Fraude Financiero en el Reino Unido 2012. www.financialfraudaction.org.uk/Publications/#/6/

La relación entre el fraude y la facturación (o mejor aún, la relación entre fraude y ganancia, en caso de conocerla) es una manera de presentar el impacto real del fraude. Esta relación entre fraude y facturación se incluye a continuación (Acción contra el Fraude Financiero en el Reino Unido, 2012) (gráfica 6.5).

Gráfica 6.5

Relación fraude/rendimiento durante el periodo 2001-2011

Las cifras de color muestran el cambio en el porcentaje con respecto al total del año anterior



Fuente: Informe de Acción contra el Fraude Financiero en el Reino Unido 2012. www.financialfraudaction.org.uk/Publications/#/6/

El cambio en las tendencias de fraude cometido por la delincuencia organizada mediante la estafa con terminales bancarias automáticas (ATM) y a través de grupos internacionales que delinquen sin la presencia física de tarjetas llevó a que, en 2003, se creara, gracias al financiamiento conjunto de la unidad policiaca Metropolitana y la policía de Londres, la Unidad Especializada en Delitos con Cheques y Tarjetas, que fue cofinanciada en principio por el Ministerio del Interior y la industria de la banca, y después fue financiada en su totalidad por la industria de la banca tras una revisión independiente que mostró que las ventajas para la industria superaban los costos de la unidad, medidos por la cantidad de tarjetas y por el número de éstas recuperadas, multiplicado por las pérdidas promedio de los fraudes con tarjetas por cada una de ellas. En la primera década en que fue implementada, generó ahorros estimados por £400 millones.

En conclusión, parece que la lucha contra las tarjetas y el fraude relacionado con éstas ha sido difícil, en este contexto la red internacional de marcas como Visa y MasterCard, los emi-

sores de tarjetas, los comerciantes adquirientes, los minoristas y las instituciones de referencia crediticia, en ocasiones actúan de manera contradictoria y a veces de modo coordinado junto con los clientes y las instituciones de aplicación de la ley, y con aquellos que tienen la finalidad de defraudarlos. A medida que el uso del *chip* y el *NIP* se ha vuelto cada vez más general en Europa y el Lejano Oriente, las tarjetas expedidas en Estados Unidos se convierten en objetivos un tanto más fáciles y parece razonable que, ya sea en Estados Unidos o en el extranjero, estas tarjetas serán más afectadas, cambiando así la relación costo-beneficio de las medidas de prevención. Ha sido más difícil generar un foro organizacional para la prevención en los Estados Unidos, aunque se tienen planes de implementar el *chip* y *NIP* a la brevedad; mientras que en Europa, el Consejo Europeo de Pagos actualmente desempeña un papel más importante como parte de la transición a la Zona Única de Pagos en Euros (SEPA, por sus siglas en inglés), una transición que ha sido exigida por la Comisión Europea como parte del mercado europeo único. En gran medida debido a los controles establecidos para confrontar el fraude actual con tarjetas, aparentemente hoy el área principal de lucha tiene que ver con el entorno del fraude sin presencia física de tarjeta. Cuantos más datos personales proporcionemos para una variedad de transacciones, ya sea por internet o de otra forma, habrá más probabilidades de que en algún momento, uno de los receptores de esta información la transfiera a los estafadores o a otros delincuentes. El uso con fines delictivos que se puede hacer con esta información depende de qué tanto se pueden utilizar los datos biométricos y el análisis de patrones a nivel nacional y transnacional para mantener el fraude dentro de un límite manejable. Ésta es un área donde los datos son relativamente buenos, las víctimas son "repetidas", y los fraudes se presentan con una alta frecuencia, son de bajo valor y, por tanto, suponen problemas menos delicados en comparación con otros delitos cometidos contra las empresas. Sin embargo, queda claro el valor de la colaboración entre los sectores público y privado en la prevención de la delincuencia y en la reducción de pérdidas para la industria. La enorme inversión realizada por el sector privado en el fraude con tarjetas es el mejor reconocimiento de la lógica en la participación del sector privado a nivel estratégico para reducir la delincuencia.

Fraude en el sector asegurador

El modelo anterior se amplió posteriormente al sector de seguros para vehículos automotores, y comenzó con el uso de los datos almacenados por la mayoría de las empresas para ubicarlos en un Buró de Fraude de Seguros fundado en 2006, además del uso de software para identificar los puntos en común entre las personas que exageran o hacen declaraciones falsas para reclamar el seguro médico y de daños a vehículos, remitiendo algunos casos a investigación y procesamiento policial una vez que han sido verificados por investigadores privados (Levi, 2008).

Todos los días las aseguradoras descubren 381 reclamaciones de seguros fraudulentas con un valor mayor a los £2.7 millones, cuyo costo estimado anual es de £1 000 millones. La

Asociación de Aseguradoras Británicas tomó como modelo los casos sospechosos y estimó que hay fraudes adicionales por un valor de £2 000 millones que no son detectados. Las aseguradoras invierten alrededor de £200 millones al año para contrarrestar las actividades fraudulentas. En 2012, se implementaron dos iniciativas industriales clave: el Departamento Judicial contra Fraudes de Seguros (IFED, por sus siglas en inglés) y el Registro de Fraudes de Seguros (IFR, por sus siglas en inglés). En su primer año de operaciones, el IFED efectuó 260 arrestos, 78 amonestaciones y 12 sentencias penales y, a finales de abril de 2013, estas cifras aumentaron a 309 arrestos (de las cuales 121 fueron "comparecencias voluntarias" en la comandancia de policía), 91 amonestaciones y 24 sentencias penales. Estas iniciativas reemplazaron las difíciles negociaciones que existían entre el IFB y elementos de las fuerzas policiales para persuadirlos de evaluar caso por caso ante la escasez de recursos de la policía. Al igual que el DCPCU, el financiamiento privado del IFED no resolvió el problema de falta de recursos —existen más redes criminales potenciales que procesar en comparación con el número de policías y procuradores que están dispuestos y son capaces de enfrentarlas—, pero permitió desarrollar un enfoque estratégico que ayudará con los problemas de la industria.

Gracias a que se cuenta con inteligencia compartida y más medidas de aplicación de la ley y de recuperación de bienes, la industria se está acercando a la implementación de una estrategia integral para contrarrestar el fraude. Sin embargo, el fraude de seguros evoluciona constantemente. Es necesario trabajar más en la prevención directa, en particular, en la concientización sobre las consecuencias del fraude de seguros, entendiendo los motivos del fraude y las actitudes cambiantes de los consumidores. De acuerdo a una encuesta aplicada a clientes de ABI, 95% de los encuestados están de acuerdo en que presentar una reclamación de seguro exagerada, falsa o excesiva debe ser clasificada como fraude, mientras que sólo 2% considera que no debe ser clasificada como tal, no obstante 76% está de acuerdo en que el fraude de seguros no es un delito sin víctimas. Asimismo, 42% considera que el fraude a las aseguradoras es una manera fácil de obtener dinero rápido, 29% asume que es poco probable que te descubran cometiendo este tipo de delito y 27% considera que, en caso de ser descubierto, la sanción probablemente sería insignificante. Además, un sondeo llevado a cabo por Mori en 2012, en representación de la IFB, descubrió que una de cada 12 personas consideraría la posibilidad de formar parte de este tipo de "estafas" con tal de obtener una ganancia monetaria. Por tanto, es necesario contar con medidas educativas y de impartición de justicia penal para complementar la recopilación de datos de la industria y los esfuerzos en las negativas de pago.

Por último, en septiembre de 2013 se estableció una unidad de policía especializada dentro de las fuerzas policiacas de Londres para combatir la piratería en línea y otras formas de delitos contra la propiedad intelectual, como la falsificación de productos. La Oficina de Propiedad Intelectual del gobierno del Reino Unido proporcionará inicialmente £2.5 millones por concepto de financiamiento durante dos años y la Unidad será sometida a revisión para verificar su efectividad.

6.3.3 Buró Nacional de Inteligencia en Fraudes (NFIB, por sus siglas en inglés)

En el Reino Unido, después de una fuerte crítica sobre la denuncia, el registro y las investigaciones de fraudes, surgió la idea de reajustar la perspectiva de prevención del fraude. Como resultado de varias revisiones, se creó la Agencia Nacional contra el Fraude (NFA, por sus siglas en inglés) con el fin de sumar esfuerzos entre el gobierno y la industria.

Sus objetivos en 2011 (NFA, 2011) fueron los siguientes:

1. desarrollar y aplicar conocimientos acerca del fraude;
2. establecer estrategias de detección de fraude y políticas públicas claras basadas en evidencias;
3. crear un perfil y concientizar a las personas, las empresas y el sector público sobre el fraude, y empoderarlos para protegerse a sí mismos;
4. coordinar la comunidad antifraude para combatir las formas más perjudiciales de fraude y a quienes las hacen posibles.

La participación del sector privado fue fundamental en el éxito o el fracaso del enfoque. Fue decisivo que existieran relaciones tanto a nivel estratégico como a nivel operativo entre la policía de Londres (la principal fuerza británica contra el fraude), la Oficina contra Fraudes Graves (organización británica que encabeza la lucha contra los fraudes graves a nivel nacional e internacional) y la industria. El grupo del sector privado incluía a una gran variedad de organizaciones representativas de diferentes empresas y a la City of London Corporation (responsable principal de la zona geográfica en que se encuentran muchos de los mercados financieros del Reino Unido).

El enfoque de la NFA consistía en reunir a los sectores dispersos para crear una propuesta en común con una sola estrategia. Dos aspectos fundamentales de la nueva propuesta ayudaron a implementar y lograr la estrategia.

El primero fue la creación del Centro de Inteligencia para obtener datos de varias fuentes, incluyendo los datos sobre delitos denunciados y los datos comerciales sobre el fraude en la industria que solían ser vistos como bases de datos separadas que, en opinión de algunos, no deberían convergir. Sin embargo, a diferencia de lo que se pensaba tradicionalmente, surgió la creencia cada vez mayor de que, a menos de que estas fuentes de datos se combinaran, el sistema no sería capaz de contar con una herramienta dinámica y eficaz para combatir el fraude.

El Buró Nacional de Inteligencia en Fraudes se creó a partir de esta estrategia y se diseñó para recibir datos provenientes de una gran variedad de fuentes de la industria y de los organismos de aplicación de la ley. El papel del NFIB es el siguiente:

"Al trabajar en colaboración con la policía de Londres, principal fuerza nacional contra el fraude, se defiende un enfoque conjunto e integral para el establecimiento y difusión de la inteligencia a través del NFIB, incluyendo el mapeo mejorado de los grupos de la delincuencia organizada y la integración de datos clave sobre los fraudes, proporcionados por el sector público" (NFA, 2012).

Las funciones del NFIB son:

- recopilar, procesar y analizar los datos sobre fraudes para proporcionar información a la comunidad antifraude del Reino Unido, que fomente una mejor comprensión del fraude, incluyendo temas y tendencias para centrarse más en la prevención colaborativa y las alteraciones;
- desarrollar y asignar paquetes de delitos para facilitar las funciones de la policía local, regional y nacional, y las investigaciones de las demás instancias encargadas de aplicar la ley en las situaciones más perjudiciales de actividad delictiva relacionada con el fraude;
- lograr una respuesta mejorada y eficaz ante las organizaciones de estafadores destacando, junto con el Centro de Coordinación de Delincuencia Organizada, la importancia de conocer y comprender a los grupos de delincuencia organizada (OCG, por sus siglas en inglés) que se relacionan directa o indirectamente con el delito de fraude; y
- hacer un uso eficaz de la información de las víctimas de fraude de todo el Reino Unido (sean individuos, empresas o el sector público), y aprovecharla para ayudar, alertar, educar y proteger, así como encontrar nuevas y efectivas formas de combatir el fraude e impactar de manera positiva los limitados recursos en la aplicación de la ley para combatir el delito de fraude en el Reino Unido (véase http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/NFIB/nfib-purposeandvision.htm#sthash.rAnLn38f.dpuf).

La participación del sector privado en la creación y puesta en marcha del NFIB fue un elemento vital. Asimismo, es de suma importancia el compromiso de las organizaciones del sector privado para superar la sensibilidad comercial y participar en las actividades diarias de la NFIB. Las empresas de servicios financieros y los bancos forman parte de la cadena de suministro de datos. Su participación no sólo debe ser considerada por "la realización de algo bueno", sino que debe ser vista como parte de una estrategia efectiva para reducir el fraude y, por tanto, mejorar la riqueza de los accionistas de las empresas. Éste es un aspecto que aún falta por evaluar formalmente, pero estos esquemas funcionan a largo plazo sólo si las sociedades establecidas entre los sectores público y privado se benefician de ellos.

El segundo pilar de la estrategia es la creación de ActionFraud, que se ha convertido en un término para describir el proceso de registro de fraudes y actúa como una herramienta de mercadotecnia para todas las iniciativas nacionales antifraude. ActionFraud cuenta con un centro de atención telefónica para alentar a las víctimas de fraude a denunciar los delitos por

teléfono o internet. Una vez más, esto implica la participación de las empresas, además del uso de una agencia comercial de administración de centros de atención telefónica. La creación de ActionFraud supuso un enorme ejercicio de negociación entre varios organismos: las 43 fuerzas policiales británicas, los Ministerios de Gobierno del Reino Unido y un conjunto de organizaciones financieras comerciales. Los socios individuales llegaron a un acuerdo respecto al nuevo proceso cuando aceptaron que el régimen anterior representaba una gran desventaja en cuanto al registro e investigación eficiente de fraudes.

En la actualidad, las víctimas pueden comunicarse al centro de atención telefónica directamente y la información que proporcionan es registrada sistemáticamente por personal capacitado. Los datos son cotejados y analizados para identificar las tendencias y, sobre todo, para detectar la vulnerabilidad de las transacciones financieras o nuevas tendencias delictivas. Como es un entorno muy dinámico, los mismos telefonistas llegan a identificar tendencias y son capaces de ofrecer información al respecto, por ejemplo, un sitio de comercio apócrifo o una nueva forma de estafa por correo electrónico. El sistema ya se amplió para incluir el registro de delitos cibernéticos, una acción innovadora para intentar normalizar el enfoque de prevención de la delincuencia y aplicación de la ley respecto a la delincuencia digital.

Una vez que todos los datos han sido analizados, el NFIB puede identificar la organización más apropiada para dar continuidad a las acciones, por ejemplo, la fuerza policiaca local, cuando el delito esté siendo planeado en una localidad en particular. El NFIB también podría entregar la información directamente al sector financiero para erradicar o reducir las vulnerabilidades presentes en un banco u otra empresa financiera. Esto permite tomar acciones inmediatas a nivel estratégico. Bajo el sistema anterior, las remisiones a las instituciones financieras podían tardar, ya que debían pasar por la estación de policía local, a través de su escuadrón antifraude (si se contara con uno), después por el ayuntamiento de Londres y finalmente llegar a la institución financiera. Este proceso podía repetirse en varias dependencias para los mismos delincuentes. Al reducir la duplicidad, las empresas pueden identificar la forma de proteger a sus clientes de una manera rápida y efectiva.

Aunque no se ha realizado una evaluación formal, la contribución del sector privado tanto en el NFIB como en ActionFraud ha demostrado lo que se puede lograr cuando la industria está consciente de las ventajas directas de que su empresa contribuya a una causa común (para ver algunos ejemplos de su trabajo, véase: http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/NFIB/nfib-newsletter.htm). Las facilidades que otorga el gobierno y el apoyo de las fuerzas policiales y los organismos nacionales de políticas públicas, son una muestra clave del compromiso que el sector público tiene con el esquema. Todavía existen expectativas sobre la actuación de la policía ante los efectos de las denuncias de fraude. Aún falta comprobar si las empresas e individuos seguirán realizando denuncias aunque no haya un beneficio de seguro (es decir, la denuncia de un delito del que pueden realizar una reclamación) ni una recompensa al ver a alguien arrestado. Ésta es un área que requerirá un manejo cauteloso de las expectativas y la legitimidad. Sin embargo,

el objetivo de maximizar la información sobre los patrones de fraude a nivel nacional es un meta que el NFIB ha estado persiguiendo, en el que también influye la cooperación entre los sectores público y privado para combatir el delito cibernético, que cada vez se presenta con más frecuencia: a) a nivel local y regional (Levi y Williams, 2012) y b) a nivel nacional, con una iniciativa que comenzó formalmente en 2012 promovida por la agencia de inteligencia de gobierno GCHQ y de la infraestructura nacional clave y empresas críticas como las del sector financiero. Debido a que muchas de estas instituciones son trasnacionales, hay lecciones que podrían aplicarse a México de manera indirecta.

ActionFraud también ayuda a los clientes al proporcionar una vasta cantidad de información a las víctimas y víctimas potenciales sobre la reducción del fraude, ya sea mediante comunicación directa o a través del sitio web. Éste es un servicio adicional que puede ser considerado un beneficio comercial directo para las organizaciones del sector privado. El sector financiero depende en gran medida de la confianza en la banca y en el entorno monetario digital. Cualquier inquietud que los clientes tengan respecto a la probidad del sistema tendrá un impacto directo en la generación de riqueza, ya que los clientes podrían irse con la competencia. Al ofrecer a los clientes los medios para que se protejan se da un servicio valioso que de otra manera quizá debería ser proporcionado por la propia compañía financiera (NFA, 2011).

6.3.4 Un contexto distinto: combate de la explotación de menores en línea mediante el apoyo de las empresas

En el Reino Unido, el ambiente ineficiente en torno a la seguridad de los niños en internet se transformó mediante el desarrollo y existencia del Centro de Protección contra la Explotación de Menores en Internet (CEOP, por sus siglas en inglés). El CEOP fue creado con la finalidad de reunir una variedad de intereses, que incluyen los del gobierno, instituciones educativas, terceros, organismos de aplicación de la ley y, sobre todo, los del sector privado. Este Centro se estableció para dar un enfoque que permita a cada uno de los sectores contribuir y entender lo que los otros sectores hacen. Dicho enfoque surgió a partir de la creencia de que el combate de la vulnerabilidad de los niños en internet no puede llevarse a cabo si no se cuenta con la integración total de todos los organismos. De hecho, el CEOP declara de manera enérgica, que "la protección de los niños nos corresponde a todos".

La Guía de Gestión de Relaciones del CEOP incluye las siguientes directrices:

- ser proactivo y no reactivo;
- identificar las áreas específicas de trabajo que podrían mejorarse con apoyo externo;
- ofrecer ventajas para ambas partes;
- ser creativo e innovador;
- solicitar a socios y patrocinadores que adopten el mismo enfoque de creatividad, innovación y flexibilidad para mantenerse a la vanguardia;

- aportar conocimientos y compartir experiencias;
- solicitar a socios y patrocinadores que usen la información que hayan obtenido del CEOP para ayudar a definir los servicios que ofrecen a los niños y jóvenes;
- ser una entidad sustentable y fomentar niveles más elevados de compromiso y participación;
- buscar establecer relaciones a largo plazo;
- tener solidez ética y ser transparente;
- fomentar el cuestionamiento ético, escuchar y respetar los puntos de vista de los demás (CEOP, 2010).

Esta amplia gama de propósitos tiene la finalidad de maximizar las oportunidades para que el sector privado participe sin perjudicar la postura ética del CEOP, particularmente dentro de un entorno sensible. Junto con la Fundación de Vigilancia en Internet (Internet Watch Foundation, creada en 1996) y GetSafeOnline (fundada en 2006), el CEOP ha trabajado de manera conjunta con la industria de tarjetas de crédito para limitar las oportunidades de las empresas de pornografía infantil por internet de brindar facilidades de pago con tarjetas de crédito a quienes desean comprar este tipo de imágenes.[114] La relación con las organizaciones del sector privado no debería implicar costo alguno. El CEOP ha establecido un compromiso firme con sus normas de ética. Por ejemplo, no establecer relaciones con organizaciones que sólo aparentan estar a favor de la protección infantil o que no defienden los derechos de los niños. Sin embargo, el compromiso de recibir retroalimentación de otros ofrece un mecanismo para la mejora continua. El CEOP declara que es fundamental "establecer sociedades" para lograr el enfoque de la organización.

"Por primera vez en una organización, los oficiales a cargo de aplicar la ley se sientan junto a especialistas provenientes de grupos de asistencia social para niños, educación, gobierno, socios empresariales y otros grupos interesados" (CEOP, 2010).

La creación de este entorno ha sido un trayecto largo y difícil. Ha implicado reunir, bajo un mismo techo, las contribuciones provenientes de una gran variedad de organizaciones, cuya historia, objetivos clave y capacidad financiera no necesariamente coinciden. Por ejemplo, quienes participaron directamente en la creación del CEOP y reconocen el valor de la participación del sector privado no tienen prohibido hacer comentarios en público sobre el sector privado. John Carr, un reconocido defensor de los niños que se involucró en gran medida en la creación del CEOP, a menudo critica fuertemente el compromiso del sector privado (véase: http://news.idg.no/cw/art.cfm?id=A7D2E722-F52F-E422-E24C391CA1BCC1E6).

114 Hay controversias constantes en el Reino Unido —con base en el principio y efectividad— respecto al grado de acción proactiva que puede y debe ser implementado por los proveedores de servicios de internet (ISP, por sus siglas en inglés) para bloquear el contenido pornográfico que involucra imágenes de abuso sexual infantil. Se realizaron cambios a los controles de los ISP en julio de 2013 después de las fuertes campañas en los medios y de la intervención del Primer Ministro.

Contar con la capacidad de ofrecer críticas independientes es un aspecto altamente valorado de la colaboración del sector privado. Por ejemplo, cuando se hacen inversiones, éstas no deben crear una obligación ineludible ni debe propiciar la crítica hacia los donantes. De igual forma, el hecho de que una organización del sector privado colabore no debe impedirle que emita críticas apropiadas e informativas sobre los socios. Los autores consideran que éste es un aspecto importante para que haya un mayor compromiso del sector privado. La inversión de tiempo o recursos no debe implicar el compromiso de abstenerse a emitir críticas ni la obligación de promover únicamente puntos de vista positivos de unos y otros.

Se debe fomentar el debate, el desacuerdo y la argumentación razonable por parte de todos. Las organizaciones del sector privado que ingresen al entorno de prevención de la delincuencia no deben considerar que su ingreso los obliga a cambiar su misión principal o que den por hecho que de alguna manera controlan a los organismos de aplicación de la ley o a otros.

Se ha adoptado un enfoque muy diferente sobre la recomendación que hace al sector privado a la Organización de las Naciones Unidas respecto al trabajo con jóvenes. Aunque tal recomendación está dirigida principalmente a las empresas trasnacionales, sus principios se pueden aplicar en cualquier contexto en el cual esté involucrado el sector privado. Su conjunto de herramientas establece algunas ideas con el objetivo de:

- destacar el papel que los jóvenes desempeñan como actores sociales, e incrementar el conocimiento general sobre el gran potencial que los jóvenes tienen para fungir como socios de desarrollo;
- estimular al sector privado para hacer equipo con la juventud al presentar varios casos de estudio y demostrar la ventaja económica que implica el invertir en este grupo, en comparación con el costo de una inversión insuficiente;
- ofrecer orientación inicial para facilitar la relación del sector privado con los jóvenes, y la formación de sociedades significativas, con el fin de influir en los procesos de desarrollo alrededor del mundo.

Los principios mencionados describen la manera en que es posible participar en identificar las estrategias que respaldan a las empresas. Por ejemplo, los principios aseveran que invertir en la juventud puede crear riqueza en el futuro y convocan al sector privado para que se relacione con los grupos de jóvenes por su propio bien, en lugar de hacerlo por motivos de relaciones públicas o simplemente para parecer socialmente responsable. Ayudar a la juventud a comprender el entorno empresarial, presentar productos y servicios y generar creadores de riqueza futura se considera como una estrategia empresarial sensata, y no como un intento caprichoso para hacer que la organización "luzca bien".

Este mismo enfoque se puede aplicar en el ámbito de prevención de la delincuencia. El activo más sólido para la mayoría de las organizaciones es su gente; invertir en las personas

para en un futuro convertirlas en empleados sobresalientes o clientes constantes, representa una decisión empresarial razonable. En el contexto de prevención de la delincuencia, lograr que el entorno donde la empresa realiza sus operaciones sea un lugar seguro y proteger al personal del temor a la delincuencia o de la situación real delictiva, es tan importante para la rentabilidad futura como la realización de inversiones en nuevas tecnologías.

En conclusión, ActionFraud, NFIB y el CEOP son ejemplos de cómo las organizaciones de los sectores público y privado pueden trabajar eficazmente de manera conjunta para crear un enfoque colectivo que resulte valioso para todos los socios. No será sino hasta que se entiendan las necesidades y capacidades del sector privado cuando los organismos de aplicación de la ley y los encargados del diseño de políticas públicas puedan crear ideas y opciones que permitan la colaboración real. Enseguida se sugiere un esquema sobre los requisitos que los autores proponen para establecer la asociación eficaz, que ayudará al sector privado a trabajar de manera más colaborativa con los demás.

6.3.5 México: algunas respuestas del sector privado

Un análisis internacional realizado por International Collegiate Programming Contest (ICPC, 2010) sobre los problemas que la delincuencia organizada supone para la seguridad pública no hizo mención alguna del sector empresarial como objetivo de la delincuencia. Capobianco (2008) señala que no se toma en cuenta al sector privado en la prevención de la delincuencia, sólo se le considera como último recurso o como contribuyente de financiamiento. Actualmente, es esencial la participación de las empresas para solucionar los delitos financieros y cibernéticos. La existencia de corporaciones transnacionales tiene la posibilidad de ayudar y obstaculizar las iniciativas de prevención de la delincuencia a través de las fronteras internacionales. En el mundo existen muchos ejemplos de redes y sociedades establecidas entre los sectores público y privado. Hay un excelente compendio sobre redes que abarcan varios ámbitos.

Existe poca bibliografía que explora el impacto de los delitos indirectos en el mundo empresarial. Las estimaciones del "costo de la delincuencia contra las empresas" están incompletas al no contar con estos datos. Capobianco considera que son costos indirectos de la delincuencia: el aumento de impuestos destinados a financiar el sistema de justicia penal, o de una forma menos burda, el efecto que tiene el temor a la delincuencia sobre el valor de los inmuebles o la capacidad de comercializar los servicios de una manera efectiva. Estos ejemplos hacen que sea esencial para el sector privado mostrar interés y compromiso en el ámbito de la delincuencia local. Sólo un sistema de registro eficaz cumplirá con esta necesidad.

Capobianco cita ejemplos de empresas del sector privado que invierten tiempo y recursos en iniciativas específicas, por ejemplo, personal de la empresa que participa con los jóvenes de la

localidad para ofrecer oportunidades de diversión, o designar a un gerente para que se dedique a dirigir una campaña particular. Sin embargo, Capobianco afirma que estas inversiones son vistas principalmente como parte de la responsabilidad social corporativa (formal) o como donaciones. También sugiere que el sector privado tiene muchas oportunidades para involucrarse directamente en la labor de prevención de la delincuencia sin que esto sea considerado una "donación". Estas oportunidades incluyen:

- desarrollar supervisores o gerentes locales que dedican tiempo a los grupos comunitarios locales;
- participar en el cambio de roles con las organizaciones del sector público;
- establecer redes entre las organizaciones del sector privado para crear un mensaje de campaña único;
- incentivar las iniciativas de prevención locales que tienen un impacto directo en los niveles de delincuencia de la localidad;
- proporcionar espacios para que los grupos del vecindario se reúnan;
- aportar y divulgar entre los empleados consejos y orientación en materia de prevención de la delincuencia;
- trabajar con los delincuentes para evitar que se conviertan en reincidentes.

La Guía del Banco Mundial para Asociaciones Público-Privadas (Banco Mundial, 2011) es un minucioso compendio sobre la participación del sector privado en todo el mundo con énfasis especial en América Latina. El siguiente es un análisis interesante sobre lo que el sector privado aporta a la prevención de la delincuencia:

- innovación;
- disponibilidad de actores sociales;
- acceso a los factores de influencia;
- flexibilidad de recursos;
- financiamiento;
- independencia.

Básicamente, el sector privado es capaz de movilizarse rápida y eficazmente, es más independiente y tiene menos restricciones que sus contrapartes en el sector público. Al hacer uso de estos atributos, de alguna manera debe existir una compensación. Ésta podría ser directa en términos financieros, por ejemplo, recurrir a los servicios de guardias de seguridad remunerados o crear un balance más equitativo entre los dos sectores. Sería conveniente para las organizaciones del sector privado contar con una mayor influencia en la priorización de los recursos del sector público, con un enfoque más flexible para la planeación y desarrollo o el suministro de datos precisos sobre la delincuencia en el área local. A menudo el sector privado se encuentra en una mejor posición de asumir el liderazgo, en particular si el delito en consideración tiene un impacto directo en las empresas de la localidad. El nivel de responsabilidad social corporativa

puede ser en sí un motivo suficiente para colaborar con los socios del sector público, quizá para ser visto como un buen empleador o para tratar de influir en el proceso de toma de decisiones que afecta a las empresas.

El sector privado también puede actuar sin depender de la influencia política del sector público y puede emplear su voz para hacer que el sector público rinda cuentas. Algunos ejemplos adicionales de la participación del sector privado incluyen el uso del voluntariado corporativo o la creación de alianzas de negocios corporativas. Estas acciones se pueden llevar a cabo ya sea de manera independiente o en conjunto con el sector público.

Las orientaciones del Banco Mundial proporcionan un gran número de ejemplos y profundizan en los que se relacionan con la participación del sector privado. Asimismo, presenta a las organizaciones argumentos sólidos para que se involucren con el sector público. Sin embargo, la guía no ahonda mucho en qué tan amplia debería ser la respuesta del sector público ante las necesidades del sector privado. El Manual de Prevención de la Delincuencia de UNODC 2010 analiza la influencia en la prevención de la actividad delictiva, los enfoques, la coordinación de acciones, la colaboración, etc., aunque no habla mucho de lo que se puede lograr cuando el sector privado participa, por lo que esta brecha debe destacarse y cumplirse.

El Compendio Internacional de Prácticas sobre Prevención de la Criminalidad 2008 es un buen texto de referencia, aunque se concentra en la juventud y en la seguridad de la comunidad en general, y resalta, una vez más, la falta de alianzas con el sector privado. México se incluye en la selección de ejemplos de este compendio.

La Unión Europea ha dedicado varios estudios que abarcan los enfoques de sus Estados miembros respecto a la prevención de la delincuencia. Estos estudios presentan pocos datos sobre los costos de la delincuencia, el financiamiento de iniciativas y resúmenes de las contribuciones de los Estados miembros. El Foro Europeo (2006) realizó una comparación útil de los enfoques existentes en la Unión Europea, aunque lo hizo con una perspectiva "descendente". Se destacan 10 niveles de participación, que van desde el gobierno que se ubica en la cima, hasta llegar a los medios, que se ubican en la parte inferior. En este rubro, el sector privado se ubica en la novena posición, haciendo énfasis en el patrocinio. Es necesario cuestionar la omisión del rol del sector privado.

La Guía de Acción para Asociaciones Público-Privadas creada por el Banco Mundial ofrece recomendaciones y orientaciones significativas para las instituciones de los sectores público y privado. Contiene, además, algunas referencias útiles sobre la creación de alianzas, particularmente en América del Sur y México. Asimismo, examina el fracaso potencial de los enfoques represivos y perfila lo que se considera una lista de control para las organizaciones del sector privado y para los organismos del sector público, como la policía. Sus recomendaciones son

realistas, pero el alcance es limitado. Esta guía debe tenerse en cuenta junto con el estudio realizado por ICPC (2005), *Sharpening the Lens: Private Sector Involvement in Crime Prevention*, que presenta una gran cantidad de ejemplos útiles que podrían ser comparados con la situación en México.

En resumen, la labor internacional en la prevención de la delincuencia se centra, por lo general, en el Estado, lo que refleja los grupos de clientes de organismos internacionales y su enfoque en la creación de políticas públicas. Esto debe sustituirse por un modelo en el que la facultad de prevención de la delincuencia esté más difundida, donde no sólo se aprecie la realidad analítica sino también la realidad política de las sociedades cuya confianza en el Estado —con fundamentos o sin ellos— es baja y que tomará tiempo recuperar al mejorar el servicio que la policía presta a la sociedad civil, a los individuos y a las corporaciones.

6.4 Identificación y establecimiento de la colaboración entre los ámbitos público y privado

Es preciso considerar los factores que pueden tener un impacto en la identificación y el establecimiento de la colaboración público-privada, basada en las asociaciones existentes en México, junto con lecciones de tareas conjuntas similares a las de los países desarrollados.

El presente documento tiene la finalidad de defender el rol integral de las organizaciones del sector privado dentro de una estrategia general de prevención de la delincuencia. La propuesta de los autores es que, tradicionalmente, el sector privado se considera como un participante marginal u opcional en el combate contra la delincuencia, sin embargo, el sector privado debe tener un papel más destacado.

Al desarrollar la prevención de la delincuencia situacional de Clarke y Homel (1997), se pueden expresar los objetivos y las posibles maneras de lograrlos en la siguiente formulación aplicada al fraude y la corrupción:

1. Aumentar el esfuerzo percibido contra el fraude y la corrupción.
   - Realizar esfuerzos de prevención basados en riesgos, con una mejor regulación del proceso de licitación de contratos y escrutinio, y medidas para hacer que los estafadores tengan que trabajar más para obtener el mismo nivel de ingresos.
2. Aumentar los riesgos percibidos del fraude y la corrupción.
   - Acelerar la detección de intentos de fraude; investigaciones eficientes e independientes y un proceso de impartición de justicia penal para equilibrar el fomento a la concientización.
   - Análisis proactivo de integridad y mecanismos independientes de presentación de quejas.

3. Reducir las gratificaciones anticipadas provenientes del fraude y la corrupción.
   - Capturar al individuo corrupto con más rapidez en los países proveedores y compradores y, realizar una mejor recuperación de activos.
4. Reducir las excusas referentes al fraude y la corrupción.
   - Fortalecer la independencia de los medios y la sociedad civil, con una condena clara para la conducta, enalteciendo los modelos a seguir en el campo empresarial y de la política que no se involucran en prácticas fraudulentas o corruptas.

Los cambios del sector privado que implicarán un mayor impacto son los siguientes:

1. Aumentar el conocimiento sobre la incidencia delictiva en su propia localidad.
2. Exigir la comprensión de la estrategia local de aplicación de la ley para reducir la delincuencia.
3. Denunciar los casos de delincuencia.
4. Trabajar con las demás organizaciones del sector privado con el fin de crear el ímpetu suficiente para ejercer influencia.
5. Dedicar tiempo o invertir recursos para las estrategias de prevención de la delincuencia.
6. Crear redes efectivas con los organismos de aplicación de la ley y de impartición de justicia penal, tomando en cuenta los intercambios de personal o la organización de actividades para compartir información.
7. Aprender a comprender el temor al delito entre el personal.
8. Comprender el alcance que la delincuencia tiene en las empresas, tanto en términos financieros como operativos.

La creación de un enfoque integral y sistémico requiere de un compromiso equitativo y oportuno por parte de las instituciones que se relacionan de manera sólida con el sector público, como la policía u otros organismos de aplicación de la ley.

6.4.1 Modelo de participación del sector privado para la prevención de la delincuencia

Entender el tipo y el nivel del delito

En primer lugar, las organizaciones del sector privado deben entender claramente el impacto del delito, y el temor al delito que afectan directamente a sus empresas, como los casos denunciados de delitos cometidos contra la empresa y los intentos de llevarlos a cabo. Asimismo, debe incluir una encuesta entre el personal para identificar sus temores e inquietudes respecto a la labor que desempeñan y las vulnerabilidades que enfrentan, por ejemplo, el riesgo de ser víctimas de un asalto o robo con violencia en la parte de la empresa que tiene contacto con el público. También puede ser necesario un Foro Confiable de Terceros en el que las empresas tengan la posibilidad

de discutir las amenazas de extorsión y las sospechas de corrupción en la contratación, para complementar el enfoque de escrutinio honesto del sector público para los contratistas.

Delincuencia digital

Los riesgos identificados en el apartado anterior deben incluir un profundo entendimiento de los riesgos del ambiente digital y del entorno físico. Es decir, ¿la empresa se ha protegido contra la intrusión digital? ¿Cuenta con un método y política de seguridad cibernética adecuados, que abarque tanto las amenazas internas como las externas? El esfuerzo que se haga para protegerse de la delincuencia digital externa debe ser reproducido al interior de la empresa considerando al delincuente digital o al empleado negligente. La atención al cliente y los datos comerciales tienen un gran valor en el ambiente digital en el que operan la mayoría de las organizaciones. Entender los delitos contra el personal ayudará a identificar los aspectos y hacia dónde deben dirigirse los esfuerzos para reducir el impacto en la empresa.

Compartir la información

Existe una cantidad enorme de material sobre la prevención de la delincuencia que puede ser reproducido o descargado directamente a los sitios web corporativos o enviarse directamente al personal. Poner atención a los problemas que le interesan al personal, aunque no sean responsabilidad directa de los empleadores, demuestra que la organización se preocupa por el personal. Al compartir información a bajos costos los empleadores podrían proporcionar con facilidad información adecuada. Las recomendaciones del área de atención a víctimas o de la policía también podrían resultar de utilidad. Asimismo, compartir las noticias sobre delitos locales provenientes de la policía o de otras instituciones puede contribuir a crear una plantilla laboral que esté consciente de la delincuencia.

Crear redes

Darse a la tarea de establecer redes con las organizaciones locales de aplicación de la ley. Al buscar presentaciones y compartir información a nivel estratégico probablemente contribuya a reducir obstáculos en caso de que la organización o el personal necesiten asistencia. Estas acciones demuestran que la empresa está enfocada en la prevención y en apoyar a su personal.

Participar a nivel local

Participar más, ya sea con los grupos antidelincuencia o grupos comunitarios que se dedican a compartir información o emprendiendo acciones para reducir la vulnerabilidad. Esto podría ser algo tan simple como suscribirse a boletines informativos sobre la delincuencia local o crear estas publicaciones. Contar con un entendimiento dinámico de los índices delictivos actuales asegura que la empresa es capaz de protegerse a sí misma.

Exigir rendición de cuentas

Una vez que se haya identificado el nivel de delincuencia local y el grado de criminalidad, hay que asegurar que las actividades de aplicación de la ley estén enfocadas en combatir la delincuencia. No se trata de ser crítico, sino de comprometerse con la policía y con el área de atención a víctimas para promover acciones efectivas contra la delincuencia y asegurarse que los servidores públicos rindan cuentas. Éste es un aspecto muy importante de la estrategia que permite que las empresas del sector privado o sus organismos representantes demuestren que están dispuestos a cuestionar y entender las estrategias de aplicación de la ley implementadas por la policía local. De igual forma, la policía local debe ser clara respecto a sus iniciativas a nivel local y debe dar a conocer sus actividades de manera efectiva.

Patrocinar con cautela

Algunas inversiones en las iniciativas de prevención de la delincuencia pueden ser valiosas. Esta inversión va desde ejercicios de relaciones públicas hasta un compromiso pleno con el equivalente local de CEOP o NFIB. En un nivel más sencillo, las donaciones destinadas a apoyar los esfuerzos de reducir la delincuencia, aunque sean pequeñas, representan ventajas en mercadotecnia y relaciones públicas, por ejemplo, la inversión en folletos con información referente a la prevención de la delincuencia en los que se muestre el logotipo de la empresa o financiar la compra de equipos para prevenir el delito.

Invertir con cuidado

La inversión también puede influir en otros organismos. Por ejemplo, ofrecer apoyo económico que esté sujeto a que otros contribuyan con una cantidad similar ayudará a activar las iniciativas o proyectos que de otra forma fracasarían. El mensaje público emitido por empresas que trabajan en colaboración, como en el caso de un proyecto con cofinanciamiento equitativo para crear un sistema de monitoreo con circuito cerrado de televisión (CCTV) podría resultar muy positivo. Asimismo, es más probable que los organismos se involucren con los lugares en que han realizado inversiones financieras o han colaborado con personal o equipos.

Capacitación conjunta

Los ejercicios de capacitación conjunta o los intercambios mutuos ayudan a eliminar barreras y a comprender mejor los problemas que otros enfrentan o su perspectiva de los problemas enfrentados por el sector privado. Ofrecer un recorrido diurno por las instalaciones de la fábrica, un día de capacitación sobre liderazgo para los gerentes o un recorrido por las oficinas, puede ayudar a reducir los malentendidos con otros organismos, en particular con los que están a cargo de la aplicación de la ley. Incluso, dedicar un poco de tiempo, para permitir que los líderes de la policía vivan la experiencia del entorno de trabajo de la empresa puede ayudar a fundar los cimientos para una

futura colaboración. Asimismo, las visitas de intercambio mutuo permitirán que el sector privado se de cuenta de las restricciones y límites de las organizaciones del sector público.

Analizar y establecer

Cualquier estrategia tendrá que cambiar al enfrentarse a nuevos mercados, políticas públicas y personas. El esfuerzo encaminado a permitir la prevención constante de la delincuencia forzosamente debe ser dinámico y adaptarse a los nuevos retos y riesgos. Las nuevas formas de cometer delitos deberán ser contrarrestadas por nuevas formas de prevención y reducción.

La información anterior representa un modelo que permite a las organizaciones del sector privado estar involucradas en los niveles más apropiados. Obviamente, el modelo depende de la confianza mutua y de la confianza en la policía, en las políticas públicas y en el sector privado. Esto es algo que al principio debe trabajarse a manera de ensayo con el objetivo de ampliarlo en caso de que funcione. El modelo británico de financiamiento privado de las unidades policiales antifraude resulta controversial en muchos países, pero no en América Latina, donde la privatización de la seguridad física es una práctica habitual. Sin embargo, los problemas de gobierno de las unidades necesitan atención especial para generar legitimidad en la comunidad empresarial y en la sociedad en general. En el Reino Unido, se tiene cuidado de asegurar que no haya una interferencia activa por parte de las empresas en los casos individuales, mientras que la policía debe rendir cuentas sobre sus estrategias y responsabilidades.

6.4.1.1 ¿Cómo podría implementarse este modelo en el contexto mexicano?

Morris (2012) examina la corrupción, el narcotráfico y la violencia en México, y describe la manera en que la corrupción y las organizaciones criminales han distorsionado el funcionamiento del Estado mexicano y de su sector privado. La participación de los organismos públicos en la delincuencia relacionada con las drogas y en los grupos criminales hace que el enfoque sea más problemático. Sin embargo, no lo obstaculiza por completo. Morris enuncia la "regla del déficit de ley" y el impacto que la guerra contra el narcotráfico tiene en éste y otros aspectos que tienen un largo historial en muchas partes de América Latina. Esta situación hace que resulte difícil, pero no imposible, implementar una estrategia de colaboración. Volver a una estrategia de aislamiento y dejar de relacionarse con los organismos públicos y la policía, amplía la brecha entre los sectores público y privado. Aunque se necesitan estrategias nuevas y creativas para emprender la guerra contra el narcotráfico, el compromiso con las nuevas formas de trabajar del sector privado ayudará a enfrentar de una mejor manera la delincuencia, la cual puede reducir la generación de riqueza.

Ferragut (2012) identifica la relación entre el narcotráfico y la vulnerabilidad, pero también explora la relación con el lavado de dinero. En particular, se enfoca en las ganancias obtenidas

por las organizaciones del sector privado a través del "lavado" de dinero proveniente del narcotráfico. Su análisis demuestra la manera en que las empresas que participan pueden obtener una ventaja injusta en términos financieros, en comparación con las empresas que no se involucran en ello. La estrategia mencionada sobre la participación del sector privado en la reducción de la delincuencia, aún podría implementarse contra el lavado de dinero ayudando a identificar a quienes estén involucrados. Así, las empresas tendrán la oportunidad de reequilibrar sus mercados y de crear una condición de equidad comercial.

Vilalta (2013a, b) analiza el temor al delito y la vulnerabilidad en México describiendo las variables que afectan la seguridad. Esto incluye la victimización directa, la edad, las muestras de incivilidad y la confianza en la policía. Todas estas variables pueden ser abordadas a través del modelo de participación del sector privado. El modelo se beneficia al identificar las acciones que se pueden implementar para enfrentar la vulnerabilidad, que concuerdan con el modelo.

El Grupo Informativo sobre la Crisis Internacional (2013, p. 13) describe los retos de corrupción que enfrenta México. También detalla el trabajo que el gobierno mexicano está llevando a cabo para abordar las preocupaciones de la ciudadanía y de la comunidad internacional. El Modelo de Participación del Sector Privado para la Prevención de la Delincuencia se puede emplear para establecer una amplia inversión interna descrita por el Grupo Informativo sobre la Crisis Internacional.

Schatz (2011) explica el impacto de los cambios en el sistema judicial tras el éxito de los procesos penales. Aunque existe un panorama difícil respecto a la capacidad para responder a los homicidios relacionados con el pandillerismo, el documento habla sobre el riesgo de que se incremente la vulnerabilidad o el temor al delito. El modelo sugiere involucrar al sector privado para entender los riesgos y temores del personal. Schatz ofrece información valiosa sobre los riesgos más graves.

Felbab-Brown (2013) menciona la manera en que el nuevo gobierno mexicano pretende abordar los problemas graves de delincuencia que aquejan al país, incluyendo la corrupción y el narcotráfico. El Modelo de Participación del Sector Privado para la Prevención de la Delincuencia corresponde con los nuevos enfoques de la policía, el espionaje y la justicia penal descritos por Felbab-Brown.

Este modelo de participación puede ser utilizado por las organizaciones individuales del sector privado, o a través de organismos de representación. El modelo depende totalmente de un compromiso por parte del sector privado para convertirse en parte de la solución que reduzca y prevenga la delincuencia, y no es ni complejo ni costoso. En caso de que requieran inversión, las organizaciones y líderes del sector privado pueden recurrir a las contribuciones o financiamiento equitativo de sus socios. El hecho de relacionarse o participar con los organismos del sector público comenzará a derribar las barreras existentes

entre ambos sectores: proporcionar oportunidades no costosas para fomentar la creación de mejores relaciones y redes efectivas creará un entorno de colaboración. La prevención de la delincuencia no es monopolio del Estado. Todos los ciudadanos tienen oportunidad y motivos para participar. Quienes gozan de influencia o poder, en particular las personas del sector privado, tienen la oportunidad de aplicar el uso de recursos para un bien común. Menos criminalidad es sinónimo de mejores empresas en una sociedad más unida, en el corto, mediano y largo plazos.

6.4.2 Recomendaciones

El punto donde México se encuentra actualmente y el punto al que desea llegar implica recorrer un camino largo y sinuoso. Algunos de los asuntos relacionados con la recolección y divulgación de datos en el sector privado y en las sociedades entre éste y el sector público se han desarrollado tentativamente, en otras partes del mundo a lo largo de los años, y requieren compromiso y energía para implementarlos. Levi *et al.* (2003) observaron que, incluso en el Reino Unido, los profesionales en el área de seguridad por lo general no consideraban que sus Juntas de Gobierno estuvieran demasiado involucradas en los asuntos de reducción de la delincuencia. Desde entonces, no hay pruebas de si esto ha cambiado o no, con la excepción del sector de servicios financieros, tras haberse publicitado la imposición de enormes multas y advertencias de procesamiento, y realizar cambios en la responsabilidad corporativa mediante la Ley de Cohecho de 2010. No obstante, se han llevado a cabo con éxito muchos esfuerzos para reducir los problemas de delincuencia en el sector empresarial, en ocasiones en combinación con los esfuerzos para reducir la corrupción en el sector público.

1. Que se adopte el principio de que el sector privado es un socio importante y esencial para la estrategia de prevención de la delincuencia.
2. Al hacerlo, las organizaciones de la red del sector privado deben tratar de identificar el verdadero alcance de la delincuencia en sus miembros, incluyendo el impacto directo e indirecto.
3. Que el Modelo de Participación del Sector Privado para la Prevención de la Delincuencia sea adoptado a nivel nacional.
4. Que los sistemas eficaces de denuncia de delitos proporcionen un máximo de oportunidades para permitir que las organizaciones del sector privado denuncien los delitos.
5. Para facilitar y mejorar el proceso de denuncias, los centros de registro de terceros no gubernamentales deben representar una alternativa eficaz. Los centros de registro de terceros motivan a la ciudadanía a denunciar los delitos sin la injerencia de la policía.
6. Como parte de una estrategia sostenida para la prevención de la delincuencia, los encargados del diseño de políticas públicas deben crear oportunidades para permitir que los interesados de los sectores público y privado compartan información y experiencias.
7. Las iniciativas locales de prevención de la delincuencia deben emplear la creatividad y flexibilidad de las organizaciones del sector privado. Depender de las contribuciones

financieras del sector privado para respaldar la reducción del financiamiento público no debe ser el principal objetivo.

8. Los encargados de la elaboración de políticas públicas deben identificar los riesgos de la asociación público- privada y describir con detalle la estrategia para reducir de manera significativa la creación de oportunidades para los actos de corrupción.
9. Los encargados del diseño de políticas públicas deben incentivar las iniciativas de los sectores público y privado para fomentar el entendimiento y los enfoques conjuntos para la resolución de problemas.

Referencias

Bamfield, J. (2010). *Shrinkage and Loss Prevention: Evidence from the Global Retail Theft Barometer*. Centre for Retail Research

Beittel, J. (2013). *Mexico's drug trafficking organizations: Source and scope of the violence*. Washington D. C.: US Congressional Research Service. https://www.fas.org/sgp/crs/row/R41576.pdf

British Columbia. (2012). *Overview of Crime Data Collection in British Columbia* 2011. Vancouver: Police Services Division, Ministry of Justice, British Columbia.

Buffat, J. (2002). *Securities Crime Prevention Europe: A comparative study of crime prevention policies in seven European cities.* http://stop-reoffending.org/fileadmin/efus/pdf/Secucities_Crime_Prevention_Europe.pdf

Caneppele, S., Riccardi, M. & Standridge, P. (2013). Green energy and black economy: mafia investments in the wind power sector in Italy. *Crime, Law and Social Change*, 59 (3), pp. 319-339.

Capobianco, L. (2008). *International Compendium of Crime Prevention Practices: To Inspire Action Across the World 2008*. Montreal: International Centre for the Prevention of Crime. http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Compendium_of_Crime_Prevention_Practices_ANG.pdf

Capobianco, L. (2005). *Sharpening the Lens: Private sector involvement in crime prevention*. Montreal: International Centre for the prevention of crime. http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/Sharpening_the_Lens._Private_Sector_Involvement_in_Crime_Prevention_ANG.pdf

Carbonari, F. (2012). *Private Sector and Community Safety in Latin America and the* Caribbean' *ICPC. Colloquium, February 2012.* http://www.crime-prevention-intl.org/fileadmin/user_upload/Evenements/10th_ICPC_Colloquium/Proceedings/Flavia_Carbonari.pdf

CEOP. (2010). *Introduction to the Child Exploitation and Online Protection Centre*. http://ceop.police.uk/Publications/

CEOP. (2011). *CEOP Relationship Management Strategy*, http://www.ceop.police.uk/Documents/ceopdocs/Relationship_Management_Strategy.pdf

CIFAS. (2013). *Fraudscape 2012*. Londres: CIFAS.

Clarke, R. & Homel, R. (1997). A Revised classification of situational crime prevention techniques. En Lab, S. P. (Ed.), *Crime prevention at a crossroads* (pp. 17-30). Cincinnati, OH: Anderson.

Commission of the European Community (2004). *Crime Prevention in the European Union*. Brussels 12.3.2004 COM(2004) 165 final.

Detica. (2012). *The Cost of Cyber Crime*. Londres: BAE Systems.

Di Tella, R., Edwards, S. & Schargrodsky, E. (Eds.). (2010). *The Economics of Crime: Lessons For and From Latin America*. Chicago: Chicago University Press.

Doig, A. & Levi, M. (marzo, 2013). A Case of Arrested Development? Delivering the UK National Fraud Strategy within Competing Policing Policy Priorities. *Public Money and Management*, 33(1), pp. 1-8.

Ernst & Young. (2013). *Growing Beyond: a place for integrity, 12th Global Fraud Survey*. Londres: Ernst & Young.

Felbab-Brown, V. (2013). *Peña Nieto's Piñata: The Promise and Pitfalls of Mexico's New Security Policy against Organized Crime*. Washington D.C.: Brookings.

Felson, M. & Clarke, R. (Eds.). (1997). *Business and Crime Prevention*. Boulder: Lynne Rienner.

Ferragut, S. (2012). Organised Crime illicit drugs and money laundering: the United States and Mexico. *International Security Programme Paper.* Londres: Chatham House.

Gabor, T., Kiedrowski, J., Hicks, D., Levi, M., Goldstock, R., Melchers, R. & Stregger, E. (2012). *Economic Sectors Vulnerable to Organized Crime: Commercial Construction*. Ottawa: Gobierno de Canadá. http://publications.gc.ca/collections/collection_2012/sp-ps/PS4-124-2012-eng.pdf

Home Office Counting Rules (n.d.) https://www.gov.uk/government/publications/counting-rules-for-recorded-crime

ICPC (2010). *International Report on Crime Prevention and Community Safety: Trends and Perspectives, 2010*. Montreal: International Centre for the Prevention of Crime.

INEGI. (2012). *National Survey on Victimization and Perception of Public Security 2012.* Ciudad Juárez, México.

Innes, M. (2004). Signal crimes and signal disorders: notes on deviance as communicative action. *British Journal of Sociology*, 55(3), pp. 335-55.

International Crisis Group. (2013). Justice at the Barrel of a Gun: Vigilante Militias in Mexico Crisis Group. *Latin America Briefing*, núm. 29, 28 de mayo de 2013. http://www.crisisgroup.org/~/media/Files/latin-america/mexico/b029-justice-at-the-barrel-of-a-gun-vigilante-militias-in-mexico.pdf

Jones, S. & Levi, M. (1983). The police and the majority: the neglect of the obvious. *The Police Journal*, LVI, pp. 351-364.

Kenney, D. & Godson, R. (2002). Countering crime and corruption: A school-based program on the US–Mexico border. *Criminal Justice*, 2(4), pp. 439–470.

Korsell, L. & Skinnari, J. (2010). Situational prevention against unlawful influence from organised crime. En Bullock, K., Clarke, R. & Tilley, N. (Eds.) *Situational Prevention of Organised Crimes*. Cullompton: Willan.

Kroll Advisory Solutions. (2013). *Global Fraud Report, Annual Edition 2012/13*. Nueva York: Kroll Advisory Group

Kulach, J. (2006). *Cultures of Prevention Urban Crime Prevention Policies In Europe: Towards A Common Culture*. París: European Forum for Urban Safety.

Latinobarómetro. (2012). *2011 Report*. Santiago: Corporación Latinobarómetro.

Levi, M. (próxima publicación). Legitimacy, crimes and compliance in 'the City': De Maximis non Curat Lex?. En Tankebe, J. & Liebling, A. (Eds.). *Legitimacy and Criminal Justice: An International Exploration*. Nueva York: Oxford University Press.

Levi, M. (2013). Trends and costs of fraud. En Doig, A. (Ed.) *Fraud: The Counter Fraud Practitioner's Handbook* (pp. 7-18). Andover: Gower Publishing.

Levi, M., Bissell, P. & Richardson, T. (1991). The Prevention of Cheque and Credit Card Fraud. Crime Prevention Unit, documento 26. Londres: Home Office.

Levi, M., Burrows, J., Fleming, M. & Hopkins, M. (with the assistance of M. Matthews). (2007). *The Nature, Extent and Economic Impact of Fraud in the UK*. Londres: Association of Chief Police Officers. http://www.cardiff.ac.uk/socsi/resources/ACPO%20final%20nature%20extent%20and%20economic%20impact%20of%20fraud.pdf

Levi, M., Morgan, J. & Burrows, J. (2003). Enhancing Business Crime Reduction: UK Directors' Responsibilities to Review the Impact of Crime on Business. *Security Journal*, 16(4), pp. 7-28.

Levi, M. & Williams, M. (2012). *eCrime Reduction Partnership Mapping Study*. http://www.cardiff.ac.uk/socsi/resources/Levi%20Williams%20eCrime%20Reduction%20Partnership%20Mapping%20Study.pdf

Liu, K. & Taylor, C. (Eds.). (2012). *The War on Mexican Cartels: Options For U.S. and Mexican Policy-Makers*. Reporte final. http://www.iop.harvard.edu/sites/default/files_new/research-policy-papers/TheWarOnMexicanCartels.pdf

Mohar, E. (2009). Fostering better policing through the use of indicators to measure institutional strengthening. *International Journal of Police Science and Management*, 12 (2), pp. 170-182.

Moloeznik, M. (2003). The challenges to Mexico in times of political change. *Crime Law and Social Change* 40, pp. 7-20.

Morris, S. (2012). Corruption, Drug Trafficking and violence in Mexico. *Brown Journal of World Affairs* Spring/Summer, 18 (2), p. 29. http://www.mtsu.edu/politicalscience/faculty/documents/Corruption%20Brown%20article%20Morris.pdf

Mugellini, G. (2012). *Crime against the private sector: existing data and future orientations to analyse the victimization of businesses*. Presentado en la *First International Conference on statistical information on government, public safety, victimization and justice*, UNODC-INEGI, Aguascalientes, 2 al 25 de mayo de 2012. http://www.cdeunodc.inegi.org.mx/doc/2.%20Crime%20against%20the%20private%20sector_Mugellini.pdf

Nataren, C. (2010). Notes on criminal process and constitutional reform in Mexico today. *Mexican Law Review* Vol. IV, núm. 1, pp. 99-125. http://biblio.juridicas.unam.mx/revista/pdf/MexicanLawReview/7/nte/nte5.pdf

National Fraud Authority. (2011). *Business Plan 2011/12*. Londres: National Fraud Authority.

National Fraud Authority. (2012) *Annual Fraud Indicator*. Londres: Home Office.

Nelen, H. (2010). Situational organised crime prevention in Amsterdam: the administrative approach. En Bullock, K., Clarke, R. & Tilley, N. (Eds.). *Situational Prevention of Organised Crimes*. Cullompton: Willan.

Political Risk Services. (2012). *Mexico, Country Conditions, Climate for Investment & Trade*, 1° de marzo de 2012. East Syracuse, NY.

Pshisva, R. & Suarez, G. (2010). Capital Crimes: Kidnappings and Corporate Investment in Colombia. En Di Tella, R., Edwards, S. & Schargrodsky, E. (Eds.). (2010). *The Economics of Crime: Lessons For and From Latin America*. Chicago: Chicago University Press.

Salt, M. (2011). *Criminal procedure law provisions on cybercrime in Latin America regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru)*.

Strasbourg: Council of Europe. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_d_LATAM_procedurallaw_Dec2011.pdf

Savona, E. (2010). Infiltration of the public construction industry by Italian organised crime. En Bullock, K., Clarke, R. & Tilley, N. (Eds.). *Situational Prevention of Organised Crimes*. Cullompton: Willan.

Schatz, S. (2011). The Mexican judiciary & the prosecution of organized crime: the long road ahead. *Trends in Organized Crime*, 14, pp. 347–360.

Sjogren, H. & Skogh, G. (Eds.). (2004). *New Perspectives on Economic Crime (New Horizons in Law and Economics)*. Cheltenham: Edward Elgar.

Svedberg Helgesson, K. (2011). Public-Private Partners Against Crime: Governance, Surveillance and the Limits of Corporate Accountability. *Surveillance & Society* 8(4), pp. 471-484.

The Economist. (2013). The new face of Mexican policing: A public-private effort to reduce violence in Mexico's wealthiest city. *The Economist*, 15 de junio de 2013. http://www.economist.com/news/americas/21579457-public-private-effort-reduce-violence-mexicos-wealthiest-city-new-face-mexican

Tyler, T. (2006). *Why People Obey the Law*. New Haven: Princeton UP.

Tyler T. (2009). Self-Regulatory Approaches to White-Collar Crime: The Importance of Legitimacy and Procedural Justice. En Simpson, S. & Weisburd, D. (Eds.). *The Criminology of White-Collar Crime*. Nueva York, Springer.

UNSC. (2013). Report of the National Institute of Statistics and Geography and the United Nations Office on Drugs and Crime on a road map to improve the quality and availability of crime at the national and international levels. Statistical Commission Forty Fourth session. *unstats.un.org/unsd/statcom/doc13/RD-CrimeStats.pdf*

UNODC. (2010). *Crime Prevention Handbook on the crime prevention guidelines: Making them work*. Vienna: UNODC.

Vilalta, C. (2013a). *Factors of the perception of insecurity in Mexico*. Roundtable: Crime and the fear of crime. Washington D. C.: Inter-American Development Bank. http://investigadores.cide.edu/carlos.vilalta/Personal/VilaltaIDBRoundtable.pdf

Vilalta, C. (2013b). Towards an understanding of community organisation against crime: the case of Ciudad Juarez. Mexico Stability (electrónico), Vol 2(1): 5, pp.1-15. http://dx.doi.org/10.5334/sta.ao;_http://reliefweb.int/sites/reliefweb.int/files/resources/Towards%20an%20understanding%20of%20community%20organization%20against%20crime_The%20case%20of%20Ciudad%20Juarez_Mexico.pdf

World Bank. (2010). *Mexico Country Profile, Enterprise Survey*. Washington, D. C.: World Bank e International Finance Corporation. http://www.enterprisesurveys.org/Data/ExploreEconomies/2010/mexico#crime)

World Bank. (2011). *Public-Private Partnerships and Community Safety: Guide to Action*. The International Centre for the Prevention of Crime (ICPC), World Bank Sustainable Development Department for Latin America and the Caribbean, Security and Coexistence Directorate of the Bogotá Chamber of Commerce and the Instituto Sou da Paz.