ALIANZAS PÚBLICO - PRIVADAS

Una aproximación a la gestión de riesgos para confrontar las amenazas a la seguridad

OEA Más derechos para más gente

unicri United Nations Interregional Crime and Justice Research Institute

OAS Cataloging-in-Publication Data

Alianzas Público-Privadas: Una aproximación a la gestión de riesgos para confrontar las amenazas a la seguridad [preparado por el Comité Interamericano contra el Terrorismo de la Secretaría General de la Organización de Estados Americanos (OEA/CICTE) y el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI)].

p. ; cm. (OAS. Official records; OEA/Ser.L/X.6.7)

ISBN 978-0-8270-7796-6

1. Security, International--Handbooks, manuals, etc. 2. Public-private sector cooperation--America--Handbooks, manuals, etc. 3. Public safety--Security measures--Handbooks, manuals, etc. I. Title. II. Organization of American States. Secretariat for Multidimensional Security. Interamerican Committee Against Terrorism. III. United Nations Interregional Crime and Justice Research Institute. IV. Series.

OEA/Ser.L/X.6.7

Con el apoyo financiero del Gobierno de Canadá

Canada

Reseña. Referencia rápida

El Manual de Alianzas Público-Privadas representa una guía para la creación y el fortalecimiento de alianzas público-privadas en las Américas, enfocadas en enfrentar y mitigar las amenazas antrópicas a la seguridad, como el terrorismo y la criminalidad organizada.

Este Manual actualiza y amplía el original publicado en 2010 por el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI). Su elaboración fue posible gracias a un proyecto conjunto entre UNICRI y el Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA), y al apoyo financiero del Ministerio de Asuntos Globales de Canadá.

Su elaboración es fruto tanto de la experiencia acumulada de las entidades mencionadas como del consultor a cargo de su redacción[1] en un trabajo que contó con la colaboración y validación de los puntos focales de los países de las Américas convocados para estos efectos.

> El objetivo del Manual es proporcionar un instrumento de trabajo que promueva, fortalezca y apoye las alianzas público-privadas en la prevención, detección y el control de las amenazas antrópicas a la seguridad. Además, busca motivar a los actores involucrados a tomar la iniciativa para identificar contrapartes en ambos sectores y comenzar a trabajar en la búsqueda de nuevos y mejores resultados en materia de reducción de riesgos a la seguridad, vinculados a las amenazas terroristas y la criminalidad organizada.

Sin duda, las alianzas público-privadas en materia de seguridad han demostrado ser herramientas valiosas para enfrentar de manera efectiva y eficiente diversos desafíos en este ámbito. A través de la colaboración bidireccional entre ambos sectores, se han logrado generar soluciones innovadoras que agregan valor a los proyectos y aumentan la tasa de retorno positivo. Este Manual actualizado procura ser un recurso esencial para todos aquellos que trabajen en la prevención y el control del terrorismo y del crimen organizado como principales fenómenos de amenaza a la seguridad en la región.

Este Manual es un documento fundamental para los interesados en establecer y fortalecer la colaboración entre los sectores público y privado en materia de seguridad. Este texto actualizado y ampliado ofrece una vasta gama de herramientas y enfoques innovadores para abordar las cambiantes amenazas a la seguridad en la región.

[1] **Marko Magdic. Consultor Internacional en Seguridad Pública y Crimen Organizado.**

Es necesario leer este manual por las siguientes razones:

* **Relevancia y actualidad:** El texto aborda temas actuales y de gran importancia, como el terrorismo y la criminalidad organizada, y ofrece soluciones basadas en la colaboración entre los sectores público y privado.

* **Enfoque integral y metodologías adecuadas:** El manual presenta un enfoque completo que abarca desde la definición de las alianzas público-privadas hasta el diseño y la gestión de proyectos conjuntos. También proporciona información sobre aspectos relevantes como la economía, las políticas de género y el tratamiento de la información.

* **Ejemplos de éxito y objetivos claros:** El documento incluye casos de éxito de alianzas público-privadas en áreas específicas de la seguridad y presenta objetivos claros para motivar a los actores involucrados a identificar contrapartes y trabajar juntos en la búsqueda de mejores resultados en materia de seguridad.

* **Colaboración internacional y experiencia acumulada:** El manual se basa en la experiencia de instituciones reconocidas, como UNICRI, CICTE/OEA, y de personal experto, lo que garantiza un enfoque bien fundamentado y respaldado por especialistas en la materia.

Este manual es una lectura altamente recomendada para aquellos que quisieran abordar de manera efectiva y eficiente los desafíos de la seguridad en las Américas, mediante la creación y el fortalecimiento de las alianzas público-privadas.

Temas clave:

- *Definición y naturaleza de las alianzas público-privadas (APP) en seguridad.*
- *Primeros pasos para establecer una colaboración efectiva entre sectores público y privado en materia de seguridad pública.*
- *Diagnóstico conjunto de problemas de seguridad y análisis de casos específicos.*
- *Establecimiento de alianzas estratégicas entre el sector público y privado en seguridad.*
- *Diseño y gestión de proyectos conjuntos con metodologías adecuadas y pensamiento creativo.*
- *Aspectos relevantes en el diseño de proyectos conjuntos: factor económico y políticas de género.*
- *Tratamiento de la información y desafíos en el intercambio de datos entre entidades públicas y privadas.*
- *Construcción de confianzas y superación de desafíos en las alianzas público-privadas en seguridad.*
- *Ejemplos e ideas de casos de éxito en alianzas público-privadas en áreas específicas de la seguridad.*
- *Comité de Crisis.*

Antes de comenzar

Antes de comenzar a leer el documento, por favor conteste las siguientes preguntas, sin tomar en consideración si usted o su entidad forman parte del sector público o, por el contrario, es integrante de la comunidad o representa un actor no estatal.

Las respuestas y su puntuación le permitirán saber si el documento pudiera ser útil y adecuado a sus necesidades.

Preguntas	Sí	No
¿Ha sido afectada su entidad, organización o el conjunto de afiliados, integrantes o personas que la componen con los problemas o externalidades negativas derivadas de una amenaza a la seguridad pública?	1	0
¿Ha diagnosticado la problemática e identificado tanto los factores que la posibilitan como aquellas que pudieran contrarrestarla?	0	1
¿Ha realizado algo al respecto que le haya dado resultados satisfactorios?	0	1
¿Considera que es posible hacer más?	1	0
¿Cuenta su entidad u organización con objetivos específicos para enfrentar proactivamente los problemas y externalidades negativas derivadas de una amenaza a la seguridad pública?	0	1
¿Ejecuta actualmente proyectos en estas áreas para prevenir, controlar, detectar tempranamente o dar respuesta a estas amenazas?	0	1
¿Ejecuta esos proyectos en el marco de una colaboración pública-privada conjunta y activa?	0	1
¿Cree que al hacer siempre lo mismo los resultados no van a cambiar, y que se requiere de un cambio en la forma de enfrentar algunos de los desafíos en seguridad pública?	1	0

Si usted o su entidad contestó todas las preguntas y el resultado de sumar las respuestas es de al menos 2 puntos, entonces recomendamos que lea este manual.

Se debería tomar la iniciativa en identificar contrapartes en ambos sectores y comenzar a trabajar en la búsqueda de nuevos y/o mejores resultados. ¿Cómo? Este Manual no resolverá todas sus dudas, ni le proporcionará absolutamente todos los elementos, pero será un primer gran paso.

Índice

Antecedentes

En el año 2010, el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI por sus siglas en inglés) publicó un Manual[2] para apoyar el establecimiento de las alianzas público-privadas con el fin de proteger objetivos vulnerables. El Manual se desarrolló dentro del contexto del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo (CTITF por sus siglas en inglés).

Para el año 2021, ya habían transcurrido poco más de 11 años desde el lanzamiento de este importante esfuerzo. Las amenazas de una década atrás habían experimentado cambios importantes, y los objetivos contra los que estas se dirigían, también.

Conscientes de esta realidad, UNICRI, junto al Comité Interamericano contra del Terrorismo de la Organización de los Estados Americanos (CICTE/OEA), y con el apoyo financiero del Gobierno de Canadá, decidieron dar un nuevo impulso a los beneficios generados en el pasado con la mencionada iniciativa, para lo que se propusieron promover un nuevo Manual que, recogiendo las buenas prácticas del documento que lo precedió, entregara nuevas herramientas de trabajo que resultaran funcionales para los actuales riesgos a la seguridad así como en la optimización de las alianzas público-privadas para prevenir, detectar y responder ante las diversas amenazas en este campo.

El apoyo y la participación activa del CICTE/OEA permitió generar actividades de levantamiento y validación de datos con expertos individuales y representantes gubernamentales de los países de las Américas, lo que explica que una parte importante de observaciones, comentarios y análisis relacionados con las principales amenazas, estuvieran vinculadas a la región.

Fue precisamente ese escenario de análisis y consultas regionales lo que permitió validar y definir las rutas a seguir en términos del tipo de amenazas a abordar, así como el momento de intervención recomendado para una alianza público-privada.

En relación con el primer punto, se pudo establecer como una de las principales amenazas a la seguridad en las Américas aquella vinculada a las amenazas antrópicas, provocadas por el hombre, que impactan directamente a la seguridad pública en sus diversas modalidades, aunque preferentemente en lo que se refiere al terrorismo y la criminalidad organizada (tráfico de drogas, tráfico de armas, trata y tráfico de personas, contrabando, lavado de activos y corrupción, entre otros).

Con respecto al segundo punto, las consultas y reuniones regionales realizadas identificaron como prioridad no solo la respuesta a incidentes y amenazas que afecten la seguridad, sino también los mecanismos de prevención, por un lado, y de detección temprana, por otro, en los cuales colaboren y trabajen conjuntamente el sector público y privado en formato de alianza. De ahí el enfoque otorgado a este manual.

[2] **Handbook to assist the establishment of public private partnerships for the protection of vulnerable targets (UNICRI - 2010). Disponible en inglés, español y portugués.**

Gestores de la iniciativa

Comité Interamericano Contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA)

> La Secretaría General de la Organización de los Estados Americanos (SG/OEA), a través de la Secretaría de Seguridad Multidimensional (SSM), promueve y coordina la cooperación entre los Estados Miembros de la OEA, y de estos con el Sistema Interamericano y otras instancias del Sistema Internacional, para evaluar, prevenir, enfrentar y responder efectivamente a las amenazas a la seguridad, con la visión de ser el principal referente hemisférico para el desarrollo de la cooperación y el fortalecimiento de las capacidades de los Estados Miembros de la OEA.

La Secretaría Ejecutiva del Comité Interamericano contra el Terrorismo (SE/CICTE) apoya a los Estados Miembros en el diseño, implementación y evaluación de políticas nacionales para prevenir, combatir, eliminar el terrorismo, y fortalecer la capacidad antiterrorista de estos, así como en el diseño y ejecución de iniciativas para reforzar sus capacidades institucionales en la materia. El programa de seguridad de los espacios concurridos tiene más de 15 años de experiencia en el desarrollo y la aplicación de estrategias nacionales destinadas a mejorar la capacidad de los Estados Miembros de la OEA, a través de la capacitación brindada a oficiales de todos los sectores, en el diseño y aplicación eficaz de planes de seguridad integrados para la protección de los espacios concurridos y de los objetivos vulnerables, como son los grandes eventos y/o los destinos turísticos.

Instituto Interregional de Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia

UNICRI es una agencia de las Naciones Unidas establecida en 1967 para apoyar a los países en la prevención del delito y facilitar la justicia penal. En este ámbito, UNICRI apoya a las organizaciones intergubernamentales, gubernamentales y no gubernamentales en la formulación y aplicación de políticas de mejora. Las metas de UNICRI son avanzar en la comprensión de los problemas relacionados con la delincuencia; promover reformas justas y eficientes de los sistemas de justicia penal; favorecer el cumplimiento de los instrumentos internacionales y otras normas; y, facilitar la cooperación policial internacional y la asistencia judicial.

Colaboración y agradecimiento

La elaboración de este Manual fue posible gracias a la colaboración de varias personas y entidades que merecen el agradecimiento de los gestores de esta iniciativa.

* A Marko Magdic, consultor senior en seguridad pública y crimen organizado, principal redactor de este Manual.[3]

* Al equipo de trabajo del Programa de Seguridad de Espacios Concurridos del Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA).

* Al equipo de trabajo del Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI).

* A los representantes de los Estados Miembros de la OEA que participaron en las actividades y validaron la información que dio lugar a este reporte.

[3] Marko Magdic es un consultor senior con 20 años de experiencia en justicia, seguridad pública y crimen organizado, que ha participado en proyectos operativos y estratégicos relacionados con políticas públicas y prevención y control de riesgos corporativos y gubernamentales. Ha trabajado en el diseño y ejecución de ejercicios, simulaciones y simulacros público-privados en América Latina, y ha participado en el diseño e implementación de estrategias y planes de acción en temas como la Resolución ONU 1325, bioterrorismo, ciberseguridad, crimen organizado, seguridad nuclear y radiológica. En los últimos años, Magdic ha enfocado su experiencia en proyectos de seguridad turística, crimen organizado y terrorismo, siendo consultor senior en el Programa de Seguridad Turística de la Organización de los Estados Americanos. Ha contribuido a la elaboración del Reporte Regional de Seguridad Turística en México, América Central y el Caribe 2016 – 2019, y colaboró en el diseño y optimización de las estrategias nacionales y planes de acción de seguridad turística tanto a nivel gubernamental como también regional. Complementa lo anterior con el trabajo en proyectos e iniciativas en más de 30 países en colaboración con diversas organizaciones internacionales y entidades gubernamentales en crimen organizado, terrorismo y seguridad turística. Magdic es miembro de la Asociación Mundial de Fiscales (IAP), Iniciativa Global contra el Crimen Organizado Transnacional (GITOC), el Colegio de Abogados de Estados Unidos, y Abogados sin Fronteras de Canadá, entre otros.

Objetivo

Proveer de un instrumento de trabajo que contenga herramientas para promover, fortalecer y apoyar las alianzas público-privadas en las Américas que tengan como objetivo prevenir, detectar y controlar las amenazas antrópicas a la seguridad, con especial enfoque en la seguridad.

Metodología y contexto

Como se desprende del objetivo de este Manual, la herramienta se estructura en torno a tres variables que le dan contexto y un marco de análisis concreto:

* Amenazas antrópicas, provenientes de la actividad humana intencional.
* Amenazas antrópicas a la seguridad.
* Amenazas antrópicas a la seguridad en las Américas.

Para la elaboración de este documento se tomaron en cuenta los insumos contenidos en el Manual elaborado en el año 2010 por UNICRI, la experiencia del consultor principal a cargo del proyecto, los aportes de los puntos focales nacionales designados por los Estados Miembros de la Organización de los Estados Americanos, así como la experiencia tanto de la OEA como UNICRI, quienes con diversos socios estratégicos han desarrollado en los últimos años programas de trabajo y han acumulado conocimiento junto a los países de la región en materia de seguridad turística, seguridad de grandes eventos y seguridad en infraestructura crítica.

Lo complementa la realización de una serie de reuniones técnicas realizadas con el objeto de levantar información y validar el enfoque y tipo de las principales amenazas, así como obtener retroalimentación. Las actividades realizadas fueron las siguientes:

01 **Caribe**
Taller subregional sobre Seguridad de Grandes Eventos Deportivos: Premier League Cricket CPL T20. Virtual. 23-25 de febrero de 2021.

02 **Sudamérica:**
Taller subregional de América del Sur sobre la Seguridad de los Grandes Eventos Deportivos. Virtual. 29-31 marzo, 2022.

03 **Costa Rica**
Taller Nacional sobre Seguridad de Grandes Eventos: FIFA Sub-20 Copal del Mundo Femenil. Presencial. 18-21 julio, 2022.

04 **República Dominicana**
Taller Regional en Seguridad Turística. 15-17 noviembre, 2022.

05 **Chile**
Taller Nacional sobre Seguridad de Grandes Eventos: 2023 Juegos Panamericanos. Presencial. 24-27 enero, 2023.

06 **Centroamérica**
Taller subregional de Centroamérica, República Dominicana y México sobre la Seguridad de los Grandes Eventos Deportivos. Presencial. 21-23 marzo, 2023.

Riesgos, amenazas y vulnerabilidades actuales

En este capítulo, se abordarán los riesgos, amenazas y vulnerabilidades actuales que enfrentan las Américas en términos de seguridad. Se analizarán la naturaleza y el impacto de las amenazas más relevantes en la región, cómo la probabilidad de materialización de estas amenazas está influenciada por distintos factores de vulnerabilidad y la importancia de abordar estos desafíos mediante las alianzas público-privadas, generando una respuesta coordinada e integral.

Los riesgos a la seguridad se conciben como el nivel de probabilidad que una determinada amenaza a esa seguridad se concrete. El grado de probabilidad, a su vez, se ve condicionado por las vulnerabilidades presentes en un momento determinado. Las Américas enfrentan una variedad de amenazas en términos de seguridad, que son variadas, dinámicas y relativamente concentradas en algunas subregiones.

Estas amenazas se pueden dividir en dos grandes grupos:

***Amenazas de resultado** (terrorismo y crimen organizado).*

***Amenazas de medio** (corrupción, lavado de activos y canalización de demandas sociales a través de violencia organizada y no espontánea).*

La probabilidad de materialización de estas amenazas depende del nivel de vulnerabilidad al que se ve expuesta la región. Las vulnerabilidades se pueden clasificar en internas (o de gestión) y externas (o de ambiente).

Riesgos

Hablar de amenazas nos lleva a hablar de un concepto más amplio: Los riesgos. Efectivamente, y tomando en cuenta el contexto mencionado, los riesgos a la seguridad pueden concebirse como el grado de probabilidad de que una amenaza, a esa seguridad, se concrete. El mayor o menor nivel de probabilidades de que ello ocurra dependerá, a su vez, de las vulnerabilidades presentes en un momento determinado.

Podríamos también decir que una mayor o menor vulnerabilidad está dada por la forma en la que nos organizamos y confrontamos esas amenazas.

Esquema 1. Riesgos. Elaborado por Marko Magdic

Lo anterior nos obliga a abordar, en primer lugar, las amenazas, para posteriormente adentrarnos en las vulnerabilidades.

Amenazas

En la actualidad, y ya comenzada la segunda década del siglo XXI, las amenazas que enfrentan las Américas en términos de seguridad son variadas, dinámicas y relativamente concentradas. Son variadas en tanto son múltiples. Son dinámicas porque son cambiantes y se manifiestan en constante evolución, si es que no por el tipo de amenaza, cuando menos por la forma y manera en la que se concreta. Tienen, finalmente, una concentración relativa, porque si bien son transversales al continente, algunas subregiones presentan mayores niveles de intensidad que otras.

La información levantada en las diversas actividades mencionadas en la sección de metodología de este informe mostraba que mientras el tráfico de armas generaba mayor preocupación en algunos países del caribe, la extorsión era un fenómeno más crítico para las naciones centroamericanas, en tanto que el tráfico de drogas y el contrabando fue mencionado recurrentemente por representantes sudamericanos.

La afirmación anterior no pretende ser un diagnóstico acabado y formal sobre qué tipo de fenómeno criminal impacta en qué país o región, sino más bien constatar el dinamismo y la concentración mencionada en párrafos anteriores.

Si se trata de listar todas las amenazas en la región, la lista sería extensa, lo que nos lleva a enumerar aquellas que consideramos más relevantes en la actualidad. El dinamismo de cada una de ellas obliga a evaluar y monitorear permanentemente para procurar tener un conocimiento actualizado tanto con relación a la manera en la que operan como por la zona geográfica en la que tienen mayor presencia.

Entre las principales amenazas consideramos dos grandes grupos. El primero, al que podríamos llamar amenazas de resultado, y el segundo, de medio.

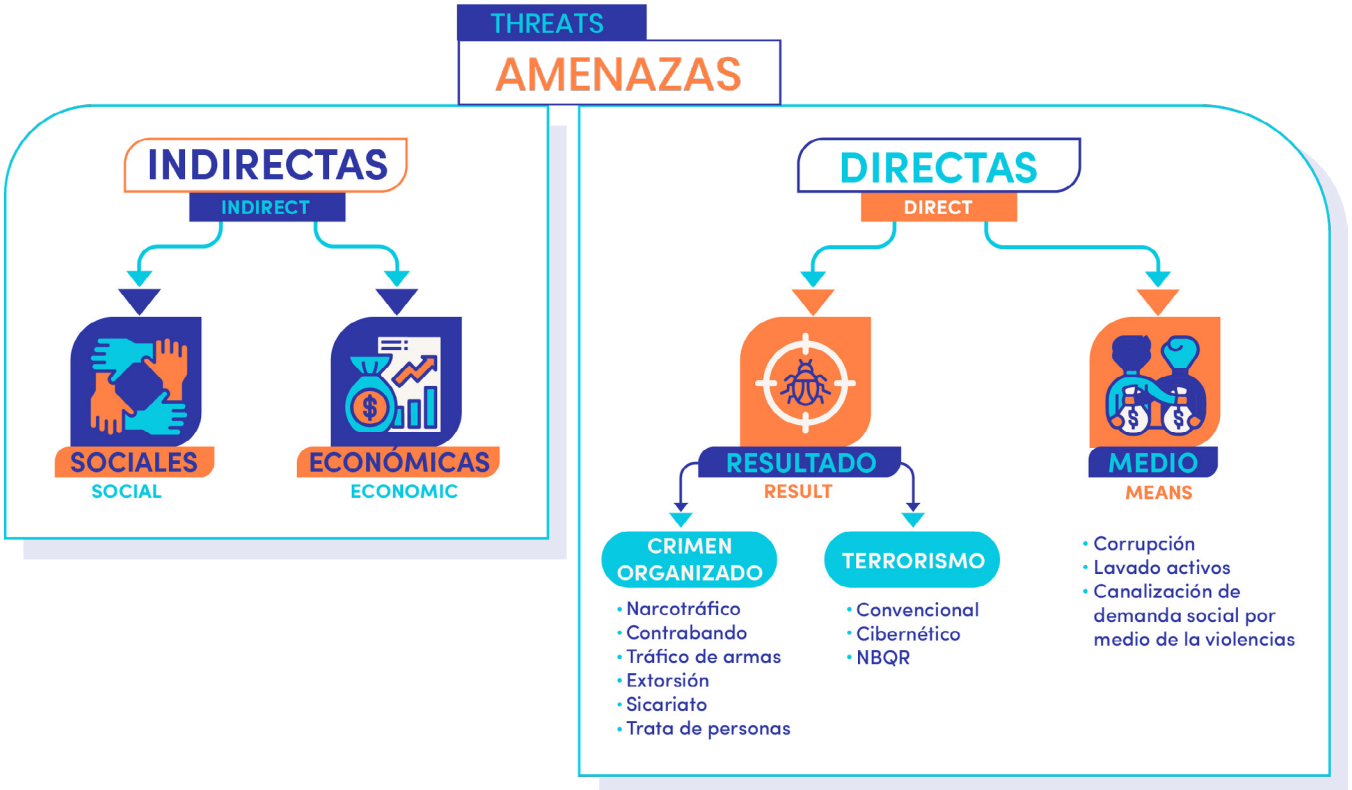
> Las de *resultado* son todas aquellas que por su forma de materializarse pueden causar un daño directo e inmediato en la seguridad. Son de percepción más inmediata. Se representan, a nuestro entender, en el terrorismo y el crimen organizado. Entre las modalidades de terrorismo consideramos tanto el terrorismo convencional o clásico, el bioterrorismo (incluyendo todo aquel que considera el uso de elementos químicos, radiológicos, biológicos y/o nucleares), y el ciberterrorismo.

En lo que a crimen organizado se refiere, podemos mencionar el narcotráfico, el contrabando, el tráfico de armas, la extorsión, el sicariato y la trata de personas como las amenazas más críticas en la región.

No son todas, pero sí las principales, las más importantes y las que están generando mayor nivel de daño. Cuando el terrorismo y el crimen organizado se unen, el impacto y desafío es aún mayor, como es el caso del narcoterrorismo, o el desarrollo de actividades criminales para financiar actividades terroristas.

El segundo grupo de amenazas, son un medio o bien un efecto del primer grupo. Se trata de la corrupción, el lavado de activos y la canalización o instrumentalización de demandas sociales a través de la violencia organizada y no espontánea. Aun cuando ellos por sí mismos causan daños, no tendrían sentido sin el primer grupo. Son funcionales cuando ambos tienen una relación simbiótica y de mutuo beneficio.

Esta clasificación no es azarosa, pues aun cuando escapa de los propósitos de este trabajo, la manera de abordar uno y otro no será igual.



Esquema 2. Amenazas. Elaborado por Marko Magdic.

Vulnerabilidades

La probabilidad de que las mencionadas amenazas se concreten dependerá del nivel de vulnerabilidad al que se ve expuesto tanto el continente, en su conjunto, como los países y también las subregiones. Diversos son los factores que influyen en el grado de vulnerabilidad, tanto internos como externos. Se trata de una distinción que nos llevará de manera más directa a las alianzas público-privadas.

En este estudio hemos clasificado las vulnerabilidades en dos categorías. Por un lado, están las internas o de gestión que se refieren a la manera en la que el Estado, la sociedad civil, el sector privado y la comunidad confrontan las amenazas a la seguridad, las cuales se integran por variables como la planificación estratégica, respuesta operativa, dotación y uso de recursos, marco legal, etc. Por otra parte, llamamos a las vulnerabilidades externas o de ambiente a aquellas que, independientemente de la respuesta directa hacia las amenazas, generan y/o representan condiciones que las facilitan o dificultan. Entre estas están las variables asociadas al nivel de desarrollo económico, pobreza, vulneración social, intensidad de la presencia estatal, informalidad laboral y del mercado, entre otras.

En tanto las condiciones y los factores de vulnerabilidad externa o de ambiente no serán abordados por este trabajo, los elementos internos son los que nos van a ocupar en este momento, a fin de identificar de qué manera incrementan o reducen la probabilidad de que una amenaza se concrete y genere daños a la seguridad pública de nuestra región.

En otras palabras, son los aspectos organizativos internos y de respuesta del ambiente en el que esta se da.

Así, y en términos más concretos en lo que a vulnerabilidades internas se refiere, hoy en día debemos considerar como un desafío a abordar la necesidad de optimizar y mejorar aún más las capacidades institucionales que permiten trabajar eficientemente en los siguientes planos, los cuales estimamos esenciales de cara a la necesidad de fomentar, incrementar e incentivar las alianzas público-privadas:

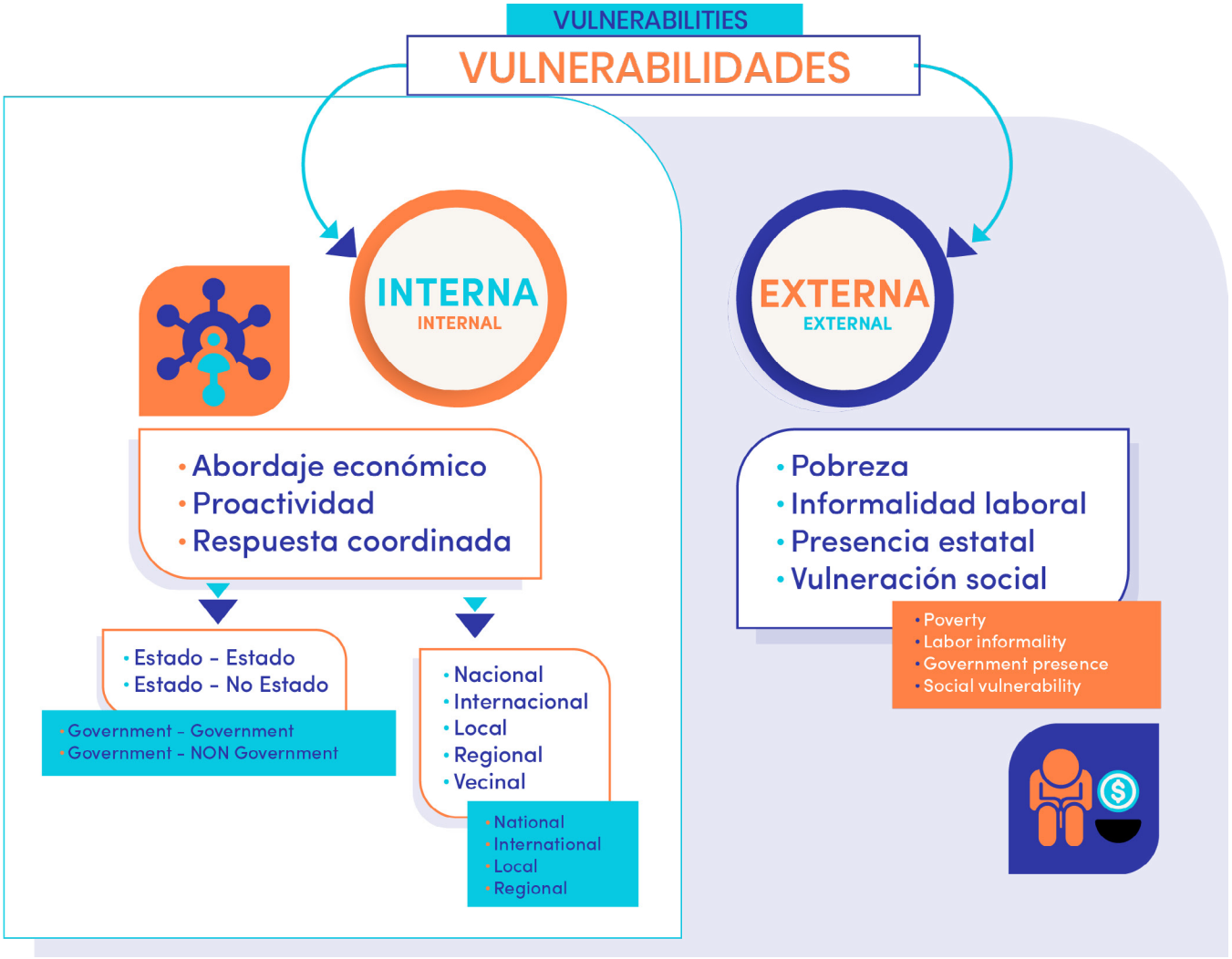
* Abordaje económico de las amenazas a la seguridad
* Proactividad
* Respuesta coordinada e integral

Abordar y enfocar económicamente las amenazas implica tomar en cuenta que, salvo algunas figuras excepcionales de terrorismo puramente ideológico, el resto de las amenazas descritas se mueven y son materializadas en búsqueda de un interés económico. Quien participa de las mismas desea incrementar ilícitamente su patrimonio y/o el de terceras personas o entidades. Resulta importante, entonces, enfrentar estos fenómenos procurando generar impacto en estos patrimonios ilícitos que adquieren los grupos criminales.

Por su parte, confrontar las amenazas con un enfoque proactivo importa al trabajar en alianzas público-privadas que no solo aborden los problemas de seguridad una vez que los hechos o actos han sido denunciados y reportados sino trabajar en su prevención como también en la detección temprana de los mismos.

Finalmente, uno de los factores que más impactan en el nivel de vulnerabilidad, en relación con las capacidades de prevención, detección y respuesta ante amenazas a la seguridad es la necesidad de incrementar y fortalecer aún más, una respuesta coordinada e integral, lo cual aplica tanto a nivel gubernamental como de alianzas, y participación que debe darse entre el sector público y privado.

Avanzar en la creación y operación integral y coordinada entre entidades públicas y privadas implica comprender que estaremos valiéndonos de una forma de trabajar que proveerá de tasas de éxito aún más grandes con relación a los efectos buscados.



Esquema 3. Vulnerabilidades. Elaborado por Marko Magdic

Lo más relevante

En este capítulo se abordan los principales riesgos, amenazas y vulnerabilidades en términos de seguridad en las Américas. Las amenazas más relevantes se dividen en dos grupos:

Amenazas de resultado: terrorismo y crimen organizado.

Amenazas de medio: corrupción, lavado de activos y violencia organizada no espontánea.

La probabilidad de materialización de estas amenazas está influenciada por las vulnerabilidades, clasificadas en internas (gestión) y externas (ambiente). La importancia de enfrentar estos desafíos mediante alianzas público-privadas se destaca como una estrategia clave para generar una respuesta coordinada e integral en la región.

Las alianzas Público - Privadas

En este capítulo, exploraremos el concepto de las alianzas público-privadas (APP) en el ámbito de la seguridad, analizando su importancia, funcionalidad y potencial para abordar los desafíos contemporáneos en materia de seguridad y prevención del delito. La colaboración entre los actores públicos y privados puede resultar en una mayor eficacia y éxito en la lucha contra las amenazas y vulnerabilidades que enfrentan nuestras sociedades.

Las APP son acuerdos establecidos entre uno o más actores del sector público y privado, con el objetivo de suministrar o proveer servicios o bienes en busca del logro de objetivos comunes, en este caso, de seguridad. Estas alianzas pueden tener un enfoque económico o social y pueden estar reguladas por contratos, marcos legales estrictos, acuerdos de colaboración o memorándums de entendimiento.

Aunque las APP han sido ampliamente utilizadas en sectores como infraestructura, energía, salud y educación, su aplicación en el ámbito de la seguridad ha sido menos prevalente. No obstante, existen numerosas oportunidades y beneficios potenciales en el establecimiento de estas colaboraciones en el sector de la seguridad, especialmente considerando el impacto transversal que tienen las amenazas a la seguridad en todos los sectores de la sociedad.

Las alianzas público-privadas en seguridad pueden abordar tanto las amenazas directas como el terrorismo, el crimen organizado, la corrupción, el lavado de activos y la violencia social planificada e instrumentalizada, así como aquellas de carácter más indirecto, como la educación y la pobreza. Estas alianzas también pueden trabajar en la disminución de los factores asociados a las vulnerabilidades internas y externas.

El factor distintivo que se propone es la manifestación conjunta de intereses, que se debiera traducir en acciones concretas, que siguen objetivos previamente definidos, en la búsqueda de resultados medibles que impacten en la reducción de los riesgos a los que está expuesta la seguridad.

Organizaciones internacionales como las Naciones Unidas, la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y el Banco Mundial han promovido y apoyado las APP en el ámbito de la seguridad ciudadana, la prevención del delito y el combate al terrorismo.

Las alianzas público-privadas en seguridad representan una oportunidad valiosa y efectiva para abordar los desafíos de seguridad que enfrentan nuestras sociedades. A través de la colaboración y el intercambio de recursos, conocimientos y experiencias, los actores públicos y privados pueden desarrollar e implementar medidas para prevenir, perseguir y castigar la delincuencia y el terrorismo en todas sus formas y manifestaciones.

¿Qué son?

La seguridad pública es resorte de los Estados o Gobiernos. De eso no hay duda, pero ello no obsta a una participación del sector privado en esta materia.

El grado de involucramiento del mundo privado, puede ir desde un rol eminentemente pasivo y subsidiario, hasta uno coparticipativo. No es el objetivo de este documento analizar la ubicación y posición exacta que le corresponde a cada uno, sino más bien promover el concepto del trabajo coordinado. Aun cuando pareciera que al sector público le cabe un rol preponderante en materia de seguridad, consideramos que este no le es exclusivo. Es la comunidad toda, organizada en sus diversas formas, económicas, sociales, políticas, y culturales, que sufre las consecuencias negativas de las amenazas a la seguridad, de manera tal que, con mayor o menor activismo y participación, tanto actores públicos o estatales como también privados tienen motivos y justificación suficiente para integrar actividades de prevención, detección y respuesta. Todos ellos, sin excepciones, tienen razones fundadas para incrementar la seguridad, confrontando las amenazas y abordando las vulnerabilidades. Todos ellos tienen mucho que perder a la vez que ganar y contribuir.

El Sector Público y el Privado

> Para los efectos de este Manual, utilizaremos el concepto de sector privado como una noción representativa de todo lo que no es público, integrando tanto a los centros de investigación, la academia y las organizaciones no gubernamentales, como las fundaciones, corporaciones, asociaciones locales, grupos de vecinos y la empresa privada propiamente como tal.
>
> Por su parte, bajo la denominación de sector público convergen, para los propósitos de nuestra herramienta, las diversas manifestaciones de organización estatal y gubernamental, considerando tanto el ámbito federal y unitario como aquellos a nivel central; estadual, provincial, distrital o regional; y local (municipios, ayuntamientos, condados, entre otros).

Aclarados los conceptos individuales de lo público y lo privado, cobra sentido abordar la noción de alianza público-privada.

No existe consenso universal en torno a su definición, a tal punto que ha presentado más de un problema el evaluar comparativamente distintos tipos de asociaciones. En efecto, mientras algunas alianzas tienen un fin eminentemente económico, en otros casos el objetivo buscado es social. Algunas se regulan por contratos o marcos legales estrictos habiendo otros que responden a acuerdos de colaboración o memorándums de entendimiento.

Un concepto amplio de alianza público-privada nos llevaría a considerar por tales al resultado que se obtiene como consecuencia un acuerdo expreso o tácito entre uno o más actores del sector público con uno o más actores del sector privado con la finalidad de suministrar o proveer servicios o bienes en busca del logro de objetivos comunes, en este caso, de seguridad.

Tradicionalmente se asocian a este tipo de acuerdos las alianzas o acuerdos de colaboración en materia de infraestructura, suministro de energía, salud, educación o, incluso gestión de desechos o residuos.

Aunque presentes y en constante desarrollo, probablemente uno de los sectores con mayor potencial y oportunidad de crecimiento en términos de una colaboración público-privada es el de la seguridad. A pesar de ello, ocurre que, al hablar de seguridad, en ocasiones el concepto se asocia a investigación y/o persecución penal, actividades públicas en las que hay una noción de participación casi monopólica del Estado. Esto explica, en opinión del consultor, que, en materia de seguridad, las alianzas público-privadas suelen tener menor presencia que en otras áreas de interés comunicatorio y estatal.

Existen manifestaciones de participación privada o social en áreas vinculadas a la seguridad que podrían ser consideradas como resultado de alianzas tácitas o expresas entre la comunidad y el estado.

Se trata de situaciones en las que, si bien confluyen en mayor o menor medida actores públicos y privados, estas están muy lejos de ser consideradas como una en los términos que propone este Manual. En efecto, y sin que su mención importe una validación o rechazo de las mismas, en algunas jurisdicciones es posible visualizar prácticas que no consideramos la alianza propiamente como tal, como es el caso de:

A. la posibilidad que el sector privado pueda contar con guardias privados, en ocasiones, armados;

B. autorizar legalmente que la comunidad pueda retener a delincuentes en casos de flagrancia;

C. contar con legislaciones que, con mayor o menor restricción, habiliten a las personas para adquirir o portar armas.

Todos estos, en su conjunto, representan actividades, como dijimos, en las que el sector privado o la comunidad puede desarrollar acciones a través de las cuales pudieran, eventualmente impactar de una u otra manera, en la seguridad. Pero ello está lejos de ser una alianza como la que promueve este Manual.

Sea que se trate de *joint ventures* o el resultado de la creación de nuevas entidades especialmente formadas para tal efecto; sea que estemos en presencia de redes de trabajo, convenios, memorándum de entendimiento o acuerdos de colaboración, el factor distintivo de la alianza público-privada lo consideramos como una **manifestación conjunta de intereses, que se traduce en acciones concretas, que siguen objetivos previamente definidos, en la búsqueda de resultados medibles que impacten en la reducción de los riesgos a los que está expuesta la seguridad, previniendo, detectando tempranamente y respondiendo a las amenazas mediante un trabajo colaborativo entre el actores del sector público y privado.**

Elementos

- Manifestación conjunta de intereses y trabajo colaborativo entre actores del sector público y privado
- Acciones concretas
- Objetivos previamente definidos
- Resultados medibles
- Reducción de riesgos a la seguridad
- Prevención, detección temprana a amenazas

Esta aproximación al concepto de alianza público-privada permite contextualizarla en dos dimensiones. Una, como un medio para abordar las amenazas a la seguridad tomando en cuenta las amenazas directas de resultado o medio (terrorismo, crimen organizado, corrupción, lavado de activos y violencia social planificada e instrumentalizada), y otra que lo hace sobre aquellas de corte más indirecto o de ambiente, como es el caso de la educación o la pobreza.

De igual manera, las alianzas público-privadas nos ayudarán a trabajar en la disminución de los niveles de aquellos factores asociados a las vulnerabilidades, sean estas internas (respuesta coordinada, abordaje económico, proactividad) o externas (informalidad laboral, pobreza, presencia estatal y vulneración social).

¿Son útiles?

Además de un conjunto de directrices de prevención de la criminalidad en las cuales hay menciones expresas a este tipo de asociaciones, las Naciones Unidas, a través de su Asamblea General, ha adoptado varias resoluciones que fomentan las Alianzas Público-Privadas que promueve programas colaborativos que pudieran impactar en materias de seguridad, entre otras.

Tal es el caso de las siguientes resoluciones, entre otras:

- Resolución A/60/288 del año 2005[5]
- Resolución A/60/215 del año 2005[6]
- Resolución A/58/129 del año 2003[7]
- Resolución A/56/76 del año 2001[8]
- Resolución A/55/215 de 2000[9]

A su turno, el XII Congreso sobre Prevención del Delito y Justicia Penal en Brasil, en abril del año 2010, fue claro al indicar en su Declaración[10] que se reconoce *"(...) la importancia de fortalecer las asociaciones público-privadas para la prevención y lucha contra la delincuencia en todas sus formas y manifestaciones".* De lo anterior, da cuenta la Resolución 65/230 del mencionado Congreso que fue posteriormente *aprobada por la Asamblea General de Naciones Unidas el 21 de diciembre de 2021 sobre la base del informe de la Tercera Comisión (A/65/457).*

[5] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/91/PDF/N0550491.pdf?OpenElement
[6] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/500/53/PDF/N0550053.pdf?OpenElement
[7] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/500/53/PDF/N0550053.pdf?OpenElement
[8] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/490/05/PDF/N0149005.pdf?OpenElement
[9] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/572/08/PDF/N0057208.pdf?OpenElement

> El documento indica que están *"(...) convencidos de que, a través del intercambio mutuo y eficaz de información, conocimientos y experiencias, y a través de acciones conjuntas y coordinadas, los gobiernos y las empresas pueden desarrollar, mejorar e implementar medidas para prevenir, perseguir y castigar la delincuencia, incluyendo los nuevos y cambiantes desafíos".*

Basándose en esa misma declaración, un mes después, tuvo lugar en Austria, la XIX Reunión de la Comisión de Prevención del Delito y Justicia Penal de las Naciones Unidas. El reporte de esta reunión (E/2010/30 E/CN.15/2010/20)[11] da cuenta de la búsqueda por fortalecer, con un respaldo internacional, las alianzas público-privadas para la prevención y lucha contra la delincuencia —como señala— en todas sus formas y manifestaciones, incluyendo el terrorismo. El mencionado documento, exhorta a los gobiernos a promover y fortalecer las alianzas de colaboración con el sector privado, a establecer áreas prioritarias, difundir las buenas prácticas, crear redes de apoyo y aumentar la sensibilización acerca de los beneficios de estas instancias de colaboración en relación con la prevención y el control de la criminalidad.

Instancias multilaterales y entidades internacionales como la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y el Banco Mundial, apoyan y promocionan igualmente las alianzas público-privadas como un mecanismo de colaboración para abordar desafíos vinculados a la seguridad ciudadana, la delincuencia, la seguridad pública y el combate al terrorismo.

A nivel de la OEA se destaca el acuerdo de los Estados Miembros de promover la colaboración público-privada en la lucha contra el terrorismo que fue abordado en la Décima Reunión Regular del Comité Interamericano Contra el Terrorismo (CICTE).

En efecto, y bajo el lema *"Colaboración público-privada en la lucha contra el terrorismo",* en marzo de 2010, delegados de los Estados Miembros de la OEA discutieron en la reunión del CICTE temas relacionados con la colaboración en la protección de infraestructura básica, la seguridad para grandes eventos y la colaboración público-privada en seguridad marítima. Las delegaciones también debatieron temas como: la lucha contra el terrorismo en cumplimiento de las leyes nacionales e internacionales; el fortalecimiento de las medidas nacionales e internacionales existentes para identificar nuevas estrategias de cooperación multilateral para el fortalecimiento de la lucha contra el terrorismo; la adopción de programas cooperativos para intercambiar información y buenas prácticas para prevenir y combatir tales amenazas; y estrechar vínculos con el sector privado y la sociedad civil para desarrollar programas de fomento de la capacidad preventiva y de protección, entre otros.

[10] **Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución.**
[11] **https://documents-dds-ny.un.org/doc/UNDOC/GEN/V10/541/37/PDF/V1054137.pdf?OpenElement**

La relevancia de las declaraciones y recomendaciones es enorme. Esto entrega directrices y pautas a los distintos gobiernos para implementar programas con componentes público-privados. Ello no es casualidad, pues el impacto de las amenazas es tremendo. Cuando los riesgos vinculados a la seguridad se hacen evidentes mediante la materialización de las amenazas, los que se ven afectados son todos: el Estado, la comunidad, las organizaciones de la sociedad civil, las empresas. Hechos concretos podrían afectar a un sector o grupo de interés específico, pero cuando estas amenazas permean y se concretan en un territorio, comunidad o sistema determinado, el impacto y daño son transversales.

Si asumimos lo anterior como cierto, en el entendido que tanto públicos como privados experimentan y sufren los efectos negativos, no podríamos sino sostener que, con mayor o menor grado e intensidad, una aproximación integral o, cuando menos colaborativa, entre ambos sectores, resultará altamente beneficiosa y hasta necesaria. Mayores niveles de seguridad impactan positivamente a unos y otros.

La importancia del Estado en las alianzas público-privadas radica en que se pueden enfocar proyectos en zonas geográficas, desarrollar áreas temáticas o impactar a población objetiva que no necesariamente sea prioritaria para los grupos privados o no estatales. Por su parte, la velocidad, flexibilidad y adaptabilidad con la que el mundo privado aproxima su trabajo a los intereses representa una inyección de dinamismo muy necesaria en un contexto de desarrollo de soluciones innovadoras y de impacto a los problemas de seguridad.

Pese a ello, cuando se trata de construir una represa o una autopista pocos dudarían de la importancia de una alianza público-privada, lo que no siempre ocurre en materias de seguridad. No obstante, ello resulta igualmente beneficioso, hecho que precisamente justifica el presente Manual.

Las instancias de colaboración público-privada son importantes para el sector público por muchas razones, incluidas las siguientes:

* Las ayudas contribuyen a conseguir el compromiso del sector privado de convertirse en una parte del proceso comunitario global de prevención de la amenaza y planificación de una respuesta de urgencia.

* La cooperación y la utilización conjunta de recursos para los objetivos vulnerables “suaves” pueden aumentar perceptiblemente la seguridad y crear un objetivo único y mucho “más duro”.

* Proporcionan una comprensión de las necesidades del sector privado y de su capacidad y disponibilidad de recursos.

* En términos de prevención, favorece de un modo activo la comunicación con el sector privado antes de un incidente.

* Da la oportunidad de discutir y planear la respuesta conjunta y estrategias de recuperación.

* Permite generar mejores condiciones y contar con más herramientas para una detección temprana de aquellas amenazas que se han concretado, facilitando una respuesta más rápida y afectando la expansión del daño.

Por su parte, estas instancias resultan importantes para el sector privado por muchas razones, incluidas las siguientes:

* Proporcionan al sector privado un canal de comunicación con el sector público y desarrollan una comprensión del apoyo que pueden tener del sector público.

* Proveen la ocasión de explicar y describir al sector público el por qué la continuidad empresarial es importante para la entidad privada y para la comunidad.

* Pueden ofrecer incentivos para que la comunidad de negocios invierta en medidas preventivas para reducir amenazas y riesgos, así como el apoyo a la academia en la formulación de políticas y desarrollo de actividades de investigación en esta materia.

* Dan la oportunidad de recibir información, apoyo adicional y asesoría sobre la prevención de delitos.

* Generan mejores condiciones para la detección temprana de amenazas a la seguridad lo que permite tanto al sector privado como al Estado intervenir más prontamente reduciendo los daños de un determinado incidente.

* Podrían ayudar a reducir la responsabilidad y los gastos derivados de costos de contratación de seguros de riesgo asociados a daños que pudieran sufrir una actividad, personas o infraestructura como consecuencia de incidentes que afecten la seguridad (criminalidad, ataque terrorista, etc.).

* Generan la oportunidad de discutir y desarrollar planes empresariales de continuidad y recuperación.

* Desarrollan una mejor comprensión de la capacidad y los recursos del sector público.

* Fomentan y promueven que los intereses y necesidades privadas sean consideradas con ocasión del establecimiento de prioridades y objetivos de seguridad del sector público.

Lo más relevante

Este capítulo explora el concepto de alianzas público-privadas (APP) en el ámbito de la seguridad y su potencial para abordar desafíos contemporáneos en seguridad y prevención del delito. Las APP son acuerdos entre actores públicos y privados con objetivos comunes, y aunque han sido utilizadas en sectores como infraestructura, energía, salud y educación, su aplicación en seguridad ha sido menos prevalente.

Los principales aspectos que destacar son:

1. Las APP en seguridad pueden abordar amenazas directas e indirectas, así como disminuir vulnerabilidades internas y externas.

2. La colaboración e intercambio de recursos, conocimientos y experiencias entre actores públicos y privados pueden mejorar la eficacia y el éxito en la lucha contra amenazas y vulnerabilidades.

3. Organizaciones internacionales promueven y apoyan las APP en seguridad ciudadana, prevención del delito y combate al terrorismo.

Las alianzas público-privadas en seguridad representan una valiosa oportunidad para enfrentar los desafíos de seguridad de nuestras sociedades de manera más efectiva.

El inicio del trabajo colaborativo: los primeros pasos

En este capítulo, abordaremos el inicio del trabajo colaborativo entre los sectores público y privado en materia de seguridad pública, enfocándonos en los primeros pasos para establecer una colaboración efectiva. La asociatividad en estos temas no suele ser espontánea, por lo que es crucial que una de las partes tome la iniciativa para identificar y abordar problemas específicos, como el incremento en los homicidios, la disminución de denuncias, los atentados terroristas, entre otros.

Para generar los primeros puentes de colaboración entre ambos sectores, se recomienda la realización de actividades como ferias abiertas, seminarios o talleres, reuniones sectoriales y reuniones dirigidas. Estas instancias permiten identificar actores interesados, conocer nuevas tecnologías o ideas, y compartimentalizar temas de interés, facilitando así la interacción y el intercambio de información.

Las entidades estatales, juntas de vecinos, centros de investigación, empresas privadas y organizaciones de la sociedad civil deben incorporar esta forma de trabajo en su planificación anual. Problemas conjuntos requieren soluciones conjuntas, y ser proactivos es clave en este proceso.

Este capítulo busca motivar a los lectores a tomar la iniciativa para identificar contrapartes en ambos sectores y comenzar a trabajar en la búsqueda de nuevos y mejores resultados en materia de reducción de riesgos a la seguridad vinculados a amenazas terroristas y criminalidad organizada.

El inicio o formulación de cualquier colaboración público-privada en materia de seguridad pública debiera ser abordado como un proyecto.

Como en toda asociación, siempre una de las partes tendrá mayores cuotas de iniciativa, la cual probablemente termine secundada por la otra. La asociatividad espontánea y automática en los temas que nos convocan es poco común.

En otras palabras, los proyectos y las primeras reuniones no se producirán solos. Será siempre necesario que uno u otro den ese primer paso. Lo anterior supone que, cuando menos una de las partes, haya visualizado un problema, como sería el incremento en los homicidios, una disminución de las denuncias y reportes de lavado de activos, una intensificación de atentados terroristas, el aumento en la violencia asociada a las extorsiones en empresas privadas, mayor cantidad de vehículos robados relacionados a la comisión de delitos graves de impacto social, etc. Este primer levantamiento o constatación, que afecta tanto a públicos como privados, debiera motivar la realización de actividades tendientes a generar los primeros puentes de colaboración entre ambos sectores, con relación a un problema específico que se desea abordar. Para ello es recomendable generar:

- Ferias abiertas[12]
- Seminarios o talleres
- Reuniones sectoriales
- Reuniones con contrapartes dirigidas y acotadas

Es bastante probable que la identificación de contrapartes y las etapas iniciales del establecimiento de una asociación pública-privada se den en el mismo orden indicado, comenzado por ferias abiertas para terminar en reuniones dirigidas. Así, es posible que mediante una iniciativa privada o pública se organice una feria que, abordando la seguridad, tenga un tema gravitante, como sería, por ejemplo, el robo de vehículos, el tráfico de drogas, el contrabando o la amenaza terrorista. En esta instancia podremos ver, por un lado, la oferta e iniciativas existentes en la materia, pero también será posible identificar de manera más fácil a aquellos actores que tienen un alto grado de interés por mostrar su trabajo. Este tipo de iniciativas resulta sumamente útil para conocer nuevos actores, tecnologías o ideas.

La realización de seminarios y talleres suelen realizarse en este tipo de ferias, pero bien podrían ser parte de un acto o evento posterior. La idea es dotar de estructura y mayores niveles de metodología a los temas tratados. En este tipo de actividades estaremos en condiciones de compartimentalizar mejor los temas de interés.

Así, podrían abordarse iniciativas de prevención, por separado de aquellas vinculadas a la detección o control. De igual manera, es posible enfocarse en un tema particular y desglosarlo. Mientras una feria sobre contraterrorismo coloque en un solo lugar a los actores más interesados en la materia para que interactúen e intercambien información de manera más espontánea, en el caso de los seminarios y talleres, el organizador puede dirigir con metodología esa interacción, promoviendo además acuerdos, declaraciones o resultados concretos.

[12] Se trata de eventos de carácter cultural, económico, social o industrial, establecidos de manera temporal, que se desarrollan en un lugar físico determinado abordado una temática común, en este caso, de seguridad. No solo permite la comunicación e intercambio de información entre los actores privados vinculados a la temática sino también entre estos y el sector público. Permite además conocer las ultimas tendencias, necesidades, desafíos y oportunidades. Colocan en un solo lugar a un grupo de actores relevantes en materia de seguridad, tanto públicos como privados, mejorando sustancialmente el conocimiento mutuo y formando instancias de colaboración.

Por su parte, las reuniones sectoriales suelen agrupar a un número más acotado de entidades públicas y privadas respecto a un tema en particular. Digamos, por ejemplo, actores de ambos estamentos a cargo y/o con interés en bioseguridad y bioterrorismo, o informática, ciberterrorismo y ciberseguridad. En ese mismo sentido, si la reunión pretende abordar el problema del narcotráfico en la frontera, es posible que por parte de sector público se encuentren representantes de las principales agencias de cumplimiento de la ley vinculadas al control fronterizo, así como autoridades de los municipios, estados o provincias ubicadas en esas zonas. Por parte del sector privado, deberían estar involucrados las cámaras de comercio, empresas de transporte, operadores logísticos y proveedores tecnológicos.

El avance de estas actividades probablemente dé pie a un trabajo más focalizado a nivel de contrapartes específicas o de corte más bilateral, lo que permitirá entender y comprender de mejor manera las expectativas, necesidades, así como también las posibles tensiones entre los distintos intervinientes en un espacio de mayor confianza.

La pandemia del COVID-19, que azotó al mundo a comienzos de la segunda década del siglo XXI, demostró que este tipo de iniciativas pueden tener soporte no solo físico y presencial, sino también virtual, lo cual evidentemente disminuye costos y tiempos a la vez que favorece la realización de una mayor cantidad de eventos.

Sea que se realicen de manera consecutiva, coetánea o se siga otro orden, lo relevante es que los actores que tengan interés en abordar un problema de seguridad tomen la iniciativa y desarrollen actividades de intercambio de opinión, conocimiento y acercamiento, recomendación que vale para ambos sectores. La proactividad es una palabra clave.

Tratándose de entidades estatales, esta manera de operar debiera formar parte de su metodología de trabajo. Se considera que, con relación a las principales amenazas señaladas en este Manual, debieran seguir una línea de trabajo público-privada para cada una de ellas, lo que se puede dar a nivel nacional, estadual, provincial, cantonal, regional, municipal o distrital, según sea el caso, dependiendo del grado y extensión del impacto negativo generado por las mencionadas amenazas.

Las juntas de vecinos o asociaciones comunitarias territoriales o funcionales, los centros de investigación, cámaras de comercio, empresas privadas y organizaciones de la sociedad civil que tengan por objetivo el tratamiento de estas amenazas de manera proactiva, o que se hayan visto afectados por las mismas, debiesen de igual manera, incorporar en su planificación anual esta forma de trabajar. **Problemas conjuntos requieren soluciones conjuntas.**

Una manera de establecer o medir la necesidad de implementar programas proactivos que confronten las amenazas a la seguridad, se logra contestando las preguntas indicadas al comienzo de este Manual.

Si está leyendo esta sección probablemente sea porque en la encuesta formulada al inicio del Manual obtuvo, cuando menos, dos puntos. Es hora, entonces, de ser proactivos y tomar la iniciativa para identificar contrapartes en ambos sectores, públicos y privados, con el fin de comenzar a trabajar en la búsqueda de nuevos y/o mejores resultados en materia de reducción de riesgos a la seguridad vinculados a amenazas terroristas y criminalidad organizada.

Lo más relevante

Este capítulo se centra en los primeros pasos para establecer una colaboración efectiva entre los sectores público y privado en materia de seguridad pública. Los principales puntos para resaltar son:

1. La importancia de tomar la iniciativa para identificar y abordar problemas específicos en seguridad.

2. La realización de actividades como ferias abiertas, seminarios, talleres y reuniones para facilitar la interacción y el intercambio de información entre ambos sectores.

3. La necesidad de que entidades estatales, juntas de vecinos, centros de investigación, empresas privadas y organizaciones de la sociedad civil incorporen el trabajo colaborativo en su planificación anual.

El objetivo es motivar a los lectores a identificar contrapartes en ambos sectores y trabajar en conjunto en busca de soluciones efectivas para abordar las amenazas terroristas y la criminalidad organizada.

El diagnóstico del problema

El presente capítulo aborda el diagnóstico del problema en el ámbito de la seguridad, enfatizando la importancia de la colaboración entre los sectores público y privado para desarrollar un análisis exhaustivo y eficiente de las amenazas y desafíos a enfrentar. Se exploran diversos factores clave que deben ser considerados en el proceso de diagnóstico y se destacan ejemplos concretos que ilustran la relevancia de incorporar a ambos sectores en la identificación, la prevención y el control de problemas de seguridad.

El capítulo expone la necesidad de realizar diagnósticos conjuntos entre los sectores público y privado, para obtener una visión más amplia y precisa de los problemas de seguridad. Se plantean 13 factores esenciales a considerar en un diagnóstico, incluyendo la amenaza, el problema, el modus operandi, entre otros. Se discuten casos específicos, como el financiamiento del terrorismo y el robo de vehículos, para ilustrar cómo la colaboración entre ambos sectores puede aportar información valiosa y mejorar la comprensión de estos fenómenos.

Se destaca que el trabajo conjunto entre entidades públicas y privadas puede identificar nuevas variables, proporcionar herramientas para una mejor comprensión del problema y, en última instancia, ayudar a diseñar estrategias más efectivas y novedosas. Se aborda la importancia de actualizar continuamente los diagnósticos y adaptar las políticas y programas en función de los resultados obtenidos.

El capítulo resalta el valor de la colaboración público-privada en el diagnóstico de problemas de seguridad, con el objetivo de mejorar la prevención, la detección temprana, el control y la respuesta a las amenazas que enfrentamos.

Los diagnósticos a los problemas y amenazas vinculadas a la seguridad han existido y se seguirán realizando. Es posible apreciar que tanto el sector público como el privado han participado de estas líneas de acción. No obstante, es más probable encontrar diagnósticos construidos desde una de las dos veredas (pública o privada), que de manera conjunta. Se recomienda, desde luego, que el desarrollo de diagnósticos se ejecute con la participación colaborativa de ambos sectores desde el comienzo.

Realizar un buen diagnóstico en materia de seguridad debiera cubrir, cuando menos, los siguientes 13 factores:

- **La amenaza.** ¿Qué amenaza quiero abordar?
- **El problema.** ¿Qué problema concreto está generando esa amenaza?
- **El modus operandi.** ¿Cómo se comete o manifiesta la amenaza?
- **Lugar, tiempo.** ¿Dónde ocurre, en qué momento?
- **Móvil.** ¿Cuál es el interés buscado para concretar la amenaza?
- **Perfil del objetivo.** ¿Contra quién o contra qué se verifica la amenaza?
- **Principales Actores involucrados.** ¿Quiénes intervienen, podrían o deberían intervenir de manera directa para prevenir, detectar, controlar y responder ante la amenaza?
- **Actores involucrados por extensión.** ¿Quiénes tienen algo que decir o aportar en términos de conocimiento, capacidades o experiencia en materia de prevención, detección temprana, control y/o respuesta ante la amenaza concreta que estamos abordando?
- **Fortalezas históricas.** ¿Qué buenas prácticas y éxitos logrados podemos identificar?
- **Debilidades históricas.** ¿Qué malas prácticas y dificultades hemos experimentado a la fecha?
- **Oportunidades.** ¿Cuáles condiciones actuales deberíamos aprovechar, sean estas institucionales, legales, mediáticas, financieras u operativas, entre otras?
- **Desafíos.** ¿Qué desafíos o amenazas enfrentamos o podríamos enfrentar en el tratamiento del problema, dado el actual o un inminente y próximo escenario?
- **Mediciones acumuladas.** ¿Cómo hemos medido hasta ahora los diversos indicadores asociados a la amenaza y al problema concreto que estamos abordando, y qué aciertos, por un lado, y problemas, por el otro, hemos tenido con este tipo de mediciones?

* **Indicadores futuros.** ¿Qué nuevos indicadores tendríamos o podríamos tomar en cuenta para evaluar de una mejor o distinta manera el problema analizado y que nos permita dar un valor agregado, una nueva perspectiva o comprensión de este?

Cuando se dieron los primeros pasos para confrontar las amenazas terroristas, la aproximación estatal era casi exclusiva. La participación del sector privado era mínima o, prácticamente nula.

En las últimas décadas, y como consecuencia de un análisis del fenómeno terrorista tanto por entes estatales como por la academia, los centros de investigación y la empresa privada, fue posible establecer que identificar las líneas del financiamiento de las organizaciones tiene dos ventajas: se puede llegar más fácil a la organización propiamente dicha, y se puede interrumpir el flujo de activos afectando su operación y poder.

Ocurre que el mayor porcentaje de las líneas de financiamiento se realiza a través del sector privado, sea mediante el envío y transferencias de dinero, la remisión de armas por barco, o la operación de empresas que son utilizadas como fachada para lavar activos vinculados al terrorismo. En todos esos casos:

¿tendrá sentido incluir a los bancos, a las empresas de logística, a las navieras, a los casinos de juego o empresas de remesas de dinero?

¿Podría resultar beneficioso que más allá de regularlos se desarrollen líneas de trabajo que los hagan socios colaboradores de iniciativas público-privadas?

La respuesta es sí.

Una cosa es el trabajo con los entes reguladores en esta materia como ocurre con las Unidades de Análisis Financiero o Inteligencia Financiera, así como el trabajo que desarrolla el GAFI, Grupo de Acción Financiera Internacional. Lo que acá se propone es avanzar un paso más allá e incorporar a los entes privados relevantes en materia de financiamiento del terrorismo para conocer, de primera fuente, y en base a sus experiencias y capacidades, las maneras a través de la cuales los grupos terroristas pudieran aprovechar sus vulnerabilidades para traspasar dinero o bienes. Los bancos y las empresas de logística necesitan desarrollar sus actividades sin contratiempos. Si obtienen retroalimentación del Estado respecto del levantamiento en el que puedan participar conjuntamente, habrá una mayor disposición para compartir datos.

En otro orden de ideas, si analizamos, por ejemplo, el problema de seguridad asociado al robo de vehículos, un diagnóstico clásico nos permitiría no solo saber la cantidad de vehículos robados, la forma en la que son sustraídos e incluso las horas y lugares. Podríamos también evaluar la legislación que sanciona el robo, el tipo de vehículo robado, e identificar fortalezas y debilidades relacionadas con el sistema de reportería y búsqueda de automóviles que le han sido despojados a sus dueños.

Una participación colaborativa con el sector privado podría arrojar datos diversos y complementarios a los existentes, que ayudarían a comprender de mejor manera algunas nuevas variables en torno a las cuales es posible considerar vías de acción alternativas y/o novedosas.

Así, podría resultar interesante conocer el porcentaje e incluso el tipo y perfil de vehículos robados que contaban con seguros y el impacto que ello pudiera tener en este delito. De igual manera, saber el tiempo que tomó en dar con los vehículos cuando estos han sido recuperados, a qué distancia o en qué lugar fueron encontrados, el tipo de daño que sufrió el vehículo recuperado para poder inferir el uso que se le dio durante el periodo que duró la sustracción.

A su turno, los martilleros, subastadores o encargados de casas de remate o agencias de subastas podrían indicar el tipo, cantidad y porcentaje de vehículos que son vendidos mediante este sistema como chatarra o desperdicio. Un cruce de datos entre compañías de seguros y casas de remate o subastas podría indicarnos el porcentaje y tipo de vehículos que, pese a ser vendidos como chatarra o desperdicio y haber sido indemnizados los afectados en su totalidad por perdida total, su inscripción o registro no ha sido cancelado, aspecto que tiene directo impacto en la clonación o gemeleo de vehículos robados.

La participación privada podría seguir más allá con muchas otras variables no consideradas tradicionalmente y que nos permitirían no solo contar con una imagen y visión distinta del problema, sino que nos entregarían herramientas y elementos para su mejor comprensión, lo que ayudaría, en definitiva, a plantear mejores y nuevas estrategias de solución o, cuando menos, contención.

Cobra entonces sentido incorporar a las autopistas en el análisis y solución de un problema como el planteado, a fin de conocer para conocer la cantidad, tipo y horarios en los que vehículos robados han circulado por sus vías. Lo mismo con los municipios, condados o territorios en los cuales la autoridad cuenta con sistemas lectores de placas o patentes. Desde luego, esta línea implica un primer nivel de colaboración consistente entre el cruce de bases de datos policiales que contienen las placas o patentes de vehículos robados, con aquellas bases de datos privadas o, incluso públicas, que incorporan el registro de circulación de vehículos basados en sus números de identificación.

Imaginemos, además, involucrar a las empresas que administran estacionamientos, sea que se trata de parqueaderos o estacionamientos destinados exclusivamente con este fin o centros comerciales que, para efectos de un cobro más eficiente, también registran las placas o patentes de sus usuarios o clientes.

¿Sería interesante conocer el porcentaje de vehículos robados que ingresaron a sus instalaciones, el tiempo que estuvieron e, incluso, si aún siguen ahí?

¿Ayudaría eso a comprender el problema? Desde luego que sí. En la sección de formulación, diseño de ideas y soluciones en el marco de alianzas público-privadas se abordará este aspecto.

Además, en aquellas ciudades o localidades en las cuales empleados públicos o empresas privadas realizan el registro y cobro de estacionamiento de vehículos en las calles o la vía pública, es bastante probable que entre otras variables tomen nota de las placas o patentes de esos vehículos. Se trata de datos que, cruzados con los de las bases de vehículos robados podrían arrojar interesantes resultados. Podríamos saber en tiempo real la ubicación de un vehículo que fue registrado como robado.

La colaboración se puede extender a otros órganos públicos no considerados tradicionalmente en estas materias como es el caso de aduanas, autoridades de control de frontera, entidades reguladoras de las compañías de seguros, organismos encargados de otorgar las placas o patentes vehiculares, agencias a cargo de regular o supervisar las agencias o casas de remates en las que se vendan vehículos chocados, entre otras.

En efecto, mientras nos quedamos con la idea de que, dependiendo del país y contexto concreto, un porcentaje de vehículos robados cruza las fronteras nacionales por lugares no habilitados, un cruce de datos y trabajo conjunto con autoridades fronterizas podría arrojar interesantes impresiones acerca de la cantidad, el tipo, los horarios, días y lugares por los cuales, incluso en frente de agencias de control de fronteras, salieron o ingresaron a nuestros países vehículos robados. Un dato como ese podría ser relevante, pues en el evento de que la cantidad de aciertos sea considerable, podríamos darnos cuenta de que la estrategia de inversión de recursos en el control y detección de vehículos que circulan por cruces informales, ilegales y no habilitados, en realidad no presentaría la misma rentabilidad que comenzar a detectar y controlar casos en aquellos lugares en los cuales existe presencia de autoridades dadas las condiciones de pasos formales y habilitados.

¿Sería útil conocer las iniciativas privadas o, incluso, público-privadas existentes en materia de marcado físico de partes y piezas de vehículos, así como la operación, cobertura y capacidades de los GPS, sean estos aplicados voluntariamente por los usuarios de vehículos o bien como respuesta a obligaciones, ya sean legales o contractuales con las compañías de seguro?

¿Tendrá alguna relevancia la información que pudieran proveer las contrapartes con relación a este tipo de antecedentes, si lo que estamos haciendo es diagnosticar un problema con una óptica distinta y, por qué no, más eficiente?

Mientras mejor sea el diagnóstico, mayor será la probabilidad de comprender la esencia del problema y mejores serán las expectativas de diseñar soluciones exitosas de prevención, detección temprana, control y respuesta a este.

Cuando un problema, en este caso, una amenaza a la seguridad no ha sido confrontada o abordada con éxito, al menos no en los términos deseados, y los números, los casos, la violencia asociada y los efectos negativos vinculados siguen al alza, podría pensarse que la intensificación de la respuesta existente, el incremento de recursos y la inyección de medios, con mayor o menor medida, debieran generar ciertos niveles de impacto positivo. La pregunta es, si con eso resolveremos el problema, al menos en un nivel tal de generar el impacto buscado o deseado. Si al inicio de un programa o proyecto, diez unidades de recursos generan impacto en un delito, y 20 unidades lo hacen en dos delitos, llegará un momento en el que incrementos sostenidos en inyección de activos, personal, tiempo y dinero, no generará el mismo nivel de impacto, de manera tal que, a modo ilustrativo, mil unidades de recursos en vez de generar impacto en cien delitos lo harán en relación a noventa, lo que comenzará a tornan cada vez más ineficiente el retorno o rentabilidad buscada.

De esta manera, las políticas o programas de intensificación continua deben necesariamente complementarse con otros sistemas, soluciones y acciones. De ahí la importancia de realizar diagnósticos, de ajustarlos continuamente, y de ejecutar este trabajo con una óptica tanto pública como privada, valiéndose no solo de la experiencia de ambos sectores, sino también de la información, capacidades, ideas y recursos que pudieran proveer, pero sin olvidar de hacer todo lo anterior en el marco de programa de trabajo previamente definido en representantes de ambos sectores.

En definitiva, sea que haya un diagnóstico previo realizado por alguna de las partes, o bien que estemos iniciando todo desde cero, es recomendable que desde el inicio se ejecute o actualice, según corresponda, el conocimiento del problema, con una intervención activa y conjunta tanto del sector público como privado, y tomando en cuenta, cuando menos, los 13 elementos provistos en esta sección. Para ello, se sugiere incorporar no solo a los actores primarios, sino también a aquellos denominados como “de extensión”, que son el conjunto de entidades públicas y privadas que tienen algo que decir o aportar en términos de conocimiento, capacidades o experiencia en materia de prevención, detección temprana, control y/o respuesta ante la amenaza particular que estamos abordando.

Lo más importante

Este capítulo destaca la importancia de la colaboración entre los sectores público y privado en el diagnóstico de problemas de seguridad. Los principales puntos por resaltar son:

1. La necesidad de realizar diagnósticos conjuntos para obtener una visión amplia y precisa de los problemas de seguridad.

2. La consideración de 13 factores esenciales en el proceso de diagnóstico, como la amenaza, el problema y el modus operandi.

3. La discusión de casos específicos, como el financiamiento del terrorismo y el robo de vehículos, para ilustrar el valor de la colaboración entre ambos sectores.

4. La importancia de actualizar continuamente los diagnósticos y adaptar las políticas y programas en función de los resultados obtenidos.

El objetivo del capítulo es resaltar el valor de la colaboración público-privada en el diagnóstico de problemas de seguridad, mejorando así la prevención, detección temprana, el control y la respuesta a las amenazas.

La dimensión de la alianza estratégica

En este capítulo, se aborda la dimensión de la alianza estratégica entre el sector público y privado en el ámbito de la seguridad, explorando las oportunidades y beneficios que surgen de esta colaboración. Se trata de promover la integración de ambos sectores, aprovechando sus fortalezas para mejorar la eficiencia y eficacia en la lucha contra las amenazas a la seguridad.

La licitación de fondos para proyectos de seguridad es un ejemplo de cómo la sinergia entre ambos sectores genera beneficios mutuos, permitiendo al sector público aprovechar la capacidad de gestión, recursos e inversión del sector privado. Estas formas de coparticipación público-privada han demostrado ser exitosas y se espera que continúen en el futuro.

Sin embargo, la propuesta de este capítulo va más allá de la simple colaboración o asistencia mutua entre los dos sectores. Se busca establecer una alianza estratégica en la que ambos participen activamente desde el inicio de un proyecto, contribuyendo con recursos, información, inteligencia, experiencia, medios y sistemas de medición.

Esta colaboración más intensa y asociativa permitiría a los actores del sector público y privado trabajar conjuntamente en la formulación, ejecución, evaluación y el ajuste de iniciativas de seguridad. De esta forma, se busca potenciar la capacidad de prevenir, detectar tempranamente, controlar y responder a amenazas a la seguridad pública, generando un impacto significativo en la protección y bienestar de la comunidad.

Este capítulo aboga por una alianza estratégica entre el sector público y privado en materia de seguridad, donde la colaboración y coparticipación van más allá de la mera ejecución delegada de unos con relación a otros. La finalidad es lograr un enfoque conjunto e integrado que permita enfrentar con mayor éxito los desafíos y las amenazas a la seguridad pública en el siglo XXI.

La licitación de fondos de para proyectos de seguridad genera sinergias entre el sector público y privado. De eso no hay duda. La tercerización de algunos servicios de seguridad desde el mundo público al privado permite a aquellos aprovechar los beneficios de la gestión, recursos y capacidad de inversión de éstos.

Como estas, muchas otras iniciativas en las que confluyen intereses de ambos sectores pueden ser consideradas tipos de coparticipación público-privada. Está bien que lo sean, y es deseable que continúen esta manera de operar. Todo aquello que permita alimentar intereses legítimos conjuntos y genere beneficios para una comunidad más segura no podría dejar de ser recomendado.

Pero la participación o, más bien colaboración público-privada que proponemos a través de este Manual es más intensa y sigue una lógica aún más asociativa. Se trata de trabajar en una alianza estratégica en la que ambos sectores participen activamente y aporten no solo recursos sino también, sobre todo, información, inteligencia, experiencia, medios, gestión y sistemas de medición.

En ese sentido, y sin perjuicio de la relevancia e importancia de otras formas de colaboración conjunta, se propone incentivar y trabajar no solo en la ejecución delegada de unos en relación a otros, o la asistencia o ayuda que pueda haber entre ellos, sino más bien, y sobre todo, que tanto el sector público como el privado participen simultáneamente desde el inicio de un proyecto, levantando diagnósticos conjuntos y actuando a la par en la formulación, ejecución, evaluación y el ajuste de iniciativas que busquen prevenir, detectar tempranamente, controlar y responder a amenazas a la seguridad pública.

Lo más importante

Este capítulo se centra en la importancia de establecer alianzas estratégicas entre el sector público y privado en el ámbito de la seguridad. Los principales aspectos por destacar son:

1. La promoción de la integración de ambos sectores para mejorar la eficiencia y eficacia en la lucha contra las amenazas a la seguridad.

2. La sinergia entre ambos sectores a través de la licitación de fondos para proyectos de seguridad, generando beneficios mutuos.

3. La búsqueda de una alianza estratégica en la que ambos sectores participen activamente desde el inicio de un proyecto, contribuyendo con recursos, información, inteligencia y experiencia.

4. La colaboración intensa y asociativa para trabajar conjuntamente en la formulación, ejecución, evaluación y el ajuste de iniciativas de seguridad.

La finalidad del capítulo es abogar por un enfoque conjunto e integrado entre el sector público y privado, permitiendo enfrentar con mayor éxito los desafíos y amenazas a la seguridad pública en el siglo XXI.

El proyecto conjunto. Metodologías y pensamiento creativo

El presente capítulo se centra en el enfoque colaborativo y asociativo en la generación de proyectos conjuntos, enfocándose en la importancia de la metodología y el pensamiento creativo en la formulación y gestión de proyectos de seguridad que involucren al sector público y privado. Se destaca la necesidad de una cooperación y coparticipación desde el inicio del proyecto, con el objetivo de maximizar la efectividad y el impacto en la prevención, detección temprana, control y respuesta a las amenazas a la seguridad.

En primer lugar, se analizan diversas metodologías y normas aplicables a la formulación y gestión de proyectos, como las normas ISO 9001, ISO 10006, ISO 21500, el Marco Lógico y el PMBOK (siglas en inglés de la Guía de los Fundamentos para la Dirección de Proyectos). Estas metodologías y normas proporcionan directrices y buenas prácticas para el diseño, desarrollo, ejecución y evaluación de proyectos en función de las necesidades y características de cada alianza y proyecto específico.

A continuación, se aborda la importancia de utilizar métodos creativos en el diseño de soluciones y líneas de acción. Se subraya el valor de la innovación y originalidad en la búsqueda de soluciones a los desafíos de seguridad, mediante la aplicación de técnicas de pensamiento crítico y creativo. Entre los ejemplos mencionados se encuentra la teoría de las ventanas rotas, que ha demostrado su efectividad en la reducción, prevención y el control de la criminalidad.

El objetivo principal de este capítulo es destacar la relevancia de seguir una metodología específica que facilite la discusión y el proceso creativo en el desarrollo de proyectos públicos y privados, evitando la improvisación y fomentando la generación de ideas innovadoras y efectivas.

Se busca impulsar la colaboración y coparticipación en la formulación y gestión de proyectos de seguridad, utilizando metodologías adecuadas y promoviendo el pensamiento creativo para lograr un impacto significativo en la reducción de riesgos y amenazas a la seguridad pública.

Aclarado el aspecto colaborativo, se recomienda comprender y abordar la alianza en el sentido que la generación del proyecto sea siempre conjunta, asociativa y coparticipativa desde el inicio.

Aceptado lo anterior, cobra interés el saber cómo seguir.

Sea que el diagnóstico se haya realizado conjuntamente, pero de manera previa o asilada del proyecto, o que esta evaluación sea parte de este como etapa inicial, lo importante es que será con base en este diagnóstico que se formulará el proyecto específico.

Las etapas que siguen consideran el diseño de la solución, ejecutar un plan de acción, controlar, medir y reportar, para finalmente evaluar eventuales ajustes.

Se trata de un proceso único, que se construye a través de la integración de una serie de actividades coordinadas y controladas, contando con una fecha de inicio y fin, y que son ejecutadas para lograr un objetivo previamente definido, y tomando en cuenta variables como liderazgo, coordinación, tiempo, recursos y activos disponibles, y costos, entre otras.

Metodologías

Desde la sola etapa de diseño deberían considerarse todas las alternativas y metodologías disponibles para la formulación y gestión de proyectos, cuya elección dependerá de cada alianza y proyecto en particular. Escapa de los propósitos de este Manual analizar todas las alternativas en detalle. No obstante, puede resultar conveniente, cuando menos, mencionarlas o listarlas.

Así, entre otras posibilidades nos encontramos con normas ISO,[13] y con modelos o metodologías como las del PMBOK o el Marco Lógico, entre muchos otros. Desde luego, hay otras normas y metodologías funcionales a la gestión, diseño y desarrollo de proyectos. En esta oportunidad, queremos aportar al usuario algunas de ellas con el fin de que puedan ser tomadas en cuenta.

[13] **Las normas ISO son estándares validados internacionalmente que establecen pautas comunes u homogéneas en relación a temas vinculados a gestión, eficiencia y seguridad tanto de productos y servicios como procesos. Que dos o más entes sigan una misma norma ISO permite velar por estándares comunes y comparables, facilitando la medición, evaluación y el control.**
Más información puede ser consultada en www.iso.org, la página web oficial de la Organización Internacional de Estandarización (ISO por sus siglas en inglés - International Organization for Standardization), organización internacional independiente e intergubernamental con sede en Suiza.

La Norma **ISO 9001**[14] entrega directrices para el diseño de desarrollo de los productos y servicios estableciendo elementos para implementar un sistema de gestión de la calidad, que proporciona orientación sobre cómo desarrollar un sistema formal, que puede ayudar a mejorar el desempeño y formar las bases para un desarrollo sostenible. Se trata de una norma que emplea un enfoque basado en procesos que incorpora el ciclo PHVA – Planear, Hacer, Verificar, Actuar.

A su turno, la Norma **ISO 10006**[15] aplicada a la gestión de proyectos contiene indicadores que, seguidos correctamente, aseguran altos niveles de calidad. Busca generar un lenguaje y tratamiento universal a la gestión de proyectos, velando por una armonización general de los distintos elementos asegurando, además, un planteamiento y un desarrollo correcto.

Finalmente, la Norma **ISO 21500**[16] se compone de directrices sobre Dirección y Gestión de Proyectos. Se trata de una guía que tiene por objeto entregar elementos para una eficiente gestión de proyectos. Nos orienta sobre los conceptos y los procesos relacionados con la gestión y dirección de cualquier tipo de proyectos.

Existen una gran cantidad de otras normas ISO que podrían ser aplicables como aquellas vinculadas a ciberseguridad, seguridad laboral, medio ambiente, riesgo operacional y cumplimiento, entre otros. Con todo, aquellas vinculadas a la gestión, dirección y el diseño de proyectos, productos y servicios parecieran ser las más relevantes.

En lo que la metodología del **marco lógico**[17] se refiere, podemos señalar que se trata de una herramienta de gestión de proyectos usada tanto en su diseño y planificación, como en ejecución y evaluación.

Por último, entre otras alternativas, vale mencionar el instrumento **PMBOK**[18] que establece un conjunto de buenas prácticas relacionadas con la dirección, administración y gestión a través de la implementación de herramientas, sistemas y técnicas que identifican una cantidad considerable de procesos distribuidos en un número menor de macroprocesos.

Sea cual fuere la metodología que se siga, tomemos en cuenta que todas ellas consideran una etapa en la cual, basado en un diagnóstico del problema, trabajan en el diseño de soluciones y líneas de acción.

[14] www.iso.org
[15] www.iso.org
[16] www.iso.org
[17] **Más información se puede encontrar en el Manual de la Comisión Económica Para América Latina – CEPAL, de las Naciones Unidas, denominado Metodología del Marco Lógico para la planificación, el seguimiento y la evaluación de proyectos y programas. Según lo indica el propio Manual, el Marco Lógico es una herramienta para facilitar el proceso de conceptualización, diseño, ejecución y evaluación de proyectos. Su énfasis está en la orientación por objetivos, la orientación hacia grupos beneficiarios y el facilitar la participación y la comunicación entre las partes interesadas.**
https://repositorio.cepal.org/bitstream/handle/11362/5607/S057518_es.pdf
[18] **Más información sobre instrumento PMBOK puede consultarse en la Guía de los Fundamentos para la Dirección de Proyectos (Guía PMBOK®) del Instituto de Gestión de Programas (Program Management Institute, en inglés)**
https://www.pmi.org/pmbok-guide-standards/foundational/pmbok?sc_camp=D750AAC10C2F4378CE6D51F8D987F49D

Métodos creativos

Existe una variada gama de sistemas y metodologías que facilitan el proceso creativo que consideramos esencial para que se puedan diseñar soluciones novedosas, originales, diferentes, eficientes y orientadas al resultado en el marco de la alianza público-privada, con el fin de generar un impacto directo en la reducción sustancial de los riesgos a la seguridad a través de actividades de prevención, detección temprana, control y respuesta.

Al igual que los métodos de gestión de proyectos, abordar con detalle las diversas metodologías y técnicas de pensamiento creativo sale de los márgenes de este Manual. No obstante, su impacto puede ser de tal trascendencia que vale la pena, cuando menos, conocer su existencia, utilidad y denominación.

Hoy en día pocos podrían discutir los efectos beneficiosos generados con el conjunto de soluciones logradas en torno a la teoría de las ventanas rotas como mecanismos de reducción, prevención y control de la criminalidad, pero antes de 1982, año de su primera formulación teórica, nadie conocía de ella.[19] Son precisamente las nuevas medidas que presentan ciertas cuotas de innovación y originalidad, aquellas que generarán un entorno con mayores probabilidades de cambio en los resultados buscados.

Mencionar o utilizar esta teoría de las ventanas rotas para el proceso de análisis o discusión que se genera en las primeras etapas de formulación de proyectos públicos privados, puede ser resultado del azar o como consecuencia de una metodología de trabajo que, al ser aplicada, promueve o genera las condiciones para que los participantes formulen este tipo de insumos o aportes.

El objetivo de esta sección es destacar la importancia de que, con ocasión del proceso de discusión y levantamiento de problemas e ideas, se siga una metodología determinada que facilite ese proceso y que tenga precisamente ese objetivo, en vez de dejar ello a la mera espontaneidad o trabajo azaroso de los integrantes del grupo de discusión.

Se trata de buscar resultados distintos, obligarse a deliberar de manera consciente y bajo una pauta metodológica determinada, para que, a través de técnicas específicas de pensamiento crítico y creativo, se logren eliminar los bloqueos que frenan la creatividad de las ideas, favoreciendo la comprensión y desarrollo a la vez que se logran resultados creativos.

[19] Teoría de la criminología según la cual los signos visibles de la delincuencia, el comportamiento antisocial y los disturbios civiles, entre otros, crean un entorno urbano que fomenta la delincuencia y el desorden, incluidos los delitos graves. Según este desarrollo teórico, los métodos estatales, en general, y policiales, en particular, que se centran en atacar los delitos menores, como el vandalismo, la vagancia, el consumo de alcohol en público, el cruce incorrecto de peatones y la evasión de tarifas, ayudan a crear una atmósfera de orden y legalidad.
Wilson, George L. Kelling, James Q. (1 de marzo de 1982). «Broken Windows». *The Atlantic* (en inglés).

No se trata de recomendar métodos específicos sino el sugerir que se siga una metodología que facilite la discusión evitando la improvisación.[20]

Lo más importante

El capítulo enfatiza la importancia de un enfoque colaborativo y asociativo en la generación de proyectos conjuntos de seguridad entre el sector público y privado. Los puntos clave a destacar son:

1. La necesidad de cooperación y coparticipación desde el inicio del proyecto para maximizar la efectividad e impacto en la seguridad.

2. El análisis de diversas metodologías y normas aplicables en la formulación y gestión de proyectos, como ISO 9001, ISO 10006, ISO 21500, el Marco Lógico y el PMBOK.

3. La importancia de utilizar métodos creativos, innovadores y originales en el diseño de soluciones y líneas de acción, aplicando técnicas de pensamiento crítico y creativo.

4. La promoción de la colaboración y coparticipación en proyectos de seguridad, utilizando metodologías adecuadas y fomentando el pensamiento creativo para lograr un impacto significativo en la reducción de riesgos y amenazas a la seguridad pública.

El objetivo principal del capítulo es impulsar una metodología específica que facilite la discusión y el proceso creativo en el desarrollo de proyectos públicos y privados, evitando la improvisación y fomentando la generación de ideas innovadoras y efectivas.

[20] Entre las variadas metodologías existentes que se pueden aplicar, se encuentran los Mapas mentales; Lista de atributos; Tormenta de ideas; Método CRE-IN; Palabras aleatorias; TRIZ - Teoría para resolver; Problemas de inventiva; Lista de comprobación; DO IT - Definir, abrir, identificar y transformar; Identificación conceptual; Eliminación de bloqueos mentales; Inversión; Los 6 Sombreros - conciliación, neutro, emoción, negativo, positivo y divergente; Método 635; SCAMPER - sustituir, combinar, adaptar, modificar, poner en otros usos, eliminar o reordenar; 4x4x4; PNI - positivo, negativo e interesante; Mapa mental; Analogías; Sinéctica

Comenzado la alianza. Los primeros pasos

Este capítulo aborda el inicio y desarrollo de una alianza público-privada exitosa, destacando la importancia de establecer una metodología común, conceptos compartidos y valores, así como los requisitos previos necesarios para llevar a cabo el proyecto.

La metodología acordada entre los socios es el primer nivel que considerar, seguido por los conceptos comunes y los valores compartidos. Una vez se llegue a un consenso en estos niveles, se discutirán los requisitos previos para el proyecto.

Esta sección aborda los llamados "Conceptos Comunes", enfatizando la necesidad de generar consenso y claridad en temas clave, tales como identificación de los interesados, definición de objetivos y sitios, desarrollo de un léxico común, estructuras predefinidas para la cooperación, tratamiento de información, ejercicios y pruebas, definición de roles y tareas, y eficiencia en el uso de recursos.

En complemento, se analiza un componente clave en las alianzas público-privadas, que dice tener relación con los valores que deben ser reconocidos y compartidos por todos los socios de un proyecto. Estos incluyen equilibrio, beneficio mutuo, dinamismo, compromiso a largo plazo, responsabilidad compartida, flexibilidad y confianza.

Por último, se abordan los requisitos previos como condición necesaria para el éxito de la alianza, entre los que se incluyen el caso empresarial, intercambio de información, confianza entre los socios, voluntad política, coordinación, aplicación de conocimiento experto, responsabilidad, voluntariedad y cumplimiento del marco legal.

Este capítulo proporciona una guía detallada sobre cómo establecer una alianza público-privada exitosa, abordando aspectos clave como la metodología, conceptos comunes, valores compartidos y requisitos previos. Siguiendo estas pautas, los socios involucrados podrán desarrollar proyectos colaborativos eficaces y sostenibles, maximizando el uso de recursos y optimizando los resultados.

En este apartado se discute con más profundidad el proceso de cómo comenzar una alianza público-privada.

Este proceso puede dividirse en tres niveles diferentes. El primer nivel, el de metodología, ya anticipado, debería ser el primero en ser considerado por todos los potenciales socios. Una vez que todos ellos se hayan puesto de acuerdo sobre la metodología a utilizar, es recomendable abordar asuntos relacionados con los *conceptos comunes* (primer nivel) y los *valores compartidos* (segundo nivel) que se explicarán a continuación. Cuando exista un acuerdo mutuo sobre ello, debería discutirse el nivel de *requisitos previos* (tercer nivel) para el proyecto.

Conceptos comunes

Cuando se esté considerando el desarrollo de un proyecto de alianza público-privada para proteger objetivos vulnerables o contrarrestar las amenazas a la seguridad, es muy necesario generar el consenso y tener claridad y acuerdo con relación a una serie de temas claves para la aplicación de la metodología de trabajo seleccionada.

* **Identificación de los interesados:** Contactar con los potenciales interesados y preguntarles si están dispuestos a unirse al proyecto. También habrá que definir quién actuará como facilitador/coordinador del proyecto de Asociación público-privada. Por muy vinculado que el proyecto esté con el concepto de seguridad, no necesariamente, y no hay que cerrarse a la idea, una agencia estatal debiera ser la coordinadora. Es relevante tomar esto en cuenta.

* **Identificar objetos:** Tiene que estar claro qué sitios, objetos y lugares entran dentro del ámbito del proyecto. Esto es, obviamente, una cuestión delicada y por lo tanto quizás debería ser clasificada como asunto reservado por todas las partes implicadas con relación a terceros externos al proyecto.

* **Léxico común:** Basado en la formación y la experiencia de los interesados, es deseable el desarrollo de un léxico común, que comprenda a todos los socios. En los sistemas gubernamentales, por ejemplo, no es inusual el uso de distintos términos para la misma cosa, o de un término similar para distintas cosas.

* **Objetivo al que se dirige:** Los socios del proyecto deberán definir cuidadosamente y de modo realista el objetivo u objetivos del proyecto de alianza púbico-privada. En definitiva, qué es lo que esperamos lograr.

* **Basado en un proceso:** Las disposiciones para la cooperación y la coordinación dentro del marco de la alianza público-privada deberán basarse preferentemente en estructuras predefinidas y acordadas. De ahí la importancia del capítulo precedente que aborda el aspecto metodológico.

* **Tratamiento de información:** Las disposiciones y el plazo o plazos deberían definirse para el intercambio de información entre los socios. El tratamiento de este concepto tiene reservada una sección aparte en este Manual dada su relevancia.

* **Ejercicio y prueba:** El desarrollo de un calendario para realizar y probar tanto ejercicios teóricos como prácticos es altamente recomendable.

* **Definición de papeles e identificación de tareas:** Se deberán definir muy claramente qué papeles y qué tareas específicas desarrollará cada individuo y cada organización, así como cualquier limitación que pueda preverse a ese respecto.

* **Eficiencia:** Intentar optimizar el uso de recursos, maximizar la eficacia y evitar la duplicación de los esfuerzos.

Los valores compartidos

En un proyecto de alianza público-privada exitoso, todos los socios deben estar de acuerdo en identificar por adelantado los valores compartidos y su significado. Dependiendo de la cultura, capacidad y los obstáculos que prevalecen, estos valores pueden ir cambiando. Una lista de algunos de ellos tiene fines ilustrativos con relación a este punto.

* **Equilibrio:** Los socios de un proyecto conjunto entre entidades públicas y privadas deberán tener el mismo estatus. Planteamiento beneficioso para ambas partes: Todos los socios deberán tener la oportunidad de "ganar algo" con su participación en el proyecto, incluida una serie de beneficios empresariales, por ejemplo. Identificar y sincerar los objetivos de cada actor en términos de comprender qué es lo que desea ganar, resultará relevante para el éxito de una asociación, sobre todo si se espera que esta perdure.

* **Dinamismo:** Todos los proyectos de colaboración entre sector público y privado deberán buscar un planteamiento dinámico tanto por parte de los socios públicos como de los privados, y todos los socios deberán estar de acuerdo en trabajar, pensar e intercambiar información de un modo dinámico.

* **Compromiso a largo plazo:** Es muy probable que un proyecto de alianza público-privada implique un compromiso a largo plazo. Con el tiempo, aumentarán la confianza y las relaciones si la pertenencia al consorcio sigue siendo tan consistente como sea posible.

* **Responsabilidad compartida:** Dado que un proyecto colaborativo debe estar basado en la confianza y la responsabilidad mutuas, todos los socios implicados son responsables de maximizar su contribución y aumentar la eficacia y eficiencia del proyecto.

* **Flexibilidad:** Todos los socios tienen que ser flexibles por el hecho de que las circunstancias y los ámbitos del terrorismo y criminalidad están cambiando constantemente. Los socios deberán estar dispuestos a redefinir sus posturas, si procede, y a discutir de un modo productivo los cambios, cuando varíen las circunstancias.

* **Afianzamiento de la confianza:** Dentro del marco de un proyecto público-privado, los socios tienen que confiar los unos en los otros, en particular, dado el nivel crítico que supone el intercambio efectivo de información entre los miembros.

Los requisitos previos

Una vez que los socios se hayan puesto de acuerdo acerca de los valores compartidos, es recomendable considerar el cumplimiento de los siguientes requisitos previos necesarios:

* **Caso empresarial:** Los detalles del proyecto del proyecto específico que aborda una alianza público-privada debería idealmente estructurarse y explicarse en un formato de caso empresarial.

* **Intercambio de información:** Todos los socios, tanto privados como públicos, deberán estar dispuestos a intercambiar, sin infringir la ley, información operativa y/o basada en la amenaza sobre los niveles de seguridad y riesgo.

* **Confianza:** Todos los socios deberían confiar los unos en los otros. Si hay socios del sector privado de la misma industria, deberán adoptarse medidas claras por adelantado para evitar un conflicto de intereses o competencia desleal. Dado que la confianza no es un elemento neutro que existe, sino que más bien un valor que se obtiene o logra, será relevante que el proyecto cuente con elementos que no solo permitan generar confianza sino también con aquellos que evitarán que se pierda, una vez lograda.

* **Voluntad política:** El apoyo y la voluntad política será siempre necesaria para asegurar que los socios gubernamentales o estatales pongan a disposición del proyecto todos sus recursos y operen de la manera más eficiente posible.

* **Coordinación:** Establecer y definir mecanismos eficientes de coordinación es esencial. Se trata de un elemento cuya eficiencia no puede descansar en la iniciativa espontánea de uno o más miembros, sino que debe ser regulada y definida conjuntamente por todos los actores.

* **Aplicación de un conocimiento experto:** Desarrollar un conocimiento experto, compartir la experiencia, apoyar a los nuevos participantes y promover el concepto de colaboración, integración, asociación y alianza público-privada.

* **Responsabilidad:** Una alianza público-privada genera siempre derechos y obligaciones para las partes, las cuales deberán reconocerse de manera tanto genérica como específica en un documento o acuerdo escrito. Mientras los memorandos de entendimientos o acuerdos marcos representan manifestaciones de interés colaborativo general, los protocolos o procedimientos de acción por tema llevan ese compromiso a un nivel más concreto, como ocurre con los procedimientos de intercambio de información, manejo de redes sociales, aspectos administrativos, operación, relación con terceros externos, etc.

* **Voluntariedad:** Aunque toda alianza conlleva obligaciones para las partes, la conformación de una asociación público-privada supone la voluntariedad, y no debe ser una consecuencia de una obligación impuesta a uno de los miembros. En las obligaciones hay restricciones a las que se someten los miembros que se fundamentan en la voluntad de estos de aceptarlo.

* **Contexto legal:** El proyecto y todos aquellos que estén implicados en él deben actuar en todo momento según lo dispuesto en las leyes locales, nacionales e internacionales.

Lo más importante

Este capítulo se centra en el inicio y desarrollo de una alianza público-privada exitosa y destaca los aspectos clave para lograrlo. Los principales puntos que rescatar son:

1. La importancia de establecer una metodología común, conceptos compartidos y valores entre los socios del proyecto.

2. La necesidad de generar consenso y claridad en temas clave, como identificación de interesados, objetivos, léxico común, estructuras de cooperación, roles y eficiencia en el uso de recursos.

3. Los valores compartidos esenciales, como equilibrio, beneficio mutuo, dinamismo, compromiso a largo plazo, responsabilidad compartida, flexibilidad y confianza.

4. Los requisitos previos necesarios para el éxito de la alianza, incluyendo el caso empresarial, intercambio de información, confianza, voluntad política, coordinación, conocimiento experto, responsabilidad, voluntariedad y cumplimiento del marco legal.

Siguiendo estas pautas, las alianzas público-privadas podrán desarrollar proyectos colaborativos eficaces y sostenibles, maximizando el uso de recursos y optimizando los resultados.

Principales focos para el diseño de soluciones Público – Privadas

Este capítulo se adentra en el análisis de los principales focos para el diseño de soluciones público-privadas en el contexto de la seguridad y la prevención de amenazas. A través de varios subcapítulos, se examinan factores críticos que impactan en el diseño de una solución y líneas de acción concretas en el marco de una Alianza Público-Privada (APP). Los temas tratados incluyen la identificación de perfiles de amenazas, análisis de objetivos y víctimas potenciales, comprensión de las motivaciones detrás de las amenazas y el estudio de los patrones de comportamiento en la ejecución de acciones delictivas o terroristas.

El capítulo aborda los siguientes aspectos clave en el diseño de soluciones público-privadas para enfrentar amenazas a la seguridad:

01 ***Identificación del perfil de la amenaza:*** *Determinar quién comete el acto delictivo o terrorista y dirigir acciones específicas para contrarrestar sus actividades.*

02 ***Análisis de objetivos y víctimas potenciales:*** *Establecer contra quién, contra qué o con relación a qué se concreta la amenaza, incluyendo personas, instalaciones críticas o servicios que podrían verse afectados.*

03 ***Comprensión de las motivaciones detrás de las amenazas:*** *Analizar las razones y objetivos económicos, ideológicos o personales que impulsan a los perpetradores a cometer actos delictivos o terroristas.*

04 ***Estudio de los patrones de comportamiento:*** *Identificar dónde y cuándo se cometen las amenazas, así como los patrones de comportamiento en la ejecución de acciones delictivas o terroristas.*

05 ***Diseño de soluciones conjuntas y colaborativas:*** *Abordar las amenazas a través de alianzas público-privadas que combinen tecnología, recursos, información y capacidades de ambos sectores.*

El éxito en la implementación de soluciones público-privadas para la seguridad depende de la colaboración efectiva entre los actores públicos y privados y del enfoque integral y programado en la ejecución de las líneas de acción propuestas en este capítulo.

En la sección de este Manual denominada “El Diagnóstico del Problema” se mencionaron un total de 13 factores claves que se recomienda tener en cuenta en esta etapa de formulación público-privada.

De estos elementos, un mínimo de cinco resulta igualmente importante para las siguientes etapas que impactan directamente en el diseño de una solución, así como de líneas de acciones concretas.

¿Quién lo comete?

Perfil del objetivo cuya acción buscamos contrarrestar. Las acciones que se desarrollen deben estar orientadas a perfiles determinados de manera que se pueda generar el efecto buscado.

Evidentemente, no se puede encasillar a todos en un solo perfil, pero se debe lograr enfocar el trabajo a un grupo determinado de personas, cuya caracterización probablemente esté asociada a las de alguna de las otras variables.

De esta manera, si el programa dice tener relación con amenazas a un evento concurrido o masivo, importa analizar y determinar el perfil de personas y/u organizaciones que tienen o podrían tener intereses y/o capacidad operativa para concretar la amenaza a través de uno o más atentados terroristas. Definir ese perfil resultará útil para alinear las demás acciones y elementos, pues todas deberían estar condicionadas y asociadas a ese perfil en particular.

¿Contra quién, contra qué y/o con relación a qué se concreta la amenaza?

¿Cuál es el público, personas, instalaciones críticas o servicios que podrían verse afectados por la amenaza que se desea abordar? Determinar ese perfil tiene la misma relevancia que hacerlo respecto a quién quisiera o pudiera atentar con ese público, personas, instalaciones o servicios.

Si estamos en presencia de un evento concurrido, como serían unos juegos deportivos, un concierto, las víctimas directas de un atentado terrorista, por ejemplo, sería el público asistente. Luego, dentro de esa categoría es importante ir más allá, pues a quienes pretendieran, pudieran o quisieran concretar un atentado, podrían tener diversos objetivos finales:

A atacar a un grupo específicos de personas que concurrirá a la actividad;

B destruir una instalación deportiva o infraestructura específica, independientemente del tipo o perfil de las potenciales víctimas;

C interrumpir un servicio o evento;

D una combinación de las anteriores, entre otras.

De esta manera, es necesario perfilar a las víctimas o población afectada cuando la amenaza se dirija contra individuos o grupos específicos, ejercicio que no será igual si se establece que la acción criminal o terrorista va dirigida en contra de una instalación. La variedad es amplia, pues bien podría tratarse de unas amenazas que al concretarse generan daños y perjuicios a las personas de manera más indirecta o difusa, como es el caso del tráfico de drogas o contrabando, situaciones en las cuales los grupos afectados podrían ser pobladores que viven en barrios o sectores tomados por los grupos narcotraficantes o aquellos locatarios que no pueden competir con productos importados de manera ilícita.

Definir el potencial objetivo de ataque, personas o instalaciones que pudieran resultar afectados permitirá generar mecanismos preventivos y dar más protección a los mismos, pero también será esencial para definir líneas de acción concretas.

Si la amenaza es en contra de un grupo determinado de personas, trabajar la amenaza con ellas será clave, así como conocer sus rutinas y principales vulnerabilidades.

En el caso del robo de autos, un análisis de este tipo nos permitiría generar líneas de acción diferenciadas cuando los robos son cometidos contra vehículos estacionados, casos en los cuales todo indica que las características del dueño o la persona no tienen mayor impacto, como sí lo será el tipo de vehículo. Pero cuando se trata de robos de vehículos a mano armada, es bastante probable que el factor definido por tipo de vehículo se complemente con el perfil de la persona que va al volante (personas mayores o con bebes, cuya capacidad de respuesta se encuentre limitada, por ejemplo).

Este simple ejemplo ilustrativo nos permite darnos cuenta de que las estrategias para un tipo de robo y otro, basado solo en el perfil del objeto o persona afectada, deben ser distintas. ¿Tiene algo que aportar el sector privado sobre esto? Desde luego. Muchas veces la sola exigencia de GPS para el otorgamiento de seguros puede no solo generar datos relevantes para el proyecto integrado sino también producir un impacto en variables críticas que queremos contrarrestar. De igual manera, un acuerdo público-privado en torno a importar todos los vehículos nuevos con corta corriente es útil. Marcar partes y piezas de vehículos podría ayudar mucho, área en la cual el sector privado tiene mucho que decir, pero que no tendría sentido si la autoridad luego no incorpora esa variable en sus operativos de búsqueda. Nuevamente la integración colaborativa es esencial.

Tratándose de una amenaza en contra de instalaciones críticas o servicios esenciales cometida por medios cibernéticos, sea que tengan fines terroristas o no, las líneas de prevención, detección temprana y mitigación de daño no serán iguales si se trata de un aeropuerto que la entidad estatal a cargo de la emisión de documentos de identidad, no porque uno y otro sea menos importante sino porque la arquitectura de sus sistemas informáticos es distinta.

Cuando nos enfrentamos a un estadio, instalación deportiva o un centro de eventos, la sola disposición de las salidas de emergencia, un elemento físico difícil de cambiar en un corto plazo podría determinar la manera en la que se desarrollen planes para mitigar atentados terroristas. El tipo de evento sea deportivo, social o político, influirá igualmente en la manera en la que se elaboren líneas de acción concretas.

¿Por qué lo comete/n?

El móvil, interés o razón que hay detrás de un atentado o de un delito entrega mucha información sobre variables tan importantes como el perfil de la persona u organización que lo comete o podría cometer, el perfil de la persona o grupo de personas víctimas, así como el modus operandi.

Es esencial considerar las motivaciones de la amenaza que queremos abordar para asegurar un diseño efectivo. Salvo algunas amenazas organizadas de corte ideológico o personal, la gran mayoría tiene un objetivo o una motivación económica. Puede que se trate de atentados terroristas, tráfico de drogas, explotación de víctimas de trata de personas, el sicariato, la extorsión o el contrabando de armas, quien está detrás de los actos que afectan la seguridad buscan generar ganancias económicas.

De esta forma, un buen diagnóstico nos permitirá comprender que mientras algunos vehículos se roban para ser desarmados y vendidos por partes y piezas, otros serán contrabandeados a otros países e intercambiados por drogas o dinero, en tanto habrá aquellos que son robados y abandonados luego de algunos días durante los cuales fueron utilizados para cometer otros delitos. Como es posible apreciar, las motivaciones son diversas. Así encontramos también casos de vehículo que ni serán intercambiados por droga, ni desarmados por partes, ni utilizados para cometer otros delitos, sino para adulterar su identidad legal a través de una clonación, con el fin de permitir su venta fraudulenta en el mercado formal.

¿Tiene algo que decir el sector privado sobre esto? Son estos quienes compran y venden las partes y piezas de los vehículos, en un mercado que se verá afectado con la introducción de productos robados. Así, su aporte, en términos de conocimiento acerca de cómo funciona la compra y venta de estos bienes, es de extrema relevancia y de ahí podrían surgir ideas específicas y prácticas acerca de cómo identificar productos robados y qué medidas adoptar para prevenir la comisión de estos delitos, como sería mediante la instalación de marcas que faciliten su identificación por parte de las policías y entes de fiscalización y control.

¿Será relevante el aporte que puedan hacer los martilleros, subastadores o casas de remate, las cuales sabiendo que muchas veces venden en subasta pública vehículos destruidos que no van a ser reparados, teniendo su compra como único fin el de utilizar su identidad a fin de facilitar la clonación con otros vehículos robados? ¿Será beneficioso el intercambio de las bases de datos de compradores o intermediarios con el objeto de identificar patrones compatibles con la amenaza que pretendemos abordar? Cualquier línea de trabajo concreta que se quiera ejecutar a partir de este aspecto, tendrá más niveles de éxito si involucramos a este representante del sector privado.

Los beneficios se verán potenciados cuando esas mismas actividades, y en el marco del mismo proyecto, se complementan e integran con actos de fiscalización de la autoridad a cargo del control de pago de impuestos, la que podría integrarse a una estrategia tradicionalmente vinculada solo a las policías y que, en este caso, podría favorecer acciones de mayor impacto.

De igual manera como ocurre con el robo de vehículos, en materia de seguridad de los espacios concurridos, comprender las razones y motivaciones resultará relevante no solo para diagnosticar el problema sino también para diseñar soluciones. No será lo mismo el robo que sufre un turista de su cámara, al atentado terrorista que experimenta un hotel. No será igual la clonación de una tarjeta de un turista, como el secuestro de este. Las motivaciones en uno y otro caso son distintas y, en consecuencia, la manera de abordar la amenaza va a varias según éstas.

Ocurre que probablemente el primer y último contacto con un turista en un país lo podría tener el sector estatal, con ocasión del control migratorio en frontera, pero el resto del tiempo será el privado el que contará con mucha más información: lugares que visitó, tipo de visita, incidentes que se presentaron, tamaño de grupo familiar, valor del paquete turístico, medios de transporte utilizados, entre muchos otros elementos. De ahí que las iniciativas como las de México, a través de los CAPTA o de Ecuador mediante los PIAT resultan interesantes de analizar.[21]

Nuevamente, una inclusión del sector privado en la identificación de problemas y en el diseño de soluciones es esencial.

¿Dónde y cuándo se comete?

Las amenazas se concretan en zonas geográficas determinadas y, por regla general, en momentos (días, horas, meses) específicos. Algunos son continuos y permanentes, como es el caso del crimen organizado, mientras que otros son más ocasionales, pero de mayor impacto como los atentados y actividades terroristas. Identificar estas variables resulta esencial en el diseño de líneas de acción público-privadas en materia de seguridad, tanto porque las acciones programáticas debieran dirigirse a esos espacios físicos y temporales, como también porque circunscribir estos conceptos nos permitirá realizar mejores mediciones de impacto.

[21] **Ver notas 39 y 40 del Manual, que explican con mayor detalle estas iniciativas.**

Volviendo a nuestro ejemplo de robo de vehículos, conocer el lugar y horario en los que se produce la mayor cantidad de apropiaciones de automóviles estacionados nos permitirá diseñar e implementar más eficientemente técnicas de prevención y control a través de autos señuelos. En efecto, el uso de vehículos equipados con sistemas de monitoreo (cámaras, GPS, micrófonos) y control (luces, bocinas, cierre de puertas, encendido-apagado del motor) a distancia representa una muy buena herramienta de trabajo para contrarrestar esta amenaza, pero también una muy cara. El objetivo de un auto señuelo es que sea robado, no tanto para detener a las personas apenas se subieron al mismo sino para conocer el destino que tome y, de esa manera, afectar a toda la cadena de disvalor.

No solo interesa que el vehículo señuelo sea robado, sino que ello ocurra en el plazo más breve posible. Tener estacionado un vehículo señuelo por semanas o meses es poco rentable. Para incrementar la probabilidad de robo, debemos habilitar como señuelo a aquel tipo, color y año del vehículo más robado y colocarlo en la zona o ubicación con más tasa de robo. ¿Los estacionamientos de los centros comerciales con lugares de alta incidencia de robos, tendrán algo que decir? ¿Tiene sentido pensar en una alianza para estos efectos? ¿Mientras desmantelemos organizaciones criminales, se verán beneficiados determinados espacios públicos, administrados por privados?

No se trata solamente de colocar el vehículo en un estacionamiento de un centro comercial. El trabajo colaborativo va mucho más allá. Desde el uso de cámaras, la generación de alertas tempranas y hasta la publicidad preventiva, son intervenciones privadas que impactan directamente en una política pública. Si queremos que funcionen de manera eficiente, deben ser parte de un programa colaborativo conjunto e integrada dentro de una solución más amplia, planificada y medida.

Un porcentaje importante de vehículos son estacionados en espacios públicos o concesionados. Las posibilidades de control y fiscalización de todos ellos se encuentran limitado a los recursos policiales disponibles para esa tarea. Si asumimos que la detección temprana de cada uno de esos automóviles, motocicletas o camiones es útil, en términos de identificar aquellas unidades estacionadas que hayan sido previamente robadas, entonces resultará esencial incorporar en el diseño de la solución a los entes privados que tienen impacto sobre esos espacios públicos o concesionados.

Veamos un ejemplo. Imaginemos que, en determinadas zonas geográficas, países o localidades, los vehículos que se estacionan en la calle, en vez de pagar el parquímetro con mensajes de texto o monedas, el control de llegada y salida lo realiza un funcionario o empelado de una empresa privada a la cual se concesionaron esos estacionamientos. Hoy en día, un porcentaje importante de ese tipo de empleados cuentan con aparatos que luego de ingresar la placa o patente comienzan a contabilizar el tiempo transcurrido, con el fin de poder cobrar directamente al conductor al momento en que este se retira. La gran mayoría de estos aparatos poseen conexión a internet y GPS para facilitar la reportería a sus matrices y tener un control en tiempo real de la operación de cobro de estacionamientos. En ese contexto, ¿qué tan útil podría resultar que esa base de datos se interconecte con la base de vehículos robados que posee la autoridad, de manera que cada vez que un empleado de estacionamientos ingrese una placa de un vehículo robado, esa información sea reportada automáticamente a las autoridades, proveyendo, incluso, la ubicación georreferencial de ese vehículo? Una aproximación similar se podría realizar con las autopistas y toda otra entidad privada que, teniendo la posibilidad y facultad de registrar datos de vehículos, no cuentan con acceso a bases de datos de vehículos robados.

Lo relevante no es ver esto como un acuerdo bilateral entre policía y empresa de estacionamientos o centro comercial, sino como una colaboración público-privada en el marco de una línea de acción específica que es parte integral de un proyecto conjunto mucho más amplio.

En otro orden de ideas, a nivel cibernético, es posible también identificar los lugares virtuales, en los cuales las amenazas se han concretado en el pasado o podrían concretarse. Eso ayudará a generar mejores mecanismos de prevención y reforzar la seguridad sistémica.

Que un ataque cibernético, sea criminal o de corte terrorista, pueda impactar en casi cualquier tipo de infraestructura virtual abierta o semi abierta, es un hecho, pero bien podría desarrollarse en conjunto con el sector privado un mapa de riesgo en función de objetivos potenciales. No cabe duda de que la base de datos de pasaportes o registros de identidad de un país podría transformarse en un objetivo de interés. Muchas bases de datos o sistemas de operación informática gubernamental o policial también, como es el caso del registro de personas prófugas o fugitivas, condenas, registros aduaneros o de impuestos.

Ocurre que atentar contra objetivos privados puede causar igual o mayor daño a un país. Imaginemos tan solo las bases de datos bancarias, o de transporte de líneas áreas, o de cualquier empresa privada que opera instalaciones que prestan servicios de utilidad pública como una empresa eléctrica, de telefonía celular o aeropuerto. La paralización de cualquiera de estas operaciones a cargo del sector privado causaría inevitablemente un gran costo a un país, a sus habitantes y a su seguridad. Aun así, esperar que el Estado, por sí solo, confronte esa amenaza, es poco recomendable. Una vez identificados los objetivos vulnerables en contra de los cuales se dirige o podría dirigirse una amenaza, si estos son operados directa o indirectamente por un ente no público, sea este una empresa privada o asociación comunitaria, su inclusión en el diagnóstico del problema, así como el diseño e implementación de líneas de trabajo, es crítica.

Los patrones de comportamiento y el diseño de soluciones conjuntas.

Una alianza público-privada, en los términos propuestos en este Manual representa una manera distinta de abordar las amenazas a la seguridad con relación con la forma en la que estas han sido tradicionalmente confrontadas.

De hecho, la esencia de ello radica en el concepto planteado precedentemente. Se busca entregar herramientas para diseñar soluciones que ayuden a lograr resultados distintos o incrementar aún más los impactos generados. Para aquel sector público o privado que quiere afectar aún más determinadas amenazas terroristas o de crimen organizado, evidentemente, haciendo lo mismo no producirá mayores efectos, no al menos en los niveles deseados. Es recomendable, en consecuencia, cambiar la manera de trabajar. Una de esas formas es, precisamente, a través de una alianza y colaboración público-privada orientada a la disminución de los riesgos derivados de las amenazas a la seguridad. El aporte del sector privado a través de tecnología, recursos, información y capacidades generará condiciones más ventajosas para prevenir y/o detectar una amenaza terrorista o una proveniente de la criminalidad organizada.

Por el contrario, mientras el Estado y el sector privado se enfrentan al desafío de incorporar cambios en su forma de trabajar, un porcentaje relevante de grupos terroristas, antisociales, antisistémicos y criminales probablemente no lo hagan, y mantendrán igual su manera de operar, materializando sus amenazas bajo patrones de comportamiento similares.

A diferencia de nosotros, y dado que muchos de sus objetivos se han ido cumpliendo, ellos no han tenido, en gran medida, mayores incentivos al cambio.

Dicho de otra manera, mientras se debiera cambiar la forma de trabajar para buscar resultados distintos, quienes están detrás de las principales amenazas a la seguridad tienden a mantener su forma de operar a fin de mantener los mismos resultados que ya están generando.

La constatación de este hecho representa una oportunidad para generar programas de impacto exitosos por parte de iniciativas conjuntas entre los sectores público y privado, quienes podrán encontrar en los patrones de comportamiento indicadores que facilitarán la medición, cuantificación e identificación de nuestras amenazas.

Todo diseño de soluciones debiera considerar esta variable para cuyo levantamiento e incorporación, tanto entidades públicas como privadas tienen mucho que aportar.

Para ello el uso de Centros de Fusión o software de análisis de datos resultará muy útil. Ambos aspectos, analizados más adelante en este Manual conllevan la participación de actores públicos y privados.

El éxito dependerá no solo del suministro de experiencias, ideas y recursos de cada una de las partes, sino de la ejecución de esta línea de acción de una manera conjunta, programada e integral, en los términos indicados en este Manual.

Lo más importante

Este capítulo analiza los aspectos clave para el diseño de soluciones público-privadas en el contexto de la seguridad y prevención de amenazas. Los principales puntos que rescatar son:

1. Identificación del perfil de la amenaza: Determinar quiénes son los perpetradores y enfocar acciones específicas para contrarrestar sus actividades.

2. Análisis de objetivos y víctimas potenciales: Establecer a quiénes o qué podrían verse afectados por la amenaza, incluyendo personas, instalaciones críticas o servicios.

3. Comprensión de las motivaciones detrás de las amenazas: Analizar las razones económicas, ideológicas o personales que impulsan a los perpetradores a cometer actos delictivos o terroristas.

4. Estudio de los patrones de comportamiento: Identificar dónde y cuándo se cometen las amenazas y los patrones en la ejecución de acciones delictivas o terroristas.

5. Diseño de soluciones conjuntas y colaborativas: Abordar las amenazas a través de alianzas público-privadas que combinen tecnología, recursos, información y capacidades de ambos sectores.

El éxito en la implementación de soluciones público-privadas para la seguridad depende de la colaboración efectiva entre actores públicos y privados y del enfoque integral y programado en la ejecución de las acciones propuestas.

El tratamiento de información

Este capítulo aborda el tema del intercambio de información entre entidades públicas y privadas en el contexto de alianzas para mejorar la seguridad. La generación, uso e intercambio de información son aspectos críticos para el éxito de estas alianzas, pero también pueden ser fuentes de desafíos y tensiones. Este capítulo analiza los desafíos relacionados con el intercambio de datos e información, la colaboración entre entidades y la difusión de información sensible.

El capítulo comienza abordando los desafíos y la resistencia al intercambio de información entre agencias de seguridad y entidades públicas y privadas. La importancia de establecer directrices y protocolos claros se enfatiza para garantizar la retención segura y el intercambio adecuado de datos sensibles.

El intercambio de datos e información se analiza en detalle, destacando la necesidad de identificar los beneficios esperados y los costos asociados al compartir información. Se sugiere que la colaboración e intercambio de información no significa necesariamente entregar toda la información, sino identificar datos específicos y concretos, así como análisis y evaluación.

Se exploran soluciones para superar la resistencia natural al intercambio de información, como los Centros de Fusión en EUA, que permiten compartir datos entre actores públicos y privados de manera estructurada y colaborativa. También se mencionan ejemplos de iniciativas similares en Europa.

Finalmente, se aborda la difusión de información sensible, destacando la importancia de adoptar protocolos que regulen este desafío. Se propone una clasificación de niveles de difusión basada en los riesgos asociados, que incluye Rojo, Ámbar, Verde y Blanco, cada uno con diferentes niveles de restricción.

En este capítulo se destaca la importancia del intercambio de información y la colaboración entre entidades públicas y privadas en alianzas de seguridad. Se examinan los desafíos y se proponen soluciones para abordar la resistencia al intercambio de datos, con el objetivo de mejorar la efectividad y el éxito de estas alianzas.

Uno de los aspectos críticos para el éxito de una alianza público-privada en materia de seguridad es la generación, uso e intercambio de información. En efecto, uno de los principales activos de las agencias de seguridad y entidades públicas vinculadas a la misma, suele ser el acceso, gestión, análisis y publicidad de información.

Tan es así que muchas veces los roces o problemas de colaboración entre varias agencias que forman parte todas de un mismo gobierno o entidad estatal, suelen ser consecuencia de la reticencia a compartir sus propios datos entre ellos mismos, aun cuando todos son parte del Estado.

En el sector privado, la situación no es muy distinta. Aun cuando existen iniciativas y actividades de intercambio de información entre los distintos actores, cuando el dato es sensible, la reticencia aflora como un mecanismo de defensa en un mercado altamente competitivo.

De una manera más común de lo que se podría pensar, el valor atribuido a la información que determinada entidad posee es tan alto que, en ocasiones, prefiere seguir trabajando de manera aislada, que obtener beneficios complementarios derivados del trabajo colaborativo. Con tal de no compartir los datos considerados claves al interior del organismo respectivo, muchas entidades, tanto público como privadas, estarán dispuesta a sacrificar externalidades positivas asociadas a su uso conjunto.

Es recomendable contar con directrices claras en cuanto a qué tipo de información pueden compartir los poderes públicos con el sector privado, de acuerdo con los reglamentos de protección de datos. Del mismo modo, deberían establecerse normas mínimas para la retención segura de dicha información, asegurándose de que todos los interesados sepan manejar correctamente los antecedentes.

Los protocolos para compartir información entre entidades privadas y públicas pueden ayudar a establecer los principios para la disposición del intercambio de datos dentro de la asociación, definiendo claramente qué tipo de información será sometida a un trabajo conjunto, por quién, con quién, con qué finalidad y con qué salvaguardias. Una comprensión compartida de los límites de dicho protocolo es fundamental.

Intercambio de datos e información

Aunque esto no se da en todos los niveles, ni con todas las agencias, el intercambio de información es un factor clave en las alianzas público-privadas que requiere ser gestionado eficientemente.

Las entidades privadas suelen identificar con mayor facilidad aspectos de interés común con otros socios estratégicos del mismo sector, y les resulta más fácil hacer concesiones compartiendo información clave, entendiendo que ello les podría dar beneficios cuantificables en el marco de un proyecto determinado. En ocasiones, esta mayor flexibilidad se genera en un entorno menos restrictivo que el que regula al sector público, en términos de intercambio de información, pero también como consecuencia de una visión más pragmática orientada a resultados, elemento más propio del mundo privado.

El desafío principal para los miembros de una alianza consistirá en lograr altas cuotas de disposición, colaboración y voluntad en proyectos de seguridad en los cuales el beneficio esperado no se logrará en el corto plazo y en el que los retornos financieros, aunque existentes, serán más difusos y difíciles de medir.

Si los retos mencionados se presentan con relación al intercambio de datos y antecedentes en proyectos de seguridad, cuando estos son desarrollados tan solo por uno de los sectores, sea este público o privado, el desafío y escenario se tornan aún más complejos cuando la necesidad de traspasar y trabajar información conjunta debe ser realizada entre ambos grupos.

1. El *primer paso* es **comprender esta natural resistencia** a difundir con terceros un activo que los diversos actores de una alianza pudieran considerar esencial, tanto por el costo que implicó generarlo como por el valor agregado que le dan a su propia entidad.

2. El *segundo paso* consiste en **identificar los beneficios** esperados o buscados por cada entidad participante, y mostrar de qué manera las concesiones que se realicen en materia de información, generarán costos menores que serán compensados con los beneficios que se espera genere el proyecto. Esto es esencial, pues la imposición normativa para el intercambio de información no siempre resulta exitosa y, por lo demás, escapa de un concepto asociativo para quedarse más bien en uno impositivo.

   Tan es así que, en ocasiones, cuando la entrega de datos e información es el resultado de una obligación o imposición, termina en eso: suministro plano de datos, perdiéndose la inteligencia y análisis que el mismo emisor de la información pudiera suministrar con relación a ésta.

Es por ello que, al momento de hablar de intercambio de información, se debe considerar no solo antecedentes neutros en términos de cantidad o tipo de datos sino también evaluaciones, análisis e inteligencia, elementos que agregan precisamente calidad y valor agregado a la información y, en última instancia, al proyecto.

3 En *tercer lugar,* una vez identificados los costos, limitaciones y resistencia individuales, por un lado, así como los beneficios y expectativas para cada uno de los integrantes, por otro, es necesario **mostrar a** cada uno de ellos que, en términos de costo – beneficio, habrá una **utilidad mayor** en un escenario colaborativo que en uno individual.

Colaborar e intercambiar información no significa necesariamente entregar todo. Implica identificar tanto datos específicos y concretos necesarios para el proyecto concreto como el análisis y evaluación de este.

La colaboración conlleva regular el tratamiento que se le dará a esa información, la manera en cómo será procesada y los mecanismos para su difusión.

Cada uno de esos aspectos deben, finalmente, ser incorporados en un protocolo o convenio específico que se integre al marco general de colaboración.

Podría ocurrir, por ejemplo, que el éxito de una línea de trabajo en un proyecto público-privado determine que ciertos actores privados que son competidores naturales en el mercado deban suministrar información cruzada. Esta colaboración podría, en determinados casos y según el tipo de proyecto, actores y datos que se trate, condicionarse a que los datos compartidos sean utilizados para el análisis integral de información, pero que el almacenamiento de toda ella lo realice un tercer integrante del proyecto, con el compromiso de mostrar solamente los resultados del análisis, pero no compartir entre todos las bases de datos proporcionadas.

Supongamos que se requiera a las autopistas enviar los datos de todas las placas patentes que circulan por éstas a fin de que esos datos sean cruzados con los registros de vehículos robados permitiendo con ello gatillar una serie de acciones de prevención y control.

Es probable que, si el proyecto considerara la creación de una gran base de datos de todas las circulaciones por todas las autopistas, eso pudiera generar cierta resistencia entre autopistas que desde el punto de vista del mercado de circulación sean competidores.

La salida pasa por identificar este natural y hasta, a veces, sano recelo, y buscar la manera de gestionar la información en su conjunto pero salvaguardando la compartimentalización, lo que se lograría —en este caso concreto— mediante tres pasos:

A la identificación del desafío, necesidades, expectativas, temores, resistencias y beneficios;

B la celebración de un protocolo o acuerdo que compatibilice todos los factores en juego, entregando bases individuales a un solo actor físico o, a un sistema informático, que procesará la información accediendo a repositorios individuales sin crear una base de datos, y sin compartir el dato fuente con los demás actores sino solo los resultados del análisis; y

C la implementación de un sistemas de control y monitoreo que aseguren de manera permanente que el punto anterior se respete, como requisito esencial para que las confianzas que se están generando no se rompan.

En seguridad, la información es —como indicamos— un activo esencial. Mientras más información se disponga, mejores serán los análisis y más exitosas las líneas de trabajo que provengan de éstos. Esperar que las entidades dejen de un día para otro su natural recelo a compartir sus datos es difícil y a veces, en algunos casos, hasta podría ser utópico. Afortunadamente, en la actualidad los sistemas informáticos permiten hacer análisis masivo, minería de datos y cruces de información sin la necesidad de crear una base de datos integrada, sino que consultando una a una las fuentes de información individuales.

De esta manera, un proyecto de seguridad que integra actores privados y públicos podría sobrepasar con éxito esta barrera natural vinculadas a las confianzas mutuas y su impacto en el intercambio y uso de información propia en beneficio colectivo.

Los Centros de Fusión se han transformado en una alternativa interesante para poder compartir datos tanto entre actores públicos, como también entre estos y los privados. Se trata de metodologías de trabajo enfocadas en recolectar, procesar, analizar y difundir una gran cantidad de datos con el fin de prevenir y/o detectar tempranamente actividades terroristas o de criminalidad organizada. Un centro de fusión representa los mecanismos y métodos estructurados y organizados de intercambio de datos interinstitucionales, que operan bajo una lógica colaborativa.

Estos son instancias en las cuales representantes de las principales agencias de investigación y prevención de terrorismo y criminalidad organizada colaboran mediante protocolos previamente definidos en el intercambio de información con el objeto de lograr una imagen más clara y completa de una determinada amenaza. Aun cuando los principales centros de fusión son integrados por agencias del Estado, varias iniciativas han comenzado a incorporar al sector privado, para lo cual resulta clave que éstos perciban beneficios de esta participación, a través de retroalimentación, pues de lo contrario sentirán que solo entregan y no reciben nada a cambio.

Más allá del modelo que se siga para implementar un centro de fusión, la ventaja comparativa que generan es disponibilizar de manera veloz la información existente entre muchas agencias y entidades sin necesidad que la autoridad solicitante acceda directamente a la base de datos de la requerida. Con ello, se resuelve uno de los principales desafíos en materia de seguridad: la resistencia natural de permitir accesos ilimitados a bases de datos propias.

Esta manera de trabajar comenzó a desarrollarse con más fuerza en los Estados Unidos después de los atentados del 11 de septiembre. Los Estados Unidos se dio cuenta que el sistema de inteligencia y de investigación poseían mucha más información de la que se pensaba, la que no fue aprovechada de la mejor manera por estar desagregada y diseminada entre una multiplicidad de entidades.

Consientes que la unificación de bases de datos es una tarea con pocas probabilidades de éxito, se buscó crear métodos que facilitaran el intercambio de información o el procesamiento conjunto de ella.

Según informa el Departamento de Seguridad Interior de este país, hay en la actualidad 78 centros de fusión en los Estados Unidos.[22] Es tanta la cantidad que hasta cuenta con una Red Nacional de Centros de Fusión. Aunque su proliferación tuvo a las amenazas terroristas como uno de los principales objetivos, hoy en día su uso está extendido a toda la criminalidad, incluyendo casos exitosos de combate a la trata de personas.[23,24]

Iniciativas similares hay en Europa, aunque con un enfoque mayoritario en amenazas terroristas,[25] destacando experiencias en Bélgica, Alemania, Italia, los Países Bajos, España y el Reino Unido.

Difusión de información sensible

Una cosa es el uso que se le otorgue a datos considerados sensibles o estratégicos en términos de procesamiento conjunto y otra distinta es la manera de difundirla. Con relación a este segundo aspecto, es necesario adoptar protocolos que regulen previamente este desafío de manera clara y precisa, con el fin de que los interesados puedan ponderar los costos y beneficios, por un lado, y —en caso de avanzar— contar con pautas predefinidas que pudieran ser controladas.

La difusión se puede generar en el marco de iniciativas aisladas o como parte de un proyecto más integral. El primer caso sería, por ejemplo, la difusión que realizan los sistemas de alerta para la prevención del terrorismo de diversos países tanto a organismos públicos como privados sobre el estado y el nivel de alerta en materia de prevención del terrorismo. Algo similar ocurre en seguridad turística, cuando un numero relevante de gobiernos deciden informar a sus ciudadanos los niveles de amenaza a los que se podrían exponer si es que acuden a un determinado destino.

[22] https://www.dhs.gov/fusion-center-locations-and-contact-information
[23] https://www.dhs.gov/2015-fusion-center-success-stories
[24] https://wvva.com/2020/01/31/w-va-fusion-center-helps-combat-human-trafficking/
[25] https://icct.nl/app/uploads/2019/02/ICCT-VanderVeer-Bos-VanderHeide-Fusion-Centres-in-Six-European-Countries.pdf

En sentido contrario, empresas del sector privado pudieran reportar a determinados organismos públicos indicadores de riesgo o variables sensibles cuya producción y almacenamiento se concentre en los primeros, pero que puestos en su conjunto permiten a la entidad pública darle un valor agregado y una visión con más perspectiva acerca del problema que se plantee abordar.

La difusión de datos tanto en un formato unidireccional como cruzada adquiere valor agregado si es que esa información compartida es analizada y procesada por una parte o todos los miembros de una asociación público-privada, sea que su resultado se difundido solo de manera interna (entre los integrantes) o también externa (medios, prensa, otros organismos, etc.).

De ahí que esa difusión —interna o externa— deba contar con regulaciones específicas. Los protocolos que aborden este aspecto deberían considerar niveles de difusión en torno a los riesgos asociados. Veamos una propuesta.

* **Rojo:** Información no-revelada y restringida a representantes presentes en la reunión o proyecto solamente.

Intercambio: Esta información solamente se intercambia con ciertas personas previamente seleccionadas o identificadas por el emisor de la información. Si el flujo de datos se realiza por escrito o electrónicamente, será necesario tomar medidas específicas en cuanto a cómo asegurar la información, incluyendo posiblemente una garantía de que la persona y entidad a la que va dirigida sea el único receptor y se encuentre debidamente identificado.

Riesgos por mitigar: Este tipo de información, catalogada como roja, es aquella que si llegara a personas no autorizadas:

* *podría poner vidas en peligro.*
* *podría perjudicar seriamente a una empresa, institución u organismo gubernamental de varias maneras.*
* *podría dañar seriamente las relaciones con otras empresas, gobiernos, organizaciones o socios.*
  identificado.

* **Ámbar:** Revelación limitada y restringida a miembros del grupo de intercambio de información y a aquellos que en sus organizaciones tienen una "necesidad de saber" para tomar medidas.

Intercambio: La información solamente se intercambia con un grupo selecto de individuos, de un número acotado de entidades. Se permite que compartan esta información dentro de su propia organización, de acuerdo con una "necesidad de saber".

Riesgos por mitigar: Esta es la información que si se pasara a personas no autorizadas:

* *podría aún perjudicar a una empresa, institución u organismo gubernamental, pero con menores consecuencias que la información "roja".*
* *puede afectar las relaciones con otras empresas, gobiernos, organizaciones o socios.*

* **Verde:** Esta información puede compartirse con un grupo más amplio de individuos o entidades, tanto dentro como fuera de la asociación público-privada, aunque su publicación pudiera no ser recomendable en papel o en las redes sociales.

Intercambio: La información solamente se intercambia con un grupo determinado de personas o entidades. Los datos pueden, sin embargo, compartirse con otras organizaciones, plataformas de información o con personas empleadas en puestos relacionados con la seguridad. La información no debería intercambiarse públicamente o ponerse en sitios web públicos.

Riesgos por mitigar: Esta es la información que si se pasara a personas no autorizadas podría:

* *tener como resultado desventajas menos significativas para la empresa, institución u organismo gubernamental.*

* *dañar las relaciones con otras empresas, instituciones u organismos gubernamentales.*

* *llevar a la publicación de la información por parte de los medios de comunicación.*

* **Blanco:** Circulación sin restricción.

Intercambio: Información pública que puede difundirse sin restricciones.

Riesgos por mitigar: Mínimos o nulos. La información no es sensible y puede hacerse pública. La información puede, si es apropiado o deseable, difundirse a través de fuentes abiertas tales como redes sociales.

Lo más importante

Este capítulo aborda el intercambio de información entre entidades públicas y privadas en alianzas para mejorar la seguridad.

Los principales puntos por rescatar son:

1. Desafíos y resistencia al intercambio de información: Establecer directrices y protocolos claros para garantizar la retención segura y el intercambio adecuado de datos sensibles.

2. Beneficios y costos del intercambio de datos: Identificar datos específicos y concretos para compartir, así como análisis y evaluación, sin entregar toda la información.

3. Soluciones para superar la resistencia al intercambio de información: Implementar Centros de Fusión y otras iniciativas que permitan compartir datos de manera estructurada y colaborativa entre actores públicos y privados.

4. Difusión de información sensible: Adoptar protocolos y clasificaciones de niveles de difusión basados en los riesgos asociados para regular el manejo de datos sensibles.

El capítulo destaca la importancia del intercambio de información y la colaboración en alianzas de seguridad, examina los desafíos y propone soluciones para mejorar la efectividad y el éxito de estas alianzas.

Construyendo confianza

En este capítulo exploramos las dificultades y desafíos que enfrentan las alianzas público-privadas en el ámbito de la seguridad y la prevención de la violencia o el terrorismo. La importancia de la confianza y la cooperación entre los sectores público y privado es fundamental para abordar eficazmente estos problemas complejos y multifacéticos.

En primer lugar, se discute la necesidad de ofrecer alternativas que no impliquen la transferencia de recursos financieros, así como de generar opciones menos burocráticas para facilitar la colaboración. Además, se enfatiza la importancia de acordar objetivos comunes, lo cual puede servir como base para la cooperación y el trabajo conjunto.

Una declaración de compromiso puede ser útil para formalizar la colaboración, estableciendo responsabilidades, actividades y metas a alcanzar por ambas partes. Se sugiere también considerar la intervención de actores más neutrales, como organizaciones de la sociedad civil, para facilitar la construcción de alianzas con el sector privado.

La comunicación es un aspecto clave en la construcción de confianza. Por un lado, es importante difundir tanto los éxitos como los fracasos de manera conjunta, evitando atribuir la responsabilidad a un solo actor. Por otro lado, se debe tener cuidado al compartir el "know how" o conocimiento específico adquirido durante el proyecto, ya que podría beneficiar a actores indeseados. Para abordar estos temas, se recomienda regular los aspectos comunicacionales mediante protocolos y políticas de comunicación acordadas conjuntamente.

Finalmente, se aborda la necesidad de establecer una normativa especial que facilite las alianzas público-privadas en materia de seguridad, proporcionando un marco legal y administrativo adecuado. Esto puede incluir acuerdos y convenios entre Estados, especialmente cuando se enfrentan amenazas internacionales como el terrorismo o el crimen organizado transnacional.

Este capítulo destaca la importancia de construir confianzas y desarrollar estrategias efectivas para superar los desafíos que enfrentan las alianzas público-privadas en el ámbito de la seguridad. La colaboración exitosa entre ambos sectores es crucial para enfrentar y prevenir situaciones de violencia y terrorismo que afecten la seguridad de la población.

El recelo institucional o corporativo es tal vez uno de los principales desafíos al momento de construir una alianza público-privada exitosa. El cómo y qué tipo de información intercambiar y difundir, es uno de los más críticos. De ahí que se le haya dedicado una sección especial. Pero hay más. En este capítulo se abordarán algunos de ellos.

Ofrecer alternativas que no impliquen transferencia de recursos

Debe ser superada la percepción de que la gran fuerza del sector privado está en la posibilidad de financiar programas. Esa es una posibilidad, pero existen otras maneras interesantes y creativas de concertar alianzas. Por eso es importante crear alternativas que no impliquen la transferencia de recursos financieros para viabilizar la ejecución de proyectos conjuntos.

Generar alternativas menos burocráticas

Las empresas suelen dejar de establecer alianzas con el sector público debido al alto grado de burocracia y al exceso de procedimientos. Aun cuando en ocasiones esos procedimientos existen para garantizar el interés público, es recomendable pensar en cómo reducir los niveles de burocracia y hacerlos más sencillos con el objetivo de incentivar el interés de las empresas y para facilitar las asociaciones.

Acordar objetivos comunes

Una forma de establecer la alianza es que el sector público y el sector privado acuerden objetivos comunes. De esta manera, si un objetivo común consiste en reducir la participación de los adolescentes y los jóvenes en situaciones de violencia y promover su pleno desarrollo, es posible establecer una alianza que integre un proyecto ya desarrollado por una determinada empresa que acoja a jóvenes que sean expresidiarios para trabajar en su plantilla, con un programa desarrollado por el sector público que ofrezca apoyo social, jurídico y psicológico a los jóvenes en conflicto con la ley y sus familias.

Se trata de dos programas ya realizados, cuyo objetivo común es el desarrollo integral de los jóvenes, a fin de reducir las posibilidades de que entren en conflicto con la ley. La empresa no necesita invertir mayores recursos adicionales de lo que ya invierte ni el sector público tampoco.

Resuelta la primera parte, esto es, identificar programas propios con objetivos comunes, entonces debe trabajarse en la segunda, que consiste en la integración de las estrategias de trabajo junto a su monitoreo para garantizar que cumpla el objetivo común acordado.

Firmar una declaración de compromiso

Una declaración de compromiso puede servir para formalizar el modelo de trabajo propuesto en el punto anterior, o para prever un nuevo proyecto, asignando nuevas responsabilidades a ambas partes. Es importante que la declaración establezca responsabilidades generales, actividades y metas que las partes deban alcanzar.

Luego, la regulación específica de derechos y obligaciones, de procedimientos administrativos y operativos será establecida a través de protocolos de trabajo concretos.

Considerar la intervención de actores más neutrales

Llevar a cabo la alianza a través de una organización de la sociedad civil es una alternativa interesante para que el sector privado participe en iniciativas de prevención de la violencia o terrorismo. El sector público puede buscar organizaciones locales de la sociedad civil y delinear propuestas conjuntas, con el involucramiento del sector privado. En general, las ONG ya tienen socios en el sector privado y desarrollar un trabajo conjunto con ellas puede tornar más sencilla la construcción de alianzas con este sector.

Difusión de éxitos y fracasos

Muchas confianzas entre socios públicos y privados fracasan cuando el éxito de los proyectos es publicitado por alguno de los actores en desmedro de otros. Es natural querer mostrar buenos resultados y recibir por ello reconocimiento de la comunidad o algún sector determinado. Olvidar por error o desplazar motivadamente a algunos de los actores del proyecto, es extremadamente dañino.

De igual forma, un fracaso, problema o dificultad experimentados en un proyecto o programa de acción público-privada para confrontar las amenazas a la seguridad no debiera serle endosado a tan solo uno de los actores.

Si el proyecto es el resultado de un trabajo conjunto, de una iniciativa colaborativa y de una alianza multientidad, tanto los éxitos como los fracasos deben ser celebrados, por un lado, y asumidos, por otro, por todos los actores que participan en el proyecto, sin excepciones.

Cuidar el *know how*

Difundir resultados al interior del grupo que conforma la alianza o proyecto público-privado es fundamental. Hacerlo hacia la comunidad y los medios es muy relevante. Si bien no es exactamente la misma información la que se comunica en uno y otro caso, se trata de actividades que deben ser desarrolladas.

El éxito de la estrategia será el resultado de una receta bien elaborada. A modo de ejemplo, podemos mostrar el pastel cocinado, e incluso explicar a grandes rasgos sus componentes. Lo que no resulta recomendable es compartir con terceros el ingrediente secreto.

Muchos integrantes de proyectos de seguridad estarán deseosos de mostrar resultados. No obstante, contar los detalles distintivos que marcaron la diferencia de un proyecto exitoso y compartir el *know how*, puede generar más costos de lo esperado.

Compartir la receta genera, desde luego, un beneficio inmediato, pues la comunidad y los medios se maravillarán con este nuevo ingrediente o fórmula. Mientras ese efecto se verá a corto plazo, lo que ocurrirá a largo plazo es que las entidades y personas que representan el foco de la amenaza sean estos grupos terroristas u organizaciones criminales, accederán a la misma información, y comprenderán de igual manera las metodologías innovadoras o distintivas utilizadas, de las cuales probablemente tomen nota, aprendan, generen contramedidas y modifiquen su actuar. Si el plan de trabajo de nuestro proyecto fue elaborado con base en un diagnóstico y la identificación de parámetros, modus operandi y patrones de comportamiento específicos, cualquier cambio que se produzca en alguna de estas variables no solo restará impacto positivo al trabajo, sino que tomará tiempo detectarlo y adecuar la intervención público-privada.

De esta manera, difundir y comunicar es necesario. Mostrar resultados aún más. Explicar los beneficios del trabajo conjunto es indispensable. Pero poner a disposición de todos el *know how* en su expresión más detallada, no resulta recomendable. Esa satisfacción debe reservarse para las reuniones de análisis interno.

Regular los aspectos comunicacionales

Para asegurar mayores cuotas de éxito, disminuir el riesgo de conflictos internos y generar más confianza entre todos los integrantes de una alianza, resultará esencial contar con un protocolo sobre difusión y relación con la comunidad, así como con los medios.

Se recomienda diseñar y acodar conjuntamente una política de comunicaciones y redactar los protocolos que la lleven al campo operativo, con aspectos como vocería, enfoque comunicacional, periodicidad de los contactos con medios y comunidad, gestión de crisis, entre otros.

Normativa especial

Junto con trabajar en la reducción de las barreras naturales que pudiera implicar un eventual y considerable grado de burocracia, en ocasiones el marco normativo, sea este legal, administrativo o, incluso, constitucional, pudiera representar un importante desafío que afecte las motivaciones —sobre todo— del sector privado. Es recomendable no solo generar un marco normativo específico que potencie actividades anticorrupción o transparencia, sino generar condiciones concretas que fomenten el interés del sector privado por entrar en alianza con el Estado.

Cuando se trata de licitaciones públicas para la construcción de grandes obras públicas como autopistas, represas o aeropuertos, muchos estados al firmar los respectivos contratos con el sector privado lo hacen en el marco de una completa normativa específica que regula este tipo de actividades conjuntas. En materia de seguridad, esta aproximación no es tan común. Mientras más grande el proyecto, y más alta la inversión o involucramiento del sector privado, más necesario será contar con marcos legales que aseguren estabilidad, proyección de resultados a largo plazo y confianza.

Si la amenaza es de corte internacional, como ocurre con el terrorismo o algunos fenómenos de crimen organizado de corte transnacional, extender la regulación normativa a acuerdos o convenios entre Estados resultará conveniente.

Lo más importante

En este capítulo se abordan los desafíos y dificultades en las alianzas público-privadas en el ámbito de la seguridad y la prevención de violencia o terrorismo. Los aspectos clave a resaltar son:

1. Ofrecer alternativas no financieras y menos burocráticas para facilitar la colaboración.

2. Establecer objetivos comunes como base para la cooperación y el trabajo conjunto.

3. Utilizar declaraciones de compromiso y la intervención de actores neutrales para formalizar y fortalecer las alianzas.

4. Fomentar la comunicación y confianza mediante la difusión conjunta de éxitos y fracasos, y el establecimiento de protocolos y políticas de comunicación acordadas.

5. Crear una normativa especial que facilite las alianzas en materia de seguridad, incluyendo acuerdos y convenios entre Estados.

Este capítulo resalta la importancia de construir confianza y desarrollar estrategias efectivas para superar los desafíos en alianzas público-privadas de seguridad, siendo la colaboración exitosa entre ambos sectores fundamental para enfrentar y prevenir situaciones de violencia y terrorismo.

Aspectos relevantes en el diseño de proyectos conjuntos

En este capítulo, se abordan aspectos relevantes en el diseño de proyectos conjuntos para la seguridad, centrándose en dos ejes fundamentales: el factor económico y las políticas de género. El objetivo es proporcionar una visión completa de cómo estos elementos pueden ser incorporados en la creación y ejecución de alianzas público-privadas eficientes y efectivas.

En primer lugar, el capítulo examina la oferta y la demanda desde una perspectiva económica, argumentando que un enfoque completo en la lucha contra amenazas como el crimen organizado, el terrorismo y la corrupción debe abordar tanto la oferta de bienes y servicios ilícitos como la demanda y sus condicionantes. Se destaca la importancia de desestabilizar las estructuras económicas que sustentan dichas amenazas, afectando sus activos y minando su capacidad financiera.

En segundo lugar, el capítulo aborda la incorporación de políticas de género en el diseño y desarrollo de proyectos conjuntos. Se resalta la importancia de integrar la perspectiva de género desde el inicio de un proyecto, tanto en términos de la organización interna como del público objetivo. Se incluyen recomendaciones prácticas para promover la igualdad de género y la inclusión en la estructura organizativa, los procesos de reclutamiento y gestión de personal, las capacitaciones, los protocolos internos, el enfoque interseccional, la imagenología y el lenguaje.

El capítulo proporciona un marco sólido para la creación y ejecución de proyectos conjuntos eficientes y efectivos en seguridad, destacando la importancia de considerar tanto el factor económico como las políticas de género en su diseño y desarrollo. Al abordar estos aspectos de manera integral, las alianzas público-privadas pueden fortalecer su enfoque y mejorar sus resultados a mediano y largo plazo en la lucha contra las amenazas actuales.

La oferta y la demanda. El factor económico

Los proyectos de seguridad, tanto autónomos de cada uno de los sectores público o privado, como también aquellos que son resultando de una alianza conjunta, suelen abordar la amenaza desde la óptica de quién o qué la genera. Si lo analizamos desde el punto de vista económico, y entendiendo que, en general, hay detrás una motivación financiera, la amenaza se suele abordar desde la oferta.

El foco se suele centrar en el traficante de drogas, en el sicario, en el lavador de activos, en el tratante de personas, en el terrorista, en el traficante de armas o en el contrabandista. En algunas ocasiones se orientan también, de manera complementaria, al objeto u sujeto del delito, esto es las drogas, el vehículo robado, las armas ilegales, las víctimas de trata.

No siempre la aproximación se extiende al conjunto de factores, actores y elementos que configuran y condicionan la demanda. El consumidor de drogas; el "cliente" que acude a las víctimas de trata; el comprador de productos piratas o de contrabando; el adquiriente de armas; el que financia las actividades terroristas.

Si entendemos al grupo criminal, al crimen organizado, al terrorismo a nuestras amenazas como una entidad entre cuyos fines se encuentran los de corte económico, como si se tratase de una empresa, entonces un plan de acción público-privado eficiente debe abordar tanto factores vinculados a la oferta y al objeto de bienes, productos o servicios ilícitos que transa, como también la demanda de estos y aquellos que la condicionan.

Mientras más amenazas se concreten, mayores serán los ingresos económicos de los grupos criminales. Mientras más ataques terroristas se cometen, más financiamiento habrá detrás. A medida que el dinero se incrementa, las entidades y grupos detrás de las amenazas adquirirán cada vez mayor fuerza, lo que a su vez les permitirá materializar nuevas y mayores amenazas, con cuotas de impunidad cada vez más significativas.

Es por ello por lo que una alianza público-privada orientada a la seguridad debiese considerar una análisis y confrontación a las bases financieras y económicas de los grupos o entidades responsables de estas amenazas, sin importar su tamaño.

La forma más eficiente de combatirlas sea que se trate del crimen organizado, el terrorismo, la corrupción, el lavado de activos o la canalización de la demanda social mediante violencia organizada, se obtiene a través de la desestabilización de las estructuras económicas que las soportan.

La afectación de activos es esencial y todo proyecto que se diseñe con ese componente mostrará efectos positivos a mediano y largo plazo.

Las políticas de género

El enfoque de género no solo debe incorporarse desde la óptica de la organización y gestión del proyecto con relación a sus integrantes, sino también al público objetivo al que está dirigido y en cuyo beneficio la actividad es desplegada.

* **Contexto e importancia**

La Guía y Manual para Planificación de Seguridad para Eventos Masivos, de UNICRI y CICTE/OEA, 2011[26] recomienda integrar la perspectiva de género desde el mero inicio de un proyecto público-privado, en su etapa de diseño, lo que debería complementarse durante el desarrollo del proyecto, así como también con ocasión de la evaluación y la reportería.

> *"La igualdad de género, la inclusión y la diversidad se logran mediante estrategias y prácticas de recursos humanos cuidadosamente diseñadas y con recursos basados en los principios de igualdad y no discriminación a los que los Estados se han comprometido en los tratados internacionales de derechos humanos. Empezando por el liderazgo de alto nivel, la gestión de la institución de una manera que refleje los principios de igualdad y no discriminación, incluida la promoción de la diversidad, y asegurando que se tomen en serio marca la pauta e indique lo que es y lo que no es permisible. El liderazgo en igualdad de género no sólo se mueve a la baja en la jerarquía, sino que idealmente incluye la apertura entre la alta dirección a los insumos, sugerencias e inquietudes de más personal junior. Los mecanismos de rendición de cuentas, disciplina, quejas y supervisión relativos al sector de la seguridad y la justicia también desempeñan un papel fundamental en el apoyo a la inclusividad, la no discriminación y la igualdad de género".*[27]

Tal como señala el Manual de Transformación Institucional de la Unión Europea[28] que entrega herramientas para la incorporación de la perspectiva de género, corresponde a toda la jerarquía organizativa de una entidad y un proyecto, incorporar en el tejido cultural de las entidades participantes la igualdad de género y los derechos humanos. La igualdad de género debe representar un principio rector en todas las áreas de la alianza público-privada y en cada uno de sus integrantes, incluyendo aspectos que interactúen con la raza, etnia, clase, religión, rango y otros factores. Estos principios deben comunicarse claramente con todos los miembros del personal y, cuando sea posible, incorporarse a las declaraciones oficiales de misión y visión, aplicarse a nivel de estructura organizativa, así como en los documentos institucionales. Supone además trabajar en la eliminación de lenguaje sexista, excluyente y discriminatorio.

[26] **Ver la Guía y Manual para Planificación de Seguridad para Eventos Masivos, de UNICRI y CICTE OEA. Documento actualizado el 2021 por los consultores Brian London, Superintendente (R) y Brendan Heffernan Superintendente Jefe (R), ambos de la Real Policía Montada de Canadá.**
[27] **DCAF, OSCE/OIDDH, ONU Mujeres (2019) Gobernanza del Sector de Seguridad, Reforma del Sector de Seguridad y Género".**
[28] **https://eige.europa.eu/gender-mainstreaming/toolkits/gender-institutional-transformation**

No se trata solo de cumplir con exigencias legales, sino de avanzar en la promoción efectiva de la perspectiva de género integrándola en todos los procesos y prácticas de una alianza público-privada.

Los procesos de reclutamiento y gestión de personal, equilibrados por género garantizarán y fortalecerán la participación de las mujeres en los roles de liderazgo y toma de decisiones. La igualdad de género en una alianza público-privada supone reconocer e involucrar a toda la comunidad lésbica, gay, bisexual, transgénero, intersexual, entre otras, tanto en los procesos de personal, como en el desarrollo de los planes de trabajo.

* **Elementos que considerar**

En la definición más concreta acerca de cómo incorporar las políticas de género, recomendamos tomar en cuenta los siguientes elementos:

Políticas externas. Deben incorporarse políticas con relación la comunidad destinataria, beneficiaria o afectada, y tipo de amenaza que se busca contrastar.

Políticas internas. De igual manera, deben considerarse estas políticas en función de la forma en la que se organiza internamente el proyecto y su equipo de trabajo y con un efecto en ellos.

Capacitaciones. Las capacitaciones en temas de género, tanto al personal y equipo coordinador del proyecto como ejecutor de este, deben realizarse al inicio y de manera continua.

Protocolos. Para efectos del trabajo interno, del personal coordinador como operativo, es importante contar con protocolos de prevención, detección y respuesta ante situaciones de posible acoso, hostigamiento, discriminación y prácticas atentatorias contra la equidad de género.

Interseccionalidad. Una serie de factores como educación, nivel de ingreso, religión, raza, discapacidad, entre otros, impactan de manera distinta a las personas, lo que debe ser tomado en cuenta. Los elementos que afectan la equidad no se comportan de igual manera, de forma tal que una situación determinada pude impactar de manera distinta a dos personas.[29]

[29] Así, y a modo de ejemplo, una mujer blanca, con formación universitaria, que vive en un país desarrollado, aunque pudiera experimentar cuotas de inequidad, el nivel de impacto no será igual al de una mujer indígena, de escasos recursos y con bajo nivel tanto educativo como económico. Esta constatación y el concepto de interseccionalidad debe motivar a identificar diferencias y desarrollar estrategias específicas para cada uno de los grupos.

Imagenología. Una de la formas más rápidas y eficientes para generar impacto y para promover mensajes asociados a la importancia de las políticas de género y equidad se logra a través de imágenes, cuyo uso recomendamos directamente.

Lenguaje. Tanto interna como externamente, el proyecto debe ocupar un lenguaje incluyente, que genere cultura y normalice la equidad y perspectiva de género entre los destinatarios de la iniciativa público-privada, pero también de los equipos de trabajo.

Lo más importante

Este capítulo se centra en dos aspectos clave para el diseño de proyectos conjuntos en seguridad dentro de las alianzas público-privadas: el factor económico y las políticas de género. Los principales puntos para destacar son:

1. Abordar tanto la oferta como la demanda en la lucha contra amenazas, desestabilizando las estructuras económicas que las sustentan y afectando sus activos y capacidad financiera.

2. Integrar políticas de género desde el inicio de un proyecto, considerando la organización interna y el público objetivo, promoviendo la igualdad de género y la inclusión en todos los aspectos del proyecto.

El capítulo proporciona un marco sólido para crear y ejecutar proyectos conjuntos eficientes y efectivos en seguridad, subrayando la importancia de considerar tanto el factor económico como las políticas de género en su diseño y desarrollo. Al abordar estos aspectos de manera integral, las alianzas público-privadas pueden mejorar sus resultados a mediano y largo plazo en la lucha contra las amenazas actuales.

Ejemplos e ideas

En el presente capítulo, se abordará la importancia de las alianzas público-privadas en el ámbito de la seguridad, analizando diversos casos de éxito en los que la colaboración bidireccional entre ambos sectores ha generado un impacto positivo en la prevención, detección, mitigación y respuesta ante distintas amenazas. Se presentarán ejemplos concretos de alianzas en áreas como la trata de personas, drogas, víctimas de violencia delictual, robo, vehículos robados, reinserción laboral, infraestructura crítica, bioseguridad, desarrollo tecnológico y turismo, entre otros.

Las alianzas público-privadas en materia de seguridad han demostrado ser herramientas valiosas para enfrentar de manera efectiva y eficiente diversos desafíos en este ámbito. A través de la colaboración bidireccional entre ambos sectores, se han logrado generar soluciones innovadoras que agregan valor a los proyectos y aumentan la tasa de retorno positivo.

Algunos ejemplos destacados incluyen la capacitación de personal en medios de transporte para la detección temprana de trata de personas, la cooperación entre compañías eléctricas y autoridades para enfrentar problemas de seguridad en zonas empobrecidas, el apoyo financiero a víctimas de violencia delictual, el marcado de productos robados, la colaboración en la vigilancia de espacios públicos, la recuperación de vehículos robados, la promoción de consejos locales de seguridad, la reinserción laboral de personas con antecedentes penales, el desarrollo de infraestructura crítica, la bioseguridad y el turismo.

En esta sección se presenta una serie de casos en los que las alianzas público-privadas han sido exitosas en abordar distintos desafíos de seguridad. Estos ejemplos sirven como referencia para futuras colaboraciones entre ambos sectores, buscando siempre potenciar la prevención, detección, mitigación y respuesta ante las amenazas que enfrentan nuestras sociedades.

A lo largo de este Manual se han ido mostrando ejemplos de alianzas público-privadas en materia de seguridad. Salvo casos excepcionales, hemos intentado excluir, aquellos proyectos en los que si bien han intervenido ambos sectores, la relación entre éstos presenta una carácter más bien unidireccional, como ocurre cuando las entidades privadas financian proyectos específicos de seguridad —como los botones de pánico comunales o una aplicación móvil de emergencias— o bien en aquellas ocasiones en las que el sector público despliega una oferta a través de fondos concursables de seguridad para que toda la comunidad pueda postular.

Varios son los ejemplos de éxito que merecen ser mencionados y en los cuales la colaboración bi o multidireccional resultó ser un factor innovador que, junto con darle valor agregado a los respectivos proyectos, permitió incrementar la tasa de retorno positivo. Más que un estudio detallado de cada uno de los casos se trata de mostrar la variada extensión que puede experimentar una alianza público-privada para abordar amenazas a la seguridad, sea desde la prevención, o bien detección temprana, mitigación o respuesta.

* **Trata de personas y medios de transporte**

Programa de capacitación y formación a sobrecargos, auxiliares de vuelo y operadores de líneas áreas comerciales para detectar tempranamente indicadores de trata de personas, que son reportados a la autoridad previo al aterrizaje de un vuelo facilitando el control y detección de sospechosos, así como la liberación de víctimas. La reportería no es azarosa y obedece a un plan previamente acordado entre las agencias de prevención e investigación del sector público, por un lado, y las líneas de transporte, por otro.

Entre los indicadores aplicados, puede mencionarse la presencia de adolescentes o mujeres jóvenes que viajan acompañados de adultos que no son sus familiares directos, que se sientan en un avión lo más lejos posible de un pasillo, limitando al máximo el contacto con el personal de la línea aérea, al punto que no los dejan solos en ningún momento para ir al baño y no les dejan hablar con la tripulación, informando a estos sus preferencias de comida. Nada de esto por sí solo indica que estamos en presencia de trata de personas, siendo más bien indicadores que sumándose a otros permiten elevar el nivel de riesgo y ayudan a la tripulación de la línea área a identificar potenciales casos.

Similares iniciativas se pueden desplegar en terminales aeroportuarias a través de organizaciones de la sociedad civil dedicadas a combatir la trata, cuyos equipos de trabajo están integrados por víctimas rescatadas o sobrevivientes y que tienen mejores capacidades para detectar potenciales casos en esos lugares. Mientras el sector público logra confrontar un delito de manera mucho más eficiente, la entidad privada desarrolla su actividad de detección en un teatro y lugar de operaciones más seguro, controlado y con mayor afluencia de casos potenciales.

Un ejemplo interesante de este tipo de alianzas o iniciativa es la Iniciativa Rayo Azul o BLI (*BLI - Blue Lightning*, en inglés), elemento de la Campaña Azul de las Naciones Unidas contra la trata de personas que desarrolló el Departamento de Seguridad Nacional de los Estados Unidos, con la participación del Departamento de Transporte y Aduanas y Protección Fronteriza de ese país.

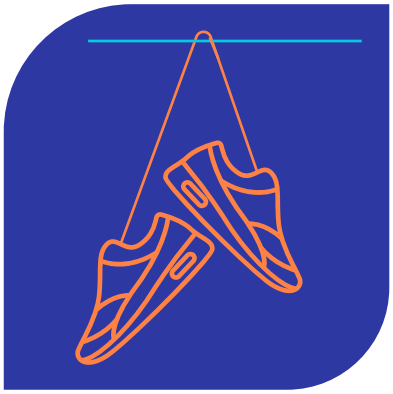
BLI capacita al personal de aviación para identificar posibles traficantes y víctimas de la trata de personas, y para informar sus sospechas a las fuerzas del orden público. Hasta finales del año 2022, más de 200.000 miembros del personal de la industria de la aviación han sido capacitados a través de BLI, y se consejos prácticos continúan dando a las fuerzas del orden.[30,31]

La comunidad internacional ha apoyado constantemente estas iniciativas validando la alianza público-privada como un mecanismo eficiente para abordar las amenazas a la seguridad derivadas de la trata de personas.[32]

* Drogas y Electricidad

Vastos sectores empobrecidos en algunas ciudades tienen colgados zapatos en sus cables de electricidad, símbolos de control territorial, venta de drogas o actividades ilícitas. Mientras que esos zapatos generan ambientes físicos que incrementan la sensación de poder de determinados grupos criminales, fomentan la sensación de inseguridad de la población representando un problema de seguridad para las comunidades que residen en esos sectores.

Lo que pareciera ser un problema exclusivo de la autoridad y de la comunidad, se transforma en un dolor de cabeza para las compañías eléctricas que deben realizar mantenimientos en zonas de alto riesgo. El resultado, muchas veces, suele pasar porque las policías no retiran los zapatos porque no es su trabajo y porque no saben cómo subirse a los postes y cables sin riesgo, mientras que las compañías eléctricas no los hacen por temor a sufrir represalias o ser atacados por los grupos o entidades responsables de estos hechos.



En ese contexto, una alianza entre sector público y privado permite la formación de cuadrillas mixtas o conjuntas entre agentes policiales y funcionarios de las compañías eléctricas. La protección que los primeros brindan a los segundos posibilita su trabajo, el cual a su vez incrementa la sensación de seguridad, mejorando el ambiente para una comunidad determinada y eliminando marcas de cooptación delincuencial.

[30] **Para más información ver** https://www.dhs.gov/news/2023/01/25/dhs-and-dot-host-joint-intersections-human-trafficking-and-international-aviation

[31] **Para conocer otros casos de interés, ver:**
-https://www.nytimes.com/2017/02/07/us/flight-attendants-human-trafficking.html
-https://www.aa.com/i18n/customer-service/about-us/combating-human-trafficking.jsp

[32] **Ver:**https://www.unodc.org/unodc/en/frontpage/2021/April/unodc-engages-public-private-partnerships-in-the-fight-against-human-trafficking.html

* Víctimas e industria financiera

Muchas víctimas de violencia delictual viven en contextos o en zonas en los que existen altos niveles de probabilidad de que vuelvan a sufrir nuevamente los mismos delitos y daños. El círculo de pobreza o las condiciones sociales de determinados lugares les impide salir de los mismos, lo que puede motivar una alianza público-privada de apoyo y asistencia a través del otorgamiento de préstamos o instrumentos financieros que —sin el aval del Estado— difícilmente un banco otorgaría a personas cuya clasificación de riesgo resulte alta. No se trata solo de facilitar la apertura de cuentas corrientes o la obtención de préstamos, lo que de por sí, en determinados casos ya es mucho, sino de acompañar a estas personas y asistirlas en términos de capacitación o coaching de emprendimiento comercial, programas de auto ayuda.

Una alianza público-privada va mucho más allá de licitar servicios y entregar dinero, o firmar como aval estatal de una obligación privada. Un factor de éxito pasa necesariamente por diseñar un programa conjunto, que identifique necesidades y beneficios para todos los actores, defina roles, asigne responsabilidades, acuerde una política de comunicación común, y contenga importantes cuotas de retroalimentación mutua.

Un ejemplo exitoso de una iniciativa que apunta en esta dirección es el Proyecto Recuperación (*Project Recover* en inglés) de Canadá. Se basa en la premisa que el fraude financiero y el robo de identidad son un componente importante en la explotación de un sobreviviente de trata de personas.

Este proyecto es liderado por una corporación bajo la Ley de Corporaciones sin Fines de Lucro de Canadá y representa una iniciativa voluntaria de ejecutivos de la industria de servicios financieros, brinda apoyo a los sobrevivientes y los defiende en su nombre frente a los acreedores. El apoyo a las víctimas y sobrevivientes es gratuito.[33] El rol del Estado no solo avala el proyecto, sino que aporta con capacitación.

Algo similar ocurre en los Estados Unidos con la Iniciativa de Inteligencia contra la Trata de Personas (ATII por sus siglas en inglés), que combate la trata de personas a nivel mundial promoviendo la responsabilidad social corporativa a través del aumento de la conciencia, facilitando la integración de inteligencia y el avance tecnológico, y fomentando la colaboración de datos estratégicos.[34]

[33] **Ver** https://projectrecover.ca/
[34] **Ver** https://followmoneyfightslavery.org/

* Robo y marcado

En un alto porcentaje, los delitos de robo son cometidos para que sus autores puedan vender las especies sustraídas. Prácticamente todos los países del planeta cuentan con mercados informales en los que ofrecen un espacio de transacción comercial de productos que mezclan objetos lícitos con otros robados. Uno de los grandes desafíos de la autoridad, al momento de fiscalizar o controlar esos mercados, es lograr asociar un producto a una víctima y delito específico, como medio para incautar el bien, detener al reducidor o vendedor de especies robadas, y devolver el bien a la víctima.

Podemos sospechar que determinados productos son robados, pero salvo infracciones tributarias por no pago de impuestos, o faltas administrativas por vender objetos sin permiso de la autoridad, es poco lo que se puede avanzar.

Las personas siguen comprando esos productos sabiendo, o no pudiendo menos que saber, que hay una alta probabilidad que hayan sido robados, sobre todo por su bajo precio. Para atacar eficientemente el robo o los delitos contra la propiedad, es necesario complementar las acciones existentes en contra de la oferta de ese mercado (quién roba y vende) con líneas de trabajo en relación con la demanda (quién compra).

Una alianza público-privada puede marcar, en este contexto, una importante diferencia para lograr aún mejores resultados, lo que se obtiene a través de diversas líneas de acción: a) trabajo continuo y fidelización de vendedores que quieren apegar su actuar a la ley; campañas publicitarias para no comprar productos robados; fiscalización interagencial a través de entidades complementarias a la policía, como es el caso de los servicios de recolección de impuestos o aduanas; integrar iniciativas privadas de marcado de productos cuyas bases de datos están en manos de privados y permiten identificar fácilmente al titular de un bien, entre otros.

Pero aun cuando tuviéramos un eficiente y amplio sistema de marcado o marcaje de productos que facilite su identificación y vinculación con el respectivo dueño, de nada servirá este aporte del sector privado, si las autoridades no cuentan con una línea de trabajo que busque esas marcas, contacte a las víctimas y retroalimente a la industria con información y resultados. Iniciativas asiladas de cada sector nunca lograrán las mismas tasas de éxitos a las que accederían a través de la integración de un proyecto conjunto.

* Espacios público y vigilancia

Cuando se comete un delito, o cuando una gran cantidad de ellos afecta una zona, en términos de convertirse en un problema serio de seguridad, el tiempo con el que reacciona la policía es esencial. Un robo o un asalto en la calle que no es resuelto en las siguientes horas tiene bajísimas probabilidades de no ser resuelto semanas después. La gran cantidad de casos archivados no solo genera una sensación de impunidad, sino que directamente la facilita.

El anterior escenario es aún más crítico en el ámbito de la seguridad turística. Los grupos criminales saben que la velocidad con la que los sistemas de justicia criminal abordan los robos en espacios públicos, juega a su favor. Si la víctima elegida es un turista, la probabilidad de desarrollar investigaciones exitosas es aún menor, en especial cuando el turista es extranjero. En efecto, cuando un turista sufre un robo —digamos de su celular o cámara— experimenta barreras idiomáticas y de conocimiento de la operación del sistema de justicia local a la vez que se dificulta su participación activa en el proceso, sea porque ese mismo día le corresponde viajar de regreso a su país o lo hará en los próximos días.

Entre las varias medidas que podrían mencionarse para abordar el desafío escrito pueden mencionarse los registros audiovisuales que suelen tener un efecto e impacto más inmediato, permitiendo dar con el/los sujeto/s que abordaron a ese turista, quien podría recuperar sus especies.

Así, el poder registrar las cámaras a los instantes de cometido un delito tiene mucho mayor y mejor resultado que hacerlo semanas o meses después. Ocurre que parte importante de esas cámaras son operadas por el sector privado. Muchas veces la autoridad no sabe quién tiene cámaras, dónde se encuentran, qué zona cubren, cuál es su sistema y duración de respaldo, y qué capacidad de resolución tienen, entre otras. Ese trabajo de levantamiento se suele realizar ante delitos graves de alto impacto, como un homicidio o violación, pero no por robos de celulares y dinero a turistas.

Así, ocurrido un hecho delictual de esta naturaleza, comienza generalmente una peregrinación en búsqueda de cámaras o filmaciones en poder de los residentes y vecinos del sector perdiéndose valioso tiempo de reacción. Si queremos darle seguimiento y ver los registros del camino que tomó el delincuente para llegar al lugar y/o para irse del mismo, será aún más difícil. Eso motiva que en un porcentaje importante de casos se trabaje con los registros audiovisuales de las cámaras del sector público (tránsito, unidades de seguridad, etc.), desaprovechándose una vasta red de vigilancia privada.

Como consecuencia de ello, y aun cuando el Estado hubiese obtenido algún resultado éstos podrían haber sido mejores si la autoridad hubiese tenido una manera más eficiente de acceder a las cámaras en tiempo real o, cuando menos, más inmediato respecto de las que se encuentran en manos del sector privado. Por su parte, el sector privado sigue siendo víctima sin que una tasa relevante de delitos pueda haberse esclarecido.

Una alianza público-privada, debiera permitir la generación de un catastro inicial, actualizado periódicamente, de todas las cámaras existentes en un sector determinado, las que mediante un protocolo de coordinación y en el marco de un proyecto conjunto, podrían integrar la red de vigilancia de la seguridad, ya sea porque tecnológicamente son incorporadas al sistema de control público —permitiendo el acceso en línea— o bien porque acuerdos previamente establecidos permiten no solo saber su ubicación y cobertura sino que facilitan la revisión y entrega en tiempos muy cercanos a la comisión del delito sin esperar órdenes o instrucciones oficiales y formales que muchas veces toman horas, días o semanas.

La autoridad accederá a más información y contará con herramientas que permiten esclarecer más delitos, identificar a los delincuentes y devolver las especies a las víctimas.

El sector privado podrá contar con un entorno más seguro que impactará positivamente en el desarrollo de actividades comerciales, generará una mejor imagen de un determinado sector o zona, lo que atraerá a más público y turistas, según el caso.

* Vehículos robados y sector privado

Una coordinación entre el sector público (agencias de control de la ley) y las autopistas, los centros comerciales y los cobradores de parquímetros, que facilita la identificación y ubicación temprana de vehículos robados representa una alianza público-privada que permitirá generar mayores tasas de éxito no solo a nivel de detección temprana y respuesta, sino también, prevención, tal como ha sido ya mencionado en el presente Manual.

De igual manera, el trabajo colaborativo entre la autoridad y las casas de remate o subasta permitirán la detección de personas vinculadas a la clonación y gemeleo de identidades de vehículos robados, generando importantes cuotas de prevención.

Asimismo, el uso extendido de autos o vehículos señuelos, mencionados en el Manual, ya no como una herramienta de control y detección, sino como un elemento que busca lograr un efecto preventivo y disuasivo, generando beneficios tanto al sector público en el control de esta amenaza, pero también al sector privado y a la comunidad que verá disminuir sustancialmente la amenaza.

En efecto, una buena campaña pública sobre el impacto de autos señuelos puede complementarse con campañas del sector privado, en especial centros comerciales los cuales tienen la posibilidad de entregar el mensaje a sus usuarios indicándoles que uno de los vehículos de sus estacionamientos pudiera ser un señuelo, de manea de desincentivar que esos espacios sean víctimas de robo.

Este tipo de avisaje o publicidad privada no tendrá efecto alguno si la autoridad no utiliza este medio como sistema de investigación criminal. Nuevamente, acciones aisladas nunca producirán el mismo impacto y efecto que aquellas desarrolladas de manera conjunta, en especial, en el marco de una alianza público-privada en la cual ambos actores integran sus necesidades, esfuerzos y recursos en un proyecto conjunto.[35]

* **Consejos locales de seguridad (comunas, cantones, condados, municipios)**

Los Consejos locales de seguridad son instancias de colaboración público-privada a nivel territorial que integran a todos los actores involucrados en los problemas de seguridad de un determinado territorio y en los que suele y debiera estar representada no solo la autoridad, sino también la comunidad, los actores más afectados y todos aquellos que pudieran contribuir a una solución a las amenazas que les afectan.

Resulta beneficioso fomentar y apoyar el liderazgo local a nivel no solo de municipalidades, ayuntamientos o alcaldías sino también juntas de vecinos, organizaciones de la sociedad civil, y otras entidades vinculadas, dado que todos ellos tienen una mayor relación, impacto y conocimiento del territorio, problemas y recursos. Trabajar a nivel local no solo contribuye a un mejor conocimiento del problema, sino altas cuotas de compromiso y un involucramiento más participativo.

Quién mejor que los vecinos de un barrio o sector saben lo que ocurre en este.
Sin herramientas y sin una alianza, este interés, información y capacidad se diluyen.

De esta manera, la buena práctica que se recomienda es que tanto gobiernos locales, como federales o nacionales fomenten la implementación y operación de consejos de seguridad al nivel territorial más básico, incorporando en las instancias relevantes actores privados, comunitarios, empresariales y de la sociedades civil, tanto por el íntimo conocimiento que tienen cada uno de ellos de los problemas locales como por el impacto directo que diversas medidas generarán en su territorio, lo cual debería asegurar altas cuotas de compromiso y participación.

[35] **Iniciativas exitosas en relación a autos señuelos han sido desarrolladas por Columbia Británica, Canadá, a través de programas enfocados en esta materia. Más información puede verse en los siguientes enlaces:**
-https://news.gov.bc.ca/factsheets/opinion-editorial-after-10-years-auto-thieves-still-hooked-on-bait-cars
-https://www2.gov.bc.ca/gov/content/justice/criminal-justice/policing-in-bc/road-safety-auto-crime/bait-cars
-https://www.baitcar.com/

* **Reinserción laboral**

Sea que se trate de personas que salen de la cárcel o de paramilitares desmovilizados, su reinserción es clave para que no cometan o reincidan en actividades criminales o actos terroristas. El interés principal por prevenir que ello ocurra es del Estado, y para ello existen muchos programas y ejemplos a nivel mundial. Con todo, la oferta estatal de trabajo puede no ser lo suficientemente amplia como la necesidad de contratación existente.

A su turno, la duración que pudiera tomar un proceso de contratación laboral en el sector público, su formalidad, y rigurosidad en términos de cumplimiento de requisitos, pudiera atentar contra el interés y deseo de generar vinculaciones laborales lo más rápido posible una vez que la persona sale de un centro penitenciario o se desmoviliza.

Cada día que pasa en la calle sin trabajo y sin apoyo, el riesgo de reincidencia se incrementa sustancialmente.

De ahí que el sector privado pudiera representar una oportunidad tremenda, tanto por su diversidad, tamaño de oferta, flexibilidad y velocidad de contratación. Desde luego, los privados tienen temores fundados de que los nuevos trabajadores vayan a cometer faltas o irregularidades si son contratados.

De igual manera, les preocupa el que no siempre pudieran acceder al historial criminal o terrorista del postulante. Por su parte, la contratación genera riesgos a la operación del negocio mismo y a sus colaboradores, lo que el privado querrá que sea compensado.

Una alianza público-privada puede abordar eficientemente cada uno de estos aspectos, los cuales deben ser regulados anticipadamente a fin de que ambas partes tengan reglas claras.

El estado debería saber con mayor nivel de certeza el tipo de oferta laboral, la velocidad y, sobre todo, capacidad y cantidad de contratación disponible.

Eso le permitirá estructurar sus planes de reinserción laboral y prevención de delitos de la mejor manera posible. Pero si desea trabajar con el sector privado, sea este la empresa privada, organizaciones de la sociedad civil o comunitarias, deberá abordar cada uno de los temores y preocupaciones. Deberá saber cautivar. Encontrar —como se señaló al inicio de este Manual— el caso de negocio que le resulte de interés al potencial reclutador.

Así las cosas, el sector público debiera asegurar la entrega de información detallada sobre el pasado del postulante, generar informes sobre el índice de peligrosidad y —por qué no— entregar subsidios directos por cada trabajador contratado o indirectos asociados a pagos de impuestos, entre otros beneficios.

Reuniones periódicas entre las áreas de desempeño laboral de las empresas, por un lado, y las de reinserción social de las unidades del Estado, por otro, debieran ser consideradas siempre a fin de generar retroalimentación con relación a los beneficios, avances, tropiezos, desafíos de la iniciativa, como también sobre el nivel de cumplimiento de las expectativas de ambos actores involucrados. Considerar la opinión y consulta de los mismos reinsertados pudiera ser relevante.

* Proyectos en zonas con baja presencia estatal

Existen a nivel mundial muchos lugares en los que una presencia territorial más intensa de grupos terroristas[36] ha motivado una histórica baja presencia estatal. A veces ello se debe a dificultades geográficas que son las que precisamente los grupos terroristas aprovechan en su beneficio; en otras es la desconfianza en el Estado por parte de la población local; y a veces es el riesgo que representa para un funcionario público para operar en un territorio en el que una organización terrorista tiene participación activa.

En todos esos lugares, y no obstante una baja presencia estatal, existen organizaciones comunitarias consolidadas, empresas privadas que desarrollan actividades comerciales o industriales de diverso tipo, y organizaciones de la sociedad civil.

Una interesante estrategia para generar intervención territorial y humana por parte del Estado en este tipo de zonas puede realizarse a través de asociaciones público-privadas en las cuales el Estado puede extender sus programas de apoyo, asistencia y fomento, mediante actores locales más vinculados al mundo privados, quien además de conocer la zona tienen interés en lograr mejores servicios para la comunidad.

* Infraestructura crítica y terrorismo

En gran parte de los países, la infraestructura considerada como crítica por el Estado recibe una especial atención en materia de seguridad, protección, análisis y recursos, sometiéndolas no solo a mecanismos intensificados de prevención, sino también en la generación de capacidades para detección temprana de amenazas y pronta respuesta ante las mismas.

Tradicionalmente, el Estado ha sido dueño o ha tenido control sobre parte importante de la infraestructura crítica de un país. Pero en las últimas décadas ello ha ido cambiando al punto que hoy en día una gran cantidad de puertos, sistemas de agua, aeropuertos, hospitales, fábricas esenciales, sistemas de transmisión eléctrica y alcantarillado están en manos de privados o, cuando menos, siendo estatales, son operados por los primeros. Se trata de instalaciones cuya destrucción o afectación podría tener un impacto debilitante en la seguridad, la estabilidad de la economía nacional y la seguridad o salud pública.

[36] FARC, en Colombia, y Sendero Luminoso, en el Perú, son algunos ejemplos de este tipo de organizaciones y el impacto que han tenido a nivel territorial.

Sin embargo, existe un tipo de infraestructura que, sin ser crítica, en los términos definidos precedentemente, ha sido objeto cada vez más recurrente de ataques terroristas. Incorporar esos nuevos potenciales blancos resulta del todo conveniente.

En efecto, es posible advertir que los últimos ataques terroristas en España, París, los Estados Unidos, el Reino Unido, Indonesia, Turquía y Somalia, por mencionar tan solo algunos, no fueron realizados en contra de instalaciones militares o gubernamentales, sino que se dirigieron en contra la población civil, en zonas operadas o con gran presencia o intervención de privados, tales como oficinas, centros comerciales, teatros y hoteles.

El objetivo de los grupos terroristas ya no solo consiste en debilitar a un Estado atacando sus recursos operativos o infraestructura crítica propia, sino en causar pánico en la población, buscando infundir temor e inseguridad en la misma. Ello debiera motivar a que los centros comerciales, estadios y hoteles, entre otros, puedan ser considerados infraestructura crítica para un Estado, tanto desde el punto de vista normativo como operativo.

Es por eso que, de cara a la prevención de riesgo de ataques terroristas a la infraestructura crítica, una primera aproximación consiste en ampliar el concepto de la misma a nivel legislativo, de manera que se aseguren aquellas instalaciones, servicios y áreas relevantes para la marcha del país, pero también para la segura y pacífica convivencia, pudieran ser consideradas e incorporadas a los planes de infraestructura crítica.

No se trata de imponer, por la vía legal o administrativa, obligaciones al sector privado que los lleven a gastar más dinero en seguridad, cámaras, guardias, detectores de metales. No se descarta esa vía de acción, pero la misma no es reflejo de la alianza público-privada que este Manual promueve.

Es evidente el interés del sector privado por evitar ataques terroristas en contra de las instalaciones que operan. El daño no solo es producido por el atentado mismo, resultado de muertes y destrucción física.

Se genera un efecto negativo a mediano plazo en el que la población, naturalmente temerosa, deja de acudir durante un tiempo a los lugares que fueron objeto de atentados. La recuperación se hace aún más lenta. Prevenir los ataques o detectarlos tempranamente no solo resulta interesante con relación al ataque mismo, sino a los efectos a mediano plazo que este produce.

Es por ello que los entes privados interesado en la continuidad del negocio deben desarrollar planes junto al Estado, como ente rector y gestor de la seguridad y protección, en un contexto de alianza público-privada como criterio de acción conjunta.

Mientras el sector privado tendrá muchas más herramientas para realizar actividades de detección, a través de videovigilancia, controles físicos o a personas y vehículos, será el Estado el que está en mejores condiciones de proveer información acerca de amenazas inminentes, y perfiles de riesgos sobre los que debe operar la detección.

* Puertos, aeropuertos, crimen organizado y terrorismo

La industria área y marítima[37] trasladan personas y carga, las cuales pueden estar asociadas no solo a movimientos o actividades terroristas, sino también a operaciones criminales vinculadas a tráfico armas y drogas, trata de personas y contrabando, entre otras. Estas últimas bien podrían ser, además, fuente de financiamiento para actividades terroristas.

Es un hecho que no se puede inspeccionar a cada uno de los pasajeros y a toda la carga. Es necesario realizar perfilamientos de riego. De hecho, la inspección física de carga de contenedores no supera el 4% de todos los movimientos a nivel mundial. Sin perjuicio de la existencia de soluciones tecnológicas y el desarrollo de nuevas, el control de carga y pasajeros inevitablemente genera demoras que, si son excesivas, afectan seriamente el comercio mundial.

Se produce entonces un conflicto. Ambos sectores, público y privado desean afectar las amenazas descritas en términos que estas no utilicen el transporte marítimo o aéreo o lo hagan en mucho menor cantidad.

Mientras que el Estado desea combatir directamente estas amenazas por el riesgo que representa para la población y la seguridad, el privado no quiere que la cadena de suministro o los procesos logísticos se vean interrumpidos ante hallazgos de actividad terrorista o criminal.

Nuevamente, y de manera muy similar a como fue señalado en el caso de la infraestructura crítica —de hecho, los puertos y aeropuertos lo son en muchos países— es necesario identificar necesidades y objetivos en cada uno de los sectores y buscar una sintonía en los mismos de manera que los recursos de cada uno puedan ir en beneficio de un interés común evitando los costos y desafíos que en la actualidad impiden que este tipo de alianzas sea masivo.

Como no se puede inspeccionar toda la carga, la información y el perfilamiento de riesgo es esencial. Si los operadores logísticos suben y cargan la información correctamente, esta permitirá tener mayores y mejores datos para el análisis. Contar con esta información, permite a los actores estatales desarrollar una mejor inteligencia lo que derivará en mejores perfiles de riesgo y, en última instancia, controles con una tasa de acierto más eficiente.

La retroalimentación constante entre ambos sectores y la realización de actividades de seguimiento y evaluación son esenciales para que la entrega de información por parte de los privados al Estado, o la generación de alertas, sea vista como un beneficio mutuo y no como un servicio prestado por un sector al otro.

[37] Para los propósitos de este Manual las actividades de transporte marítimo consideran también las fluviales y lacustres.

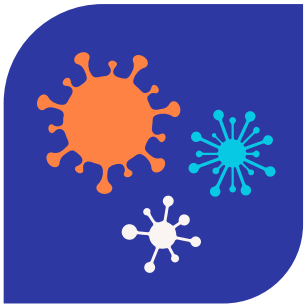
* Bioseguridad y terrorismo

La pandemia que experimentó el mundo entero por el coronavirus demostró que una necesidad pública de salud no podía ser abordada eficientemente solo desde el Estado, sino que requería de un importante aporte e intervención privada, pero no desde la colaboración espontánea, sino de una alianza público-privada que, en este caso, se dio a niveles locales, nacionales y también internacionales.

Mientras que el Estado aportó sendos recursos y líneas de financiamiento, así como todo el know how e información acumulados a la fecha en materia de desarrollo de vacunas, lo cual complementó con estrictas normativas para disminuir el contagio, el sector privado contribuyó con su capacidad de investigación y desarrollo tecnológico, así como de producción de vacunas.

En términos de distribución, ambos trabajaron a la par, en un esfuerzo sin precedentes.

Aun cuando todo indica que la última pandemia fue originada de manera natural, bien podría haberse creado, esparcido y propagado de forma intencional bajo la modalidad de un ataque bioterrorista que podría complementarse con diversos virus y agentes bacterianos.



Aunque con un desarrollo más crecientes como consecuencia de la pandemia del coronavirus, existe —en comparación a otras especialidades— una necesidad de contar con más expertos en ciencias microbiológicas e inmunológicas. Se trata de un escenario en el que una alianza público-privada debiera ser considerada, esta vez no solo con laboratorios, sino también con universidades y centros de formación a fin de generar más especialistas en la materia.

Desarrollar vacunas es un proceso largo y caro. El Estado sin dudas necesita avanzar en esta línea, pero entendiendo que hay mayor capacidad en los privados quienes eso sí, enfrentan en ocasiones, burocracia, así como limitaciones legales, regulatorias y de financiamiento.

Si de bioterrorismo se trata, será el Estado quien tendrá más información sobre las principales y más relevantes amenazas, lo que permitirá direccionar el trabajo de los laboratorios.

Una alianza entre ambos sectores pudiera abordar con eficiencia estos desafíos como también la necesidad de generar un compromiso a largo plazo porque la inversión —sin importar quien la realice— toma mucho tiempo en mostrar resultados.

Aspectos que tradicionalmente han sido una barrera en la colaboración público-privada para el desarrollo de soluciones a amenazas biológicas es el de la propiedad intelectual, la cual debe ser regulada de la manera más clara posible al iniciarse el proyecto.

Sin asegurar la totalidad o una cuota de los derechos de propiedad intelectual al sector privado le será difícil ver en esta alianza un caso de negocio.

Una asociación como la descrita permite compartir los riesgos financieros a la vez que los beneficios. De paso, ayudará a centralizar conocimiento disperso y tecnología diversa. Iniciativas como estas, en el marco de amenazas bioterrorista, se deben considerar no solo el desarrollo de soluciones médicas, sino también en un trabajo conjunto para la detección temprana de entidades o grupos que pudieran tener conocimientos y capacidades para desarrollar armamento biológico; la detección temprana en casos de infección y propagación; tareas de contención y finalmente vacunación, si fuere el caso.

Al día de hoy, probablemente los patógenos con mayor nivel de riesgo y que representan una mayor amenaza son los virus del Ébola y Viruela, y la bacteria del Ántrax.

* Desarrollo tecnológico para prevenir y combatir el terrorismo

Una de las lecciones aprendidas luego de los ataques terroristas en los Estados Unidos en septiembre de 2011 es la necesidad de desarrollar programas de cooperación en materia de seguridad, no solo entre los actores públicos o estatales, sino también entre estos y el sector privado.

Esta coordinación, idealmente en formato de alianza público-privada, permite contar con una mejor preparación, pero también con una respuesta ante ataques biológicos y químicos, terroristas convencionales y ciberataques.

El sector privado cuenta con una importante y variada capacidad tecnológica, recursos e información, que el Estado no debiera nunca desaprovechar dada la utilidad que puede representar las sinergias entre ambos. De hecho, el sector privado ha sido líder en el desarrollo de vacunas, equipamientos de detección de materiales o partículas representativas de amenaza (metales, explosivos, elementos radioactivos, patógenos, etc.), sistemas de información y programas de protección cibernética, las cuales han apoyado a los países en mayores y mejores niveles de protección y seguridad.

Sin ir más lejos, la gran mayoría de los sistemas de control de pasaportes y documentos de identidad en controles fronterizos se realizan en la actualidad de manera automatizada mediante el uso de escáneres desarrollados por el sector privado para ese único fin, de manera tal que empresas diseñaron productos para dar solución a necesidades públicas. Con todo, el escaneo de pasaportes realizado de manera aislada no genera el mismo beneficio que representaría contar con esos mismos datos, pero analizados de manera cruzada con bases de datos estatales, o procesados con softwares de análisis y perfilamiento de riesgo desarrollados por la industria privada.

Así como el uso de inteligencia artificial para construir modelos de predicción en materia de seguridad requiere idealmente de información proveniente de los actores estatales quienes debieran aportar importantes antecedentes sobre lo que se desea predecir, en qué términos y formatos, existen otros desarrollos del mundo privado, cuyo valor agregado se obtiene solo a través de un trabajo conjunto con el sector estatal, en término de necesidades y retroalimentación.

Un ejemplo de ello pueden ser los programas o software que permiten realizar análisis de datos masivos y definir patrones de comportamiento, diseñados para ser usados por el sector privado, pero que con los correctos insumos y retroalimentación del Estado permitieron el diseño y operación de módulos enfocados al sector público y de investigación y prevención de criminalidad y terrorismo.

En efecto, en un mundo globalizado que provee al investigador o prevencionista de amenazas de innumerables datos, su procesamiento tanto en tiempo como en forma representa un enorme desafío. Analizar años de registros bancarios o migratorios, exportaciones de productos o miles de llamadas telefónicas es una tarea extremadamente difícil.

El desafío diario de los analistas criminales y antiterroristas es descubrir y destapar redes, patrones y tendencias de los actuales y crecientes volúmenes de datos complejos estructurados y no estructurados para lo cual en la actualidad existe una diversa oferta tecnológica de programas (softwares) que permiten analizar los datos desde ópticas distintas y que son utilizados no solo en el mundo privado, sino también en el públic.[38]

Es un hecho, eso sí, que muchas veces los desarrolladores tecnológicos y lideres de la industria son competidores entre sí. Una colaboración espontánea es posible, pero no fácil de lograr. De ahí que el Estado es quien debiera generar condiciones legales, financieras y de planificación, que permitan que competidores reales y naturales se reúnan para trabajar de manera conjunta, tanto para la identificación de obstáculos tecnológicos asociados a las amenazas a la seguridad, como también para desarrollar planes que permitan superar colectivamente esos obstáculos.

[38] Por un lado, están los programas como el *I2, Visallo, Neo4J, DataWalk o Cellebrite* que en términos generales analizan datos y establecen relaciones y patrones cuando estos datos provienen de bases de datos estáticas como archivos.
Así, cuando un investigador se enfrenta a un listado de 1500 llamadas telefónicas entre varios sujetos investigados, estos programas realizarán un dibujo en cosa de minutos a través del cual será fácil apreciar quiénes hablan con quiénes, con qué frecuencia y en qué horarios, por ejemplo. Arribar a esa misma información sin contar con un programa como los descritos, podría tomar días o semanas incluso al mejor de los investigadores o prevencionistas.
Por otro lado, se encuentran los programas como *Maltego, Social Links, Lampyre o Geph* que -con algunas diferencias- realizan un similar trabajo de relacionamiento y detección de patrones, pero alimentados con información de fuentes abiertas disponibles en internet. De esta manera, cuando queremos analizar, por ejemplo, perfiles sociales u ofertas de servicios en la web, será más fácil hacerlo con estos softwares que tienen la capacidad de ir a buscar el dato en una fuente abierta a la cual se accede vía internet. Los otros programas necesitan ser alimentados con información que sería muy difícil transportar desde la web.
El primer grupo será más fácil para analizar transacciones bancarias o movimientos migratorios cuando los programas son alimentados por bases de datos estáticas contenidas en archivos. El segundo grupo resulta más eficiente si se desea establecer vínculos entre personas basados en la información contenida en *Instagram, Facebook, Linkedin, Twitter, Snapchat e, incluso, la Dark Web.*

Con todo, es posible apreciar interesantes casos de colaboración público-privada donde la iniciativa vino desde el sector privado y fue acogida por el Estado potenciando aún más los beneficios del trabajo conjunto. Un interesante ejemplo en esta materia lo representa el Programa BENS[39] en los Estados Unidos, que supo combinar esfuerzos, conocimiento, experiencia, capacidades y recursos de ambos sectores, en este caso, bajo la iniciativa del sector privado, pero siempre con el fin de mejorar las capacidades de prevención, detección y respuesta ante amenazas a la seguridad, parte de las cuales se vinculan a actividades de tipo terrorista.

* **Prevención del terrorismo. Estado y comunidad.**

El trabajo con la comunidad para prevenir violencia asociada no solo al crimen organizado, sino también al terrorismo, resulta ser más rentable que abordar solo la respuesta una vez que el ataque se ha concretado o el delito cometido.

La comunidad tiene mucho que aportar en términos de información y apoyo social. Uno de los principales desafíos es la necesidad de desarrollar líneas de confianza mayores con los entes gubernamentales.

Resulta recomendable trabajar con toda la sociedad para establecer y ampliar los marcos de prevención locales. A través de asistencia técnica, financiera y educativa, es posible apoyar exitosamente los esfuerzos locales que evitan que las personas se radicalicen hacia la violencia.

Este tipo de iniciativas tiene un alto impacto en la comunidad en general, pero de manera muy especial en la protección de espacios escolares y universidades, así como en eventos de alta concurrencia. Un buen ejemplo de este tipo de iniciativas es CP3[40] en los Estados Unidos.

[39] **BENS – Ejecutivos de Negocios para la Seguridad Nacional en Estados (Business Executives for National Security). Se trata de una organización nacional, no partidista, sin fines de lucro que tiene por objetivo apoyar a los altos ejecutivos comerciales y de la industria que aplican las mejores prácticas y experiencia del sector privado y los negocios para ayudar a mejorar la seguridad nacional. BENS busca reunir el mejor talento en el mundo de los negocios junto a los principales actores en seguridad, con el objeto de aplicar las mejores prácticas e ideas de vanguardia para resolver algunos de los desafíos de seguridad más complejos y apremiantes.**
Para más información ver en https://bens.org/

[40] **CPR – Centro de Programas de Prevención y Asociaciones del Departamento de Seguridad Interior de los Estados Unidos (Center for Prevention Programs and Partnerships). Este programa promovido por el sector público, busca generar las condiciones para que las comunidades estén unidas para ayudar a poner fin a la violencia y el terrorismo. Trabajan con toda la sociedad para construir marcos locales de prevención. La iniciativa trabaja para diseñar e implementar programas para generar confianza, asociaciones y colaboración en todos los niveles de gobierno, el sector privado, las organizaciones no gubernamentales y las diversas comunidades del país. Entre otras líneas de trabajo, CP3 trabaja con la comunidad apoyado en recursos metodológicos y guías que brinda una descripción general de los equipos tanto públicos como privados y comunitarios de gestión y evaluación de amenazas, vinculadas a terrorismo y violencia.**
Para más información ver https://www.dhs.gov/CP3

* Turismo y seguridad

La generación de alianzas público-privadas en materia de seguridad turística es crucial a la hora de generar espacios más seguros para turistas, generando no solo programas de prevención y detección temprana de amenazas, sino respuestas rápidas que disminuyan el impacto de determinado incidente.

Un turista está expuesto tanto a las amenazas del crimen organizado, como también a atentados terroristas. Mientras el Estado desea fomentar una zona, un lugar o el país completo como un destino seguro, el privado desea evitar la caída de reservas y viajes como consecuencia de incidentes que afecten la seguridad de los visitantes.

No se trata solo de trabajar conjuntamente en impedir que estas amenazas se concreten, pues llevar el riesgo a cero, implicaría cerrar un país al turismo. Junto con actividades de prevención, es recomendable desarrollar líneas de trabajo en materia de atención al turista. Varios países han avanzado en esta línea, como es el caso de México, a través de los CAPTA[41] o Ecuador mediante los PIAT.[42]

[41] Un ejemplo interesante lo representan los Centros de Atención y Protección al Turista – CAPTA de México, encabezados por las autoridades turísticas de los estados y municipios en que se encuentran, con representación de dependencias de los tres órdenes de gobierno. En ellas, participan activamente tanto entidades consulares de países con mayor índice de turistas, organismos internacionales como la Cruz Roja, a través de su filial mexicana, y el sector privado a través de los prestadores y operadores de servicios turísticos. Los CAPTA tienen por función principal atender y orientar a los turistas nacionales y extranjeros, tanto para recibir información y apoyo, como para canalizar y dar seguimiento a las denuncias, quejas y situaciones de riesgo. Explicación más detallada puede ser consultada en http://scm.oas.org/pdfs/2019/CICTE01300D.pdf

[42] El Plan Integral de Asistencia Turística de Ecuador (PIAT) es una herramienta con la que cuenta Ecuador para garantizar la movilidad y el desplazamiento seguro de los turistas que visitan el país. Tiene como objetivo implementar estrategias y protocolos con un enfoque integral que fortalezcan la participación activa del sector público, el sector privado y las comunidades en la evaluación de riesgos, la prevención de daños y el manejo de emergencias y crisis, tomando en cuenta las necesidades del destino. Explicación más detallada se puede consultar en https://amevirtual.gob.ec/wp-content/uploads/2017/05/PLAN-INTEGRAL-DE-ASISTENCIA-TURISTICA-PIAT.pdf

Lo más importante

Este capítulo destaca la importancia y el éxito de las alianzas público-privadas en el ámbito de la seguridad, presentando casos concretos en áreas diversas. Los principales puntos para destacar son:

1. La colaboración bidireccional entre sectores públicos y privados genera soluciones innovadoras y efectivas en la prevención, detección, mitigación y respuesta ante amenazas.

2. Ejemplos notables incluyen la capacitación para detección temprana de trata de personas, cooperación en zonas empobrecidas, apoyo financiero a víctimas de violencia delictual, recuperación de vehículos robados, reinserción laboral, y desarrollo en áreas como infraestructura crítica, bioseguridad y turismo.

Los casos presentados en este capítulo demuestran el éxito de las alianzas público-privadas en abordar desafíos de seguridad y sirven como referencia para futuras colaboraciones, buscando siempre mejorar la prevención, detección, mitigación y respuesta ante amenazas que enfrentan nuestras sociedades.

Los comités de crisis de seguridad y las alianzas Público - Privadas

En este capítulo, abordaremos un tema crucial para la seguridad y el bienestar de la sociedad: los Comités de Crisis de Seguridad y las Alianzas Público-Privadas. Estos comités son entidades de colaboración público-privada creadas para enfrentar situaciones críticas que ponen en riesgo la seguridad de la población. Su función es continua y permanente, y su eficacia radica en la gestión conjunta e integrada de los sectores público y privado.

El capítulo se estructura en tres secciones temporales: antes, durante y después de una crisis. Cada sección presenta una serie de acciones y medidas que permiten una mejor preparación y respuesta ante situaciones críticas. Algunas de las acciones clave incluyen el análisis de riesgos, la elaboración de planes de respuesta genéricos, la comunicación y la estructuración de un Comité de Crisis. Además, se abordan aspectos relacionados con la infraestructura, la designación de integrantes del comité, la capacitación y la realización de simulacros.

Durante una crisis, es fundamental la activación y operación del comité, así como la toma de decisiones efectivas y coordinadas para reducir los efectos negativos. Por último, después de una crisis, se enfatiza la importancia de la recuperación y la evaluación para aprender de la experiencia y mejorar en el futuro.

El capítulo concluye destacando la importancia de designar a un equipo encargado de implementar las recomendaciones y asegurar su ejecución tanto en las acciones previas a la crisis como en las evaluaciones posteriores. La conformación y gestión de un mecanismo de gestión de crisis en seguridad pública con representatividad público-privada generará mayores beneficios y contribuirá a la protección de la comunidad y la actividad económica.

Los comités de crisis son instancias de colaboración público-privadas diseñados como un mecanismo para enfrentar una determinada situación grave y decisiva que pone en peligro el desarrollo de un asunto o un proceso vinculado, en este caso, con la seguridad.

A diferencia de lo que muchos podrían pensar, el comité no se crea y muere con una crisis. Son entidades de operación continua y permanente en el tiempo que, con ocasión de una crisis, experimentan una actividad intensa y altamente demandante.

Prácticamente todas las crisis de seguridad impactan tanto al sector público como al privado. Ante problemas conjuntos debe trabajarse integradamente para ejecutar situaciones conjuntas.

Saber cómo gestionar eficientemente un comité de la mano de actores públicos y privados impactará en el éxito del trabajo de esta instancia, lo cual redundará en una disminución de los riesgos, pero también de los impactos que las amenazas representaron para la seguridad pública de una comunidad. La operación y gestión de un comité de crisis supone necesariamente que se haya conformado un comité y que nos encontremos en medio de una crisis.

Las diversas actividades en las que participa una comunidad, vinculadas al turismo, comercio, transporte, deporte, vivienda e, incluso, salud no están ajenos a verse afectados por situaciones graves vinculadas a la seguridad pública, que pongan en peligro su proceso y operación, perjudicando no solo el crecimiento futuro sino su desarrollo actual. El sistema de gestión de continuidad de negocio que regula la Norma ISO 22301[43] considera la crisis como una situación con un alto nivel de incertidumbre que afecta las actividades básicas y/o la credibilidad de una organización, requiriendo medidas urgentes.

Fuera de la norma ISO, pudiera sostenerse que las diversas actividades o sectores mencionados, enfrentan una crisis de seguridad cuando estas se ven expuestas a hechos negativos que escalan rápidamente, cuando se pierde el control de la comunicación y/o cuando se genera una imagen perjudicial de carácter grave.

> En lo que a seguridad se refiere, el daño —de nivel crítico— se produce por eventos complejos, catastróficos o de gran envergadura o impacto, que afectan tanto a la comunidad, a la actividad económica, y al sector que esta actividad mueve.
>
> Una buena preparación —previa a situaciones de crisis— permite enfrentarlas de mejor manera, contribuyendo a disminuir el impacto de los daños y a acelerar la recuperación. Así, la presente sección del Manual pretende ser una guía que entrega los conceptos y herramientas esenciales que debieran tomarse en cuenta para enfrentar una crisis de seguridad en sus tres dimensiones temporales: antes, durante y después.

[43] Norma de estandarización internacional que tiene por fin entregar directrices y procedimiento para implementar, mantener y mejorar un sistema de gestión para proteger contra una interrupción de servicio, producción u operación, así como para reducir la probabilidad de que ocurra, prepararse para el evento que suceda y recuperarse de las interrupciones cuando se verifiquen. Ver más detalles de esta norma en la publicación de la Organización Internacional de Estandarización (ISO en inglés por su nombre International Organzation for Standarization) https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf

Con el objetivo de entregar una herramienta de gestión de crisis que pueda ser aplicada conjunta e integradamente por los sectores público y privado, no solo en crisis a la seguridad pública, sino que, en toda situación grave, proveeremos una aproximación más amplia. Con todo, su aplicación a los problemas generados a la seguridad pública, cuando estos alcanzan dimensiones o niveles críticos es absoluta y total.

Previo a una crisis (A)

* Análisis de riesgos

Las crisis, vinculadas a la seguridad, así como a otras actividades o sectores se producen cuando los riesgos a los que se expone determinado sector, comunidad o actividad, se concretan, de forma que la mejor manera de poder prevenir y/o gestionar esos riesgos supone su identificación previa.

Identificar y evaluar los riesgos provenientes de las amenazas supone un ejercicio mediante el cual se establecen y ponderan cuatro factores, los cuales se analizan en función de los principales activos —tangibles y no tangibles— del turismo tales como imagen, país, comunicación, turistas, operadores del sector, etc. Estas variables se pueden combinar con los 13 elementos que, según el presente Manual, se recomienda tomar en cuenta al momento de desarrollar un diagnóstico de las amenazas que se deseen abordar.

Los factores que considera son:

- ***La naturaleza de la amenaza.*** Establecer los tipos de amenaza, las cuales pueden clasificarse en dos categorías:
    - *amenazas reales vs las de percepción,* que en ocasiones pueden ser igual de dañinas que las primeras; y
    - *amenazas de origen físico-natural (terremotos, tsunamis, aluviones, inundaciones, volcanes, etc.) vs las de tipo humano-social-económico* (terrorismo, epidemia, conflicto político o social, guerra, actividad criminal, ciberataque, desplome de mercados, grave alteración de los tipos de cambio, errores en la operación de sistemas o equipos, entre otros).
- ***La magnitud o nivel de la amenaza.*** Se requiere categorizar las amenazas identificando y asignando niveles de impacto en función del activo tangible o intangible que se está evaluando.

- ***La vulnerabilidad ante la amenaza.*** Luego de analizar el factor externo (amenazas) es necesario establecer y evaluar el factor interno, esto es, las amenazas y vulnerabilidades internas. Se trata de determinar los aspectos de organización, equipamiento, recursos humanos y financieros, construcción y coordinación que hacen que determinada infraestructura, sector, organización o actividad sea más o menos vulnerable ante las amenazas previamente identificadas.
- ***Las consecuencias y daños, en el evento de que la amenaza se concrete.*** Esta etapa busca establecer el impacto que se genera cuando la amenaza se concreta y que puede ser categorizada y evaluada en función de cuatro factores:

    - ***Salud pública.*** Efecto en las vidas humanas y bienestar de la población (muertes, enfermedades, heridos, etc.).

    - ***Economía.*** Pérdida económica directa o indirecta (costo de reconstrucción; costo de respuesta; costo de recuperación; costo o impacto en otra infraestructura o servicio; daños a largo plazo por contaminación ambiental; etc.).

    - ***Psicología e imagen.*** Efecto en la moral pública y confianza en la economía nacional y en las instituciones públicas o privadas. La forma en la que se gestiona una crisis impactará positiva o negativamente en este aspecto, el cual abarca los cambios en las percepciones que surgen después de un incidente de mayor escala y que afecta la sensación de seguridad y bienestar del público, el cual podría incluso manifestarse en comportamientos disruptivos.

    - ***Gobernanza e institucionalidad.*** Efecto derivado de la habilidad del Estado, Gobierno y/o sector privado para mantener el orden, asegurar la continuidad operaciones y de los servicios básicos, velar por la salud y llevara adelante acciones de seguridad pública y estabilidad, según corresponda.

* Planes de respuesta genéricos

En función de los principales riegos y amenazas detectados, es posible y recomendable construir y elaborar planes de trabajo y respuesta genéricos para enfrentar de mejor manera posibles futuros escenarios. Estos planes, posteriormente deberán ser capacitados y respecto de ellos se realizarán simulacros y simulaciones.

Se recopilan en esta sección del Manual todas las indicaciones y referencias sobre la importancia de una aproximación conjunta tanto del sector público como privado, pues las crisis a la seguridad afectan a toda la comunidad e institucionalidad de manera transversal.

* Activación

Independientemente que un Comité de Crisis puede ser convocado por indicación de su director o coordinador, este también puede conformarse como consecuencia de la ocurrencia de determinados hechos que han sido previamente determinados con ocasión del levantamiento de riesgos. Son las llamadas *alertas o indicadores*, como sería un motín en un centro carcelario, un incremento inusitado de sicariato u homicidio, un atentado terrorista o la aparición de grupos criminales que actúan con extrema violencia, poder de fuego o impunidad amparada en altas cuotas de corrupción, entre otros ejemplos.

Es importante tener presente que al momento de elaborar las hipótesis de activación del Comité estas podrían haber ocurrido o estar ocurriendo (terremoto, ataque terrorista, etc.) o bien tratarse de una amenaza (convocatoria a huelga en aeropuerto o paralización de carreteras, epidemia en países vecinos, temporal que aún no toca tierra, fenómenos criminales complejos en los países vecinos con alta probabilidad que comiencen a verificarse en el lugar de planificación, etc.).

* Catastro

Elaborar un catastro que contenga una clara identificación de las principales entidades vinculadas al sector o actividad afectada, incluyendo tanto sector público como privado, señalando sus competencias y roles, puntos de contacto formales, enlaces en casos de emergencia, y capacidad de respuesta y apoyo en situaciones de crisis.

El objetivo es saber con qué recursos y capacidades se cuenta tanto para la elaboración de los planes de respuesta como para la gestión de la crisis propiamente como tal. El levantamiento debe realizarse y actualizare de manera periódica, incluyendo a los principales *stakeholders* relacionados con temas de seguridad.

* Comunicación

Una gestión de crisis eficiente requiere de una eficiente gestión de las comunicaciones.

- **Mensajes**

> Un elemento que coadyuva al logro de este objetivo es la elaboración previa de mensajes tipo dirigidos a la comunidad y los *stakeholders* atendido el tipo de información que se desee proporcionar. Esta acción disminuye los riesgos en la improvisación y prepara de mejor manera la forma en la que se comunica el Comité de Crisis.

Cada crisis es distinta y prácticamente ninguna se parece a otra. Cubrir todos los escenarios es imposible, por lo que una forma de abordar este desafío consiste en desarrollar mensajes comunicacionales genéricos diseñados según el tipo de riesgo, y que se adaptarán caso a caso.

No es lo mismo entregar información sobre turistas víctimas de un terremoto que de un atentado terrorista, como tampoco lo es enfrentar una crisis de la naturaleza —generalmente de un impacto temporal acotado a segundos, minutos o días— que una vinculada a causas sociales, humanas o económicas, que en algunos casos puede durar meses como la canalización de demandas sociales promovida con fines de generar violencia planificada. Los desafíos son, claramente, distintos.

En tanto las crisis de corta duración —con un inicio y fin definidos— se pueden manejar con una menor cantidad de comunicados, preparados y anticipados de mejor manera, los escenarios de larga duración como problemas estructurales a la seguridad pública, crisis económicas, pandemias o conflictos sociales, requieren un manejo más fino, flexible y adaptable a la manera en que la situación va evolucionando.

Por ello, la mejor manera de responder los distintos escenarios es con mensaje cortos, reiterados, específicos que contengan información oportuna, objetiva, transparente, veraz y precisa.

Estos mensajes deben:

* *describir los acontecimientos (lugar, fecha, impacto, daños, causas),*
* *indicar las medidas tomadas y las que se van a implementar a futuro,*
* *solidarizar con las víctimas o afectados por la crisis,*
* *señalar cuando será el próximo comunicado,*
* *indicar en que lugares, medios y formatos pueden encontrar información actualizada*

- **Pautas**

Es importante diseñar pautas predefinidas que ayuden en la capacitación de los grupos vinculados a manejo comunicacional, y mediante las cuales se entrene a los operadores de esta área sobre la mejor manera de comunicar en crisis. Se trata de enseñar qué es lo que se debe decir, cómo se debe decir, cuándo se debe decir y, qué es lo que **no** se debe decir cuando se está en una crisis.

Las reglas de comunicación en crisis presentan ciertas características diferenciadoras de otros escenarios que vale la pena tener siempre en cuenta. Los equipos de comunicaciones deben estar preparados.

* Estructurar un Comité

Un comité de crisis debe tener a su disposición a un grupo de personas que se hagan cargo de coordinar, ejecutar y/o supervisar una serie de labores o tareas. No siempre todas estas personas deben estar sentadas detrás de la mesa del Comité. Algunas participarán de las sesiones de trabajo grupal cuando se aborden los temas que les competen (área legal, por ejemplo) y otras, por la naturaleza de su labor, estarán siempre presentes (como es el caso del coordinador o del encargado de comunicaciones).

Todos ellos deben estar a disposición del Comité, en el mismo edificio o área en el que este opere y serán convocados según las necesidades. Desde luego, la experiencia indica que, en las primeras sesiones, en las que se está midiendo todavía el impacto de una crisis y se está coordinando las primeras respuestas, es deseable la presencia de todos.

* Integrantes

- **Dirección**
  - Dirige el Comité.
  - Decreta o valida la crisis.
  - Asigna tareas y delega responsabilidades.
  - Determina quien integrará cada una de las sesiones.
  - Aprueba y valida plan comunicacional, mensajes y líneas de acción.
  - Actúa como vocero, si las circunstancias lo demandan.
  - Mantiene estrecho contacto y coordinación con otros comités de crisis sectoriales (si es que hubiera más de uno).

- **Operación y Control Interno**
  - Se asegura que las cosas sucedan (acuerdos, instrucciones).
  - Supervisa ejecución de tareas delegadas y/o asignadas.
  - Realiza seguimiento y evaluación del trabajo interno del Comité.

- **Estudio y Evaluación**

  - Levanta información permanente acerca de la crisis, su impacto y su desarrollo.

  - Genera reportería periódica para el Comité para la correcta toma de decisiones.

  - Utiliza información proporcionada por medios, encuestas, redes sociales, *stakeholders* públicos y privados, así como visitas a terreno.

  - Se coordina con encargado de comunicaciones del Comité para el monitoreo de medios tanto nacionales como internacionales.

- **Comunicación**

  - Ejerce la vocería (salvo que esta recaiga en el Director del Comité).

  - Elabora estrategia comunicacional y la propone al Director o Coordinador: qué se va a decir, cuándo, a quién, a través de qué medios.

  - Prepara y tiene a mano información actualizada para ser utilizada en conferencias de prensa, en fichas informativas y en declaraciones tanto externas como internas (empleados).

  - Mantiene relación con medios.

  - Elabora y actualiza listado de medios y puntos de contacto.

  - Se coordina con evaluación y estudios para el monitoreo de medios tanto nacionales como internacionales.

- **Tecnología y Comunicaciones**

  - Asegura y vela por el óptimo y continuo funcionamiento y operación de sistemas informáticos y de comunicaciones.

- **Finanzas**

  - Identifica los recursos disponibles propios como también externos (financieros, equipamiento, humanos, etc.).

  - Gestiona la disponibilidad, asignación y gestión de recursos.

  - Controla el uso de recursos.

- **Respuesta externa**

  - Coordina y supervisa respuesta operativa (cuando corresponda), trabajo que se puede realizar autónomamente por parte del organismo que conforma el Comité o con bien con el apoyo y asistencia de otras entidades (salud, seguridad, transporte, etc.).

  - Coordina su trabajo con encargado de enlaces, cuando fuere procedente.

- **Legal**

  - Analiza escenarios e implicancias legales de la crisis.

  - Proporciona información técnico-jurídica para una mejor toma de decisiones del Comité.

- **Registro**

  - Lleva un registro detallado de todas las acciones del Comité (decisiones y acuerdos adoptados, instrucciones formuladas, presentación de informes y estudios, piezas comunicacionales, seguimiento de ejecución de tareas, entre otros).

- **Enlaces**

  - Mantiene relación con otros enlaces o con entidades o personas externas al Comité.[44]

  - Coordina su trabajo con encargado de operaciones, cuando fuere procedente.

  - La cantidad de enlaces dependerá del tipo de crisis, su envergadura, la extensión y complejidad de las entidades o personas involucradas, sean estas contrapartes o afectados.

    * *Público*. Mantiene relación coordinada con *stakeholders* del Estado, embajadas, consulados y organismos internacionales.

    * *Privado*. Mantiene relación con *stakeholders* privados y las ONG.

[44] El o los enlaces se vinculan con toda otra entidad externa al Comité, con excepción de los medios de comunicación. Para la coordinación con los medios se recomienda contar con una persona especialmente designada para ello, que tendrá por esa como su única función.

- *Personas*. Mantiene relación con víctimas y afectados (atención a entidades afectadas, personas víctimas y familiares).
- *Interno*. Mantiene relación con estructuras internas (áreas de trabajo y personal).

- **Asesores externos según especialidad**

  • Dependiendo del tipo de crisis, su envergadura, duración, especificidad y complejidad, podrán convocarse de manera permanente o esporádica asesores externos que puedan apoyar en temáticas concretas como seguridad pública, salud, protección civil, imagen pública y medios, etc.

- **Stakeholders y otras entidades externas**

  • Con el fin de facilitar la coordinación de aspectos puntuales, o para obtener información más detallada, es recomendable considerar que en ciertas sesiones se convoque a determinados *stakeholders*, públicos o privados, nacionales o internacionales.

* Infraestructura

El Comité debe funcionar en un espacio físico que proporcione condiciones ideales de trabajo. Para ello, en la etapa previa a una crisis, deberá contemplarse el lugar en el que el Comité podrá operar, así como los recursos mínimos necesarios con los que deberá contar.

Junto con la definición del lugar y recursos, es importante asegurar que estos estén disponibles al momento que sea convocado el Comité. Dentro de los elementos a considerar se sugiere:

- **Espacio físico**

  • Una sala principal de crisis para trabajo grupal que tenga capacidad para reunir al Comité ampliado (20 personas mínimo).

  • Dos salas de trabajo grupal para reuniones que aborden temas específicos tanto entre los integrantes del Comité como entre estos y entidades externas.

  • Sala de prensa o lugar habilitado para emitir declaraciones a la prensa.

  • Una sala para trabajo individual que permita que aquellos integrantes del Comité que no participen de una sesión de este puedan trabajar óptimamente en una zona cercana al lugar en el que opera el Comité.

- **Estacionamiento**

  • Facilidad de acceso y estacionamiento seguro y disponible para ser usado por parte de los integrantes del Comité.

- **Recursos Financieros**

  • Disponibilidad de fondos para alimentación y gastos varios de menor envergadura y que permiten asegurar y facilitar la operación del Comité.

- **Equipamiento**

  • Equipos de comunicación (radio, telefonía celular, telefonía satelital, telefonía o comunicación IP, entre otros).

  • Equipos de trabajo e insumos (cuadernos, impresoras, hojas, lápices, pizarra, plumones, proyector, telón de proyección, entre otros).

  • Equipos de iluminación de emergencia y generadores de electricidad.

  • Mobiliario adecuado para el trabajo (mesas, sillas, etc.).

- **Comunicación**

  • Líneas de comunicación operativas (telefonía, internet, etc.).

- **Servicios básicos**

  • Operación óptima de agua, luz, calefacción, entre otros.

- **Seguridad**

  • Personal de seguridad que controle el acceso al lugar en el que opera el Comité y que brinde protección en caso de ser necesario.

* Designación de integrantes del Comité

Es necesario designar a personas concretas en cada uno de los cargos individualizados para el Comité, aun cuando este no se convoque. A estas personas se deberá capacitar de manera primordial (ver siguiente punto).

Cada vez que una de estas personas es cambiada de posición, debe designarse a una nueva en su remplazo, de manera tal que en todo momento se cuente con un catastro y listado actualizado de las personas que forman parte del Comité, aun cuando nunca lleguen a integrarlo operativamente.

* Capacitación, simulaciones y simulacros.

Es importante diseñar y contar con un plan de capacitación dirigido a todos los actores vinculados a una potencial crisis, tanto en relación con aquellos que integrarían el Comité como aquellos que pudieran verse afectados por los efectos dañinos de la situación. El contenido de la capacitación debe preparar a los destinatarios en el conocimiento de esta Guía y de todos aquellos elementos que pudieran complementarla (ejemplo: cómo manejar una crisis comunicacional).

El plan de capacitación debe ejecutarse periódicamente cuando menos una vez al año, aunque es recomendable que se ejecute cada seis meses. Dada la rotación de personal que pudiera existir entre las personas que integrarían el Comité, es necesario velar por que la capacitación se imparta tanto a nivel grupal como también individualmente a cada una de las personas que asumen funciones vinculadas a la operación del Comité.

En complemento a la realización de capacitaciones, es recomendable realizar de manera periódica simulaciones y simulacros. Las primeras son ejercicios de mesa que construyen escenarios ficticios y evalúan conocimientos y capacidades de respuesta tomando en cuenta solamente variables teóricas. Los simulacros, en cambio, van un paso más allá, y agregan una variable operativa.

En efecto, en conjunto con ejercicios de mesa, los participantes de un simulacro concurren a terreno y validan empíricamente algunas de las variables más críticas. Los actores de la actividad saben que son parte de una situación hipotética y se les pide mostrar operativamente sus capacidades.

Es mediante un simulacro que podemos determinar que una ambulancia, que teóricamente se demoraría 15 minutos en llegar a un lugar, en realidad lo hace en 25 minutos cuando el traslado es un lunes de 8 a 9 horas de la mañana. De igual manera, cuando consideramos el uso teórico de trajes *hazmat* para protección química, radiológica o biológica, o trajes antiexplosivos, solo un ejercicio práctico permitirá saber que en condiciones ambientales de 30° C una persona no puede ocupar ese traje por más de 20 minutos, y que el proceso de postura y sacado del mismo toma otros 20 minutos.

Una última herramienta de formación y entrenamiento son los llamados *testeos* o *simulacros reservados*. Se trata de simulacros en los cuales solo un grupo muy reducido de personas sabe que se trata de un ejercicio. Aun cuando representan la mejor forma de aprender, pues testean la real capacidad de respuesta sin que el operario sepa que es parte de una actividad de formación y entrenamiento, los desafíos para gestionar exitosamente esta iniciativa sin causar alarma pública son enromes. Esta forma de entrenar se recomienda solo para aquellas entidades o grupos que ya han realizado exitosamente varias simulaciones y simulacros previos.

Durante una crisis (B)

* Activación del Comité

El comité se convoca:

- **Por Indicación.**
  - Por disponerlo así el Director o Coordinador.

- **Automáticamente.**
  - Por la ocurrencia de determinados hechos que han sido previamente determinados con ocasión del levantamiento de riesgos (ver apartado A3).

Tal como se indicó en el apartado A3, es importante tener presente que los hechos que motivan la activación del Comité podrían tratarse solamente de amenazas que aún no se han concretado o bien estar en presencia de hechos que ya ocurrieron o que están sucediendo (terremoto, ataque terrorista, etc.).

* Operación del Comité

La operación del Comité, los temas a tratar, el enfoque con el que se abordan, la periodicidad de las reuniones ampliadas y sectoriales, así como la intensidad y frecuencia de los comunicados dependerán de la forma en la que se desarrolla cada una de las crisis.

Así, en situaciones de terremoto, tsunami, atentado terrorista consumado, en las que la emergencia mayor ya ocurrió, es probable que las reuniones iniciales se presenten de manera muy concentrada para luego dar paso a convocatorias semanales con el fin de dar seguimiento. Por el contrario, escenarios de duración larga o indeterminada como es una crisis económica, convulsión social, problemas estructurales de seguridad pública o una epidemia es bastante probable que distribuyan su actuación en un período más largo de tiempo.

En uno y otro caso, la primera actuación que debe realizar el Comité es: a) realizar una convocatoria amplia de todos sus integrantes; b) designar a un vocero; y, c) realizar un primer catastro tanto por sus propios medios como a través de los enlaces con el fin de dimensionar el impacto y tipo de crisis a la cual que se está enfrentando, la envergadura del daño producido y la cantidad de afectados, entre otras variables.

Con el mérito de esta primera evaluación, que se irá ajustando en función de las evaluaciones posteriores, el Comité adoptará todas aquellas decisiones que, estando a su alcance, tengan por fin disminuir los efectos de la crisis tanto en su duración como en el nivel de daño producido. Para ello: a) desplegará acciones coordinadas a través de cada una de sus áreas (finanzas, operaciones, legal, comunicaciones, etc.); b) definirá y comenzará a ejecutar una política comunicacional; c) acotará y precisará aún más los mensajes comunicacionales previamente elaborados; d) establecerá las entidades con las que se relacionarán los enlaces (gobierno, privados, embajadas, etc.), así como los objetivos y metas de estas coordinaciones externas; e) definirá el cronograma inicial de reuniones así como su duración; f) establecerá la disponibilidad de recursos para afrontar la crisis; g) acotará los integrantes que deban participar de las respectivas sesiones velando por integrar tanto al sector público como representantes del sector privado vinculado a la crisis particular que se esté abordando; entre otras.

Después de la crisis (C)

La crisis no termina con la crisis. Una vez que los hechos más graves han comenzado a dar paso a la calma, es importante trabajar en dos ámbitos:

* Recuperación

- Trabajar coordinadamente en otros actores en diseñar, implementar y apoyar planes de recuperación, tanto a nivel operativo y financiero como mediático. Siempre basado en la verdad, la transparencia y la honestidad, es muy importante recuperar la imagen y percepción de seguridad.

- La recuperación tiene una triple dimensión: a) garantizar el acceso libre, tranquilo, limpio y seguro, y la circulación de las personas y las organizaciones; b) reestablecer y optimizar las capacidades operativas del sector público y privado afectados; c) recuperar la paz social y las confianzas institucionales público-privadas.

* Evaluación

- **Es importante medir dos aspectos:**

  - La crisis en sí. ¿Por qué se produjo? ¿Pudo haberse evitado o anticipado de mejor manera? ¿Qué impacto produjo? ¿Cómo podemos aprender para enfrentar de mejor manera la próxima?, etc.

  - El manejo de la crisis. ¿Cómo se manejó la crisis? ¿Cómo operó el Comité? ¿Cuáles fueron los mejores aciertos y los peores errores? ¿Estuvimos preparados? Si se repitieran los hechos ¿qué habríamos hecho distinto?, etc.

Implementación (D)

Resulta importante designar a una persona o a un equipo que esté a cargo de la implementación de estas recomendaciones vinculadas a la conformación y gestión de un mecanismo de gestión de crisis en seguridad pública. Una conformación o representatividad público-privada generará mayores beneficios. Son estos quienes deberán velar por que se ejecuten cada una de las acciones previas a la crisis (sección A), y que se realicen las evaluaciones después de la misma (sección C de este capítulo).

Lo más importante

En este capítulo se analiza la importancia de los Comités de Crisis de Seguridad y las Alianzas Público-Privadas para enfrentar situaciones críticas en la seguridad de la población. Los principales puntos por resaltar son:

1. La estructura del capítulo abarca tres etapas temporales: antes, durante y después de una crisis, con acciones y medidas clave en cada etapa.
2. Entre las acciones previas a la crisis se incluyen el análisis de riesgos, la elaboración de planes de respuesta, la comunicación y la formación del Comité de Crisis.
3. Durante una crisis, es crucial la activación y operación del comité y la toma de decisiones efectivas y coordinadas.
4. Después de una crisis, es fundamental la recuperación y evaluación para aprender de la experiencia y mejorar en el futuro.
5. La designación de un equipo encargado de implementar las recomendaciones asegura la ejecución efectiva de las acciones y evaluaciones.

La conformación y gestión de un mecanismo de gestión de crisis en seguridad pública con representatividad público-privada es esencial para proteger a la comunidad y la actividad económica.

ALIANZAS PÚBLICO - PRIVADAS

Una aproximación a la gestión de riesgos para confrontar las amenazas a la seguridad

OEA Más derechos para más gente

unicri United Nations Interregional Crime and Justice Research Institute