

TNTD/SPMU serie de publicación vol. 13

# Guía de la OSCE sobre actividad policial basada en la inteligencia



Viena, junio de 2017

© OSCE 2017

Todos los derechos reservados. El contenido de esta publicación puede ser utilizado y copiado libremente para fines educativos y otros fines no comerciales, siempre que junto a su reproducción se haga constar a la OSCE como fuente.

ISBN 978-3-903128-04-0

Secretaría OSCE

Departamento de Amenazas Transnacionales

Unidad de Asuntos Policiales de carácter  
estratégico

Wallnerstrasse 6

A-1010 Viena, Austria

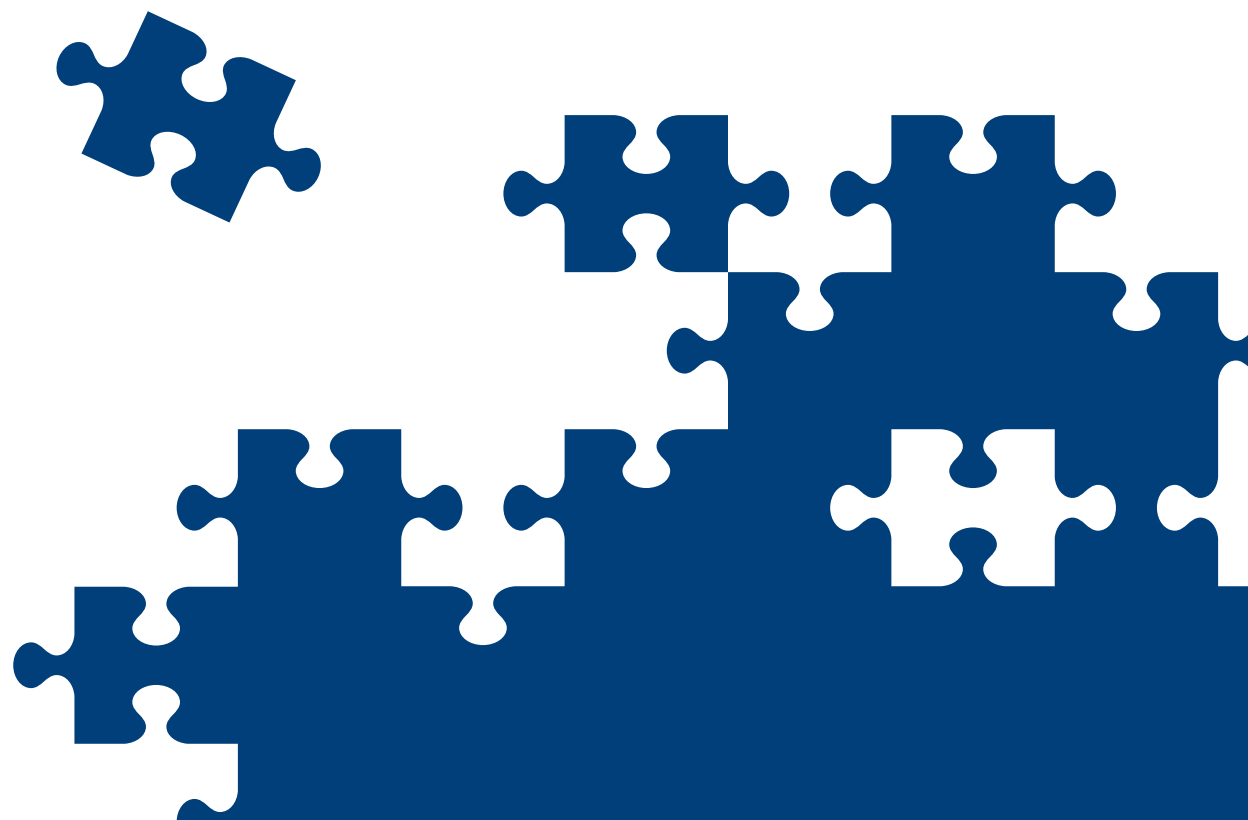
Tel: +43-1 514 36 6942

E-mail: [spmu@osce.org](mailto:spmu@osce.org)

[osce.org/secretariat/policing](http://osce.org/secretariat/policing)

[polis.osce.org](http://polis.osce.org)

# Guía de la OSCE sobre actividad policial basada en la inteligencia



# Índice

<b>Prólogo</b>	<b>4</b>
<b>Resumen ejecutivo</b>	<b>8</b>
<b>Agradecimientos</b>	<b>10</b>
<b>Introducción</b>	<b>12</b>
<b>1. Modelos contemporáneos de actividad policial</b>	<b>18</b>
<b>2. Información, conocimiento e inteligencia</b>	<b>20</b>
<b>3. Definición de la actividad policial basada en la inteligencia</b>	<b>22</b>
<b>4. Ventajas de la actividad policial basada en la inteligencia</b>	<b>26</b>
<b>5. Consideraciones legales, derechos humanos y protección de datos</b>	<b>30</b>
<b>6. El proceso de inteligencia criminal</b>	<b>38</b>
6.1 Asignación de tareas y planificación	40
6.2 Recopilación y evaluación	42
6.3 Cotejo y procesamiento	44
6.4 Análisis	45
6.5 Notificación y difusión de los productos de inteligencia	48
6.6 Información de retorno y seguimiento	50
<b>7. Puesta en práctica de la ILP</b>	<b>52</b>
7.1 El modelo de ILP de la OSCE	53
7.2 Retos y requisitos fundamentales para la puesta en práctica	57
7.3 Análisis y toma de decisiones en materia de aplicación de la ley	62
7.4 Niveles de los mecanismos de inteligencia criminal	63
7.4.1 Mecanismo de inteligencia criminal de nivel local/ de comisarías	63

7.4.2	Mecanismo de inteligencia criminal de nivel regional	64
7.4.3	Mecanismo de inteligencia criminal de nivel central	65
7.5	Reuniones de asignación de tareas y coordinación	66
7.5.1	Reuniones de asignación de tareas estratégicas y coordinación	66
7.5.2	Reuniones de asignación de tareas operativas y coordinación	67
7.6	Capacitación y concienciación	67
<b>8.</b>	<b>La ILP en la práctica</b>	<b>70</b>
8.1	ILP, evaluaciones de amenazas y planificación estratégica en la lucha contra la delincuencia organizada	70
8.1.1	El ciclo de actuación de la UE	71
8.1.2	La herramienta Sleipnir de evaluación de la delincuencia organizada	77
8.2	Ejemplos de aplicación nacional de la ILP	79
8.2.1	Modelo Nacional de Inteligencia del Reino Unido	80
8.2.2	Renania del Norte-Westfalia (Alemania): elaboración de políticas y planificación estratégica	85
8.2.3	Suecia: estructuras organizativas y decisorias de la ILP	88
8.2.4	República de Serbia: estructuras operativas y de inteligencia de la ILP	94
8.2.5	Montenegro: evaluaciones de la amenaza de la delincuencia grave y organizada	96
8.3	La ILP y la actividad policial de proximidad	102
8.4	La ILP en la prevención y lucha contra el terrorismo y el VERLT	106
	<b>Referencias</b>	<b>110</b>

# Prólogo

Las actividades relacionadas con la policía son un elemento clave de los esfuerzos de la OSCE para reforzar la seguridad y la estabilidad en su área geográfica, y constituyen un aspecto importante de la contribución de la Organización al refuerzo de las iniciativas de los Estados participantes para hacer frente a las amenazas que plantea la actividad delictiva. Desde 1999, las actividades relacionadas con la policía han sido uno de los componentes básicos de las iniciativas de la OSCE en los ámbitos de prevención de conflictos, gestión de crisis y rehabilitación posconflicto.

De conformidad con su mandato, la OSCE se esfuerza constantemente por ayudar a sus Estados participantes a ampliar sus competencias, mejorar la eficacia de sus sistemas de justicia penal e incrementar las capacidades de sus servicios policiales y de aplicación de la ley. La evolución de las amenazas transnacionales, el continuo cambio de los patrones delictivos y la demanda creciente de servicios policiales, exigen una renovación constante de estrategias, prioridades, planes y métodos. La Guía de la OSCE sobre actividad policial basada en la inteligencia es un paso importante para que la Organización pueda hacer frente a esos retos.

Esta guía presenta la actividad policial basada en la inteligencia (ILP)\* como un modelo moderno y proactivo para velar por el cumplimiento de la ley, y como una alternativa realista a las formas reactivas tradicionales de actividad policial para los Estados participantes de la OSCE. La ILP, que ya ha sido adoptada en algunos países en los últimos años, con resultados prometedores, combina la recopilación, la evaluación y el análisis de la inteligencia con procedimientos y mecanismos decisorios fundamentados, facilitando así una gestión más eficiente y eficaz de la aplicación de la ley a nivel nacional.

---

\* Acrónimo en inglés de *intelligence-led policing*, que se utilizará en adelante en la presente guía.

La investigación ha revelado que la ILP tiene un gran potencial como modelo moderno para velar por el cumplimiento de la ley, pero su éxito depende en gran medida de requisitos concretos que se detallan en la guía. El apoyo político y una gestión directiva concienciada y comprometida son algunos de los requisitos previos esenciales.

Quiero expresar mi agradecimiento a los más de 30 expertos en aplicación de la ley de los Estados participantes de la OSCE, del mundo académico, de organizaciones internacionales y de las operaciones de la OSCE sobre el terreno que, con sus valiosas aportaciones y su labor de revisión de borradores, han ayudado a la Unidad de Asuntos Policiales de Carácter Estratégico del Departamento de Amenazas Transnacionales de la OSCE a elaborar la presente guía. También quiero dar las gracias a nuestros colegas de la Oficina de Instituciones Democráticas y Derechos Humanos de la Organización por compartir su experiencia en materia de derechos humanos y protección de datos, que son importantes para la ILP y para su aplicación.

Las Presidencias alemana (2016) y austríaca (2017) de la OSCE han respaldado con firmeza la iniciativa de la ILP en el marco de la Organización. La publicación de la presente guía no habría sido posible sin su apoyo.

**Lamberto Zannier**

*Secretario General de la OSCE*

Actualmente, la labor de velar por el cumplimiento de la ley se enfrenta a problemas más complejos que nunca. Al mismo tiempo, ha aumentado considerablemente la demanda ciudadana de una mayor efectividad, eficiencia y responsabilidad policiales. La actividad policial basada en la inteligencia (ILP), desarrollada en los últimos años, es una respuesta a esas crecientes dificultades. El modelo no solo aporta un enfoque moderno para identificar y planificar medidas correctivas para combatir el incremento de amenazas transnacionales como el terrorismo y la delincuencia organizada, sino que también puede aplicarse a la planificación y la gestión policiales proactivas cotidianas. En una época de medidas de austeridad y restricciones presupuestarias, la ILP facilita la gestión de la aplicación de la ley con métodos y herramientas para la identificación de prioridades y la correspondiente asignación de los recursos.

La presente guía aborda la ILP desde cuatro perspectivas principales. En primer lugar, define la ILP y los fundamentos para promover el modelo como un enfoque contemporáneo del cumplimiento de la ley aplicable a toda el área de la OSCE. En segundo lugar, abarca los importantes aspectos de los derechos humanos y la protección de datos a la hora de aplicar la ILP. En tercer lugar, aborda el análisis de los datos y la información, que se traduce en la utilización de productos de inteligencia estratégica y operativa como base de un proceso decisorio fundamentado y documentado. En cuarto y último lugar, la guía introduce recomendaciones prácticas de estructuras organizativas nacionales, regionales y locales, así como normas mínimas necesarias para departamentos de inteligencia criminal y mecanismos decisorios.

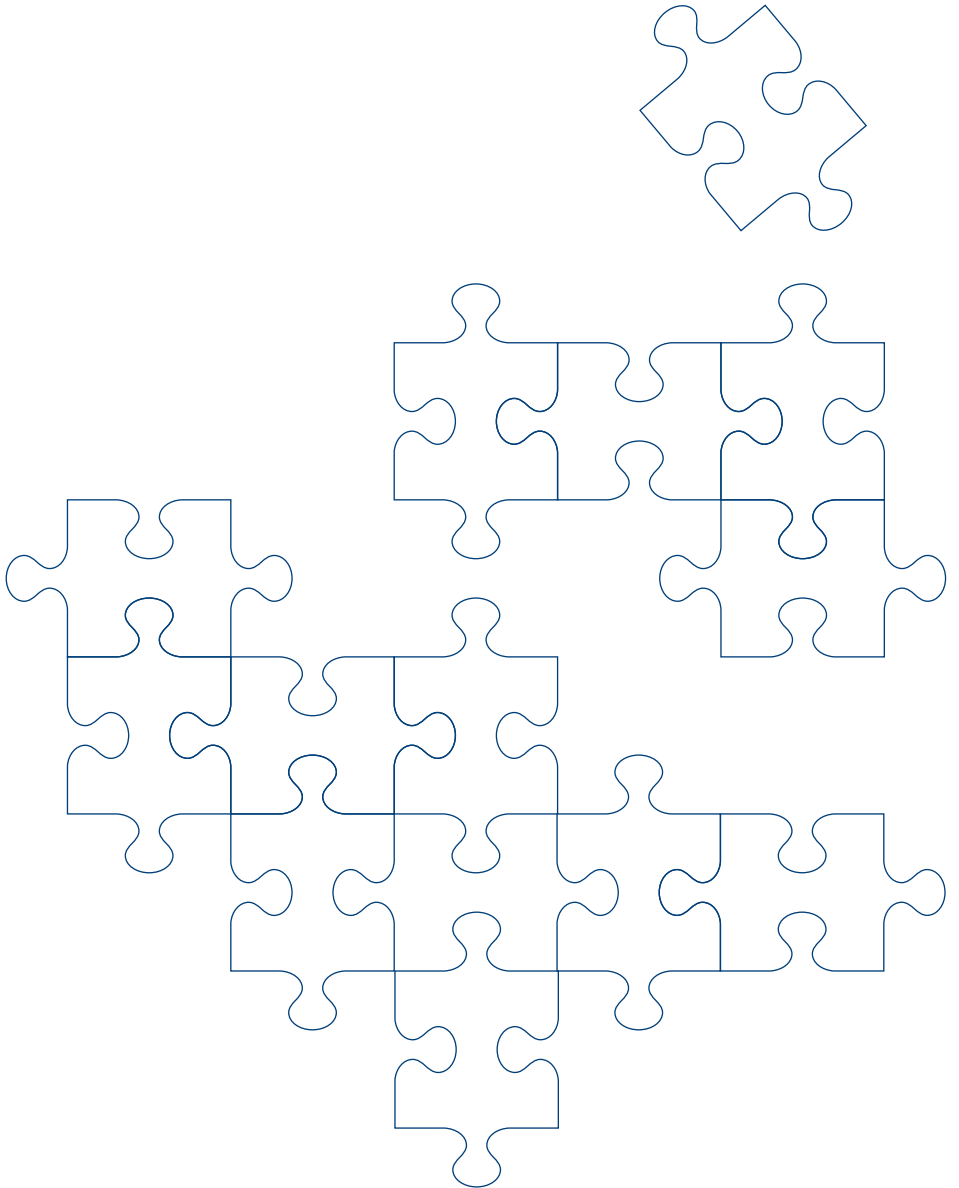
La ILP considera el análisis de la inteligencia criminal como un elemento esencial de la aplicación de la ley. También establece una relación más estrecha entre el análisis criminal y el proceso decisorio que otros modelos de actividad policial contemporáneos, exigiendo nuevas aptitudes y competencias a los gestores y analistas de dicho cumplimiento.

El objetivo principal de la presente guía es proporcionar a los Estados participantes de la OSCE herramientas para reforzar la profesionalidad de sus encargados del cumplimiento de la ley, mejorar la calidad y la eficacia de sus actividades, y optimizar la gestión de sus recursos, lo que dará como resultado un incremento de la confianza de los ciudadanos y unas medidas más concretas contra las amenazas para la seguridad y la protección públicas.

### **Rasa Ostrauskaite**

*Coordinadora de las Actividades de Lucha  
contra las Amenazas Transnacionales,  
Secretaría de la OSCE*





## Resumen ejecutivo

La actividad policial basada en la inteligencia (ILP) es un enfoque moderno de la labor de velar por el cumplimiento de la ley. Introducida por primera vez en el Reino Unido en el decenio de 1990, se ha utilizado principalmente para combatir la delincuencia grave y organizada. Los prometedores resultados obtenidos en los últimos años han animado a los encargados de dicho cumplimiento a ampliar la metodología proactiva basada en la inteligencia a todos los ámbitos de la gestión policial, como un modelo de actividad integral. La ILP se centra en la recopilación y la evaluación sistemáticas de datos e información, a través de un proceso analítico definido que los convierte en productos analíticos estratégicos y operativos que sirven de base para un proceso decisorio mejorado, fundamentado y documentado.

Actualmente, dos de los principales retos para la labor encaminada al cumplimiento de la ley son la complejidad creciente y la naturaleza transnacional del delito, así como el incremento de la demanda ciudadana de una mayor eficiencia financiera, es decir, “hacer más por menos”. El modelo de ILP aborda esos retos enfatizando e implantando la priorización basada en la inteligencia, seguida por una asignación de tareas y recursos disponibles que estén en consonancia con las prioridades definidas.

Al esbozar mecanismos de inteligencia criminal, procedimientos decisorios y estructuras organizativas claros y definidos, a niveles local, regional y nacional, la presente guía no se limita a presentar el modelo conceptual de ILP sino que también brinda herramientas prácticas para su aplicación. Estas incluyen prácticas policiales cotidianas, planificación estratégica proactiva y planes de acción operativos, así como instrumentos para combatir la delincuencia grave y organizada. Además, explica cómo la ILP puede ser un excelente complemento de la actividad policial de proximidad y, al mismo tiempo, proporcionar también una herramienta eficaz en la lucha contra el terrorismo, y el extremismo violento y la radicalización que conducen al terrorismo (VERLT).

La ILP da más importancia al análisis de la inteligencia criminal que otros modelos de actividad policial contemporáneos. Eso requiere aptitudes analíticas y competencias ampliadas, y a veces innovadoras, en el ámbito del cumplimiento de la ley. El enfoque proactivo y prospectivo de la ILP se basa también en que los encargados de dicho cumplimiento sepan cómo trabajar con analistas y cómo utilizar los resultados analíticos en sus procesos de planificación y adopción de decisiones. Así pues, al adoptar y aplicar la ILP se debe prestar especial atención a la preparación y la formación del personal directivo y de gestión de nivel medio y superior que se ocupa del cumplimiento de la ley.

La investigación ha revelado que si se quiere aplicar la ILP aprovechando todo su potencial, es esencial contar con un respaldo político y una gestión de nivel medio y superior concienciada y comprometida. En la guía se exponen además otras condiciones previas importantes para el éxito de la aplicación de la ILP, que son las siguientes: un enfoque interinstitucional de la aplicación de la ley; mecanismos claros de asignación de tareas; transformación de la mentalidad de la “necesidad de saber” en la de la “necesidad de compartir”; presencia de canales de comunicación de tecnologías de la información (TI) para la presentación de información; bases de datos analíticas y analistas expertos; y estructuras organizativas pertinentes que respalden la ILP.

Para que la ILP funcione con eficacia, la información de retorno sobre los productos de inteligencia y la evaluación de dichos productos, así como el control constante de la gestión y la calidad del modelo, tienen una importancia fundamental y deben estar integrados en sus prácticas.

En la presente guía se insiste en la absoluta obligación de todos los que se ocupan del cumplimiento de la ley de respetar los principios en materia de derechos humanos y protección de datos, y de atenerse a ellos a la hora de aplicar la ILP. La recopilación, el procesamiento y la utilización de datos e información deben cumplir estrictamente, en todo momento, las leyes nacionales y las normas internacionales en materia de derechos humanos. La ILP, con sus mecanismos de control interno y externo, y sus procedimientos decisorios transparentes y fundamentados, tiene como objetivo mejorar la responsabilidad de la gestión de la aplicación de la ley.

La presente guía proporciona un marco general para la ILP y su aplicación en toda el área de la OSCE. No se incluyen detalles técnicos sobre dicha aplicación, dejando así margen para que los Estados participantes de la OSCE adapten el modelo a sus respectivas necesidades y circunstancias, con arreglo a sus marcos jurídicos nacionales.

# Agradecimientos

El Departamento de Amenazas Transnacionales de la OSCE quiere agradecer a Arnar Jenson, Director de Proyecto de la presente guía, su contribución a la elaboración y la redacción de esta publicación. Un grupo de destacados expertos policiales, formado por representantes de Estados participantes de la OSCE, organizaciones regionales e internacionales pertinentes, organizaciones de investigación independientes y estructuras ejecutivas de la OSCE, han contribuido a la elaboración de la guía con aportaciones por escrito y participando en una reunión de expertos para revisar el borrador, que tuvo lugar en Viena y duró dos días. La Unidad de Asuntos Policiales de Carácter Estratégico del Departamento de Amenazas Transnacionales (SPMU/TNTD) reconoce y aprecia el valioso asesoramiento y las provechosas contribuciones aportadas al proceso de redacción de la guía por las siguientes personas:

Georgi Aladashvili, Jefe de Policía de Tiflis (Georgia)  
Roberto Arcieri, Jefe en funciones del Departamento de Estudios e Investigación,  
Oficina de Evaluación y Formación, Italia  
Leena Anonius, Asesora de Género, Sección de cuestiones de Género,  
Secretaría de la OSCE  
Pero Bozovic, Jefe del Departamento de Recopilación de Inteligencia e Información/  
Organismo Estatal de Protección e Investigación, Bosnia y Herzegovina  
Maryse Chureau, Analista estratégica/Equipo de Análisis Estratégico de la Europol,  
Europol  
Anders Danielsson, Oficial de asuntos policiales, SPMU/TNTD, Secretaría de la  
OSCE  
Lotta Ekvall, Asesora en cuestiones de género/Sección de cuestiones de Género,  
Secretaría de la OSCE  
Nino Gakharia, Jefe de la División de Integración Euroatlántica, Ministerio del  
Interior, Georgia  
John Gustavsson, Asesor Superior en delincuencia organizada, Misión de la OSCE en  
Kosovo  
Johannes Heiler, Asesor en cuestiones de lucha contra el terrorismo, Departamento de  
Derechos Humanos, OIDDH  
Jesús Hernández Álvarez, Analista, Policía Nacional, España  
Iris Hutter, Unidad de Análisis Criminal Estratégico y Operativo, Policía Criminal  
Federal, Austria  
Adrian James, Profesor titular de Investigación Criminal, Instituto de Estudios de  
Justicia Penal, Universidad de Portsmouth  
Erik Johansen, Asesor Policial, Capacidad Civil de Planeamiento y Ejecución, Servicio  
Europeo de Acción Exterior  
Ivan Jokić, Inspector Jefe/Departamento de Inteligencia Criminal, Dirección de  
Policía, Montenegro

Maxim Klepov, Ministerio del Interior, Federación de Rusia

Nenad Kostadinović, Jefe Adjunto del Departamento de ILP, Ministerio del Interior, República de Serbia

Dejan Lazaroski, Jefe de la Unidad de Inteligencia Estratégica, Departamento de Inteligencia y Análisis Criminal, Oficina de Seguridad Pública, ex República Yugoslava de Macedonia

Andrei Muntean, Oficial Superior de Programas, Oficina del Coordinador de las Actividades Económicas y Medioambientales de la OSCE, Secretaría de la OSCE

Susanna Naltakyan, Oficial nacional de Programas, Oficina de la OSCE en Ereván

Tarik Ndifi, Analista e Investigador, Centro para la Prevención de Conflictos, Secretaría de la OSCE

Marua O'Sullivan, Asesora Policial, Departamento de Seguridad Pública y Divulgación Comunitaria, Misión de la OSCE en Skopje

Seda Öz Yildiz, Directora, Instituto de Ciencias de la Seguridad, Academia de Policía, Turquía

Hans-Juergen Pechtl, Director Adjunto, Subdirección de Análisis Criminal, Secretaría General de la Interpol, Lyon (Francia)

Mark Reber, Asesor Policial Superior, Asociación Internacional de Jefes de Policía

Joerg Rosemann, Superintendente Jefe, Dirección de Investigación Penal, Autoridad Policial de Distrito de la región de Rheinisch Bergischer Kreis, Renania del Norte-Westfalia (Alemania)

Matej Seljak, Dirección de Policía Criminal, Dirección General de Policía, Eslovenia

Bjordi Shehu, Analista/Especialista, Dirección de Análisis e Información Criminal, Dirección General de Delincuencia Grave y Organizada, Policía Estatal, Albania

Simon Smith, Inspector Jefe, Oficina central de la actividad policial de lucha contra el terrorismo, Jefe de Prevent Delivery, Reino Unido

Thorsten Stodiek, Jefe Adjunto de la SPMU/TNTD, Secretaría de la OSCE

Marco Teixeira, Oficial de Programas, Sección de Apoyo a la Aplicación, Departamento de Delincuencia Organizada y Tráfico Ilícito, División para Asuntos de Tratados, UNODC

Adriana Tostón Díez, Capitán, Guardia Civil, España

Per Wadhed, Departamento de Operaciones Nacionales, Policía sueca

Dra. Ireen Winter, Jefa de la Unidad de Análisis Criminal Estratégico y Operativo, Policía Criminal Federal, Austria

Maica Wurmböck, Ayudante de Proyecto, SPMU/TNTD, Secretaría de la OSCE

# Introducción

## Antecedentes y fundamentos

Los modelos de aplicación de la ley reactivos, utilizados tradicionalmente, se han encontrado con grandes dificultades a la hora de hacer frente a los riesgos y las amenazas actuales, y de reaccionar ante las nuevas oportunidades delictivas propiciadas, entre otras cosas, por el incremento de la movilidad personal y la migración, los cambios rápidos en materia de tecnología y comunicaciones, la libre circulación de bienes y servicios, y la creciente desigualdad de los ingresos. El extremismo violento y la radicalización que conducen al terrorismo (VERLT), así como los atentados terroristas de los últimos años, han puesto de relieve la necesidad de compartir, conectar y analizar de forma centralizada los datos y la información pertinentes (inteligencia) obtenidos a todos los niveles, de conformidad con las leyes nacionales, las normas internacionales en materia de derechos humanos y los compromisos de la OSCE. La actividad policial basada en la inteligencia (ILP), desarrollada como respuesta a esos crecientes retos, al inspirar y facilitar la aplicación de un enfoque policial *proactivo* que complementa el modelo tradicional de actividad policial *reactiva*, ha demostrado ser una herramienta eficaz para combatir la delincuencia organizada, aprovechar mejor los recursos, e identificar y realizar tareas prioritarias de forma selectiva. El enfoque proactivo y prospectivo de la ILP facilita la prevención, la reducción, la represión y la desarticulación de la delincuencia. Un elemento clave de ese enfoque es la recopilación y el análisis sistemáticos de la información y los datos pertinentes para la prevención y la reducción de la delincuencia, seguida por la elaboración de informes de inteligencia. Sobre esa base se pueden adoptar decisiones administrativas y políticas fundamentadas y prospectivas, y asignar recursos para hacer frente a los problemas, amenazas, y tipos de delitos y delincuentes más preocupantes para la seguridad. La ILP también ha demostrado ser una herramienta efectiva y sostenible para combatir el terrorismo y el VERLT.

Basándose en su mandato de prestar ayuda a los Estados participantes para mejorar la profesionalidad y las capacidades, y respaldar la reforma y el desarrollo generales de la policía, especialmente elaborando documentos orientativos<sup>1</sup>, la Unidad de Asuntos Policiales de Carácter Estratégico del Departamento de Amenazas Transnacionales (SPMU/TNTD) ha elaborado la presente guía sobre *Actividad policial basada en la inteligencia*. En la redacción se han seguido las conclusiones de la Reunión anual de expertos policiales de 2016, celebrada en Viena los días 9 y 10 de junio de ese año, cuyo tema principal fue la ILP. Uno de los principales resultados y conclusiones de dicha reunión fue la necesidad de instaurar una definición común de la OSCE para el concepto de ILP y de elaborar una guía sobre ese tema para los Estados participantes de la Organización. La Presidencia alemana de la OSCE de 2016, la Presidencia austríaca de la OSCE de 2017 y el Secretario General de la OSCE han expresado claramente su gran interés en seguir promoviendo el concepto de ILP y su

---

1 Decisión N° 1049 del Consejo Permanente. "Marco estratégico de la OSCE para las actividades relacionadas con la policía" (PC. DEC/1049, Viena, 26 de julio de 2012).

aplicación, así como su firme apoyo al mismo, empezando por encargar a la SPMU/TNTD que redactara una guía de la OSCE sobre ese tema.

En la preparación y redacción de la presente guía se prestó especial atención a evitar la duplicación de esfuerzos y tomar como base la labor ya realizada sobre ese tema por autoridades nacionales de Estados participantes de la OSCE y por organizaciones regionales e internacionales. Por ese motivo, se recopiló material bibliográfico para su elaboración, con el permiso de los interesados. El material sobre ILP de la presente guía recoge la labor de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), del Departamento de Operaciones de Mantenimiento de la Paz de las Naciones Unidas (UNDPKO), de la Interpol, del Servicio de Acción Exterior de la Unión Europea y de la Europol, y se basa en esa labor.

Se recopilaron documentos jurídicos, instrucciones oficiales, manuales nacionales y otras contribuciones por escrito, relacionados con la ILP, de diversas autoridades nacionales de Estados participantes de la OSCE y operaciones de la OSCE sobre el terreno. La hoja informativa conjunta OSCE/UNODC sobre ILP, publicada en abril de 2016 para la Reunión anual de expertos policiales de la OSCE, sirvió de base para el modelo de ILP de la OSCE, que se expone en el subcapítulo 7.1, como el marco propuesto para aplicar el concepto de ILP en los Estados participantes de la Organización.

Se invitó a todos los Estados participantes y a todas las estructuras ejecutivas de la OSCE, así como a una serie de organizaciones regionales e internacionales, a que designaran expertos para que revisaran los borradores e hicieran aportaciones a la presente guía. Unos 30 expertos designados participaron en un curso práctico de revisión del borrador, de dos días de duración, celebrado en Viena en diciembre de 2016. De ellos, 15 participaron en el proceso de redacción de la presente guía.

El marco teórico del modelo de ILP de la OSCE recomendado en el subcapítulo 7.1 se basa en las investigaciones académicas del Profesor Jerry H. Ratcliffe, presentadas en 2016 en su libro *Intelligence-Led Policing*<sup>2</sup>. El Profesor Ratcliffe es el investigador citado con mayor frecuencia sobre ese tema. En la Reunión anual de expertos policiales de la OSCE de 2016, tres académicos de prestigio internacional presentaron y expusieron sus trabajos de investigación sobre temas relacionados con la ILP<sup>3</sup>. El Dr. Adrian James participó en el curso

---

2 Ratcliffe (2016).

3 Esos académicos son: el Dr. Adrian James, Profesor universitario e investigador del Instituto de Estudios de Justicia Penal de la Universidad de Portsmouth; la Dra. Elke Devroe, Profesora Asociada y Criminóloga del Instituto de Seguridad y Asuntos Globales de la Universidad de Leiden; y la Dra. Monica den Boer, Profesora Adjunta del Departamento de Seguridad y Criminología de la Universidad Macquarie de Sydney (Australia) y Directora de SeQure Research and Consultancy.

práctico de revisión del borrador, aportó su contribución por escrito y dio su punto de vista académico sobre el contenido a lo largo del proceso de redacción de la guía.

En el proceso de establecer una definición común de la OSCE para la ILP, hubo que superar problemas lingüísticos, porque el significado del término “inteligencia” no es el mismo en los distintos idiomas. Por ejemplo, la traducción del concepto de ILP del inglés al ruso puede generar cierta confusión. En ruso, el término *intelligence* significa normalmente datos e información reservada, en poder de los servicios de seguridad y de otros organismos autorizados, incluidas unidades policiales autorizadas (responsables), mientras que en inglés *intelligence* se refiere a todo tipo de datos e información analizados, elaborados por organismos que se ocupan del cumplimiento de la ley y a los que dichos organismos tienen acceso. Es importante tener en cuenta esas discrepancias lingüísticas a la hora de referirse a la ILP y señalar que, en la presente guía, el término *intelligence* tendrá este último significado, es decir, datos e información analizados.



## Objetivo y valor añadido

La ILP no es un tema nuevo en la OSCE. Algunas operaciones de la Organización sobre el terreno ya están ayudando a los Estados participantes a aplicar la ILP o algunos componentes del modelo. Aunque la aplicación parcial o total de la ILP en países de la región de la OSCE ha dado resultados positivos, parece que hay discrepancias en cuanto al significado, el enfoque y las formas de aplicar el concepto.

El objetivo de la presente guía es explicar y perfilar el marco y los principales componentes de la ILP, con el fin de lograr un entendimiento y una aplicación uniformes en el área de la OSCE. Su finalidad es servir de herramienta práctica para responsables políticos, encargados de tomar decisiones relativas al cumplimiento de la ley y analistas de delitos, en sus esfuerzos por mejorar la profesionalidad, la eficacia y la eficiencia de la policía. En la guía se expondrán algunos ejemplos reales de prácticas recomendadas para la aplicación de la ILP, basadas en experiencias de Estados participantes de la OSCE y de organizaciones internacionales, que pueden adaptarse a las circunstancias nacionales.

Aunque está dirigida especialmente a responsables de formular políticas, altos cargos y encargados del cumplimiento de la ley, la presente guía también puede ser útil para todas las instituciones que se ocupan de dicho cumplimiento y de actividades de formación, así como para universidades y círculos académicos.

Hay una bibliografía académica y teórica muy variada sobre ILP, así como un conjunto de material de orientación técnica sobre los distintos componentes del modelo de ILP, como por ejemplo los manuales de orientación técnica de la UNODC que figuran en el capítulo de referencia y algunos manuales nacionales. La presente guía incluye parte de ese material, respondiendo así a la necesidad de contar con una guía sobre el enfoque general de la ILP que pueda utilizarse como marco para todos los Estados participantes y Socios para la Cooperación de la OSCE. Abarca la ILP de forma integral, desde el marco teórico, mediante definiciones e introducción de conceptos clave y componentes esenciales del modelo, hasta una presentación práctica de la aplicación de la ILP, incluido análisis de información, evaluaciones de amenazas y estructuras decisorias y organizativas.

De conformidad con su concepto integral de la seguridad, la OSCE considera la protección de los derechos humanos, del Estado de derecho y de los principios democráticos, como un elemento integrante de la seguridad. Los Estados participantes han reconocido que la seguridad no puede

lograrse a expensas de los derechos humanos, sino que ambos son objetivos integradores que se refuerzan mutuamente. En consecuencia, las medidas de aplicación de la ley para hacer frente a las amenazas contra la seguridad solo pueden ser efectivas si respetan los derechos humanos. Por eso, uno de los capítulos se centra en las consideraciones legales y en los derechos humanos y la protección de datos, a fin de contribuir al debate sobre el concepto de ILP y su aplicación práctica en la presente guía.

## Estructura de la guía

Tras una breve introducción en el Capítulo 1 de los modelos más comunes de actividad policial, los Capítulos 2 y 3 se centran en aclarar y exponer definiciones de ILP y de algunos términos clave del concepto. El Capítulo 4 ofrece un breve resumen de las principales ventajas potenciales de la aplicación de la ILP en el cumplimiento de la ley en la actualidad. El Capítulo 5, redactado por la Oficina de Instituciones Democráticas y Derechos Humanos de la OSCE (OIDDH), destaca las cuestiones de los derechos humanos y la protección de datos que se aplican a la ILP. El proceso de inteligencia criminal, especialmente el análisis, es el pilar de la ILP y la base del marco decisorio expuesto en la presente guía. En el Capítulo 6 se explican los seis pasos tradicionales del ciclo de inteligencia y el modo de aplicarlos en el contexto de la ILP.

Después de exponer el modelo conceptual de ILP, los derechos humanos y la protección de datos, y el proceso de inteligencia criminal, el Capítulo 7 se centra en el funcionamiento y la aplicación práctica de la ILP, empezando por una presentación gráfica del modelo de ILP propuesto por la OSCE y una breve descripción de cada uno de sus principales componentes. A continuación hay un subcapítulo en el que se identifican algunos problemas y se introducen algunos requisitos esenciales para la aplicación. Puesto que el análisis y los informes de evaluación, así como otros productos de inteligencia criminal, son la base de la planificación estratégica y operativa, la presente guía insiste en subrayar la importancia de la relación entre el análisis y la adopción de decisiones. Por ello, hay un subcapítulo que trata exclusivamente de la adopción de decisiones en el marco de la ILP, al que le siguen los subcapítulos 7.4 y 7.5 sobre departamentos y mecanismos de inteligencia criminal, nacionales, regionales y locales, y sobre la estructuración propuesta para las reuniones de asignación de tareas y adopción de decisiones. En esos capítulos se hacen sugerencias claras acerca del modo de aplicar la ILP en la práctica a niveles nacional, regional y local, desde el punto de vista de los encargados del cumplimiento de la ley. El Capítulo 7 concluye con un breve resumen de los fundamentos de la formación para todos los niveles involucrados en la aplicación de la ILP.

En el Capítulo 8 y último de la guía, se exponen algunos ejemplos prácticos de aplicación de la ILP, empezando por la ILP para combatir la delincuencia grave y organizada, y se presentan dos metodologías de evaluación de amenazas ampliamente reconocidas, la Evaluación de la Amenaza de la Delincuencia Grave y Organizada (SOCTA) de la UE, y la herramienta Sleipnir para la evaluación de riesgos y amenazas. A continuación se hace una presentación de la ILP en cinco países: Reino Unido, Alemania (Renania del Norte-Westfalia), Suecia, República de Serbia y Montenegro. También se estudia el modo en que la ILP puede incrementar la eficacia y la eficiencia en otros dos ámbitos del cumplimiento de la ley, a saber, la actividad policial de proximidad y la lucha contra el terrorismo y el VERLT.

# 1. Modelos contemporáneos de actividad policial

Los investigadores y las publicaciones sobre la labor encaminada al cumplimiento de la ley suelen dividir las metodologías de dicha labor en cinco modelos de actividad policial: actividad policial tradicional, actividad policial de proximidad, actividad policial orientada a la resolución de problemas, actividad policial basada en estadísticas informatizadas e ILP. Cada uno de ellos tiene distintos objetivos estratégicos, y distintas ventajas e inconvenientes, y puede complementar a los demás cuando se utilizan de forma simultánea. Por ejemplo, la ILP se está aplicando cada vez más para reforzar la actividad policial de proximidad, ya que aporta procesos, estructuras de gestión y procedimientos de comunicación claros a la hora de recopilar, analizar y divulgar datos e información<sup>4</sup>. Otro ejemplo de ello es cuando el modelo reactivo tradicional es el predominante pero se aplica la ILP solo para combatir la delincuencia grave y organizada. Un factor común de los cuatro primeros modelos mencionados, que suele considerarse como un punto débil de la aplicación de la ley en la actualidad, es que centran su atención en áreas y amenazas locales.

Los rápidos e importantes cambios acaecidos a escala mundial han modificado el entorno delictivo y esas metodologías ya no poseen las cualidades necesarias para hacer frente a la gravísima amenaza de la delincuencia organizada transnacional. La actividad policial basada en la inteligencia es el único método que está en una situación inmejorable para combatir eficazmente ese tipo de delincuencia.<sup>5</sup>

**La actividad policial tradicional** es probablemente el modelo más conocido y sigue siendo el modelo habitual para garantizar el cumplimiento de la ley. Se trata de un estilo reactivo y de respuesta a incidentes en el que los agentes de policía responden a los delitos y a las solicitudes de servicio o de reacción. Respuesta a llamadas telefónicas, recepción de quejas, patrullaje aleatorio de las comunidades para que haya una presencia policial visible, e investigación de delitos que se han cometido o se estén cometiendo, son la esencia de la actividad policial tradicional. Mientras que este modelo considera que la labor de la policía consiste en reaccionar ante los problemas de seguridad y protección ciudadanas, la actividad policial de proximidad se centra en la asociación entre la policía y los ciudadanos para hacer frente de forma proactiva a los problemas de seguridad y protección.

---

4 Véase el subcapítulo 8.3 sobre ILP y actividad policial de proximidad.

5 Bell y Congram (2013: 19).

**La actividad policial de proximidad** tiene como objetivo fomentar la confianza e incrementar la comunicación entre la policía y los ciudadanos. Los programas de este tipo de actividad incluyen la creación de foros comunitarios en los que participan representantes de diversos grupos e instituciones comunitarios, y en los que se exponen y se debaten problemas relacionados con la seguridad, especialmente incidentes y novedades locales en materia delictiva.

En la **actividad policial orientada a la resolución de problemas**, la labor policial se centra básicamente en la identificación y el análisis del “problema”, en lugar de hacerlo en un delito, un caso, una llamada o un incidente. El modelo hace hincapié en el problema que origina el delito o las inquietudes en materia de seguridad. La policía tiene que diseñar por anticipado estrategias de prevención para tratar de resolver problemas, en lugar de limitarse a reaccionar ante sus consecuencias perjudiciales.

**El modelo de estadísticas informatizadas** (CompStat) es un sistema de gestión inspirado en “la teoría de las ventanas rotas”, en el que se trata de resolver delitos menores para reducir el número de delitos graves. Basándose en el análisis de estadísticas de delitos ya cometidos, los encargados locales del cumplimiento de la ley son responsables de llevar a cabo actividades a nivel local diseñadas en consecuencia.

## 2. Información, conocimiento e inteligencia

Antes de entrar en más detalles acerca de la ILP, hay que aclarar algunos conceptos esenciales. El término *inteligencia* tiene distintas definiciones, dependiendo del contexto, las culturas, los idiomas y las tradiciones. En la bibliografía examinada para redactar la presente guía, el uso que se hace del término indica que puede significar simultáneamente una metodología, una estructura, un proceso y un producto. En la revisión también se pusieron de manifiesto opiniones contradictorias y un entendimiento poco claro del significado de los conceptos *datos*, *información* y *conocimiento*.

“La falta de claridad y de un entendimiento común sobre la terminología y los procesos relativos a la inteligencia criminal entorpece el intercambio de información entre organismos”.

– **Asociación Internacional de Jefes de Policía (2002)**

De ahí que sea necesario abordar y aclarar el significado de esos conceptos. Tras estudiar los documentos publicados por la UNODC, el UNDPKO, la Interpol y la Unión Europea (UE), así como diversa bibliografía académica, la presente guía utiliza las siguientes definiciones de los términos mencionados, que gozan de aceptación general<sup>6</sup>:

Por *datos* se entenderá observaciones y medidas sin procesar y sin interpretar. Por ejemplo, aspectos de la actividad delictiva fácilmente cuantificables, tales como informes y otras estadísticas sobre delitos, bases de datos de delincuentes y tareas policiales.

Por *información* se entenderá datos puestos en contexto y dotados de significado, lo que les confiere una mayor importancia y un mayor sentido.

Por *conocimiento* se entenderá información que ha sido interpretada y comprendida. Cuando una persona ha añadido su sabiduría a la información, la convierte en conocimiento.

Por *inteligencia* se entenderá datos, información y conocimiento que han sido evaluados, analizados y presentados en un formato decisorio, con miras a la adopción de medidas.

---

<sup>6</sup> Las definiciones de “datos”, “información”, “conocimiento” e “inteligencia” se basan en : Ratcliffe (2016: 70-74); UNODC, Criminal Intelligence – Manual for Analysts (Viena: Publicación de las Naciones Unidas), (2011a: 1); Interpol, “Análisis de información policial” Fact Sheet (2014); y Consejo de la Unión Europea, “Decisión Marco del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la UE”. Diario Oficial de la Unión Europea (2006/960/JHA, 18 de diciembre de 2006).

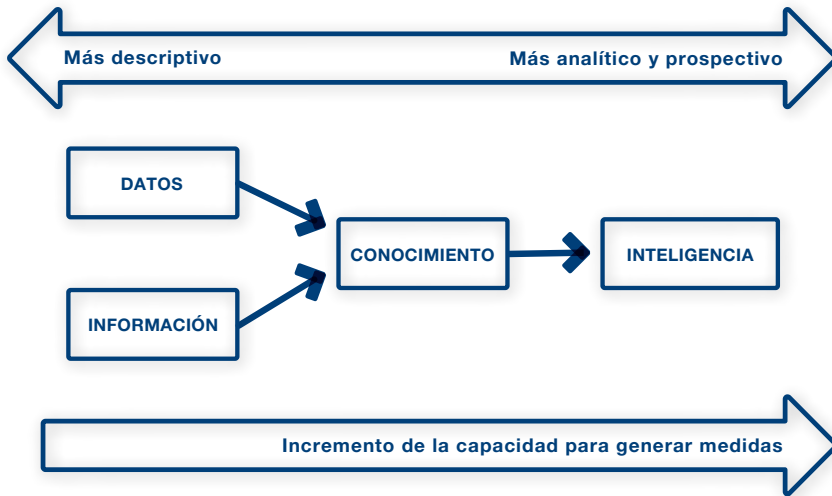


Figura 2.1 **De los datos a la inteligencia**

Fuente: *Ratcliffe* (2016: 72).

En una comisaría de policía local, los incidentes de robos en viviendas se introducen en la base de datos policial. Esos registros informáticos son **datos**. Cuando un analista de delitos accede a esos datos, los configura y reconoce una nueva pauta de robos en una zona, los datos se convierten en **información**. Básicamente, se ha dotado a los datos sin procesar del significado suficiente para poder reconocer una pauta. Si a continuación el analista trata y comparte esa información con un inspector, la comprensión y las ideas de ambos la convierten en **conocimiento**. Tras recopilar y analizar nuevos datos e información, el inspector y el analista podrán hacerse una idea general, que indudablemente tendrá sus fallos pero que tiene el suficiente fundamento para respaldar hipótesis y entrañar consecuencias. El analista y el inspector redactan un informe de análisis operativo e informan a su superior. Este decide investigar e iniciar una operación de vigilancia para localizar a los ladrones, basándose en la **inteligencia** aportada por ambos.

Nota: Un ejemplo simplificado y reformulado de *Ratcliffe* (2016: 73-74).

# 3. Definición de la actividad policial basada en la inteligencia

Al igual que ocurre con los conceptos expuestos en el Capítulo 2, hay ideas distintas y a veces contradictorias sobre el modo de definir la ILP. Algunos creen que consiste en hacer evaluaciones de amenazas, mientras que para otros se trata de un proceso de recopilación de datos e información. Esos puntos de vista aportan contribuciones y componentes valiosos al marco de la ILP pero no abarcan la totalidad del concepto. Es comprensible que haya distintas interpretaciones porque el concepto de ILP es relativamente nuevo<sup>7</sup> y está evolucionando. Hasta hace muy poco, la ILP se utilizaba principalmente en relación con la delincuencia organizada y los delincuentes peligrosos. La experiencia positiva ha convencido a profesionales y académicos de que hay que crear un marco de ILP más integrador, que incorpore todas las actividades policiales, por ejemplo, un modelo de proceso con una infraestructura organizativa que respalde el modo en que se lleva a cabo la actividad policial en general. Esa evolución ha hecho que el análisis se convierta en el centro de todos los ámbitos de actividad policial y que se haga más hincapié en la estrecha colaboración entre analistas y encargados de tomar decisiones relativas al cumplimiento de la ley, lo que requiere que estos últimos conozcan el potencial del análisis y el modo de utilizar sus resultados. Así pues, la actividad policial proactiva integrada en la ILP exige nuevas aptitudes y competencias por parte de analistas, responsables de la formulación de políticas, encargados del cumplimiento de la ley y otros entes decisorios. Este importante tema se desarrollará más adelante en el Capítulo 7. Aunque la presente guía alienta la aplicación proactiva de la ILP en todos los ámbitos posibles de la actividad policial, la mayoría de los países que ya la están utilizando han limitado su aplicación operativa a la delincuencia grave y organizada, a los delincuentes reincidentes, a los puntos conflictivos y a los delitos que suelen preocupar a los ciudadanos.

“La actividad policial basada en la inteligencia hace hincapié en el análisis y la inteligencia como ejes centrales de un marco decisorio objetivo que priorice los puntos conflictivos, las víctimas reiteradas, los delincuentes reincidentes y los grupos delictivos. Este facilita la reducción, la restricción y la prevención de los delitos y los perjuicios causados, mediante una gestión, un despliegue y una aplicación tácticos y estratégicos”.

– Ratcliffe (2016: 66).

---

7 El Ministerio del Interior del Reino Unido fue el primero en introducir el concepto de actividad policial basada en la inteligencia, en 1993, pero la primera en hacerlo operativo fue la Policía de Kent. Después del 11-S, los servicios de seguridad de los Estados Unidos adoptaron la ILP como metodología para combatir el terrorismo. Para más información, véase Peterson (2005).



Por ILP se entiende un marco de gestión para la inteligencia criminal y la labor policial operativa planificada, en el que la inteligencia es la base para definir prioridades y objetivos operativos y estratégicos en la prevención y represión del delito y otras amenazas para la seguridad. También incluye la adopción de decisiones adecuadas sobre medidas y actuaciones policiales operativas, la utilización racional de los recursos humanos disponibles y la asignación de recursos materiales y técnicos.<sup>8</sup>

Aunque la ILP supone un desafío para la actividad policial tradicional dominante, reactiva y basada en la respuesta, su adopción y el hecho de que las actividades encaminadas a garantizar el cumplimiento de la ley se hayan alineado con el pensamiento, la priorización y la planificación proactivos, no van a cambiar la realidad de que la policía siempre tendrá que ser reactiva ante los incidentes de seguridad y los delitos cometidos. En una estructura organizativa donde la información importante se recopila, se comparte y se analiza de forma sistemática, en el marco de una estrategia, unas prioridades y unos objetivos definidos, la ILP está diseñada para ayudar a los encargados de hacer cumplir la ley a adoptar decisiones fundamentadas y con base empírica, no solo en su labor de priorización estratégica sino también en su planificación operativa cotidiana. En ese sentido, la ILP complementa la actividad policial tradicional reactiva.

La ILP es un modelo decisorio y de gestión descendente, aunque en este caso la comunicación y el intercambio de información funcionan en ambos sentidos. Por el contrario, la actividad policial de proximidad tiene el típico enfoque ascendente, encaminado a mejorar la confianza entre la policía y los ciudadanos.

“La actividad policial basada en la inteligencia es una forma de combatir el delito que se guía por la recopilación y el análisis efectivos de inteligencia, y que tiene el potencial suficiente para convertirse en la innovación más importante en materia de cumplimiento de la ley en el siglo XXI”.

– Kelling y Bratton (2006: 5).

---

8 Ministerio del Interior de la República de Serbia, Handbook on the police intelligence model (2016: 16).

El modelo 4-i (*intención, interpretación, influencia e impacto*) es útil para explicar las funciones y la relación entre los componentes clave del concepto de ILP, que son: el entorno delictivo, el analista de inteligencia criminal y el responsable policial de la adopción de decisiones. Si se quiere que la ILP desarrolle todo su potencial, los cuatro componentes “i” deben estar operativos y funcionar adecuadamente. El modelo hace hincapié en la relación entre el análisis criminal y los encargados de adoptar decisiones. Estos últimos (gestores) asignan tareas, dirigen, asesoran y orientan a los analistas de inteligencia criminal. En primer lugar, los encargados de adoptar decisiones tienen que asegurarse de que sus *intenciones* se han explicado y comprendido correctamente. En segundo lugar, los analistas se encargan de la *interpretación* del entorno delictivo, y en tercer lugar ejercen *influencia* sobre los encargados de adoptar decisiones mediante los resultados de sus análisis. Basándose en esos resultados, los encargados de adoptar decisiones (cuarto paso) causan un *impacto* sobre el entorno delictivo mediante una gestión estratégica, planes de acción, investigaciones y operaciones, según se muestra en la figura 3.1.<sup>9</sup>

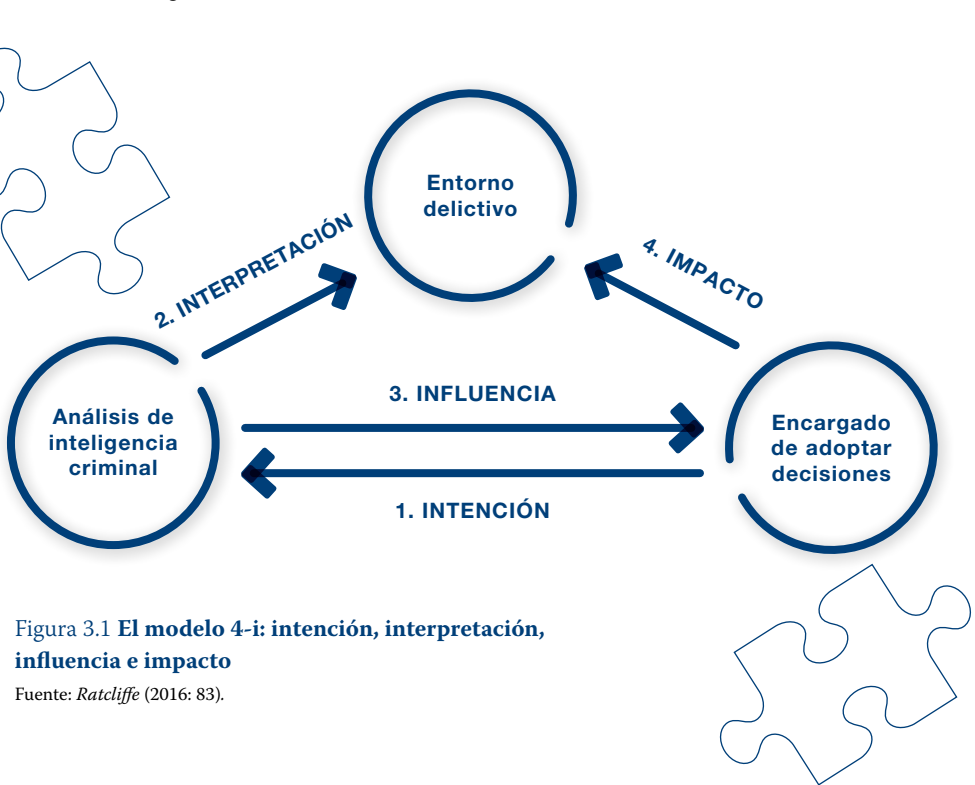
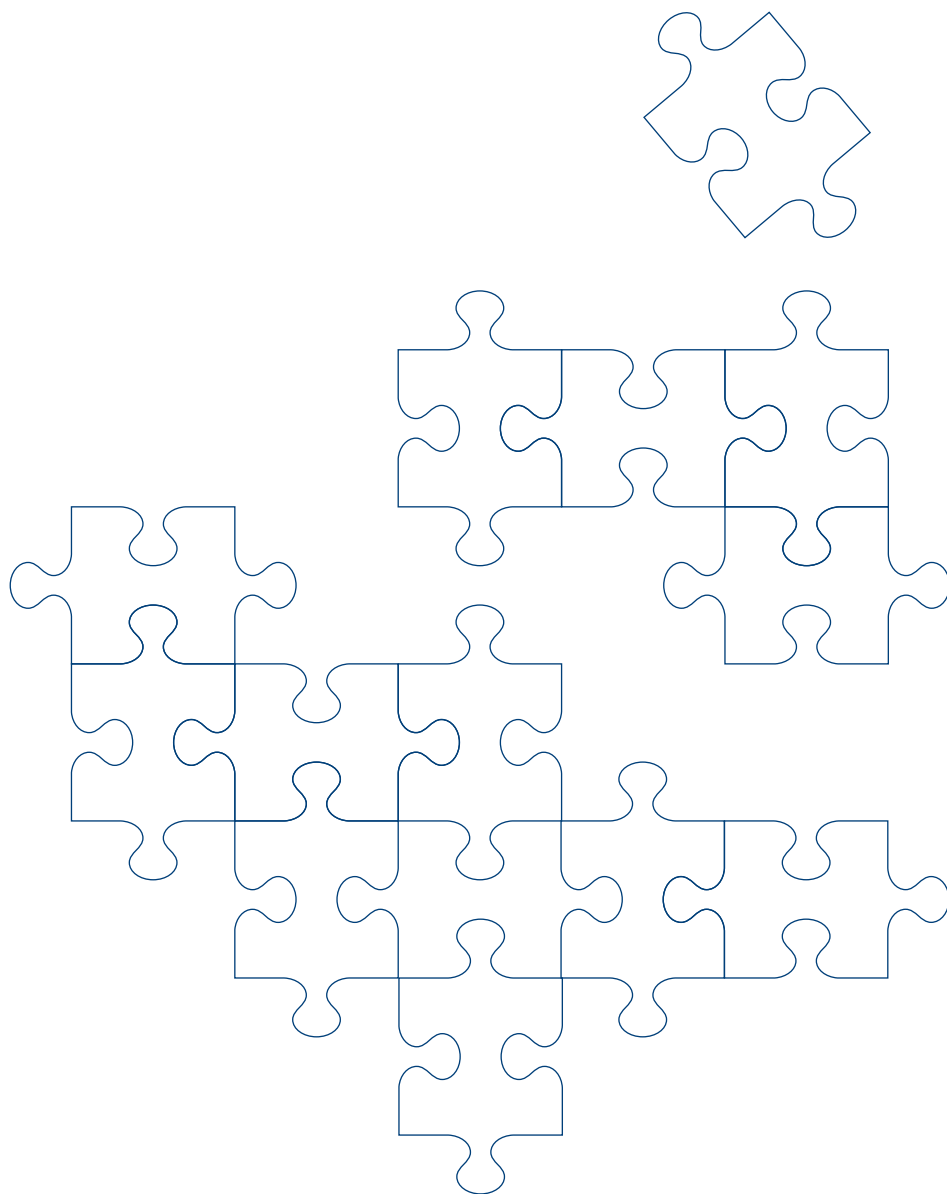


Figura 3.1 El modelo 4-i: intención, interpretación, influencia e impacto

Fuente: Ratcliffe (2016: 83).

<sup>9</sup> En su material de orientación técnica, la UNODC ha subrayado la función esencial del analista y de los productos del análisis en el proceso decisorio. Véase el modelo de asignación de tareas presentado en la UNODC (2011b: 5).



## 4. Ventajas de la actividad policial basada en la inteligencia

En la empresa privada y en la comunidad empresarial, la información y la inteligencia son factores esenciales para crear ventajas competitivas. En ese aspecto, la labor encaminada al cumplimiento de la ley no es diferente, puesto que la ventaja estratégica basada en la información, el conocimiento y la inteligencia incrementa su eficacia para prevenir delitos e incidentes relacionados con la seguridad, y desarticular redes y grupos delictivos. Pero no basta con poseer información, conocimiento e inteligencia. Es necesario tener un marco o un modelo adecuado para gestionar esa inteligencia y aprovecharla al máximo, así como para asegurar que los datos y la información son recopilados, procesados y utilizados en estricto cumplimiento de las leyes nacionales y las normas internacionales en materia de derechos humanos.

La ILP permite adoptar un enfoque prospectivo y proactivo de la gestión policial. El éxito de su aplicación en los últimos años en algunos países de todo el mundo para hacer frente a los delitos graves y las amenazas transnacionales, ha impulsado la aplicación de este concepto, que ha pasado de utilizarse principalmente en la lucha contra la delincuencia organizada a convertirse en un modelo de actividad estratégico, más general, para resolver una amplia variedad de problemas policiales a nivel local, regional y nacional. Ese avance está directamente relacionado con la búsqueda de métodos para garantizar el cumplimiento de la ley que permitan a la policía tener una mayor repercusión en la delincuencia, en su evolución y en el perjuicio social que ocasiona, contando con recursos limitados y en momentos en que hay una mayor demanda de responsabilidad.

En los últimos años, la demanda de respuesta y servicios policiales ha sobrepasado la disponibilidad de recursos de la policía, obligando a establecer prioridades y a incrementar la eficiencia de los recursos destinados al cumplimiento de la ley. Al mismo tiempo, han aumentado las expectativas políticas y ciudadanas en cuanto a la exigencia de responsabilidades. La ILP se ha presentado como una opción para resolver esas cuestiones, puesto que posee el fundamento y las herramientas precisas para analizar y evaluar las amenazas para los ciudadanos, y posibilita procedimientos decisorios más documentados, transparentes y responsables para asignar los recursos existentes donde son más necesarios.

“La necesidad de introducir la actividad policial basada en la inteligencia (ILP) no debe ponerse en duda. En épocas de restricciones presupuestarias y de recursos, toda persona y organización responsables han de establecer prioridades para resolver los problemas más acuciantes. Para ayudar a establecer prioridades, se han de adoptar decisiones basadas en los hechos y en la inteligencia, que a su vez se basan en la información. La ILP contribuirá a optimizar la asignación de recursos y a concentrar los esfuerzos de forma más estructurada. Eso ayuda a hacer frente al incremento de la sofisticación y la agilidad operativa de los delincuentes para socavar la ley y el orden”.

– **Servicio Europeo de Acción Exterior (2013: 12).**

El hecho de que extremistas violentos relacionados con los recientes atentados terroristas, incluidos los lobos solitarios, permanecieran en el radar de los encargados del cumplimiento de la ley ha exigido la aplicación de un enfoque proactivo y ha puesto de relieve la necesidad de un intercambio exhaustivo y un análisis centralizado de los datos y la información pertinentes. El reconocimiento de que un ataque terrorista y una detección temprana de otros incidentes graves no pueden resolverse de forma reactiva, coloca a la ILP en el foco de la escena internacional de la aplicación de la ley. Eso se hizo evidente después de los atentados del 11-S y quedó reflejado en las investigaciones de la Comisión del 11-S de los Estados Unidos, en las que se llegó a la conclusión de que antes de los atentados ya se disponía de ciertas informaciones a distintos niveles, pero los organismos fallaron a la hora de compartir esas informaciones y no lograron coordinarse para dar una visión global de la situación.

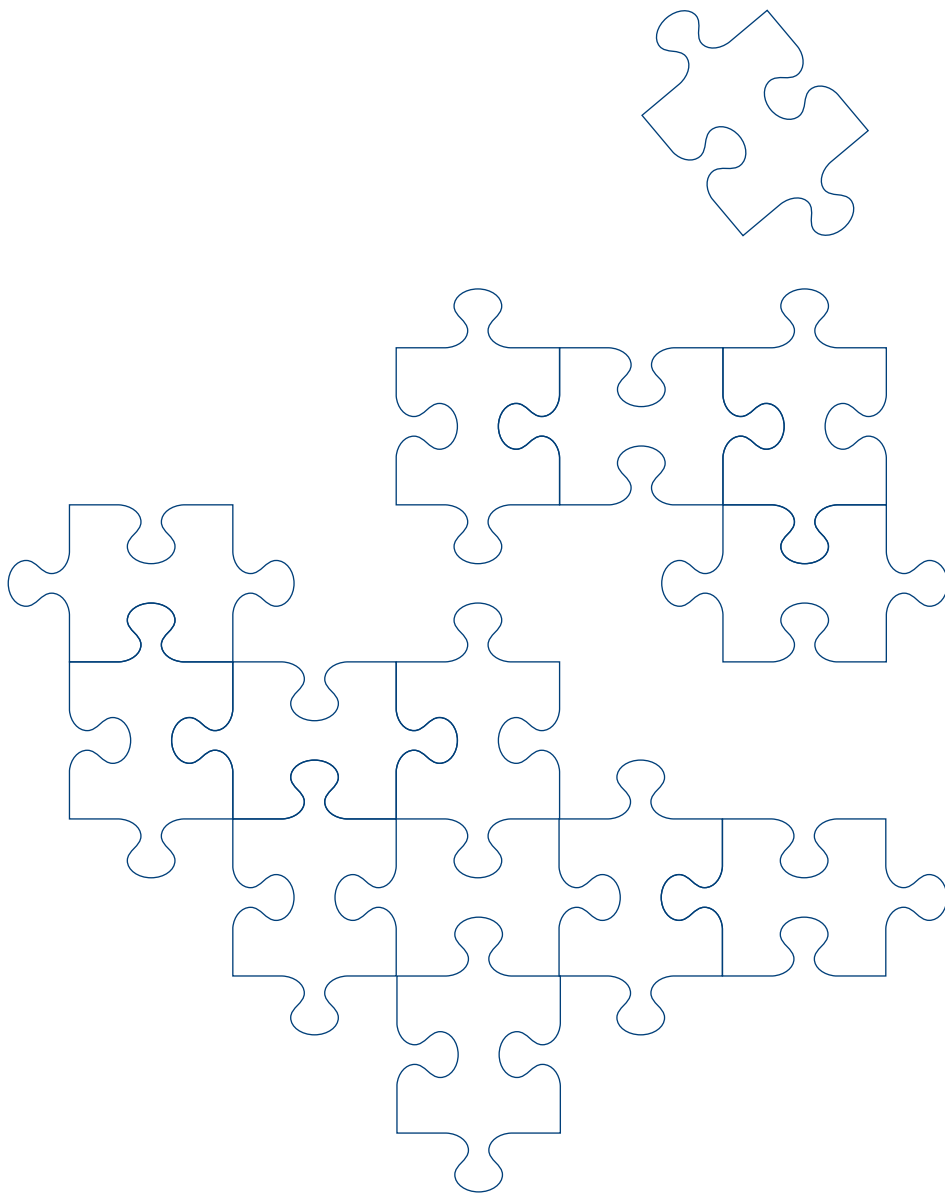
La identificación y la gestión de riesgos forman parte de la actividad policial moderna. El funcionamiento adecuado de la ILP en lo tocante a la recopilación y el análisis de datos e información permite identificar y evaluar riesgos, incluidos los relativos a eventos importantes, áreas geográficas, tipos de delito, perjuicio social, delincuentes peligrosos y redes delictivas.

“Los estudios sugieren que aunque, en general, incrementar el número de agentes de policía puede ser efectivo, es más útil tener en cuenta la forma en que son desplegados. El patrullaje aleatorio no es una táctica efectiva para reducir la delincuencia, otras tácticas más específicas, que tengan una base empírica (un componente fundamental de la actividad policial basada en la inteligencia) pueden ser más provechosas a la hora de prevenir la delincuencia que la cantidad de tiempo que los agentes dediquen presencialmente a un foco de delincuencia”.

– **Ratcliffe (2016: 139).**

El modelo de ILP incorpora estructuras organizativas y de gestión claras, incluidos mecanismos decisorios y de asignación de tareas a nivel local, regional y nacional, así como procesos definidos de comunicación y cooperación entre los encargados nacionales del cumplimiento de la ley y en el marco de la cooperación internacional.

La mejora de la gestión de los datos y la información es una ventaja importante de la ILP para la labor relacionada con el cumplimiento de la ley en la actualidad. En la era moderna de la circulación de la información, el modelo de ILP permite una recopilación orientada y selectiva de los datos y la información pertinentes, con arreglo a políticas, estrategias, objetivos y prioridades definidos.



# 5. Consideraciones legales, derechos humanos y protección de datos

El respeto de los derechos humanos es importante para la eficacia policial, tanto a corto como a largo plazo, y también para la ILP. Las medidas destinadas a garantizar el cumplimiento de la ley que no respetan ni protegen los derechos humanos son contraproducentes a largo plazo porque socavan la confianza de los ciudadanos en la policía y además son ineficaces. Por ejemplo, la elaboración de perfiles étnicos<sup>10</sup> es una práctica discriminatoria y ha demostrado su ineficacia porque puede ser fácilmente eludible. Los grupos delictivos pueden evitar ser detectados reclutando personas que no se ajusten a perfiles predeterminados. El empleo de técnicas alternativas y legítimas de elaboración de perfiles, basadas en pruebas concretas acerca del comportamiento delictivo y en inteligencia, en lugar de en suposiciones discriminatorias, puede ser una herramienta policial más efectiva.

## La ILP en el marco de los derechos humanos

Las normas de derechos humanos están establecidas en instrumentos jurídicos internacionales y normativas tipo tratados vinculantes, como por ejemplo el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH).<sup>11</sup> Para aplicar los derechos establecidos en esos tratados, los Estados deben instaurar un marco jurídico e institucional para el cumplimiento de las obligaciones en materia de derechos humanos a nivel nacional. Dentro de ese marco, una de las principales obligaciones de la policía es proteger a las personas de actos que pongan en peligro sus derechos humanos, incluidos los derivados de la delincuencia y el terrorismo, y respetar esos derechos. A la hora de combatir y prevenir el delito, la policía debe actuar de acuerdo con las leyes nacionales y las normas internacionales. La ILP, como forma proactiva de actividad policial, debe estar firmemente cimentada en el marco de los derechos humanos. También debe incrementar la protección de los derechos y las libertades de las personas, y llevarse a cabo de forma que respete plenamente esos derechos, lo que está en consonancia con los principios esenciales de la actividad policial democrática.<sup>12</sup>

---

10 La elaboración de perfiles étnicos, en lo que respecta a la actividad policial, significa que la policía ejerce su poder contra las personas basándose en estereotipos generales y suposiciones arbitrarias relacionadas con la nacionalidad, la etnia o la religión.

11 Todos los Estados participantes de la OSCE, excepto la Santa Sede, han ratificado el PIDCP y por tanto son partes del tratado. Además, 47 Estados participantes de la OSCE son también miembros del Consejo de Europa y por consiguiente partes del CEDH. Los Estados participantes de la OSCE han prometido cumplir sus obligaciones emanadas de los tratados internacionales de derechos humanos de los que forman parte, de conformidad con el derecho internacional. Véase Conferencia sobre la Seguridad y la Cooperación en Europa, *Acta Final* (1975).

12 OSCE (2008b).



## Principios generales de derechos humanos

Para garantizar que la ILP cumple las normas internacionales en materia de derechos humanos y no repercute negativamente en el disfrute de esos derechos, se deben cumplir algunos principios fundamentales a la hora de diseñarla y aplicarla a nivel nacional.

*El marco jurídico, administrativo e institucional para la aplicación de la ILP:* En primer lugar, la ILP debe basarse en disposiciones jurídicas y administrativas claras y precisas, que fijen las condiciones en las que se va a aplicar y proporcionen las garantías adecuadas para asegurar que no pone en peligro los derechos humanos. El marco nacional de la ILP debe incluir leyes y reglamentos que definan con claridad y precisión los poderes que se otorgan a los organismos pertinentes y los requisitos que se han de cumplir en la recopilación, el procesamiento, el análisis y el intercambio de los distintos tipos de información e inteligencia. Todas las leyes, reglamentos, políticas y prácticas nacionales relacionados con la ILP deben cumplir plenamente las normas internacionales de derechos humanos y los compromisos de la OSCE. Además, los funcionarios encargados del cumplimiento de la ley que participan en la ILP deben recibir la formación adecuada para aplicar esas leyes y reglas de conformidad con las normas internacionales de derechos humanos.

*Legalidad, necesidad y proporcionalidad de las limitaciones de los derechos humanos:* Aunque algunos derechos humanos, como por ejemplo la prohibición de la tortura y ciertos elementos del derecho a un juicio imparcial, son absolutos y no pueden restringirse en ningún caso, los tratados internacionales de derechos humanos permiten limitar determinados derechos, pero solo dentro de unos parámetros estrictamente definidos.<sup>13</sup> En consecuencia, las injerencias impuestas en relación con la ILP solo son permisibles si están estipuladas por la ley, si son necesarias en una sociedad democrática, en aras de un objetivo legítimo al que se hace referencia concreta en las normas internacionales de derechos humanos pertinentes, y si son proporcionadas para el logro de dicho objetivo: es decir, el derecho es la regla, la limitación debe ser la excepción y la injerencia siempre debe utilizar el medio menos invasivo para lograr el objetivo.

*Igualdad y no discriminación:* Los Estados participantes de la OSCE, con arreglo a sus obligaciones internacionales en materia de derechos humanos, garantizarán a todas las personas que se encuentren bajo su jurisdicción el goce de sus derechos humanos y libertades fundamentales, sin hacer distinción alguna por motivos de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.<sup>14</sup> Defender la igualdad ante la ley y prohibir la discriminación son deberes esenciales de la policía en una sociedad democrática.<sup>15</sup> Así pues, a la hora de recopilar, procesar y analizar la información y la inteligencia, los encargados de la aplicación de la ley deben abstenerse, por ejemplo, de elaborar perfiles discriminatorios.

13 Entre los derechos que podrían estar sujetos a limitaciones se incluyen la libertad de circulación, el derecho a la intimidad, la libertad de expresión, reunión y asociación, y la libertad de manifestar la propia religión o creencia.

14 OSCE (1989), *Documento de Clausura de la Reunión de Viena de 1986 de los representantes de los Estados participantes en la Conferencia sobre la Seguridad y la Cooperación en Europa, convocada sobre la base de las disposiciones del Acta Final relativas a la continuidad de la Conferencia.*

15 OSCE (2008b).

Igualmente, en lo que respecta al proceso decisorio basado en la inteligencia, las autoridades deben estar atentas para evitar el exceso de control policial de determinadas comunidades, que podría llegar a considerarse como discriminación. También se debe prestar especial atención a la diferente repercusión que ciertas decisiones estratégicas relacionadas con la actividad policial pueden tener en los hombres y las mujeres. Por ello, habría que incorporar en todas las actividades de la ILP un enfoque que tenga en cuenta la diversidad y la perspectiva de género, y revisarlo periódicamente para detectar cualquier repercusión discriminatoria que pueda tener en hombres o mujeres, o en determinadas comunidades.

*Recursos efectivos, supervisión y rendición de cuentas:* Las normas internacionales de derechos humanos estipulan el derecho de toda persona cuyos derechos o libertades hayan sido violados a disponer de un recurso efectivo, así como a interponer ese recurso y a que la autoridad competente judicial, administrativa o legislativa decida sobre el mismo.<sup>16</sup> Puesto que la ILP puede tener injerencias de gran alcance en una amplia gama de derechos humanos, es esencial contar con recursos efectivos y accesibles para las violaciones de esos derechos que puedan derivarse de su aplicación. También hay que crear mecanismos sólidos de supervisión externa e interna, a fin de asegurar que las instituciones y los responsables individuales del cumplimiento de la ley, que participan en la ILP, rindan cuentas. Dichos mecanismos podrían incluir el control y la supervisión de los comités de supervisión de la función ejecutiva y legislativa, así como mecanismos independientes de supervisión externa y de reclamación que proporcionen a los ciudadanos medios de reparación. El control judicial sobre actividades como la recopilación de inteligencia secreta es especialmente importante para proporcionar las garantías adecuadas contra los abusos en la aplicación de la ILP.

## El derecho a la intimidad

La recopilación de datos e información, al igual que su procesamiento, análisis e intercambio, que son elementos integrantes de la ILP, pueden tener graves repercusiones en la protección de los derechos humanos, en particular, aunque no únicamente, en el derecho a la intimidad.

El Artículo 17 del PIDCP estipula que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y que toda persona tiene derecho a la protección de la ley contra esas injerencias.<sup>17</sup> Para que las injerencias no sean “arbitrarias” o “ilegales” se han de cumplir una serie de requisitos similares a los mencionados anteriormente: tienen que haber sido establecidas por ley, que a su vez debe estar en consonancia con las disposiciones, los propósitos y los objetivos del Pacto, y ser razonables, en todo caso, en las circunstancias particulares del caso.<sup>18</sup> Los Estados participantes de la OSCE reconfirmaron el derecho a que se

---

16 Asamblea General de las Naciones Unidas, “Pacto Internacional de Derechos Civiles y Políticos (PIDCP).” Núm. 14668, *Series de Tratados de Naciones Unidas*, Vol. 999 (Nueva York: 16 de diciembre de 1966): Art. 2(3).

17 Una disposición similar sobre el derecho a que se respete la vida familiar y privada figura en el *Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales* (CEDH) (4 de noviembre de 1950): Art. 8.

18 Comité de Derechos Humanos de las Naciones Unidas, *HRC Observación general n° 16: Artículo 17 (Derecho a la intimidad), Derecho de toda persona a ser protegida respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como de ataques ilegales a su honra y su reputación [Derecho al respeto de la intimidad, la familia, el hogar y la correspondencia, y la protección del honor y la reputación]* (8 de abril de 1988).

garantice la protección de la vida familiar y privada, del domicilio, de la correspondencia y de las comunicaciones electrónicas, y la necesidad de evitar toda injerencia abusiva o arbitraria del Estado en la esfera personal del individuo.<sup>19</sup>

Los diferentes métodos abiertos y encubiertos de recopilación de información tienen diversos grados de injerencia en el derecho a la intimidad. Algunos de ellos, como por ejemplo el uso de técnicas de investigación especiales y otras tácticas de investigación encubierta, incluida la vigilancia en instalaciones privadas o en domicilios, la interceptación de comunicaciones, la utilización de agentes e informantes encubiertos, así como el acceso a las cuentas bancarias y otros tipos de información confidencial, se estudian con más detalle en el manual conjunto OIDDH/TNTD de la OSCE, *Human Rights in Counter-Terrorism investigations* (Los derechos humanos en las investigaciones relacionadas con la lucha contra el terrorismo)<sup>20</sup>. El control efectivo por parte de autoridades judiciales o de otras autoridades independientes, mediante autorización previa, supervisión o revisión ex post facto, es primordial para que esas medidas sean legales. Además, solo deberán utilizarse en casos graves y de forma proporcional a la gravedad del asunto que se esté investigando.<sup>21</sup>

Una cuestión a la que se ha prestado mucha atención son las consecuencias de la vigilancia masiva de las comunicaciones para el derecho a la intimidad. El Tribunal Europeo de Derechos Humanos dictaminó que los sistemas de vigilancia violan el derecho a la intimidad, permitiendo que se intercepten comunicaciones y multitud de datos de prácticamente cualquier persona de un país, incluso de las que son ajenas al ámbito inicial de una operación, cuando la solicitud de esas medidas tiene lugar enteramente en el ámbito del poder ejecutivo y no se ha evaluado si son estrictamente necesarias<sup>22</sup>. A diferencia de la vigilancia selectiva, que suele basarse en una sospecha previa y está sujeta a autorización judicial o ejecutiva previa, los programas de vigilancia masiva no permiten una evaluación previa de la proporcionalidad de las medidas empleadas en cada uno de los casos, y por tanto se podría considerar que socavan la verdadera esencia del derecho a la intimidad.<sup>23</sup>

## Protección de datos

La protección de datos es una parte importante del derecho a la vida privada y tiene especial importancia para la ILP. El Comité de Derechos Humanos de las Naciones Unidas, que es el órgano encargado de supervisar la aplicación del PIDCP, ha hecho hincapié en

19 OSCE, *Documento de la Reunión de Moscú de la Conferencia sobre la Dimensión Humana de la CSCE* (Moscú, 3 de octubre de 1991).

20 OSCE, OIDDH/TNTD (2013: 33-46). Para más información acerca de los aspectos jurídicos y técnicos de la vigilancia electrónica en particular, véase también UNODC, *Current practices in electronic surveillance in the investigation of serious and organized crime* (2009).

21 OIDDH/TNTD (OSCE) (2013).

22 Tribunal Europeo de Derechos Humanos. *Caso de Szabo y Vissy contra Hungría*. Demanda núm. 37138/14 (Estrasburgo: 12 de enero de 2016); y Tribunal Europeo de Derechos Humanos. *Caso de Roman Zakharov contra Rusia*. Demanda núm. 47143/06 (Estrasburgo: 4 de diciembre de 2015).

23 Asamblea General de las Naciones Unidas. "Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emmerson." Informe Anual presentado a la Asamblea General de las Naciones Unidas, 23 de septiembre de 2014, A/69/397: párrafo 52. Para más información acerca de la vigilancia digital masiva con fines de lucha contra el terrorismo, véase Asamblea General de las Naciones Unidas. "Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo." Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 21 de febrero de 2017, A/HRC/34/61: 10-13.

que la recopilación y el almacenamiento de información personal en ordenadores, bancos de datos y otros dispositivos, deben estar regulados por la ley. Además, los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por la ley para recibirla, tratarla y emplearla.<sup>24</sup> Algunos instrumentos internacionales y regionales contienen más principios concretos sobre protección de datos, que se han de acatar para garantizar el pleno respeto del derecho a la intimidad.

Por ejemplo, el *Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* exige que las partes del Convenio garanticen que los datos de carácter personal que sean objeto de un tratamiento automatizado:

- se obtendrán y tratarán legal y legítimamente;
- se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;
- serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
- serán exactos y si fuera necesario puestos al día;
- se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.<sup>25</sup>

Además, el Convenio prohíbe que los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud, a la vida sexual o a los antecedentes penales, se traten automáticamente, a menos que el derecho interno prevea garantías apropiadas.<sup>26</sup> También proporciona garantías complementarias para las personas concernidas.<sup>27</sup>

El Convenio establece excepciones y restricciones estrictas para esas disposiciones, similares a las mencionadas anteriormente. Toda excepción será posible si está prevista por la ley y constituye una medida necesaria en una sociedad democrática, en interés de una reclamación legítima enunciada en el Convenio, como por ejemplo la protección de la seguridad del Estado, de la seguridad pública, o para la represión de infracciones penales.<sup>28</sup> “Necesidad”, según se entiende en las normas internacionales de derechos humanos, significa proporcionalidad con respecto a la finalidad que se persigue.

---

24 Comité de Derechos Humanos de las Naciones Unidas (abril de 1988).

25 Consejo de Europa, *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, Serie de Tratados Europeos, N° 108 (Estrasburgo: 28 de enero de 1981): Art. 5. Los 47 Estados miembros del Consejo de Europa y, por consiguiente, una gran mayoría de Estados participantes de la OSCE son partes del Convenio.

26 *ibid.* Art. 6.

27 *ibid.* Art. 8.

28 *ibid.* Art. 9.

El manual conjunto OIDDH/TNTD (OSCE), titulado *Human Rights in Counter Terrorism Investigations* (Los derechos humanos en las investigaciones relacionadas con la lucha contra el terrorismo), proporciona un resumen de las mejores prácticas internacionales basadas en los principios mencionados anteriormente y en otras normas internacionales establecidas en ese ámbito<sup>29</sup>. Esos principios y normas también deberán orientar la labor de los encargados de la formulación de políticas y de los funcionarios que se ocupan del cumplimiento de la ley, a la hora de diseñar y aplicar la ILP, con el fin de asegurar el cumplimiento de las normas internacionales de derechos humanos.

## Otros posibles riesgos para los derechos humanos relacionados con la actividad policial basada en la inteligencia

El derecho a la intimidad, incluida la protección de datos, es esencial para el ejercicio de otros muchos tipos de derechos y libertades fundamentales, como por ejemplo: el derecho a la libertad de opinión y de expresión; la libertad para recabar, recibir y transmitir información; la libertad de reunión y asociación pacíficas; y la libertad de religión o creencia, entre otras. Pero la recopilación y la utilización de información e inteligencia también pueden afectar directamente al disfrute de otros derechos, como el derecho a un juicio imparcial, el derecho a la libertad y la seguridad personales, y la prohibición de la tortura y el maltrato.

Por ejemplo, en la actuación policial en manifestaciones públicas de protesta, el uso de la estrategia de control de multitudes conocida como “encapsulamiento” para recabar información, obligando a manifestantes pacíficos e incluso a transeúntes no vinculados a la protesta, a dar sus nombres y direcciones cuando abandonan el “cerco policial”, ha sido criticado por el efecto disuasorio que puede tener en el derecho de reunión pacífica<sup>30</sup>. Una detención basada en que la persona detenida figura en una base de datos de vigilancia de los organismos que se ocupan del cumplimiento de la ley, que no ofrece la protección adecuada contra injerencias arbitrarias en el derecho a la intimidad y que no se base en ninguna otra información que demuestre una sospecha razonable de que esa persona haya cometido o vaya a cometer un delito concreto, contraviene el derecho a la libertad y la seguridad.<sup>31</sup>

En lo relativo a la recopilación, el procesamiento, el análisis y el intercambio de información, incluso como parte de la ILP, también tiene especial importancia que el empleo en procesos judiciales de información obtenida mediante tortura está totalmente prohibido en virtud del derecho internacional. Su admisión como prueba en un tribunal viola el derecho a un

29 OIDDH/TNTD (OSCE) (2013): 30-31. Entre otros instrumentos pertinentes se puede citar la resolución 45/95 de la Asamblea General de las Naciones Unidas, sobre “Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales.” A/RES/45/95, 14 de diciembre de 1990.

30 Asamblea General de las Naciones Unidas. “Relator Especial sobre el derecho a la libertad de reunión pacífica y de asociación, Maina Kiai, Addendum, Misión al Reino Unido de Gran Bretaña e Irlanda del Norte.” Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 17 de junio de 2013, A/HRC/23/39/Add.1: párrafo 38.

31 Tribunal Europeo de Derechos Humanos. *Caso de Shimovolos contra Rusia*. Demanda núm. 30194/09 (Estrasburgo: 21 de junio de 2011).

proceso legal e imparcial.<sup>32</sup> Pero aun cuando no haya intención de utilizarla en procesos judiciales, recopilar, intercambiar y recibir información obtenida mediante tortura deberá estar prohibido.<sup>33</sup>

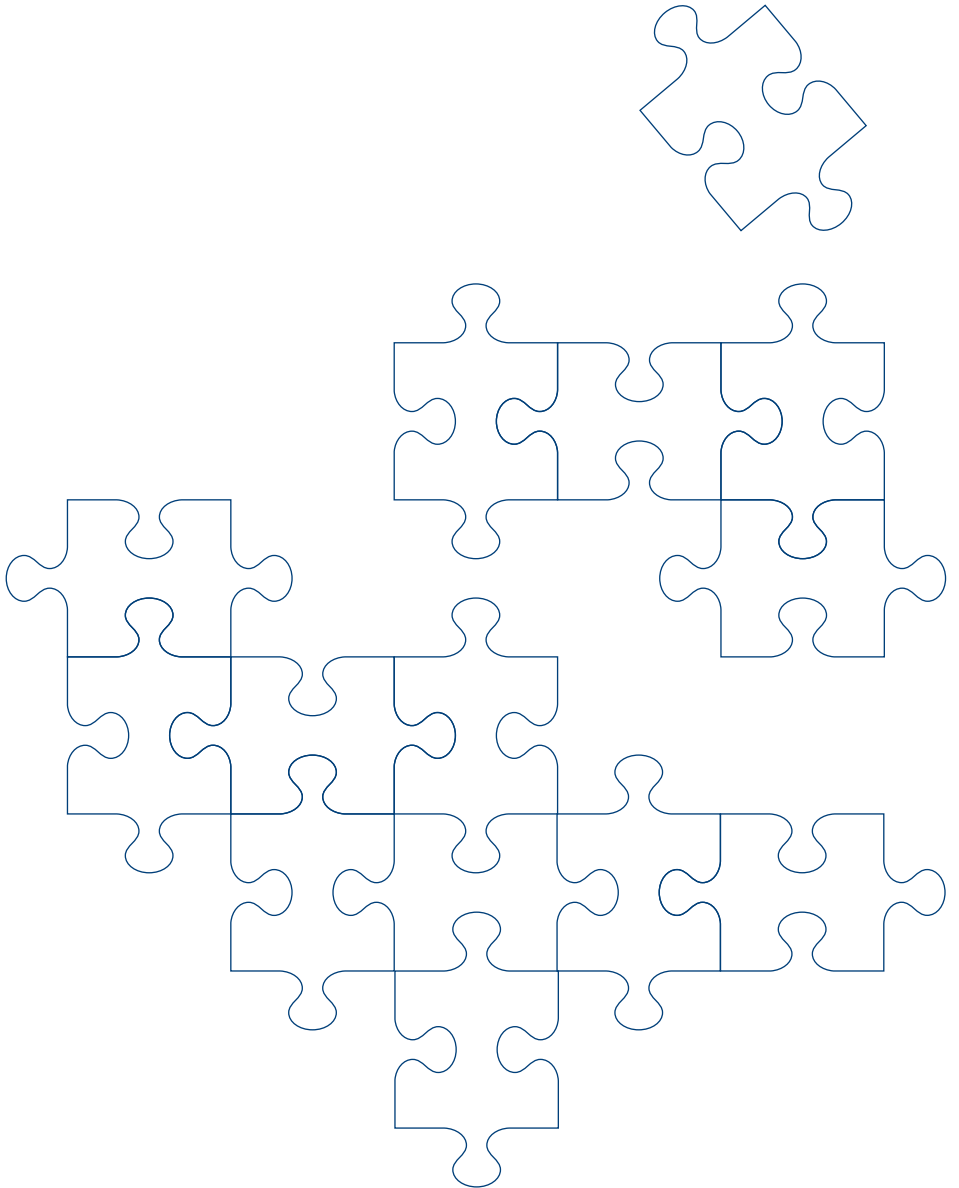
Esos problemas son especialmente importantes cuando se trata de intercambios de información e inteligencia transfronterizos. La utilización de información obtenida en otro país por medio de torturas, aunque se obtenga con fines únicamente operativos, puede convertir al Estado receptor en cómplice en la comisión de hechos internacionalmente ilícitos.<sup>34</sup> De ahí que, en la aplicación de la ILP, deberán establecerse las garantías adecuadas para velar por que no se utilicen información e inteligencia obtenidas por medios ilegales, ya sea dentro o fuera del país, en contravención de las leyes nacionales e internacionales.

---

32 Véase Asamblea General de las Naciones Unidas. "Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos y degradantes, Juan E. Méndez." Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 10 de abril de 2014, A/HRC/25/60: párrafo 21.

33 *ibid.*: párrafo 73. Véase también OSCE y OIDDH/TNTD (2013: 28).

34 *ibid.* Véase también Asamblea General de las Naciones Unidas. "Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin." Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 4 de febrero de 2009, A/HRC/10/3: párrafos 55-57; y OSCE, OIDDH/TNTD (2013: 28-29).





## 6. El proceso de inteligencia criminal

El proceso de inteligencia, conocido tradicionalmente como *ciclo de inteligencia*, describe y esboza seis pasos ampliamente reconocidos que se utilizan para transformar datos e información sin procesar en inteligencia con un valor añadido, orientada a la adopción de medidas. Lo mejor es que se inicie con una decisión o una asignación de tareas, seguida por una fase de planificación, tras la cual los analistas se dedican a recopilar datos e información que deben ser evaluados conforme a un sistema de evaluación oficialmente reconocido (véase página 35). El siguiente paso es la verdadera fase de procesamiento, que empieza por el cotejo y la estructuración de los datos e información disponibles, y su inserción en una base de datos. A continuación se analizan los datos y la información, lo que da como resultado un producto de inteligencia para su entrega al cliente (gestor, investigador, u otros, que han hecho el encargo a los analistas o han solicitado su ayuda) y a otros interesados pertinentes. El cliente evalúa el producto de inteligencia con relación a sus necesidades y exigencias. La información de retorno recibida se utiliza para mejorar el producto ya existente o como aportación metodológica para futuros productos similares.

El ciclo de inteligencia no es una secuencia estática de seis pasos, sino más bien un proceso dinámico en el que las diferentes fases están estrechamente vinculadas y se retroalimentan mutuamente, lo que obliga a los analistas a avanzar y retroceder en el ciclo. El ciclo esbozado en la figura 6.1 proporciona una estructura y un proceso ordenados y fáciles de comprender, que pueden utilizarse como proceso básico para el análisis tanto operativo como estratégico.<sup>35</sup>

---

<sup>35</sup> La UNODC ha publicado algunas directrices técnicas sobre la inteligencia criminal y el proceso de inteligencia, para agentes de policía de primera línea, funcionarios de inteligencia, analistas y encargados del cumplimiento de la ley. Véase [www.unodc.org](http://www.unodc.org).



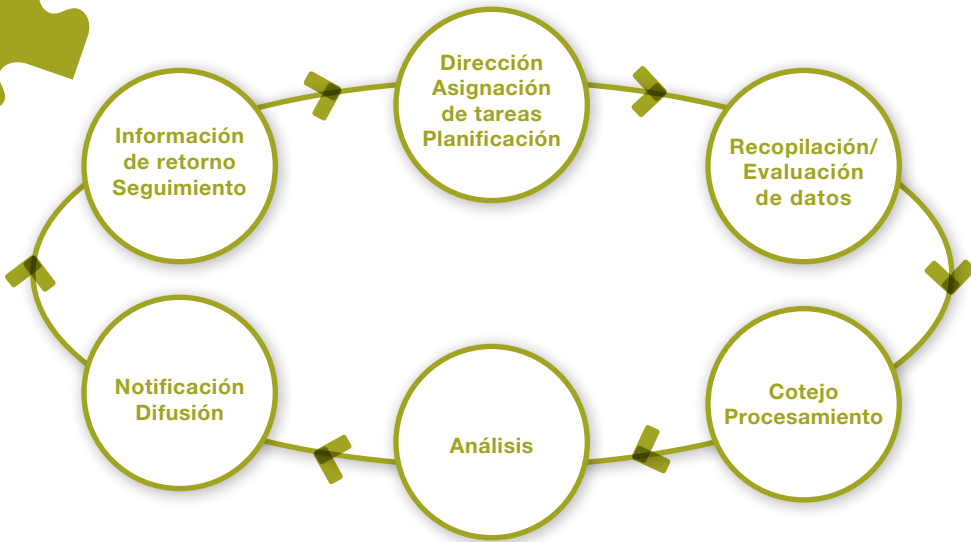


Figura 6.1 **El ciclo de inteligencia criminal**

El ciclo de inteligencia se inicia con una asignación clara de tareas, para que se elaboren productos de inteligencia concretos. Sin embargo, el proceso de inteligencia criminal se lleva a cabo a varios niveles distintos y no suele limitarse al ciclo de inteligencia. Además del ciclo expuesto en la figura 6.1, podría ser necesario un proceso más amplio y más constante de evaluación estratégica de los requisitos de inteligencia. Esa evaluación continuada identifica amenazas y deficiencias en la inteligencia, tanto ya existentes como nuevas, y se lleva a cabo de conformidad con prioridades, políticas y objetivos estratégicos. El proceso requiere una organización de inteligencia y unos procedimientos operativos normalizados, con una estructura y funcionamiento correctos, que permitan aportar información al ciclo de inteligencia y definan el resultado que se espera del mismo, así como su seguimiento. La evaluación estratégica de los requisitos de inteligencia, así como el ciclo de inteligencia criminal contribuyen al proceso de planificación estratégica de un país y son un reflejo de las prioridades estratégicas nacionales, regionales y locales. Eso se explica con más detalle en el próximo capítulo.

En los subcapítulos siguientes se explicarán los principales componentes y la finalidad de cada uno de los pasos del ciclo de inteligencia.

## 6.1 Asignación de tareas y planificación

El ciclo de inteligencia comienza por una decisión directiva en la que se encarga a los analistas que elaboren inteligencia sobre el problema o el tema objeto de investigación. Basándose en ese encargo, el gestor y el analista negociarán y llegarán a un acuerdo sobre el mandato, que es un documento en el que se definen el alcance, los objetivos principales, el contenido y el plazo de entrega del producto de inteligencia. El mandato es el punto de partida oficial del ciclo de inteligencia.

La importancia de una asignación clara de tareas y de un acuerdo claro sobre los objetivos de un producto de inteligencia suele subestimarse. Para asignar una tarea clara a los analistas, los encargados del cumplimiento de la ley y de la adopción de decisiones deben conocer las posibilidades y las limitaciones del análisis de inteligencia. Asimismo, los analistas tienen que saber cómo ayudar a los investigadores, gestores y encargados de tomar decisiones (clientes), creando productos a la medida y haciendo recomendaciones concretas. La fase de asignación de tareas, denominada en ocasiones “fase decisoria”, requiere una estrecha colaboración entre los analistas y los clientes. Tienen que llegar a un acuerdo sobre el *tema de estudio, los objetivos, la finalidad, el alcance, el plazo de entrega y el tipo de informe, incluidas la divulgación y el destinatario del producto de inteligencia*. El analista necesita tener una idea clara de las expectativas y las intenciones del cliente.

Es esencial considerar esas tareas como proyectos y planificar con sumo cuidado sus diferentes fases. Los proyectos complejos pueden exigir una considerable cantidad de tiempo y recursos. Basándose en el mandato y en el alcance del proyecto, el analista deberá elaborar un plan de proyecto detallado que incluya los objetivos, el alcance y el plazo de entrega convenidos, así como la secuencia de actividades y la lista de recursos necesarios para completar con éxito la tarea. Esa fase es indispensable porque servirá de guía en la recopilación y el posterior análisis de la información. Por tanto, es importante que el plan de proyecto esté avalado por los gestores. Ese plan también tendrá en cuenta los posibles problemas legales y de protección de datos que puedan surgir en la ejecución del proyecto de inteligencia. En particular, en caso de que se utilicen datos personales o métodos encubiertos de recopilación de datos e información, los requisitos legales y las posibles restricciones deberán tenerse en cuenta en las fases preliminares del proceso de planificación, a fin de asegurar que la recopilación, el intercambio y la utilización de los datos y la información se llevan a cabo en estricto cumplimiento de las leyes nacionales y las normativas internacionales.

Una planificación clara ahorra tiempo a largo plazo y permite una utilización eficiente de los recursos, lo que se traduce en unos resultados de mayor calidad.<sup>36</sup> También reduce el riesgo de que la recopilación, el almacenamiento, el intercambio y el manejo de los datos y la información no estén en consonancia con las normas jurídicas nacionales e internacionales, y en consecuencia se ponga en peligro el éxito de todo el proyecto. Con una asignación de tareas y una planificación adecuadas, los productos del análisis de inteligencia pueden ayudar a elaborar planes estratégicos para hacer frente a los problemas actuales y prepararse para los que puedan surgir.<sup>37</sup>

<sup>36</sup> Para más información véanse los subcapítulos 6.2 y 8.1.

<sup>37</sup> UNODC (2011b: 10-13).

---

## Evaluación estratégica y requisitos de inteligencia

Los requisitos de inteligencia tienen su origen en el proceso de evaluación estratégica. La evaluación preparada por la unidad/el departamento/el organismo de inteligencia proporciona a las estructuras ejecutivas encargadas del cumplimiento de la ley una visión general de los problemas en materia de actividad policial con los que se enfrenta o puede enfrentarse la institución. Se trata de un documento de gran alcance que refleja las prioridades estratégicas nacionales, regionales y locales. La preparación del documento es la primera etapa del proceso de planificación estratégica.

En el documento se abordarán todas las amenazas, existentes y nuevas, identificadas en el proceso de exploración de la evaluación estratégica, sin omitir nada que pueda ser importante. A continuación el documento se examinará en un foro estratégico, donde se estudiarán todas esas amenazas en el contexto de los recursos disponibles y se adaptarán las prioridades a dichos recursos. El número de amenazas incluidas en cualquier estrategia de control viene determinado por los recursos disponibles para abordarlas; aquellas a las que el foro estratégico otorgue la máxima prioridad se incluirán en la estrategia de control. Eso define el programa operativo, que a su vez es supervisado por directivos de nivel medio que asumen personalmente la responsabilidad de cada una de las prioridades identificadas y se encargan de elaborar planes para gestionar esas amenazas.

Es probable que la estrategia de control incluya una mezcla de prioridades nacionales, regionales y locales, por lo que podría incluir fenómenos que aparentemente no están relacionados entre sí, como por ejemplo el terrorismo internacional, los robos callejeros y la conducción en estado de embriaguez. Eso se mantendrá sin cambios hasta que se prepare la siguiente evaluación estratégica o hasta que surjan amenazas más importantes y se pongan en conocimiento de las estructuras ejecutivas. Mientras tanto, las evaluaciones tácticas/operativas presentadas en las reuniones tácticas/operativas periódicas garantizan que esas prioridades siguen siendo el centro de atención de la institución. En dichas reuniones se examinan los planes operativos elaborados por los directivos de nivel medio y se brinda un foro para debatir las nuevas amenazas, a fin de asegurar que los directivos siguen centrando su atención en las amenazas identificadas para que sus estructuras ejecutivas puedan adoptar medidas.

En la evaluación estratégica se identifican también otras amenazas que no conviene ignorar, aunque no haya suficientes recursos para ocuparse de ellas de forma inmediata; lo que se suele hacer es incorporarlas a la estrategia de control para crear el requisito de inteligencia. La responsabilidad de establecer prioridades que estén en consonancia con la estrategia de control recae en todo el personal de una institución encargada del cumplimiento de la ley. Es deber de la secretaría o del departamento de inteligencia seguir revisando los requisitos de inteligencia y evaluar si las amenazas que se han identificado exigen mayor atención (quizá introduciendo modificaciones o adiciones en una nueva estrategia de control), así como estar atentos para detectar la aparición de alguna nueva amenaza.

---

## 6.2 Recopilación y evaluación

Recopilar información para proyectos de inteligencia es un proceso difícil. Aunque los analistas deben velar por que se recojan datos suficientes para cubrir todos los aspectos del tema o de los temas que se vayan a analizar, también deben evitar la sobrecarga de datos y la recopilación de información innecesaria o inadecuada. En esta fase es esencial que el personal de inteligencia conozca la existencia, la pertinencia, la accesibilidad y la fiabilidad de todas las fuentes y todos los organismos escogidos para que lleven a cabo una determinada tarea de recopilación, así como las limitaciones legales y los requisitos de autorización que pueden aplicarse a la utilización de los diferentes tipos de fuentes de información. El conocimiento de los datos y las fuentes de información externos e internos, y el acceso a los mismos, así como el ser conscientes de sus posibles limitaciones y requisitos, son condiciones previas para que la recopilación y el análisis de inteligencia sean efectivos.

Ejemplos de fuentes de datos e información utilizadas por analistas de delitos:

### Fuentes oficiales:

- Ministerios, organismos estatales, fiscalía
- Bases de datos de organismos encargados del cumplimiento de la ley
- Organizaciones internacionales
- Dependencias de inteligencia financiera
- Agentes de la policía de vecindad
- Datos de control fronterizo
- Registros públicos
- Agentes de patrulla
- Investigaciones
- Vigilancia
- Informantes

### Fuentes no oficiales:

- Organizaciones no gubernamentales
- Industria del transporte
- Informes anónimos
- Sector comercial
- Sector financiero
- Sociedad civil
- Redes sociales
- Comunidades
- Círculos académicos
- Medios informativos

## Plan de recopilación

La elaboración de un plan de recopilación es la fase que sigue al acuerdo sobre el mandato y el plan de proyecto, según lo dicho anteriormente. Ese plan es imprescindible para garantizar la recopilación ordenada y precisa de los datos y la información necesarios para cumplir los requisitos encomendados/exigidos. Debe considerarse como un proceso ininterrumpido capaz de adaptarse y responder a las modificaciones de los requisitos. El plan de recopilación se basa en la definición, el objetivo, el alcance y el plazo de entrega de la tarea, y en él se describe: **qué** información debe recopilarse o está disponible, incluidos el objetivo y el valor de los datos recopilados; **qué** fuentes deben utilizarse; **dónde** puede obtenerse la información; **cómo** puede obtenerse la información y **quién** debe recopilarla; **cuántos** datos pueden manejarse; y **cuándo** debe recogerse cada dato. En algunos casos, podría ser necesario incluir **por qué** hay que recopilar determinados datos e información. El plan de recopilación, al igual que el plan general del proyecto, también ha de tener en cuenta los diferentes requisitos legales que se

aplicarán a las tareas de recopilación de datos, dependiendo del tipo de información, así como de las fuentes y los medios utilizados para obtenerla.<sup>38</sup>

Elaborar un plan de recopilación detallado, que incluya una evaluación de necesidades, así como las autorizaciones legales necesarias y los requisitos de supervisión aplicables, es esencial para que el proyecto tenga éxito. Por tanto, el plan velará por que todas las partes implicadas se atengan a los objetivos convenidos y a las normas aplicables.

## Evaluación

De forma simultánea o inmediatamente después de haber recopilado la información, se han de evaluar los datos en el contexto en el que han sido obtenidos. La evaluación de los datos debe basarse en un criterio profesional objetivo, puesto que su calidad determina la validez de la inteligencia elaborada. La evaluación analiza la validez y la fiabilidad de la información, así como su utilidad para la tarea en cuestión<sup>39</sup>. Un primer paso habitual es identificar lo que es importante y lo que es irrelevante, así como evaluar la urgencia de actuar en consecuencia. La fiabilidad de la fuente, y la validez y la exactitud de la información, han de ser evaluadas de forma independiente por el agente/analista que obtuvo y registró esa información en concreto.<sup>40</sup>

Todas las fuentes y toda la información deben evaluarse siguiendo un sistema de evaluación reconocido oficialmente. Los sistemas 4x4 o 5x5x5 son los más utilizados.<sup>41</sup>

**Cuadro 6.1 Códigos de evaluación con arreglo al sistema de evaluación 4x4**

EVALUACIÓN DE LA FUENTE		EVALUACIÓN DE LA INFORMACIÓN	
A	Totalmente fiable en todos los casos	1	No hay duda de la exactitud
B	Normalmente fiable	2	Conocida personalmente por la fuente pero no conocida personalmente por el agente que la transmite
C	Normalmente no fiable	3	No conocida personalmente por la fuente pero corroborada por otra información disponible
D	No puede evaluarse la fiabilidad	4	La exactitud no puede ser evaluada ni corroborada de ninguna manera (en ese momento)

38 Véase OIDDH/TNTD (OSCE) (2013: 34).

39 National Policing Improvement Agency, *Practice Advice on Analysis* (Asociación de Jefes de Policía, 2008).

40 UNODC (2011b: 25-28).

41 *ibid.* Véase también información sobre sistemas de evaluación 6x6. El sistema 5x5x5 incluye "Códigos de tratamiento" que no se explican en la presente guía.

Cuadro 6.2 Códigos de evaluación con arreglo al sistema de evaluación 5x5x5

EVAUACIÓN DE LA FUENTE		EVALUACIÓN DE LA INFORMACIÓN	
A	Siempre fiable	1	Se sabe con certeza que es cierta
B	Fiable en la mayoría de los casos	2	Conocida personalmente por la fuente pero no por la persona que informa
C	Fiable en algunos casos	3	No conocida personalmente por la fuente pero puede ser corroborada
D	No fiable	4	No se puede valorar
E	Fuente no comprobada	5	Se sospecha que es falsa

Nota: El sistema 5x5x5 incluye “Códigos de tratamiento”, que no se explican en la presente guía.

La evaluación de la pertinencia, la fiabilidad y la exactitud de la información, así como la elección de un código de tratamiento para su utilización posterior, son esenciales para la exactitud de los productos de inteligencia finales y para sus modalidades de divulgación. Pero la evaluación también es importante desde la perspectiva de los derechos humanos y de la protección de datos. Según lo expuesto en el Capítulo 5, las normas de protección de datos requieren, entre otras cosas, que la información de carácter personal registrada sea exacta, adecuada y pertinente, y que no sea excesiva en relación con la finalidad para la que está siendo almacenada. Por tanto, la evaluación es esencial para demostrar que el registro de información que suponga una injerencia en el derecho a la intimidad de la persona de la que se obtienen los datos/la información, está justificado y es necesario y proporcionado, y por tanto permisible, en virtud de las normas aplicables en materia de derechos humanos y protección de datos aplicables.

Los evaluadores también han de ser conscientes de que existen otros posibles problemas de derechos humanos que podrían ser importantes, relacionados con el modo en que se utiliza determinada información. Eso tiene especial trascendencia a la hora de evaluar información procedente de terceros países, cuando haya razones para creer que puede haber sido obtenida por medios ilegales. Por ejemplo, el uso en procesos judiciales de pruebas obtenidas mediante tortura o maltrato está absolutamente prohibido en virtud del derecho internacional. Pero aun cuando no se tenga intención de utilizarlas en procesos judiciales, la información o la inteligencia obtenidas por esos métodos también deberán descartarse.<sup>42</sup>

### 6.3 Cotejo y procesamiento

La fase de procesamiento y cotejo requiere un sistema adecuado y consistente. Esta fase implica clasificar, priorizar y referenciar la información recogida. Durante la fase de cotejo, el analista organiza y da estructura a la información recogida para que adquiera un formato indizado y con referencias cruzadas, y finalmente lo transfiere a un sistema de almacenamiento

<sup>42</sup> OSCE, OIDDH/TNTD (2013: 28).

(es decir, una base de datos). Verificar la pertinencia, exactitud y utilidad de la información es un paso importante antes de introducirla en un sistema de almacenamiento. Es de vital importancia haber establecido previamente un sistema accesible mediante el cual se pueda obtener y analizar la información.

El procesamiento de la información puede estar tan estrechamente relacionado con la fase analítica que incluso resulta difícil distinguir claramente entre ambos procesos.<sup>43</sup>

## 6.4 Análisis

Tal y como ocurre con los diferentes tipos de inteligencia, también existen diversas formas de clasificación de los análisis. Lo que en una organización se denomina análisis operativo, en otra se llama análisis táctico, y el análisis de redes en un departamento de policía se conoce como análisis de enlaces o trazado de enlaces en el país vecino. Las clasificaciones más comunes a ese respecto distinguen entre análisis estratégico, análisis operativo y análisis táctico. La presente guía fusiona los análisis táctico y operativo dentro del análisis operativo.<sup>44</sup>

---

El **análisis estratégico** apoya la toma de decisiones, la formulación de políticas, la planificación y priorización; la asignación de recursos policiales; y establece el enfoque apropiado para abordar los diversos tipos de delitos. También proporciona apoyo basado en la inteligencia a los encargados del cumplimiento de la ley que están en primera línea, facilitando la identificación de amenazas clave, vulnerabilidades, riesgos y oportunidades de actuación (evaluaciones de amenazas y riesgos). El análisis estratégico no incluye información personal.

El **análisis operativo** ayuda en la gestión y ejecución en primera línea de tareas a corto plazo para lograr objetivos operativos concretos, y apoya las investigaciones en curso. El análisis operativo puede incluir información personal sobre los sospechosos.

---

El proceso analítico es necesario para transformar en inteligencia real los datos e información no procesados y para dirigir los objetivos relacionados con el cumplimiento de la ley, tanto los operativos a corto plazo como los estratégicos a largo plazo. La credibilidad y el alcance del análisis dependen en gran medida, por un lado, de la calidad y la exactitud de los datos recopilados previamente y, por otro, de las aptitudes de los analistas. Durante el análisis de la información, así como en todas las demás fases del ciclo de inteligencia, es absolutamente crucial que se dé una estrecha cooperación entre los analistas y los clientes (oficiales, investigadores, altos funcionarios), también mediante la organización de reuniones periódicas de examen, para garantizar que la inteligencia se desarrolle de acuerdo con las necesidades de inteligencia y/o los requisitos de los clientes.

---

43 *National Policing Improvement Agency* (Organismo Nacional para la Mejora de la Actividad Policial) (2008).

44 La UNODC, Interpol y Europol utilizan esa misma clasificación. Véase UNODC (2011b: 35-38).

La fase de análisis es fundamental para el proceso de inteligencia, ya que tiene que ver con la identificación y el examen del significado, el contexto y las características esenciales de la información disponible. El análisis de los datos pone de relieve las lagunas de información, los puntos fuertes y débiles de dichos datos, y define el camino a seguir. El objetivo principal de la fase de análisis es extraer significado de la información original para permitir que la inteligencia pueda ponerse en práctica. Cuando los resultados del análisis de inteligencia criminal están directamente vinculados y responden a la tarea o al problema investigados, el análisis se convierte en una valiosa herramienta operativa.

El proceso analítico se compone de dos fases: *integración de datos e interpretación de datos*. La primera fase (integración de datos) combina información evaluada y cotejada de diferentes fuentes para desarrollar hipótesis iniciales y predicciones, identificar un patrón de inteligencia y extraer deducciones. La segunda fase (interpretación de datos) implica ir más allá de los datos disponibles e interpretarlos. En esta fase se comprueban las hipótesis iniciales, lo que tiene como resultado el respaldo, la modificación o la refutación de las hipótesis que se hayan desarrollado previamente.

Una *hipótesis* es una teoría de trabajo preliminar que se basa en premisas e indicadores previamente desarrollados a partir de datos e información disponibles y que requiere de información adicional para corroborar o rebatir previas suposiciones. Las hipótesis ayudan a identificar lagunas de inteligencia, orientar la recopilación de datos adicionales y extraer deducciones, conclusiones, predicciones y estimaciones exactas.

El desarrollo y la comprobación de hipótesis han ganado en importancia dentro del análisis de inteligencia. Las hipótesis contienen una gran cantidad de especulación y, por lo tanto, necesitan ser comprobadas (confirmadas, modificadas o rechazadas) por analistas. La comprobación de hipótesis deberá incluir: los argumentos a favor y en contra de la hipótesis, sus repercusiones, un examen del proceso de razonamiento y la recopilación y revisión de los datos necesarios. Una hipótesis o cualquier inferencia debe incluir respuestas a las siguientes preguntas clave (a menudo denominadas en inglés “5Ws’ and 1H”):

- ¿Quién? Individuo/Individuos clave
- ¿Qué? Actividades delictivas
- ¿Cómo? Métodos empleados
- ¿Dónde? Información y ámbito geográficos
- ¿Por qué? Motivo
- ¿Cuándo? Localización en el tiempo

El uso de hipótesis para probar y examinar un fenómeno delictivo o un problema de seguridad es un paso importante del razonamiento estratégico, en el que se pasa del “dime todo lo que sepas” a un proceso específico y orientado a la actuación. Esta técnica y el resto de las que se incluyen en el presente capítulo ponen de relieve que la capacitación, las aptitudes y la experiencia, tanto de los responsables de la adopción de decisiones como de los analistas, son vitales para el éxito de la ILP.



---

## Ejemplos de métodos analíticos

El modelo nacional de inteligencia (MNI) de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) se basa en nueve técnicas y productos analíticos que corroboran una adopción de decisiones estratégicas u operativas fundamentada y el desarrollo de conocimientos profesionales sobre técnicas eficaces y proactivas de aplicación de la ley:

- El **análisis de patrones delictivos** es un término amplio que agrupa un conjunto de tipos de análisis, entre ellos, la identificación de tendencias y el análisis de puntos conflictivos.
- El **análisis de tendencias demográficas y sociales** evalúa los efectos de los cambios socioeconómicos y demográficos en la delincuencia, así como los cambios en la composición de la población y la cuestión de las personas sin hogar.
- El **análisis de redes** evalúa la direccionalidad, frecuencia y fuerza de los vínculos entre los distintos colaboradores de una red delictiva.
- Los **perfiles de mercado** evalúan el mercado delictivo de una mercancía o actividad en particular, como las drogas o la prostitución.
- El **perfil de negocio de actividades delictivas** determina el modelo y las técnicas de negocio que utilizan los delincuentes o los grupos de delincuencia organizada.
- El **análisis de riesgos** evalúa la magnitud de los riesgos o amenazas que representan los delincuentes u organizaciones para las víctimas potenciales, la policía y el público en general.
- El **análisis del perfil del sujeto investigado** describe al delincuente, sus puntos fuertes y débiles, el estilo de vida, las redes, las actividades delictivas y los posibles puntos de interceptación en la vida de un delincuente identificado como objetivo.
- La **evaluación de la inteligencia operativa** analiza si la recopilación de información se ajusta a los objetivos previamente acordados e identifica lagunas en los esfuerzos de inteligencia de una operación (desplegados en proyectos y operaciones a gran escala).
- El **análisis de resultados** evalúa la eficacia de las actividades de aplicación de la ley y supervisa el progreso de los planes.

Fuente: Basado en UNODC (2011b: 35-38).

---

Además de los métodos de análisis mencionados, los analistas utilizan otras técnicas cualitativas de análisis<sup>45</sup> que tienen un propósito común: son herramientas para desglosar problemas complejos en porciones analíticas más manejables.

### 6.5 Notificación y difusión de los productos de inteligencia

Los productos de inteligencia son el resultado del proceso de inteligencia y generalmente se difunden en forma de informes claramente estructurados y concisos. Los informes de análisis de inteligencia tienen por objeto reflejar información objetiva y precisa, e identificar y recomendar intervenciones estratégicas u operativas eficaces. Para garantizar el valor en la práctica de los productos de inteligencia, estos deben ser siempre claros y concisos. Como se ha destacado anteriormente, una estrecha colaboración entre el analista y el cliente, incluida la organización de reuniones periódicas de revisión, es por tanto imprescindible para la entrega de un producto de inteligencia específico y la presentación de sus conclusiones. Un buen enfoque general a la hora de redactar cualquier tipo de producto de inteligencia es la utilización de la *escritura en pirámide invertida*, en la que se empieza por los mensajes más importantes para el cliente y se pasa después a cuestiones más generales.

Dependiendo de las necesidades de los clientes, estos productos se pueden dividir en productos de inteligencia estratégica y operativa.

El objetivo de los **informes de análisis operativo** es apoyar las investigaciones en curso y las tareas operativas y tácticas a corto plazo. Dirigidos a los profesionales, estos productos deben ser concisos, priorizar una redacción clara y directa, y centrarse en la información con valor añadido operativo. Las principales conclusiones deben enumerarse al principio, para permitir que el lector extraiga rápidamente las informaciones más importantes y decida cómo dar prioridad a la información recibida. A continuación, los productos de inteligencia deberían entrar en más detalles, comenzando con breves descripciones de los antecedentes operativos, seguidas de sus metas y objetivos. La parte principal de los productos de inteligencia debe proporcionar información detallada sobre el caso, explicar el proceso de análisis que ha llevado a la hipótesis y aclarar sus conclusiones. Los productos deben incluir al final requisitos de inteligencia y recomendaciones para la adopción de medidas concretas. Los productos de inteligencia operativa son una fuente importante de información para los productos estratégicos.

El objetivo de los **informes de análisis estratégico** es apoyar la toma de decisiones fundamentada y el diseño de las operaciones. Se pueden preparar varios tipos de documentos dependiendo de los requisitos y objetivos:<sup>46</sup>

---

45 Véase UNODC (2011a) para consultar descripciones y ejemplos de estas técnicas. También se puede visitar la página web de *Problem-Oriented Policing*: [www.popcenter.org/about/?p=whatispop](http://www.popcenter.org/about/?p=whatispop). Además, en el sitio web de la *International Association of Law Enforcement Intelligence Analysts* se hace referencia a información y orientación sobre varios tipos y métodos de análisis: [www.ialeia.org](http://www.ialeia.org)

46 En su Ficha técnica sobre análisis de información policial, Interpol clasifica los productos analíticos en informes analíticos, evaluaciones del riesgo sobre un acontecimiento concreto y publicaciones de información policial (boletines, informes mensuales, etc.). Europol divide primero los informes de análisis en informes operativos y estratégicos, pero a continuación clasifica los informes estratégicos en evaluaciones de amenazas, informes de situación y notificaciones de inteligencia.

Las *notificaciones de alerta temprana/de inteligencia* ponen de relieve cambios, tendencias y evoluciones en el entorno, nuevos o recientes, que pueden ser de carácter temático o geográfico. Su principal propósito es describir los cambios y evaluar los posibles efectos en los mercados delictivos, en la situación de la seguridad y en la comunidad o en una zona geográfica más amplia. Estas notificaciones son breves y específicas, su objetivo es informar al cliente de un nuevo cambio o tendencia de manera proactiva y rápida, y dar breves indicaciones sobre los efectos esperados de ese cambio o tendencia.

Las *evaluaciones de amenazas* analizan y evalúan la amenaza de los fenómenos delictivos. Pueden centrarse en grupos de delincuencia organizada, en ámbitos delictivos concretos o en regiones concretas. Las evaluaciones suelen tener un alcance a medio y largo plazo y están orientadas al futuro. Proporcionan inteligencia estratégica y recomendaciones a los encargados de tomar decisiones.

Los *informes de evaluación de riesgos* describen la evaluación de riesgos potenciales y en ellos, la evaluación de amenazas va acompañada de una evaluación de probabilidad, efectos y vulnerabilidades relacionadas. Un ejemplo clásico de lo antedicho es un informe de evaluación de riesgos presentado para los preparativos de un evento importante.

Los *informes de situación* son principalmente descriptivos. Su objetivo es proporcionar una visión general detallada de un tema concreto. Contrariamente a las evaluaciones de amenazas, por lo general no incluyen recomendaciones para la adopción de medidas y se limitan a constataciones fácticas. Pueden centrarse en diversos temas, desde un ámbito delictivo o modus operandi específicos, hasta un grupo delictivo o área geográfica concretos.

El último paso en el proceso de inteligencia es la difusión del producto de inteligencia y la presentación de información al cliente o los clientes acerca de su contenido. Los consumidores de análisis de inteligencia pueden ser investigadores, fiscales, altos cargos del cumplimiento de la ley y otros organismos policiales o gubernamentales. Cuando sea posible y apropiado, el producto de inteligencia debería hacerse público. Eso puede ser beneficioso para el cumplimiento de la ley ya que con ello se puede elevar la conciencia pública sobre temas específicos (como parte de la prevención del delito), incrementar la transparencia y la visibilidad, y recibir información valiosa de los ciudadanos en respuesta a informes publicados. Es importante elegir el método/formato adecuado para difundir y presentar el producto de inteligencia a los destinatarios seleccionados y asegurarse de que les llegue a tiempo para apoyar las decisiones y medidas<sup>47</sup>. La fase de difusión es crítica para toda la estructura del modelo de ILP, ya que informa al cliente así como a todos los cuerpos policiales apropiados sobre las actividades y los fenómenos delictivos pertinentes, así como sobre los autores de delitos. Dada la sensibilidad de los datos que suelen presentarse en los productos de inteligencia, debe adoptarse una reglamentación clara y transparente, basada en los principios básicos del “derecho a saber” y la “necesidad de saber”, de conformidad con las normas nacionales e internacionales en materia de derechos humanos y protección de datos.

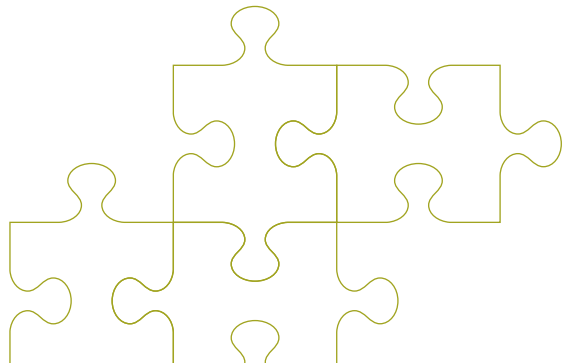
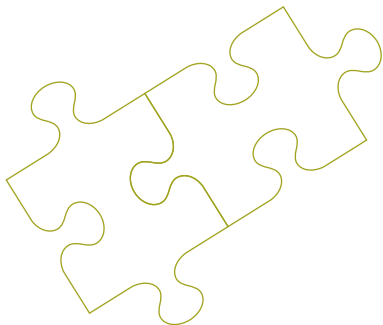
---

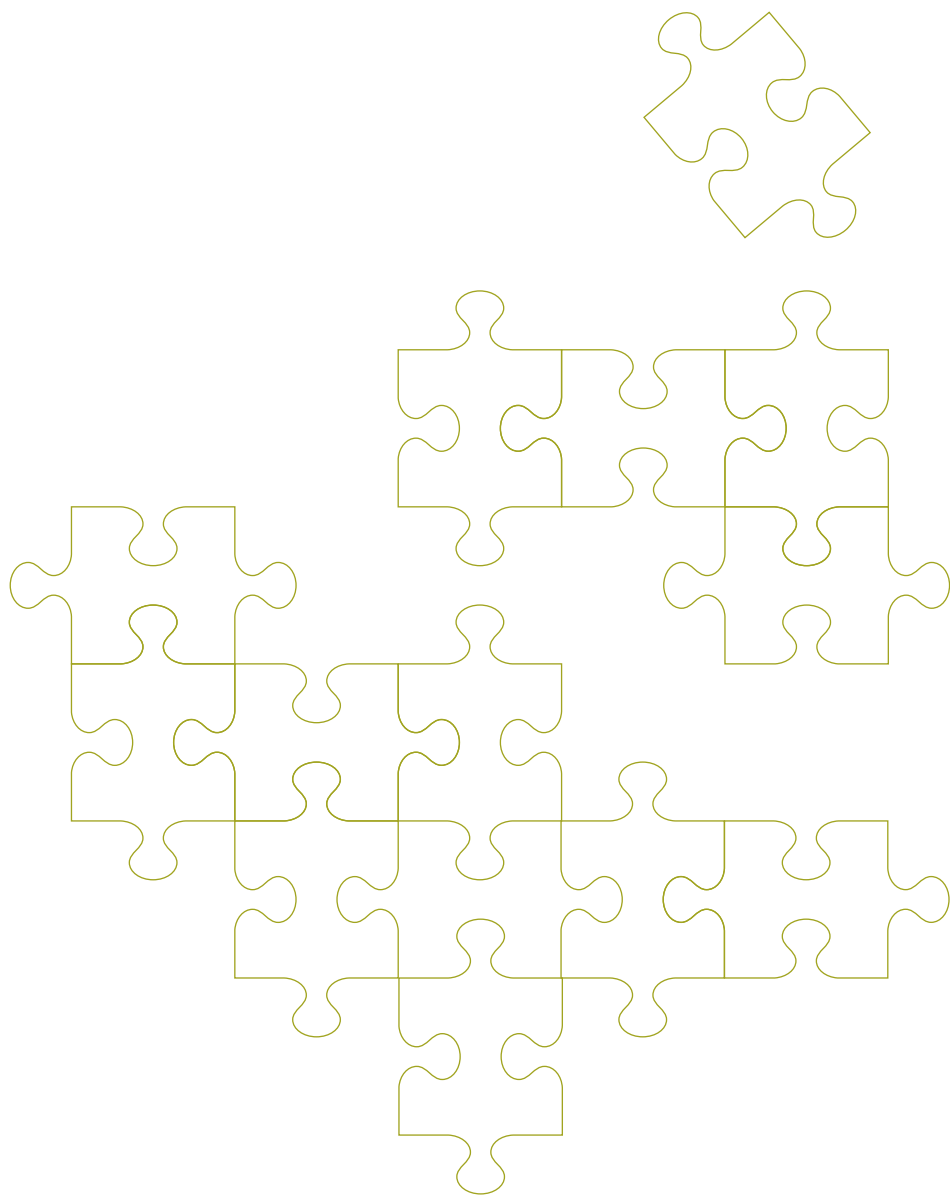
47 Para obtener más información práctica sobre informes y presentaciones orales, véase UNODC (2011a).

Es necesario concretar los detalles sobre la difusión de productos de inteligencia en respectivos manuales o guías nacionales, de conformidad con las instrucciones y requisitos legales nacionales y con la normativa internacional sobre derechos humanos.

### 6.6 Información de retorno y seguimiento

La importancia de una colaboración activa entre el cliente/encargado de adoptar decisiones y el analista es una cuestión que se destaca repetidamente en la presente guía. Esto también se aplica a la evaluación del producto de inteligencia y a la información de retorno del cliente, de la persona encargada de adoptar decisiones o de otros usuarios del producto analítico. Los analistas y sus superiores deben saber si el producto ha cumplido los requisitos y si las recomendaciones han contribuido a la adopción de decisiones o acciones de seguimiento. El analista también debe recibir información de retorno sobre posibles mejoras. Enviar un formulario de información de retorno al cliente poco después de hacerle llegar el informe de análisis y presentarle el producto de inteligencia, es una práctica muy útil. Debe organizarse una reunión de seguimiento en la que se debatan el producto de inteligencia, la información de retorno, la cooperación y las decisiones, medidas u operaciones subsiguientes. Estos mecanismos no solo aumentan la calidad de la tarea en cuestión, sino que también son necesarios para el desarrollo profesional.







## 7. Puesta en práctica de la ILP

En este capítulo se presentará una representación gráfica de un modelo de ILP recomendado por la OSCE y se explicarán sus componentes principales; seguidamente se examinarán en detalle los requisitos clave para hacer operativa y poner en práctica la ILP. Aunque resulte tentador presentar una matriz o una fórmula para la puesta en práctica de la ILP, no existe un modelo universal, ni debería existir, ya que las circunstancias locales y nacionales varían considerablemente. Cada país debe evaluar su situación y elaborar su propio plan de aplicación a la luz de su marco jurídico vigente, la cultura, las necesidades, los recursos y otros factores básicos nacionales y locales, y adaptar su enfoque a esos requisitos clave. No obstante, sobre la base de algunos principios comúnmente aceptados, la OSCE ha desarrollado un modelo marco para la aplicación de la ILP, y se invita a los Estados participantes de la OSCE a utilizarlo cuando adopten y pongan en práctica su ILP.

Aunque las circunstancias nacionales varíen, la investigación ha demostrado que los logros de las políticas, estrategias y aplicación de ILP en cada país generalmente dependen de los siguientes factores clave para tener éxito:

- un marco legislativo claro para la ILP que se ajuste a las normas internacionales en materia de derechos humanos y protección de datos, e incluya poderes y procesos claramente definidos para que los organismos recopilen, analicen y compartan la información pertinente;
- estructuras organizativas que faciliten una orientación estratégica clara y una cooperación operativa, así como procesos de toma de decisiones en un entorno interinstitucional y con una supervisión adecuada;
- tecnología que facilite el intercambio de información mediante la interoperabilidad de los sistemas;
- conocimientos y aptitudes de todo el personal pertinente; y



- una actitud colaborativa en el intercambio de información para apoyar la toma de decisiones en todos los ámbitos operativos.<sup>48</sup>

Todos estos temas serán tratados más adelante en esta guía.

## 7.1 El modelo de ILP de la OSCE

Como se explicó en el Capítulo 3, la ILP es un marco de gestión y toma de decisiones descendente. Proporciona una estructura, una metodología y múltiples procesos para la recopilación, el intercambio y el análisis sistemáticos de la información pertinente, que sirve de base para planificar y tomar decisiones fundamentadas en la gestión de la aplicación de la ley. Se ha considerado que la ILP es un modelo de actuación en materia de aplicación de la ley, es decir, una metodología que sirve de guía para llevar a cabo y gestionar la actividad policial.

El modelo conceptual 4-i, presentado en el Capítulo 3, destaca la relación entre los tres elementos clave de la ILP: el entorno delictivo, los analistas de inteligencia criminal y los encargados de tomar decisiones. El modelo 4-i muestra que los encargados de tomar decisiones encomiendan tareas y dirigen a los analistas explicándoles sus intenciones. Los analistas interpretan el entorno delictivo a través de sus análisis e influyen en los encargados de tomar decisiones aportando sus conclusiones. Sobre la base de los productos de análisis, los encargados de tomar decisiones causan un impacto en el entorno delictivo por medio de actuaciones de aplicación de la ley.

“La actividad policial basada en la inteligencia es un modelo de actuación policial [...] capaz de incorporar áreas de actividad policial que no están directamente relacionadas con la delincuencia, pero que aun así representan un problema importante para las comunidades y los organismos policiales. Con esta evolución, la actividad policial basada en la inteligencia se está convirtiendo en un método de actuación para ‘todos los delitos, todos los peligros, todos los daños’ que muchos están buscando en la policía”.

– Ratcliffe (2016: 67).

La figura 7.1 es una representación gráfica simplificada de los pasos principales y los elementos, los procedimientos y los productos clave para poner en práctica el concepto de ILP. El modelo puede aplicarse parcial o totalmente en la aplicación de la ley a nivel nacional, regional o local.<sup>49</sup>

48 Véase *Australian Criminal Intelligence Management Strategy 2012-2015* (Commonwealth de Australia, 2012); y James et ál. (2016).

49 Esta ilustración gráfica del modelo de ILP propuesto por la OSCE ha sido desarrollada por la Unidad de Asuntos Policiales de Carácter Estratégico del Departamento de Amenazas Transnacionales de la OSCE, sobre la base de las definiciones de Ratcliffe (2016). La presentación de la Circulación de la información contenida en *Sistemas policiales de información e inteligencia* de la UNODC (2006) también se utilizó en la elaboración del gráfico.

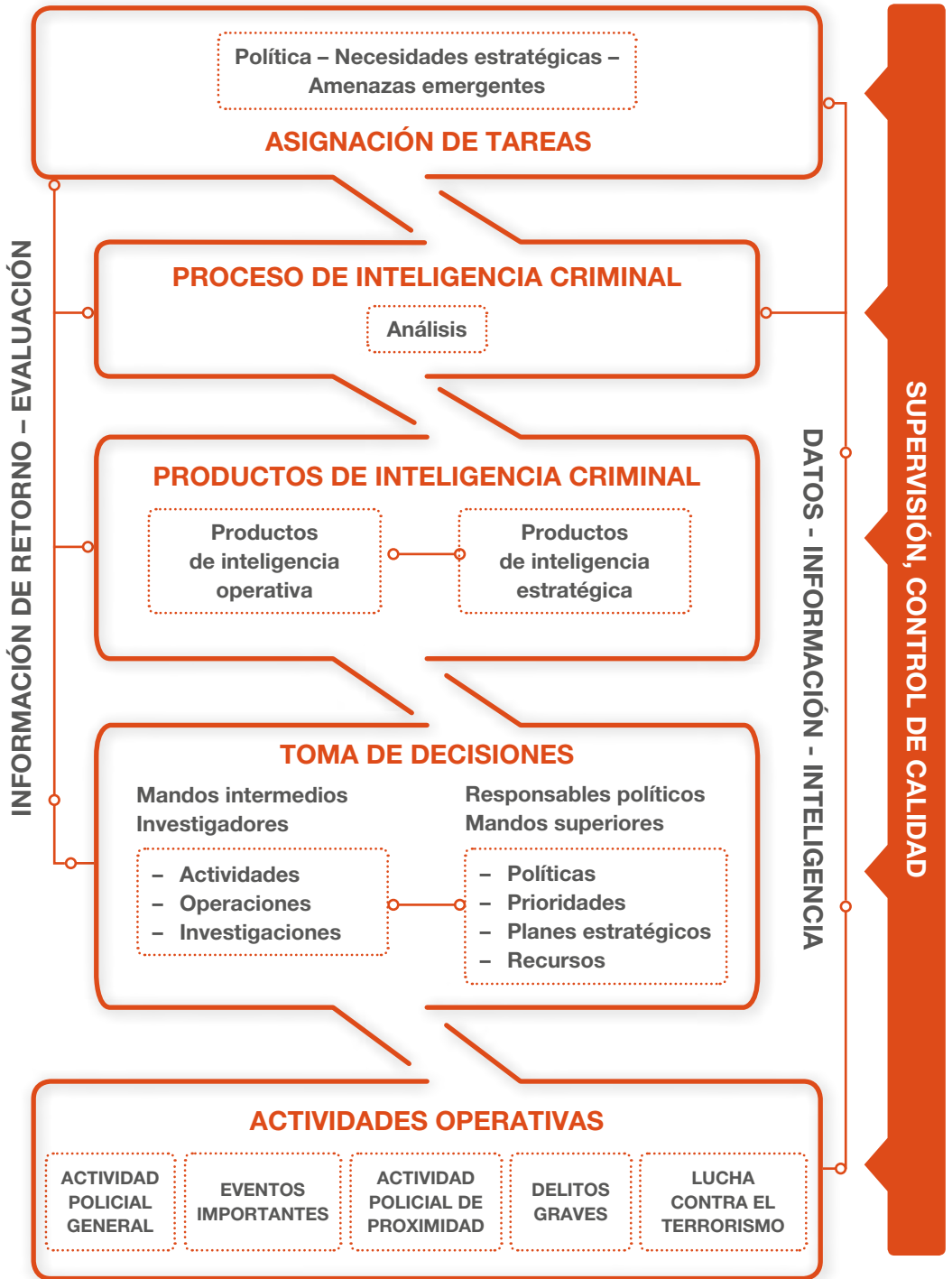


Figura 7.1 El modelo de la OSCE de actividad policial basada en la inteligencia



El modelo de ILP incluye las siguientes etapas y componentes principales:

### **ASIGNACIÓN DE TAREAS**

Sobre la base de políticas, planes estratégicos y operativos, amenazas emergentes o necesidades identificadas, los encargados del cumplimiento de la ley a nivel nacional, regional o local asignan tareas y dan instrucciones a los directores de análisis, quienes encomiendan las tareas a los distintos departamentos, unidades de análisis o analistas individuales.

### **ANÁLISIS DENTRO DEL PROCESO DE INTELIGENCIA CRIMINAL**

Siguiendo instrucciones y encargos de los directivos o peticiones de los investigadores, los analistas desarrollan la inteligencia de acuerdo con un proceso de inteligencia definido. Si bien el análisis constituye el eje central de los procesos, estos incluyen además la recopilación, el procesamiento y el cotejo de la información. (En el Capítulo 6 se ofrece una descripción detallada de los seis pasos del proceso de inteligencia criminal.)

### **PRODUCTOS DE INTELIGENCIA CRIMINAL**

El proceso de análisis genera productos de inteligencia criminal estratégica y operativa, que se utilizan como base para elaborar planes estratégicos y operativos, y para apoyar las investigaciones criminales y otras operaciones relacionadas con el cumplimiento de la ley, así como para priorizar y asignar recursos humanos y técnicos.

### **TOMA DE DECISIONES**

Esta guía recomienda que cada país mantenga una estructura de toma de decisiones sobre ILP en los planos nacional, regional y local, donde los informes de análisis o los productos de inteligencia se utilicen como base para la toma de decisiones. En el subcapítulo 7.5 se describe un mecanismo orientativo y en el subcapítulo 8.2 se presentan ejemplos de buenas prácticas nacionales.

### **ACTIVIDADES OPERATIVAS**

En la figura 7.1 se enumeran cinco ejemplos de ámbitos policiales en los que pueden aplicarse los principios de la ILP. No se trata en ningún caso de una lista exhaustiva, ya que la aplicación proactiva de la ley, basada en datos e información evaluados y analizados, puede encontrar cabida en muchos otros ámbitos de la policía. Las áreas de policía operativa generan datos, información e inteligencia que se transmiten a través de canales de comunicación claramente definidos y se almacenan en bases de datos que permiten su análisis posterior.

### Circulación de datos e información

Para que la ILP funcione bien, todos los funcionarios encargados de hacer cumplir la ley deben compartir y transmitir, a través de mecanismos y canales de comunicación claramente definidos, los datos, la información y los informes de inteligencia pertinentes que reciben y recopilan a lo largo de sus actividades y su trabajo diario. El intercambio de datos, información e inteligencia debería ser una obligación de todos los encargados de hacer cumplir la ley prevista en la legislación nacional u otras directrices oficiales.

### Información de retorno y evaluación

Los analistas y directores de análisis reciben información de retorno sobre la calidad de sus análisis y productos de inteligencia criminal por parte de los encargados del cumplimiento de la ley, investigadores y otros usuarios de sus informes. Los principales indicadores de calidad de los productos de inteligencia criminal son su conformidad con las metodologías y normas definidas, así como la medida en que satisfacen las expectativas y necesidades de sus usuarios, especialmente en lo que respecta a la adopción de decisiones estratégicas y operativas.

### Supervisión y control de calidad

La creación y el mantenimiento de un sistema de supervisión y control de calidad del modelo de ILP es responsabilidad de los mandos superiores encargados del cumplimiento de la ley. Esto se aplica a todos los planes, objetivos, procesos y fases, incluidos la evaluación de los productos de inteligencia criminal, el seguimiento de la asignación de tareas y de las decisiones, la observancia de la normativa en materia de derechos humanos y protección de datos, y los recursos asignados a las tareas. Cada país debe establecer su propio sistema de gestión y control de calidad. Además de la supervisión interna y el control de calidad, las funciones relacionadas con la ILP, como la recopilación, el almacenamiento, el procesamiento y el intercambio de datos, información e inteligencia, también deben estar sujetos a una supervisión independiente.<sup>50</sup>

Aunque el modelo de ILP se divide en cinco fases y subprocesos principales, se ha de destacar que todos los componentes del modelo son interactivos y se retroalimentan, por lo que a menudo es necesario volver a examinar procesos anteriores. Por ejemplo, el proceso de análisis suele revelar lagunas en materia de inteligencia, que a veces requieren una nueva asignación de tareas o una investigación.

Como se ha mencionado anteriormente y se destaca con frecuencia en esta guía, todos los funcionarios encargados de hacer cumplir la ley son participantes activos y proveedores de la ILP. El modelo de ILP se basa en datos e información procedentes de todos los niveles, departamentos y unidades encargados del cumplimiento de la ley. Por lo tanto, son necesarias una concienciación y una capacitación al respecto, así como que se hayan establecido unos claros procedimientos operativos normalizados en materia de ILP para todos los niveles, además de mecanismos apropiados de garantías, rendición de cuentas y supervisión.

---

<sup>50</sup> Para consultar un ejemplo de buenas prácticas, véase Ministerio del Interior de la República de Serbia (2016: 45-49).

## 7.2 Retos y requisitos fundamentales para la puesta en práctica

La investigación sobre el tema ha detectado varios retos y requisitos previos que han de cumplirse para que la ILP funcione desplegando todo su potencial. Se ha demostrado que la ILP solo puede tener efectos significativos y cuantificables si se lleva a cabo introduciendo cambios sustanciales en la organización, la cultura y el liderazgo<sup>51</sup>. También se ha observado que las reticencias a realizar tales reformas han resultado ser un obstáculo significativo para su puesta en práctica. Además de los retos mencionados, la adopción y puesta en práctica de la ILP a menudo “amenaza el orden establecido, la cultura, la identidad de la organización y las normas, los valores y la moral de su personal” y “al personal raras veces le entusiasman los cambios”<sup>52</sup>. El predominio de la cultura del desempeño y las estadísticas operativas, en las que lo importante es cuantificar los resultados, ha sido identificado como uno de los principales motivos de la reticencia a aceptar cualquier cambio en el ámbito de la aplicación de la ley<sup>53</sup>. Por lo tanto, la introducción de la ILP como nuevo marco de toma de decisiones para la aplicación de la ley plantea un particular desafío, ya que a menudo requiere nuevos métodos de gestión y un cambio cultural dentro de la dirección de la policía. Para maximizar el potencial de la ILP, se debe llevar a cabo una gestión integral del cambio que incluya una preparación exhaustiva, consultas y medidas de concienciación en todos los niveles de la organización antes y durante su puesta en práctica.

“En última instancia, las perspectivas de cualquier reforma en una organización están invariablemente limitadas por la medida en que los que ostentan un poder real en esa institución crean que el cambio favorecerá a sus propios intereses, además de reportar beneficios prácticos a la institución”.

– James (2016: 26).

A los problemas mencionados para la puesta en práctica con éxito de la ILP hay que añadir otros requisitos previos, entre ellos:

- una selección de personal de calidad, una capacitación adecuada y un personal cualificado;
- una dirección, gestión y control competentes para los trabajos de inteligencia;
- bases de datos, equipos informáticos y programas de análisis adecuados; y
- gestores cualificados que sepan cómo hacer buen uso de los productos de análisis de inteligencia.<sup>54</sup>

51 Flood y Gaspar (2009).

52 James (2017: 7).

53 Comisión Mixta Parlamentaria sobre aplicación de la ley, *Inquiry into the gathering and use of criminal intelligence* (Canberra: Comisión Mixta Parlamentaria sobre aplicación de la ley, Commonwealth de Australia), (2013: 47-49).

54 James et al. (2016: 24-25); Ratcliffe (2016: 127).

Los puntos siguientes ofrecen orientaciones generales para planificar la adopción y puesta en práctica de la ILP. Aunque el modelo básico de ILP se puede aplicar en cualquier lugar, estos puntos se deberán ajustar al contexto nacional y local.<sup>55</sup>

### ***Marco jurídico nacional que permita la puesta en práctica de la ILP y sea conforme a las normas jurídicas internacionales***

- El ordenamiento jurídico nacional debería incluir disposiciones específicas sobre ILP y permitir su aplicación.
- La recopilación, el almacenamiento, el procesamiento y el intercambio de datos e información deben basarse en la legislación nacional, que cumplirá estrictamente las normas internacionales en materia de derechos humanos y protección de datos. Se alienta a los Estados participantes de la OSCE a que soliciten asistencia técnica y asesoramiento para evaluar la conformidad de sus leyes con las normas internacionales.
- El marco, las metodologías y los procesos internos de la ILP, así como el intercambio y la utilización de productos de inteligencia criminal, deben ser conformes a los principios de la OSCE en materia de actividades policiales democráticas, que reafirman la importancia del Estado de derecho, los derechos humanos, la protección de datos, la ética policial, la rendición de cuentas y la transparencia, y la supervisión y el control externos.<sup>56</sup>

### ***Apoyo político y máximo compromiso gubernamental y de los altos cargos***

- Antes de adoptar o poner en práctica la ILP, deberá garantizarse y quedar claro el apoyo político, así como un alto nivel de concienciación y compromiso gubernamental/ministerial y por parte de los altos cargos relacionados con el cumplimiento de la ley.
- No se alcanzará la plena capacidad de la ILP a menos que todos los niveles de las instituciones encargadas de hacer cumplir la ley conozcan el modelo, sus estructuras y procesos, así como sus propias funciones y responsabilidades en el mismo.

### ***Un enfoque para todos los niveles institucionales***

- La ILP se puede aplicar a todas las áreas de la actividad policial.
- La ILP debe aplicarse en todos los ámbitos institucionales, no solo en unidades especializadas.
- Los esfuerzos para cambiar la cultura existente por una que subraye la “necesidad de compartir” información deben ser parte integrante de la gestión del cambio en la introducción y puesta en práctica de la ILP.
- La ILP cuenta con analistas que trabajan apoyando directamente a los responsables de la toma de decisiones en todos los niveles de la institución.

### ***Planificación estratégica nacional en materia de aplicación de la ley basada en análisis estratégicos, incluidas las evaluaciones de amenazas***

- Los planes estratégicos nacionales, incluido el establecimiento de prioridades, deben formularse sobre la base de análisis y evaluaciones estratégicos.

---

<sup>55</sup> Debido a las particularidades de cada país, esta guía no ofrece una lista detallada sino que se centra en cuestiones generales y comunes a todos los Estados participantes de la OSCE, sobre la base de una bibliografía revisada y las aportaciones de expertos en el cumplimiento de la ley seleccionados, que revisaron los borradores de la presente guía y contribuyeron a su redacción.

<sup>56</sup> OSCE (2008a: 12-13). 48

- Estos planes deberían seguir desarrollándose para que se conviertan en planes de acción operativos.
- Se deberán asignar recursos humanos, técnicos y financieros de conformidad con dichos planes.

***Reuniones de asignación de tareas estratégicas y operativas***

- Las reuniones de asignación de tareas estratégicas y operativas deben celebrarse periódicamente a nivel local, regional y nacional (véase el subcapítulo 7.5).
- Se ha demostrado que una recopilación y un análisis eficaces de la información de inteligencia criminal generan más oportunidades operativas y de investigación de las que la aplicación de la ley puede llegar a satisfacer. Por lo tanto, la identificación, así como una asignación de tareas y un establecimiento de prioridades meticulosos, deben ser cometidos imprescindibles en las reuniones estratégicas y operativas.
- Para garantizar una toma de decisiones basada en la inteligencia, los productos de inteligencia operativa y estratégica deben integrarse en los marcos de toma de decisiones y de asignación de tareas.

***Recopilación e intercambio de datos, información e inteligencia***

- Todos los funcionarios encargados de hacer cumplir la ley deberían estar obligados por ley u otras decisiones oficiales a compartir la información que hayan recibido sobre un presunto delito o un presunto delincuente, a través de mecanismos y canales de comunicación claramente definidos y de conformidad con la legislación nacional y las normas internacionales.
- Deben existir suficientes garantías para proteger los derechos humanos de las personas que se mencionan en la información recopilada con fines de análisis.
- Deben adoptarse las medidas necesarias para proteger la identidad y garantizar la seguridad de los informantes y confidentes.
- Dentro de los marcos jurídicos nacionales e internacionales aplicables, los códigos de tratamiento y la normativa sobre protección de datos, las autoridades deberán permitir el intercambio de datos e información entre los organismos estatales y otras instituciones oficiales.
- Las autoridades competentes podrán cerrar acuerdos oficiales que les permitan obtener y utilizar datos e información pertinentes de fuentes externas a los organismos estatales, incluidas las autoridades locales, las organizaciones no gubernamentales, la sociedad civil, el sector privado, las organizaciones regionales e internacionales, los medios informativos y el público, a condición de que estos acuerdos se encuentren dentro de los límites de los marcos jurídicos nacionales e internacionales aplicables. En los acuerdos también deberán establecerse las garantías adecuadas para evitar que las autoridades tengan acceso a dichos datos en contravención de las normas en materia de derechos humanos y protección de datos.
- Deberían decidirse los sistemas nacionales de evaluación de la información, incluidos los códigos de tratamiento y difusión, e incluirse en una decisión de carácter oficial.
- Todos los funcionarios encargados de hacer cumplir la ley deben estar plenamente familiarizados con esos códigos y aplicarlos a toda la información que reciban y envíen.

### ***Organismo/Departamento centralizado de inteligencia criminal***

- Esta guía recomienda que cada país disponga de un departamento nacional centralizado de inteligencia criminal (DNIC).
- El DNIC debería estar formado por miembros del personal de diversos organismos.<sup>57</sup>
- Los representantes de diferentes entidades encargadas del cumplimiento de la ley y de otras autoridades representadas en el DNIC deberían tener acceso a los datos e información de sus propios organismos y estar autorizados por ley a compartirlos con representantes de otras entidades/autoridades representadas en el DNIC, conforme a los marcos jurídicos nacionales e internacionales.
- El DNIC debería ser el responsable de una base de datos nacional de inteligencia criminal.
- El DNIC debería ser el responsable de realizar los análisis estratégicos y operativos, incluidas las evaluaciones de amenazas, a nivel nacional.
- El DNIC debería prestar asistencia a los departamentos y unidades regionales/locales de análisis de la información de inteligencia criminal, cuando proceda.<sup>58</sup>

### ***Análisis criminal y evaluación de amenazas***

- Las autoridades nacionales deben presentar decisiones oficiales y procedimientos operativos normalizados sobre transparencia en los métodos y procesos de análisis y evaluaciones de amenazas.
- Los tipos y estructuras de los productos de inteligencia criminal deben decidirse a nivel nacional, proporcionando a todos los encargados de hacer cumplir la ley un marco común de presentación de informes.
- Los informes de inteligencia criminal basados en normas y formatos internacionales comúnmente aceptados facilitan e incentivan la cooperación transfronteriza e internacional en materia penal.

### ***Interoperabilidad y seguridad en materia de tecnología de la información (TI)***

- Deben gestionarse a nivel nacional, regional y local estructuras de TI interconectadas, interoperables o de plataforma única en apoyo de la ILP.
- El DNIC debería tener acceso a todos los datos, información e inteligencia disponibles que posean los departamentos regionales y locales de inteligencia criminal y otros órganos encargados de hacer cumplir la ley.
- Es necesario contar con elementos de seguridad adecuados conforme a las decisiones oficiales y los procedimientos operativos normalizados, la legislación nacional y las normas internacionales, incluidos registros pormenorizados y mecanismos de control interno, así como niveles de acceso claramente definidos y registrados.
- Estas decisiones oficiales y procedimientos operativos normalizados deben abarcar la seguridad física, la seguridad de los documentos, la seguridad de la TI y la seguridad del personal, incluida la investigación y la verificación de los antecedentes del personal, cuando proceda.<sup>59</sup>

---

57 Véase también el subcapítulo 7.4.3 sobre el mecanismo de inteligencia criminal a nivel central. Véase también en el subcapítulo 8.2.3 un ejemplo de buenas prácticas en Suecia.

58 La UNODC presenta recomendaciones sobre gestión de las unidades de inteligencia en el documento 2011b: 51-59.

59 UNODC (2011b: 39-50).

- Las bases de datos de inteligencia criminal y el intercambio de datos, información e inteligencia deben estar sujetos a la supervisión y el control de una autoridad de control externa e independiente, establecida por ley para garantizar el cumplimiento de la legislación nacional de conformidad con las normas internacionales de derechos humanos y las disposiciones relativas a la protección de datos, y prever recursos eficaces y accesibles en caso de violación de las mismas.

***Mecanismos y práctica en materia de información de retorno***

- Los gestores y analistas que reciban información de los funcionarios encargados de hacer cumplir la ley deben proporcionar información de retorno para seguir fomentando los intercambios.
- Los gestores, los investigadores y otros usuarios de productos de análisis deben proporcionar información de retorno a los analistas sobre la calidad de los productos analíticos a fin de estimular los progresos y las mejoras.

***Gestión y control de la calidad***

- Los gestores a nivel nacional en el ámbito de la aplicación de la ley son responsables de las siguientes cuestiones: el desarrollo y mantenimiento de un sistema de supervisión y control de calidad en todos los niveles de aplicación de la ILP; la asignación de tareas y la toma de decisiones; los objetivos y resultados; los procesos internos; los productos de inteligencia criminal; el material y el equipo; y los recursos humanos, incluida la capacitación y el desempeño del personal.
- La totalidad del proceso de inteligencia de cada país deberá estar sometida a mecanismos de supervisión interna y externa.

***Cooperación e intercambio de información de inteligencia con los organismos encargados de hacer cumplir la ley en los planos regional e internacional***

- De conformidad con la legislación nacional, las normas internacionales y los instrumentos de asistencia jurídica mutua, los análisis estratégicos y las evaluaciones de amenazas nacionales deben compartirse con los países colaboradores pertinentes y con las organizaciones regionales e internacionales que proceda.
- El intercambio de inteligencia con autoridades de un Estado extranjero debe basarse en una normativa nacional que establezca parámetros claros para dicho intercambio, incluidas las condiciones que deben cumplirse para compartir la información, las entidades con las que se puede compartir la inteligencia y las garantías aplicables a los intercambios de inteligencia.<sup>60</sup>
- Deberían adoptarse medidas proactivas para establecer investigaciones y operaciones conjuntas basadas en la inteligencia en los planos regional e internacional, que se centren en problemas delictivos comunes que hayan sido identificados y presentados en informes de análisis y evaluación de amenazas.

---

60 Asamblea General de las Naciones Unidas. "Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo". Consejo de Derechos Humanos de las Naciones Unidas, 17 de mayo de 2010, A/HRC/14/46: Artículos 26, 38 y 90.

### 7.3 Análisis y toma de decisiones en materia de aplicación de la ley

La aplicación proactiva de la ley requiere información de inteligencia y planificación estratégica. Además de una exigencia cada vez mayor respecto a la mejora en la eficiencia de los recursos, la transparencia y la rendición de cuentas, hay una serie de factores condicionantes, externos y personales, que afectan a los encargados de la toma de decisiones, tal y como se muestra en la figura 7.2.



Figura 7.2 **Influencias externas y personales que afectan a los encargados de la toma de decisiones**

Fuente: Ratcliffe (2016: 118).

Los responsables de la toma de decisiones en el marco de la aplicación de la ley moderna tienen que vivir con el hecho de que hay una amplia gama de factores condicionantes que afectan a su trabajo diario y a sus decisiones clave. La gestión policial de calidad, incluida la toma de decisiones, requiere productos de análisis de calidad y analistas capacitados que puedan ayudar a los gestores a proporcionar informes a medida. Dado que la mayoría de las decisiones en el ámbito de la aplicación de la ley afectan directamente a la vida de las personas, y dado que todos los funcionarios encargados de hacer cumplir la ley son responsables



de sus acciones<sup>61</sup>, la base informativa de su adopción de decisiones pasa a ser una cuestión especialmente importante. Estos hechos enfatizan aún más la relevancia de la ILP como marco para la toma de decisiones del personal directivo.

“Suele ser algo típico en los sistemas débiles de toma de decisiones de la policía que los analistas se autoasignen tareas o tomen la iniciativa en la determinación de prioridades estratégicas. En los sistemas de toma de decisiones consolidados, los altos cargos policiales desempeñan un papel más directo al comunicar sus intenciones cuando asignan tareas a la unidad de inteligencia y análisis. Aunque siguen abiertos a posibles influencias de amenazas emergentes que podrían no aparecer en su radar, los mandos experimentados no dejan al grupo de análisis de su departamento de policía a la deriva y sin orientaciones, sino que le proporcionan supervisión y dirección”.

– **Ratcliffe (2016: 83).**

Aunque los analistas siempre deben basar sus conclusiones analíticas en evaluaciones y valoraciones neutrales, también deberían tener conocimiento del entorno que rodea a los responsables de la toma de decisiones, incluidas las posibles limitaciones legales, políticas, organizativas y financieras. Esto debe tenerse en cuenta a la hora de desarrollar y presentar recomendaciones. Es inútil que los analistas presenten recomendaciones que resulten claramente inapropiadas para los clientes o que estén fuera de su alcance.

## **7.4 Niveles de los mecanismos de inteligencia criminal**

La ILP requiere estructuras organizativas, procedimientos administrativos y de toma de decisiones, y mecanismos de comunicación entre todos los niveles. En este subcapítulo se presentan los mecanismos de inteligencia (unidades/departamentos/organismos) que brindan apoyo a la ejecución de la ILP. Una de las tareas principales del mecanismo de inteligencia criminal de cada nivel es proporcionar análisis y evaluaciones a las estructuras de gestión para que adopten decisiones fundamentadas.

### **7.4.1 Mecanismo de inteligencia criminal de nivel local/de comisarías**

El mecanismo de inteligencia criminal de nivel local/de comisarías abarca los delitos, los delincuentes y los problemas de seguridad y protección que afectan a las unidades básicas de mando policial en la demarcación correspondiente a la comisaría de policía. Dependiendo

61 Consejo de Europa, *The European Code of Police Ethics* (Estrasburgo: Publicaciones del Consejo de Europa, marzo de 2002): Art. 26, 38 y 90.

de su tamaño y estructura, cada nivel local debería disponer de una unidad de inteligencia criminal o un equipo responsable de todas las tareas operativas de inteligencia criminal correspondientes a su nivel. Esa unidad debería estar encabezada por un mando policial del mismo rango que los jefes de unidades operativas y de investigación de nivel local o de comisarías.

La inteligencia criminal de nivel local o de comisarías presta apoyo a la planificación, las operaciones y las investigaciones locales. Más concretamente:

- apoya a los servicios policiales operativos en general para luchar contra la delincuencia cotidiana y mantener la seguridad y el orden público a nivel local o en el radio de acción de las comisarías;
- proporciona apoyo analítico a las investigaciones de nivel local o de comisarías;
- proporciona datos e información para los registros, las bases de datos y los procesos de inteligencia criminal de la policía;
- remite datos, información e inteligencia pertinentes a los departamentos de inteligencia criminal regionales y/o nacionales para su posterior procesamiento;
- lleva a cabo y presenta análisis y evaluaciones de riesgos sobre eventos locales; y
- proporciona apoyo analítico para la prevención de la delincuencia local.

### 7.4.2 Mecanismo de inteligencia criminal de nivel regional

La sección regional de inteligencia criminal abarca las tareas de aplicación de la ley que afectan a más de una unidad básica de mando policial. Sus tareas y responsabilidades fundamentales son la identificación de amenazas criminales comunes en el ámbito regional, el intercambio de información apropiada y la prestación de capacidades y recursos para apoyar las actividades en el plano local y regional. La sección regional de inteligencia criminal debería tener el mismo nivel y estar encabezada por personal del mismo rango que los jefes de operaciones e investigaciones regionales, justo un nivel por debajo del responsable regional de la policía.

El departamento o la sección regional de inteligencia criminal presta apoyo a las unidades locales de inteligencia criminal que lo soliciten. Su función principal es de apoyo a la planificación, las operaciones y las investigaciones regionales. Más concretamente:

- elabora y pone en práctica planes regionales anuales de inteligencia criminal;
- recopila sistemáticamente los datos, la información y la inteligencia pertinentes a nivel regional y los remite a una base de datos regional centralizada, accesible para la entidad centralizada de inteligencia criminal de cada país (en adelante, el Departamento Nacional de Inteligencia Criminal (DNIC));
- transmite los datos, la información y los informes de inteligencia pertinentes a los niveles local y nacional;
- lleva a cabo análisis y evaluaciones estratégicas para apoyar a los gestores en la toma de decisiones y la planificación a nivel regional;
- presta apoyo para la prevención de la delincuencia regional; y
- apoya las investigaciones y operaciones contra la delincuencia regional y transfronteriza, incluida la delincuencia organizada transnacional.

### 7.4.3 Mecanismo de inteligencia criminal de nivel central

El DNIC debería estar ubicado en la sede nacional de los organismos encargados del cumplimiento de la ley (dirección de policía/organismo nacional de lucha contra la delincuencia) y estar encabezado por un oficial de alto rango.

La función principal del DNIC es elaborar informes de inteligencia para apoyar la adopción de decisiones en la lucha contra las amenazas nacionales graves, en particular la delincuencia organizada transnacional, el terrorismo, y el extremismo violento y la radicalización que conducen al terrorismo. Sus responsabilidades principales incluyen:

- elaborar y ejecutar un plan nacional anual de inteligencia criminal;
- redactar y presentar una evaluación de amenazas en materia de delincuencia grave y organizada a nivel nacional;
- redactar y presentar otras evaluaciones estratégicas para apoyar la gestión y planificación de la aplicación de la ley a nivel nacional;
- proporcionar apoyo de inteligencia criminal a nivel regional;
- establecer normas y coordinar la labor de inteligencia criminal en todo el país;
- actuar como punto de contacto nacional con las autoridades y organizaciones extranjeras encargadas de hacer cumplir la ley, en relación con la labor de inteligencia criminal; y
- llevar a cabo investigaciones y luchar por el desarrollo profesional a nivel local, regional y nacional.<sup>62</sup>

Lo ideal sería que el DNIC fuera una entidad dedicada a la aplicación de la ley de alcance interinstitucional, cuyo personal estuviera compuesto por expertos de diversos organismos e instituciones estatales pertinentes, en la que cada experto tuviera acceso a la información y las bases de datos de su institución, y estuviera autorizado por ley a compartir datos e información con el personal de otros organismos/instituciones representados en el DNIC. Dependiendo de las estructuras de seguridad de cada país, las siguientes autoridades estatales podrían estar representadas en el DNIC:

- Policía de Fronteras
- Autoridades del sistema penitenciario
- Aduanas
- Unidad de Inteligencia Financiera
- Guardacostas/Policía marítima
- Organismos de inteligencia y seguridad
- Policía
- Autoridades tributarias
- Organismos especializados pertenecientes al ámbito de la aplicación de la ley, cuando proceda

Los organismos/instituciones representados en el DNIC podrían preferir la concertación de acuerdos formales de cooperación entre ellos y el DNIC. En el marco de esos acuerdos, algunos Estados participantes de la OSCE han optado por nombrar a representantes de los organismos e instituciones mencionados como oficiales de enlace dentro del DNIC.

<sup>62</sup> Véanse también las recomendaciones de la UNODC sobre gestión y establecimiento de normas para unidades de inteligencia criminal (2011b: 51, 61).

## 7.5 Reuniones de asignación de tareas y coordinación

Varios Estados participantes de la OSCE han desarrollado mecanismos de toma de decisiones proactivos y basados en la inteligencia, denominados comúnmente “reuniones de asignación de tareas y coordinación”, “reuniones de dirección y coordinación” o “reuniones de intercambio e información”. Las *reuniones de asignación de tareas y coordinación* se llevan a cabo en los tres niveles: local, regional y nacional. Sus objetivos principales son los siguientes: reunir a representantes de la aplicación de la ley pertinentes de todos los niveles para que tomen decisiones sobre planes, establecimiento de prioridades, operaciones e investigaciones, sobre la base de documentos de análisis y evaluación; determinar las deficiencias en materia de información/inteligencia que deben subsanarse; y decidir la asignación de recursos financieros y humanos. Este sistema constituye el cimiento de la ILP, ya que traslada los resultados de los análisis a los procedimientos de gestión, haciendo que la toma de decisiones esté mejor fundamentada, se base en la inteligencia, y sea transparente y responsable. Además, la creación de mecanismos de inteligencia criminal que sirven para la adopción de decisiones en cada nivel permite a la dirección policial dar prioridad a determinadas tareas de aplicación de la ley en función de las amenazas identificadas y evaluadas, y asignar los recursos financieros, humanos y de otro tipo disponibles a las prioridades en cuestión. Determinar las deficiencias y las necesidades en materia de inteligencia y asignar tareas a los departamentos o unidades de análisis para que satisfagan esas necesidades es también una labor importante de las reuniones de toma de decisiones en cada nivel. Para garantizar la circulación de información y la coordinación entre los niveles, el presidente u otro representante del nivel inferior participa también en las reuniones del nivel superior.

Esta guía sugiere que las reuniones de asignación de tareas y coordinación se dividan en *reuniones de asignación de tareas estratégicas y coordinación*, y *reuniones de asignación de tareas operativas y coordinación*.

### 7.5.1 Reuniones de asignación de tareas estratégicas y coordinación

Como su propio nombre indica, estas reuniones deben centrarse en cuestiones estratégicas y tienen lugar con mucha menos frecuencia que las reuniones operativas, normalmente dos veces al año o cada trimestre. En algunos países, las *reuniones de asignación de tareas estratégicas y coordinación* se celebran en los tres niveles, pero lo más habitual es que solo tengan lugar en el nivel central/nacional. Estas reuniones deben centrarse en la planificación de estrategias y el establecimiento de prioridades y objetivos estratégicos, sobre la base de análisis estratégicos y evaluaciones de amenazas, así como de los ciclos de planificación de la actuación institucional y presupuestaria. Se recomienda que las *reuniones de asignación de tareas estratégicas y coordinación* determinen y establezcan prioridades para las necesidades nacionales de inteligencia, para la prevención y la aplicación de la ley, sobre la base de las conclusiones de análisis estratégicos y evaluaciones de las amenazas. Una vez tomado ese conjunto de decisiones, en las reuniones se deberá determinar la cantidad de recursos necesarios para la aplicación de las medidas estratégicas seleccionadas.<sup>63</sup>

---

63 Véanse los ejemplos nacionales de buenas prácticas descritos en el subcapítulo 8.2.

### 7.5.2 Reuniones de asignación de tareas operativas y coordinación

Esta guía recomienda que las reuniones de toma de decisiones operativas en materia de ILP se lleven a cabo en los tres niveles una vez a la semana o cada dos semanas. Los responsables de operaciones e investigaciones deben asistir a ellas junto con los gestores del departamento de inteligencia criminal y de la unidad/departamento de análisis pertinente, así como con otros expertos, si se considera necesario. Se recomienda que el gestor operativo de más alto rango dirija cada reunión. Dependiendo de los niveles y de las circunstancias nacionales/regionales/locales, las *reuniones de asignación de tareas operativas y coordinación* principalmente tienen los siguientes cometidos: convertir los planes estratégicos en planes de acción, armonizar las necesidades, prioridades y recursos; evaluar los informes operativos de inteligencia nuevos o actualizados y tomar decisiones sobre nuevas investigaciones o actividades operativas, o bien cerrar o combinar actividades; identificar las deficiencias en materia de información e inteligencia y encomendar a las unidades/departamentos de inteligencia criminal la tarea de subsanarlas; y supervisar los progresos operativos en curso.

### 7.6 Capacitación y concienciación

La capacitación es un factor clave para el progreso de cualquier organización. Cuando se planifica y se pone en práctica la ILP, es esencial desarrollar un plan de capacitación y llevar a cabo una capacitación coordinada de todos los encargados de hacer cumplir la ley. Se espera de todos los miembros del personal que no solo adquieran las competencias necesarias para su desempeño, sino que también comprendan las funciones del resto de miembros para contribuir a lograr los resultados globales pretendidos en la aplicación de la ILP. Mediante la capacitación, el personal deberá entender qué es la ILP, cómo funciona el proceso de inteligencia, qué aportar y cómo contribuir a ese proceso y cómo hacer uso del mismo. La cultura del intercambio de información debería ser un elemento destacado dentro de la capacitación en todos los niveles. Además, la capacitación deberá incluir los requisitos legales relacionados con las funciones de la ILP y las normas internacionales pertinentes en materia de derechos humanos y protección de datos, en la medida adecuada según el nivel y el cometido de los funcionarios.

“Para que la actividad policial basada en la inteligencia tenga éxito y se convierta en el paradigma central de la labor policial en el siglo XXI, será fundamental abordar la capacitación y la educación sobre reducción de la delincuencia no solo para los analistas, sino también para los mandos policiales y los principales responsables de la toma de decisiones en el sistema de justicia penal, y es muy posible que este termine siendo el factor determinante que decida el futuro de la actividad policial basada en la inteligencia”.

– Ratcliffe (2016: 143).

### ***Concienciación de las altas esferas***

Como se ha subrayado anteriormente, el apoyo político y un alto grado de compromiso gubernamental con la ILP son requisitos previos para su aplicación satisfactoria. Para ello es necesaria la concienciación de las altas esferas, en particular de los políticos, los funcionarios gubernamentales de todos los ministerios y organismos estatales pertinentes, los fiscales generales y otros representantes clave de la fiscalía, así como de los altos cargos de todos los organismos y servicios encargados de hacer cumplir la ley.

### ***Capacitación de directores y gestores en materia de aplicación de la ley***

El objetivo principal de esta capacitación consiste en demostrar de qué manera el marco y el análisis de la ILP, en particular, pueden ayudar a los responsables de la formulación de políticas y a los altos cargos relacionados con la aplicación de la ley a la hora de tomar decisiones y llevar a cabo sus planificaciones. El éxito en la capacitación de los altos cargos se traducirá en un mayor nivel de comprensión del potencial de la ILP, de cómo asignar tareas a los analistas y de cómo hacer uso de los productos de análisis en la toma de decisiones y la planificación operativa y estratégica. Esta capacitación también debería facilitar a los responsables de la toma de decisiones nociones sobre las normas nacionales e internacionales pertinentes en materia de derechos humanos y protección de datos, así como sobre las posibles cuestiones de derechos humanos que puedan surgir en la ILP y la forma en que pueden abordarse.

### ***Capacitación de analistas***

Esta capacitación se divide normalmente en formación sobre análisis estratégicos y sobre análisis operativos, de acuerdo con las dos categorías principales de análisis. Los analistas deben recibir la capacitación más compleja para comprender el papel y las funciones del análisis criminal en el ámbito de la aplicación de la ley, y el marco legislativo y los requisitos legales que se aplican a los diferentes métodos de recopilación de información, así como al intercambio y la utilización de la información. El desarrollo de aptitudes y competencias en la recopilación y estructuración de datos e información, así como en la realización de análisis detallados, la extracción de conclusiones y la presentación de recomendaciones, también deberían formar parte de esa capacitación. Además, la capacitación de analistas abarca las siguientes cuestiones: la competencia para redactar informes; la colaboración entre el análisis y la investigación, y entre el análisis y la toma de decisiones; los métodos, las herramientas y las técnicas de análisis y los programas informáticos de análisis; las fuentes de información; los códigos de evaluación; y los marcos jurídicos, los derechos humanos y la ética policial en relación con todas estas tareas. La capacitación puede estructurarse en diversas fases y para diferentes niveles.

### ***Capacitación de investigadores***

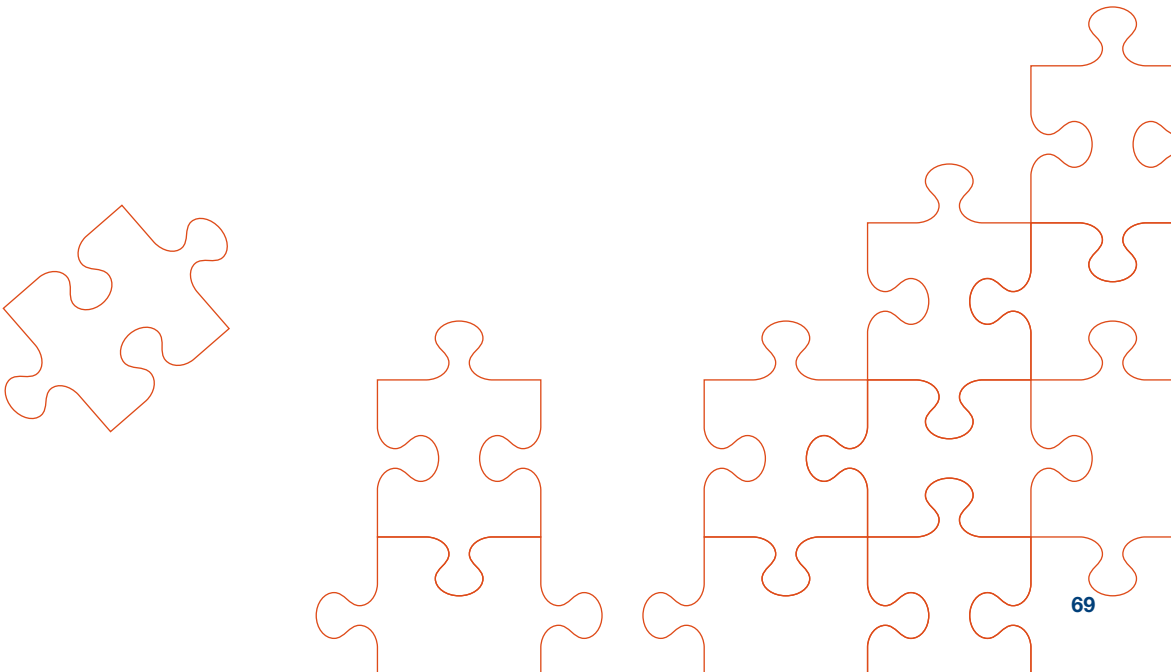
Las investigaciones también incluyen el trabajo de inteligencia operativa. Por ese motivo, los investigadores han de recibir una capacitación adecuada en materia de ILP antes de comenzar a trabajar en las investigaciones. La capacitación de los investigadores debe incluir una introducción al análisis operativo y a la forma en que este puede prestar apoyo a las investigaciones criminales, así como la cooperación entre analistas e investigadores.

***Capacitación de agentes de policía uniformados***

Los agentes de policía uniformados están en contacto directo con el público y con personas involucradas en delitos y, por lo tanto, representan una valiosa fuente de información para el sector de la inteligencia. Todos los agentes uniformados deben recibir capacitación general sobre la ILP y sus principales componentes, incluidas sus responsabilidades dentro del modelo de ILP.

***Capacitación de agentes en formación***

La capacitación en materia de ILP ya debería estar integrada en la instrucción básica de los agentes de policía. Es particularmente importante aclarar todos los conceptos básicos pertenecientes al ámbito de la ILP para evitar tergiversaciones innecesarias en relación con el mundo de la inteligencia criminal. Habría que esforzarse para lograr que los trabajos de inteligencia criminal formen parte de las actividades policiales habituales, un campo atractivo para futuros agentes de policía.





## 8. La ILP en la práctica

Los capítulos anteriores se han centrado en explicar el concepto de ILP y el proceso de análisis de la inteligencia criminal; en ellos se han expuesto algunos de los retos y condiciones fundamentales para lograr una aplicación satisfactoria de la ILP, y se han presentado sugerencias sobre la estructura organizativa necesaria para facilitar una puesta en práctica efectiva de la ILP.

Sobre la base de los capítulos anteriores, el Capítulo 8 presenta una serie de ejemplos de ILP en la práctica, precedidos de un subcapítulo acerca del papel fundamental que pueden desempeñar las evaluaciones de amenazas en la lucha contra la delincuencia grave y organizada. A continuación, se presentan cinco ejemplos de buenas prácticas en la aplicación nacional de la ILP o de sus componentes clave. Por último, los subcapítulos 8.3 y 8.4 presentan la ILP y la actividad policial de proximidad, así como la ILP en la prevención y la lucha contra el terrorismo, y contra el extremismo violento y la radicalización que conducen al terrorismo.

### 8.1 ILP, evaluaciones de amenazas y planificación estratégica en la lucha contra la delincuencia organizada

La delincuencia organizada amenaza la paz y la seguridad humana, pone en peligro el disfrute de los derechos humanos y socava el desarrollo económico, social, cultural, político y civil de las sociedades de todo el mundo.<sup>64</sup> Sin embargo, las autoridades encargadas de hacer cumplir la ley solo pueden investigar un pequeño porcentaje de la información e inteligencia que reciben sobre las redes de delincuencia organizada en sus respectivas jurisdicciones. Por ese motivo, es vital evaluar la gravedad de estas amenazas y decidir sobre su orden de prioridad, así como asignarles los recursos humanos, financieros y técnicos disponibles. El modelo de ILP proporciona el marco necesario para un enfoque moderno y para que las estructuras organizativas adopten lo que se reconoce comúnmente como la única opción viable para hacer

64 [www.unodc.org/unodc/en/organized-crime/index.html?ref=menuaside](http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuaside)





frente a la delincuencia organizada transnacional, a saber, el análisis de datos e información, el intercambio y la cooperación, y el examen de las amenazas identificadas y evaluadas estableciendo prioridades y seleccionando objetivos.

“La delincuencia grave y organizada seguirá siendo muy dinámica y muy rápida a la hora de explotar cualquier cambio que se dé en el entorno más amplio. Las autoridades encargadas de garantizar el cumplimiento de la ley [...] tienen el reto de seguir el ritmo de la innovación tecnológica y de la creciente complejidad de las actividades delictivas que invaden todos los sectores de la economía y la sociedad, al mismo tiempo que han de limitar sus gastos o, en muchos casos, hacer frente a una reducción de sus presupuestos. Al igual que la delincuencia, la policía se está volviendo cada vez más compleja y la lucha contra los delincuentes requiere ahora un grado de especialización y conocimientos especializados sin precedentes. Las autoridades encargadas de garantizar el cumplimiento de la ley tendrán que encontrar la manera de conciliar las limitaciones presupuestarias con la necesidad de poseer conocimientos altamente especializados. [...] El análisis avanzado de datos puede ayudar a las autoridades encargadas de garantizar el cumplimiento de la ley a priorizar sus esfuerzos y a participar en una labor policial verdaderamente efectiva y basada en la inteligencia”.

– **Europol (2015: 44).**

### 8.1.1 El ciclo de actuación de la UE

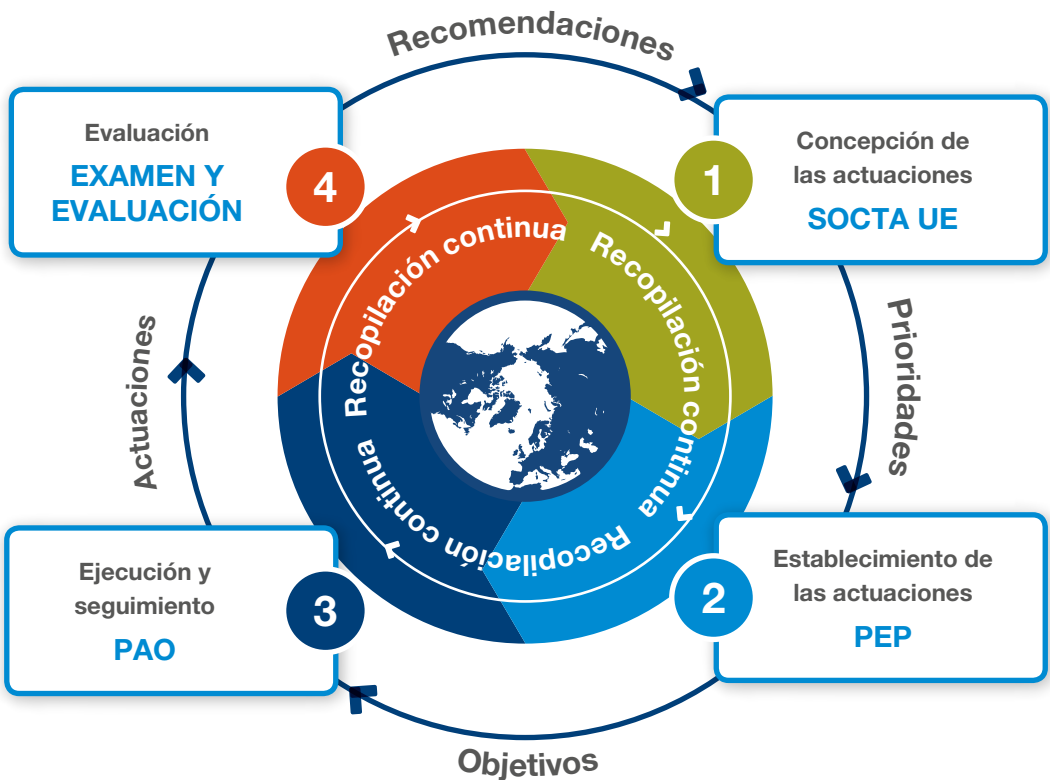
La UE introdujo formalmente la ILP en 2005.<sup>65</sup> Desde entonces, la planificación estratégica común de la UE y sus planes de acción operativos para hacer frente a la delincuencia organizada se han desarrollado utilizando el enfoque de la ILP. En 2010, la UE adoptó el *Ciclo de Actuación de la UE contra la Delincuencia Organizada y las Formas Graves de Delincuencia*, que se presenta aquí como un ejemplo de buenas prácticas para abordar la delincuencia organizada transnacional de acuerdo con los principios de la ILP.<sup>66</sup>

65 Consejo de la Unión Europea. “Conclusiones del Consejo sobre las funciones policiales basadas en la inteligencia y el desarrollo de la evaluación de la amenaza de la delincuencia organizada (EADO)”. Doc. 10180/4/05, REV 4 (Bruselas: 3 de octubre de 2005).

66 Consejo de la Unión Europea. “Council conclusions on the creation and implementation of a EU policy cycle for organized and serious international crime.” Sesión nº 3043 del Consejo de Justicia y Asuntos de Interior (Bruselas: 8 y 9 de noviembre de 2010).

El ciclo de actuación de la UE pretende ofrecer un marco coherente y acciones operativas sólidas para hacer frente a las amenazas delictivas más acuciantes a las que se enfrenta la UE. El ciclo de actuación brinda la oportunidad de integrar las diferentes estructuras mediante un enfoque multidisciplinar, y está orientado hacia ese fin, e incluye la generación de sinergias entre las autoridades encargadas de hacer cumplir la ley y las encargadas de la gestión de fronteras, así como la facilitación de una mayor cooperación entre los organismos europeos, y también con las partes interesadas no pertenecientes a la UE.

Cada ciclo de actuación tiene una duración total de cuatro años y consta de cuatro fases principales, como se indica en la figura 8.1.



PEP: Planes estratégicos plurianuales  
PAO: Planes de acción operativos

Figura 8.1 El Ciclo de Actuación de la UE contra la Delincuencia Organizada y las Formas Graves de Delincuencia

Fuente: Consejo de la Unión Europea (2014).

## **FASE 1 – Evaluación por la UE de la amenaza que representan la delincuencia organizada y las formas graves de delincuencia internacional (en lo sucesivo, evaluación SOCTA)**

Europol se encarga de desarrollar y publicar la evaluación SOCTA, en colaboración con el Grupo Asesor de la evaluación SOCTA (compuesto por Estados miembros de la UE, organismos de la UE, la Comisión Europea y la Secretaría General del Consejo) y con el apoyo de terceros países y organizaciones asociados con Europol. Dado que su metodología ha sido aprobada por el Consejo de Ministros de Justicia y Asuntos de Interior de la UE, cuenta con un marco jurídico claro y un sólido respaldo político.<sup>67</sup>

“De las prioridades estratégicas a la acción operativa, [la evaluación SOCTA] velará por que un enfoque basado en la inteligencia sea el eje central de la lucha contra las principales amenazas criminales a las que se enfrenta la UE”.

– **Europol (2010).**

El proceso de la evaluación SOCTA de Europol incluye:

- preparación y respaldo de las necesidades detalladas de los clientes;
- preparación y respaldo de la metodología;
- identificación de las necesidades de inteligencia;
- recopilación de datos;
- análisis de datos;
- redacción del informe de la evaluación SOCTA, incluida una lista de amenazas y riesgos clave; y
- presentación de los resultados y las prioridades recomendadas.

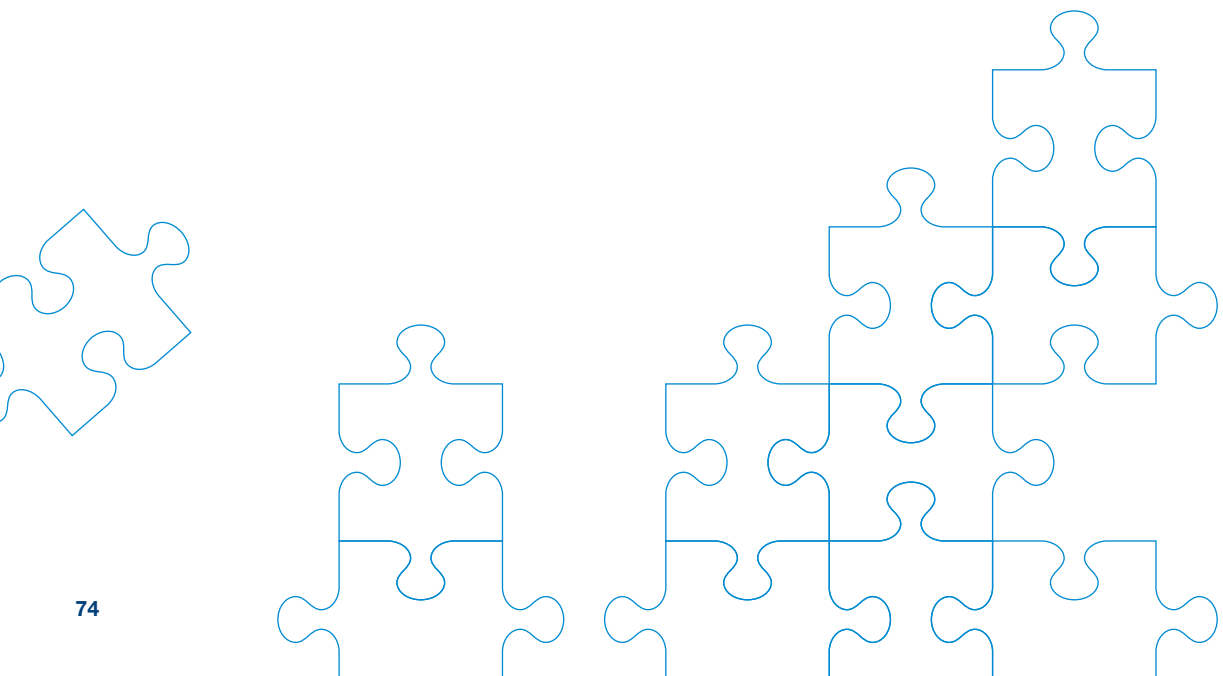
El proceso de análisis se lleva a cabo centrándose en cuatro elementos; para cada uno de ellos se recopilan datos específicos (véase el cuadro 8.1):

- **ámbitos/tipos de delincuencia** grave y organizada;
- **grupos/redes delictivas** organizadas e individuos implicados en delitos graves que actúan en solitario;
- **entorno:** vulnerabilidades, oportunidades e infraestructuras; y
- **efectos y daños.**

<sup>67</sup> Consejo de la Unión Europea. *Serious and Organised Crime Threat Assessment 2017 – Revised methodology*. (Evaluación de la amenaza de la delincuencia grave y organizada 2017 - Metodología revisada). Doc. 14913/15, CRIMORG 128 (Bruselas: 11 de diciembre de 2015).

La evaluación básica de la amenaza se lleva a cabo mediante la realización de un análisis cualitativo de dos tipos de indicadores, que se muestran en las dos primeras columnas del cuadro 8.1. Sin embargo, una amenaza solo puede causar algún daño si existen vulnerabilidades. Por lo tanto, con el fin de proporcionar una evaluación exhaustiva de los riesgos derivados de esas amenazas, es necesario identificar, analizar y evaluar otros elementos de vulnerabilidad y de posibilidad o probabilidad, así como sus efectos y daños. El documento metodológico público de la evaluación SOCTA enumera los siguientes indicadores de amenaza y riesgo para ser evaluados en el proceso de la evaluación SOCTA, que se muestran en el cuadro 8.1.

Las evaluaciones de amenazas no son informes descriptivos de la situación actual, sino que están orientadas al futuro. Presentan conclusiones mediante una lista de amenazas clave y recomendaciones sobre cómo darles prioridad. Los informes de la evaluación SOCTA de Europol se envían al Comité Permanente de la UE de Cooperación Operativa en materia de Seguridad Interior (COSI), donde se debaten en el marco del proceso político de elaboración de políticas de la UE. Por lo tanto, la decisión finalmente adoptada será una mezcla de evaluaciones de expertos profesionales y perspectivas políticas.



**Cuadro 8.1 Conjunto de los indicadores analizados durante el proceso de la evaluación SOCTA**

EVALUACIÓN DE LA AMENAZA		EVALUACIÓN DE LA AMENAZA Y LOS RIESGOS	
Ámbitos/ Tipos delictivos	Grupos/ Redes delictivas	Factores del entorno relevantes para la delincuencia	Efectos/Daños
Disponibilidad de recursos	Ámbitos/Tipos delictivos en los que actúan	Situación económica	Repercusión financiera
Demanda y suministro	Actividades multidelictivas	Situación geopolítica	Repercusión social
Número de grupos activos en el ámbito/ tipo delictivo	Nacionalidad	Infraestructura de transportes y logística	Repercusión sanitaria
Evolución del ámbito/ tipo delictivo	Tamaño del grupo	Actitudes del público	Impacto medioambiental
Dimensión geográfica	Recursos financieros	Innovación	
Otros ámbitos/tipos delictivos conexos	Recursos humanos	Internet y nuevas tecnologías	
Modus operandi utilizado	Beneficio económico	Legislación	
	Otros recursos	Actuación en materia de aplicación de la ley	
	Estructura, tipo	Prioridades de la UE en relación con la delincuencia establecidas por el Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI)	
	Conocimientos especializados		
	Cooperación		
	Modus operandi		
	Dimensión geográfica		
	Flexibilidad y capacidad de adaptación		
	Contramedidas		
	Corrupción e influencia en el sector público		
	Uso de estructuras comerciales legales		
	Blanqueo de dinero – grado de sofisticación		
	Violencia externa		

### FASE 2 – Planes estratégicos plurianuales

Sobre la base de la evaluación SOCTA, el Consejo de Ministros de Justicia y Asuntos de Interior de la UE toma una decisión oficial sobre los ámbitos delictivos prioritarios para los cuatro años subsiguientes. Al establecer estas políticas, el Consejo tiene en cuenta las observaciones de los Estados miembros de la UE, de sus organismos y de los países asociados no pertenecientes a la UE.

Para cada una de las prioridades, un grupo de expertos de los países más afectados elabora un Plan estratégico plurianual (PEP) de cuatro años. Estos planes multidisciplinarios contienen una lista de objetivos estratégicos que deben cumplirse durante el ciclo cuatrienal correspondiente. En todos los planes se incluyen indicadores clave de desempeño, calendarios, metas y organismos/personas responsables. El COSI aprueba los PEP, confiriéndoles un estatus oficial y garantizando los recursos financieros.

### FASE 3 – Planes de acción operativos (PAO) y la Plataforma multidisciplinaria europea contra las amenazas delictivas (EMPACT)

Cada PEP se desarrolla en Planes de acción operativos (PAO) establecidos por orden de prioridad y por año. Todos los PAO describen las medidas y actuaciones de las instituciones y organismos de la UE, así como aquellas acciones que deberán llevar a cabo las autoridades nacionales.

Las acciones conjuntas dentro de los PAO se ejecutan en el marco del mecanismo de la Plataforma multidisciplinaria europea contra las amenazas delictivas (EMPACT). Este mecanismo proporciona una plataforma de cooperación estructurada para los Estados miembros pertinentes, las instituciones y los organismos de la UE, así como para los socios exteriores de la UE. La ejecución de cada PAO está dirigida por un “impulsor” del Estado miembro de la UE que se ha ofrecido como voluntario, y se somete a supervisión nacional por parte de los Coordinadores Nacionales de la EMPACT, designados en cada Estado miembro. Europol ofrece apoyo administrativo y logístico a los proyectos EMPACT y supervisa sus progresos. También designa a gestores de apoyo a la plataforma EMPACT para garantizar el apoyo analítico y operativo a todas las prioridades en materia delictiva. El COSI aprueba los PAO y supervisa su ejecución a través de informes presentados semestralmente.

Se invita y alienta a todas las autoridades nacionales de la UE a que integren los PEP y los PAO en sus procesos nacionales de planificación y en sus esfuerzos encaminados a la aplicación de la ley para luchar contra la delincuencia grave y organizada. También se anima a los organismos pertinentes de la UE a que incluyan las prioridades y los planes de acción en sus programas de trabajo anuales.

### FASE 4 – Examen y evaluación

La efectividad de los PAO y sus repercusiones en las amenazas prioritarias serán revisadas por el COSI. La presentación de informes anuales por parte de los impulsores nacionales y una evaluación intermedia por parte de Europol ofrecen la oportunidad de adaptar o mod-

ificar los PAO, o las prioridades, si fuera necesario. Se presenta anualmente el estado de la cuestión al COSI, el cual lleva a cabo una evaluación exhaustiva e independiente al final de cada ciclo de actuación. Las enseñanzas que se desprenden de esa evaluación se aportan al siguiente ciclo de actuación.

### 8.1.2 La herramienta Sleipnir de evaluación de la delincuencia organizada

La técnica Sleipnir fue desarrollada para mejorar el establecimiento de prioridades estratégicas, proporcionando un método fiable, objetivo y basado en la experiencia en relación con el análisis de inteligencia criminal para ayudar a clasificar y comparar la amenaza de los grupos delictivos organizados, así como para identificar lagunas en la labor de inteligencia.

La técnica Sleipnir proporciona a los analistas de inteligencia especializados en grupos de delincuencia organizada un método integral y transparente para elaborar y presentar recomendaciones y apoyar a los servicios de inteligencia de manera concisa. Sin embargo, el objetivo no consiste en aislar el marco y la matriz resultantes, sino que estos deben ser desarrollados en el contexto de una evaluación analítica estratégica que explique los detalles y la importancia de las comparaciones.<sup>68</sup>

Originalmente se establecieron 19 criterios o atributos para evaluar los niveles relativos de amenaza. A todos ellos se les asigna un valor (o bien “desconocido”, o bien de “nulo” a “alto”) sobre la base de la magnitud observada en cada uno, pero una versión actualizada de la técnica Sleipnir ha reducido el número de atributos a 12. Eso hizo que el proceso de recopilación de información fuera más eficiente, mientras que los atributos restantes se centrarían en comportamientos más fáciles de observar.

Sin embargo, debe entenderse que Sleipnir es una herramienta estratégica utilizada para ayudar a determinar las prioridades de una organización y no está diseñada para ser utilizada como una herramienta de inteligencia táctica. La técnica Sleipnir también se basa en ciertos supuestos que pueden no reflejar los vínculos cada vez más complejos y sofisticados entre los grupos delictivos organizados internacionales y entre estos grupos y las organizaciones terroristas. Esto podría conducir al desarrollo de prioridades estratégicas que se centraran demasiado en organizaciones grandes y sofisticadas, ignorando a grupos más pequeños y potencialmente más peligrosos vinculados con la delincuencia organizada en otros países o con el terrorismo.<sup>69</sup> Además, Sleipnir se basa en suposiciones que determinan las mayores amenazas percibidas por la sociedad canadiense, y el orden de clasificación de esos atributos puede no reflejar necesariamente el de otras sociedades o jurisdicciones.

68 Inteligencia Criminal de la Real Policía Montada de Canadá. “Sleipnir Version 2.0, Organized Crime Groups Capability Measurement Matrix” (Versión Sleipnir 2.0, Matriz de Medición de Capacidad de Grupos Delictivos Organizados). Real Policía Montada de Canadá (Ottawa, 2011).

69 Ratcliffe, Strang y Taylor (2014: 206-227).

Cuadro 8.2 Comparación de cinco grupos delictivos mediante el modelo Sleipnir

	GRUPO 1	GRUPO 2	GRUPO 3	GRUPO 4	GRUPO 5	GRADO DE AMENAZA	
Corrupción	Alto	Alto	Medio	Bajo	Nulo	Alto	Alto
Violencia	Alto	Alto	Medio	Bajo	Bajo	Medio	Medio
Infiltración	Alto	Alto	Bajo	Alto	Bajo	Bajo	Bajo
Blanqueo de dinero	Alto	Alto	Alto	Bajo	Bajo	Nulo	Nulo
Colaboración	Alto	Bajo	Bajo	Bajo	Alto	Desconocido	Desconocido
Aislamiento	Alto	Bajo	Bajo	Alto	Bajo	Desconocido	Desconocido
Monopolio	Alto	Bajo	Alto	Bajo	Alto	Desconocido	Desconocido
Alcance	Bajo	Alto	Alto	Bajo	Nulo	Desconocido	Nulo
Uso de inteligencia	Bajo	Bajo	Alto	Bajo	Alto	Desconocido	Desconocido
Diversificación	Bajo	Bajo	Bajo	Nulo	Medio	Desconocido	Medio
Disciplina	Alto	Bajo	Alto	Bajo	Alto	Desconocido	Desconocido
Cohesión	Nulo	Nulo	Medio	Nulo	Bajo	Desconocido	Bajo

La diferencia fundamental entre los grados de amenaza ‘nulo’ y ‘desconocido’ estriba en si se recopiló o no información sobre el grupo al respecto. Si un grupo no ha sido investigado o no ha sido objeto de inteligencia criminal, los atributos de los que no se posea información deben calificarse como “desconocidos”. También se debe utilizar el término “desconocido” cuando haya motivos para sospechar que un grupo tiene la capacidad de representar una amenaza, pero no hay pruebas de que esté utilizando esas capacidades, y cuando haya información contradictoria disponible sobre su capacidad o no se tenga la certeza suficiente para confirmar ese criterio.<sup>70</sup>

**Subcomponentes de la técnica Sleipnir**

La herramienta Sleipnir consta de 12 atributos o “valores”, que corresponden a la amenaza que representan para la sociedad canadiense. En la herramienta, se clasifican desde la mayor hasta la menor amenaza para una sociedad. Por ejemplo, la “corrupción” se considera la mayor amenaza de la delincuencia organizada, seguida de la “violencia”.

A continuación se encuentra la lista ordenada por rangos que describe los 12 valores (P, véase la lista que sigue) utilizados para calificar a los diferentes grupos delictivos:

- 12. Corrupción
- 11. Violencia
- 10. Infiltración

70 Real Policía Montada de Canadá. “Sleipnir Version 2.0”. (2011: 2).



9. Blanqueo de dinero
8. Colaboración
7. Aislamiento
6. Monopolio
5. Alcance
4. Uso de inteligencia
3. Diversificación
2. Disciplina
1. Cohesión

### **Puntuación**

Cada uno de los 12 valores se puede puntuar utilizando el siguiente método:

- Alto = 4 x P
- Medio = 2 x P
- Bajo = 1 x P
- Nulo = 0
- Desconocido = 2 x P

Donde P es el número del subcomponente en la lista anterior; por ejemplo, si Monopolio (#6) es alto, Uso de inteligencia (#4) es medio, y Violencia (#11) es bajo, se puntuarán de la siguiente manera:

- Monopolio = 4 x 6 = 24
- Uso de inteligencia = 2 x 4 = 8
- Violencia = 1 x 11 = 11

El resultado total sería 43. Una puntuación más alta, en comparación con otras organizaciones que también se estén controlando, representa un nivel más alto de amenaza.

## **8.2 Ejemplos de aplicación nacional de la ILP**

Los subcapítulos 8.2.1 a 8.2.5 presentan ejemplos de aplicación de la ILP en cinco países de Europa. El subcapítulo 8.2.1 comienza con la presentación del Modelo Nacional de Inteligencia (MNI) del Reino Unido, donde la ILP fue desarrollada por primera vez en la década de 1990. La aplicación práctica y las estructuras organizativas de la ILP del Reino Unido han sido utilizadas desde entonces como modelo de buenas prácticas por muchos países de todo el mundo. El MNI va seguido de una breve presentación de la elaboración de políticas basada en la inteligencia y la planificación estratégica de la aplicación de la ley en el Estado alemán de Renania del Norte-Westfalia. El subcapítulo 8.2.3 presenta el modelo sueco de ILP, así como los Esfuerzos Nacionales Conjuntos basados en la inteligencia para hacer frente a la delincuencia grave y organizada en Suecia. La República de Serbia incorporó disposiciones jurídicas específicas sobre ILP en una nueva Ley de policía aprobada en 2016 y elaboró un Manual nacional sobre ILP para las fuerzas y cuerpos de seguridad del país. Estas medidas se

presentan en el subcapítulo 8.2.4. El último ejemplo nacional describe el enfoque montenegrino de las evaluaciones de amenazas respecto de la delincuencia grave y organizada.

### 8.2.1 Modelo Nacional de Inteligencia del Reino Unido

El Modelo Nacional de Inteligencia (MNI) constituye el marco de la actividad policial basada en la inteligencia (ILP) en el Reino Unido.<sup>71</sup> El MNI tiene por objeto proporcionar orientación a la actividad policial operativa y lograr un efecto desproporcionadamente mayor a partir de los recursos disponibles. Se basa en un marco claro de análisis de datos e información, que permite adoptar un enfoque orientado a resolver problemas con respecto a las técnicas de aplicación de la ley y de prevención de la delincuencia. Los resultados esperados se traducen en una mejora de la seguridad comunitaria, reducción de la delincuencia y control de la delincuencia y los disturbios, lo que conduce a una mayor confianza y seguridad públicas. El MNI no está limitado o restringido a su uso por parte de especialistas. Es relevante para todas las áreas del cumplimiento de la ley: la delincuencia y su investigación, los disturbios y la seguridad comunitaria. En general, el MNI es un modelo de gestión para la actividad policial operativa.

El MNI es tanto un modelo de adopción de decisiones en materia de gestión como una descripción de procesos y productos de inteligencia. El factor decisivo para asegurar que disminuya la delincuencia es el papel proactivo de la gestión de la aplicación de la ley.

El proceso se lleva a cabo en tres niveles: Nivel 1 (comunidad/local), Nivel 2 (entre organismos/regional) y Nivel 3 (nacional/internacional).

En cada uno de esos niveles, los procesos y la naturaleza de los productos de inteligencia son idénticos en su esencia, aunque sí varían el contenido detallado de los productos y la naturaleza de los datos a los que se accede y que se procesan. Esta similitud en todo el modelo se destaca expresamente para ampliar el entendimiento entre profesionales que trabajan en diferentes niveles.

El MNI funciona como un sistema autónomo para un nivel de actividad o como un modelo integrado en el que en cada nivel interactúa con los demás para identificar mejor los problemas y sus posibles soluciones. El modelo describe cada unidad de inteligencia dentro de un nivel, estableciendo sus propias necesidades locales de inteligencia. La normalización de los productos de inteligencia brindará la mejor base para proporcionar dicha inteligencia, pero requiere sistemas de acceso que permitan a cada unidad de inteligencia utilizar los datos que poseen sus colegas.

El producto clave en el Nivel 3 es la Evaluación Anual de Amenazas del Reino Unido, que más concretamente recibe el nombre de *The National Strategic Assessment of Serious and Organised Crime* (Evaluación Estratégica Nacional de la Delincuencia Grave y Organizada, NSA por sus siglas en inglés). La *National Crime Agency* del Reino Unido (Agencia Nacional contra

---

71 El presente subcapítulo se ha elaborado sobre la base de dos documentos: i) *The National Intelligence Model* (El Modelo Nacional de Inteligencia) del *Criminal Intelligence Service* (Servicio Nacional de Inteligencia Criminal, NCIS por sus siglas en inglés) (NCIS Corporate Communications, 2000); ii) el *Code of Practice – National Intelligence Model* (Código de Prácticas: Modelo Nacional de Inteligencia) del *National Centre for Policing Excellence* (Centro Nacional de Excelencia Policial) (Ministerio del Interior del Reino Unido, CENTREX, 2005).



Figura 8.2 Modelo Nacional de Inteligencia del Reino Unido

Fuente: NCIS (2000: 9).

el Crimen, NCA) se encarga de su elaboración basándose en los datos proporcionados por las fuerzas de seguridad, la *HM Customs and Excise* (Administración de Aduanas e Impuestos Especiales del Reino Unido), los organismos de inteligencia y seguridad, y otros órganos encargados del cumplimiento de la ley.

La NSA expone un panorama general del riesgo que supone la delincuencia grave y organizada para el Reino Unido y sus intereses. Proporciona a la respuesta nacional información sobre cuáles son las prioridades y qué medidas se adoptarán, los resultados esperados y cómo se medirá el éxito.

Los *Grupos de Asignación de Tareas y Coordinación*, que se reúnen en los tres niveles, constituyen el núcleo del MNI. Las reuniones de estos grupos se dividen en *Reuniones de Asignación de Tareas Estratégicas y Coordinación* y *Reuniones de Asignación de Tareas Tácticas y Coordinación*. El objetivo de estas reuniones es acordar una Estrategia de Control que defina las necesidades de inteligencia y establezca el programa de prioridades en materia de inteligencia, prevención y cumplimiento de la ley, con el fin de obtener una repercusión máxima. Para ello, los responsables del cumplimiento de la ley deben conocer muy bien la verdadera naturaleza de los problemas a los que se enfrentan y disponer de un mecanismo de toma de decisiones que identifique las prioridades y los recursos necesarios, y que pueda encargar la adopción de medidas. El proceso de asignación de tareas y coordinación es ese mecanismo.

## ASIGNACIÓN DE TAREAS Y COORDINACIÓN

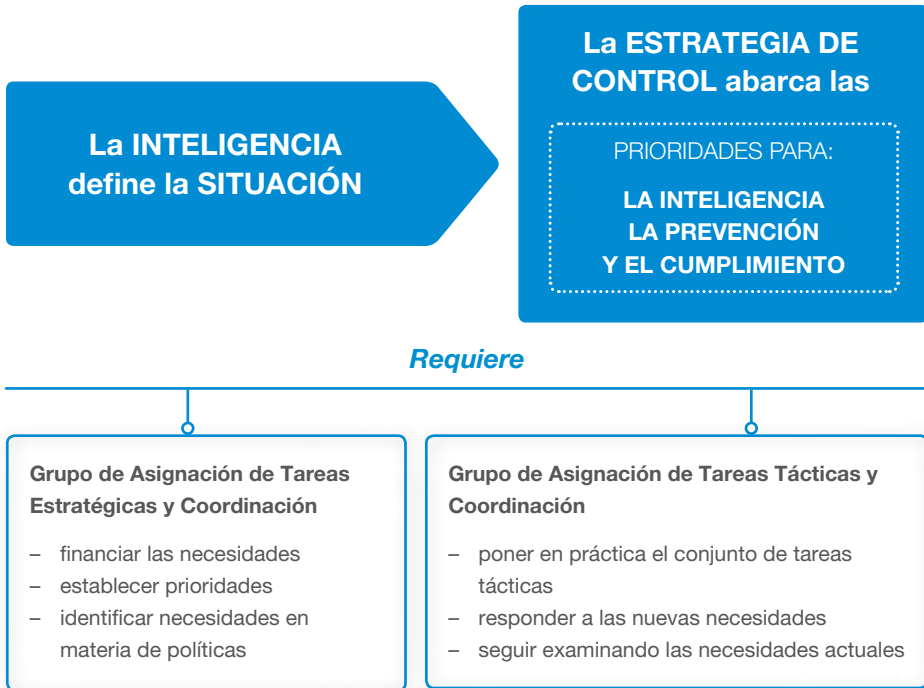


Figura 8.3 **Procesos de Asignación de Tareas Estratégicas y Tácticas y de Coordinación en el Reino Unido**

Fuente: NCIS (2000: 14).

### Asignación de tareas estratégicas

Las *Reuniones de Asignación de Tareas Estratégicas y Coordinación* tienen como objetivo establecer o modificar la estrategia de control y hacer que los principales compromisos de recursos se ajusten a las prioridades establecidas. Por lo tanto, el Grupo de Asignación de Tareas Estratégicas y Coordinación se reúne trimestral o semestralmente y adapta su ciclo a la ronda de planificación de las actividades. La labor del Grupo se lleva a cabo sobre la base de los problemas y cuestiones identificados en la Evaluación Estratégica (NSA), que, una vez examinada a la luz de los objetivos gubernamentales y locales, se utiliza para determinar y establecer las prioridades en materia de inteligencia, cumplimiento y prevención. Su trabajo se completa con la asignación de recursos y el establecimiento de las políticas necesarias para aplicar la estrategia de control.

### Asignación de tareas tácticas

El *Grupo de Asignación de Tareas Tácticas y Coordinación* se reúne semanalmente o cada dos semanas. Tiene tres funciones principales: encargar y aplicar la gama de tareas tácticas a la Estrategia de Control, responder a las nuevas necesidades y comprobar que los planes

acordados y la labor de cumplimiento siguen su curso para cumplir los objetivos deseados. Un Informe de Evaluación Táctica es el producto de inteligencia clave que impulsa la toma de decisiones tácticas.

Los objetivos tácticos constan de cuatro elementos:

- detección de delincuentes de acuerdo con las prioridades de la Estrategia de Control;
- gestión de los puntos conflictivos relacionados con la delincuencia y los disturbios;
- investigación de delitos e incidentes que se pueda demostrar que están vinculados en “series”;
- aplicación de un conjunto de “medidas preventivas” como por ejemplo sistemas de videovigilancia y o iniciativas de acción comunitaria.

Supervisar los progresos y fomentar la labor en los cuatro ámbitos de los objetivos tácticos son partes esenciales del programa de la Reunión de Asignación de Tareas Tácticas y Coordinación.

Los procesos de coordinación y asignación de tareas estratégicas y tácticas basados en la inteligencia se fundamentan en cuatro informes de inteligencia principales que a continuación se explican brevemente.

### **Evaluaciones estratégicas**

El objetivo principal del informe de evaluación estratégica es proporcionar al Grupo de Asignación de Tareas y Coordinación un panorama exacto de la situación en su área de responsabilidad, y de cómo está cambiando y puede cambiar este panorama en el futuro. Se trata, por definición, de un examen de alto nivel, a largo plazo, de las cuestiones relativas al cumplimiento de la ley y, por lo tanto, no solo tendrá en cuenta las actividades en curso, sino que también tratará de proporcionar una previsión de posibles acontecimientos. Una evaluación estratégica elaborada localmente ayudará a la planificación y la formulación de políticas en la zona, y contribuirá a obtener un panorama más amplio de las pautas y tendencias en la región y en el plano nacional.

### **Evaluaciones tácticas**

La evaluación táctica constituye la base del trabajo que realiza el Grupo de Asignación de Tareas Tácticas y Coordinación. En ella se podrán determinar nuevas pautas y tendencias que requieren atención, incluido un análisis más detallado. También se podrán abordar los avances conseguidos en las investigaciones o las iniciativas preventivas, así como las necesidades inmediatas de cambios en la financiación de las opciones tácticas.

### **Perfiles de objetivos**

Un perfil de un objetivo es específico para cada persona y contiene detalles suficientes para iniciar una investigación/operación relacionadas con el objetivo o apoyar una operación en curso contra un individuo o grupo de individuos organizados en redes. Muestra los vínculos con otras investigaciones (en todos los niveles del modelo) y puede incluir perfiles de riesgo de delincuentes potencialmente peligrosos. Sobre la base de la inteligencia revelada, el perfil del objetivo incluye una interpretación de la mejor forma de actuar y propuestas para subsanar las deficiencias en el panorama general de la inteligencia.

### Perfiles de problemas

En el perfil de un problema se identifican series de delitos o incidentes habituales y emergentes. También identifica “puntos conflictivos” relacionados con delitos e incidentes establecidos y emergentes, así como las posibilidades de llevar a cabo una labor preventiva en base a la inteligencia revelada. En el caso de la identificación de series de delitos en los que se confirman los métodos y se establecen vínculos con posibles delincuentes, el perfil sirve de apoyo a la detección y la investigación reactiva, así como a iniciativas preventivas.

### Unidades de inteligencia: dar prioridad a la labor de inteligencia

Una unidad de inteligencia eficaz y segura necesita cuatro activos principales que se describen brevemente a continuación: *fuentes de información* adecuadas, *personal* debidamente organizado y cualificado, acceso a todo el conjunto de *productos basados en conocimientos* y *productos basados en sistemas*.

### Fuentes de información

Las fuentes a las que el personal de inteligencia necesita tener acceso son muy diversas, como las víctimas, los testigos, los presos, los informantes y los productos de vigilancia. Un régimen de inteligencia bien equipado podrá acceder a una amplia gama de datos existentes y buscar y desplegar fuentes proactivas para subsanar las deficiencias de inteligencia detectadas.

### Personal

El segundo activo necesario son las personas. Es sumamente importante que se designe a un gestor de los servicios de inteligencia de categoría adecuada para que dirija la unidad, a fin de garantizar que se da un mayor significado e importancia a las técnicas y productos analíticos antes de ser presentados al grupo de asignación de tareas y coordinación.

Es igualmente importante que la inteligencia, como disciplina, esté adecuadamente representada en los debates de gestión sobre recursos financieros y humanos. Las unidades de inteligencia deben estar equipadas no solo para gestionar datos e información ya conocidos, sino también para reunir información a través de medios proactivos o encubiertos. A menudo se identificarán deficiencias en la inteligencia que no pueden subsanarse mediante el análisis y cotejo del material disponible. Las unidades de inteligencia deben poseer las aptitudes y las capacidades necesarias para gestionar fuentes directas, así como tener la posibilidad de llevar a cabo operaciones de vigilancia técnica.

Se necesitan analistas capacitados para alcanzar los estándares inherentes al modelo. Las técnicas y los productos analíticos forman parte de una gama estándar que sirve de base a los acuerdos nacionales de formación profesional para los analistas encargados de hacer cumplir la ley.

### Productos basados en conocimientos

El modelo constata que la disciplina de la inteligencia se ha de aprender. El personal necesita tener acceso a los productos basados en conocimientos que proporcionan garantía de calidad al modelo. Estos productos, tanto nacionales como locales, definen las reglas de conducta de la actividad o la práctica recomendada para completar los procesos especializados y las condiciones en las que puede tener lugar el trabajo entre diferentes órganos. Poder acceder a

productos basados en conocimientos hace que el personal esté preparado para desempeñar sus funciones. Por lo tanto, el término productos basados en conocimientos describe una diversidad de normas e información local, regional o nacional que la estrategia de inteligencia de una organización puede necesitar adoptar.

### **Productos basados en sistemas**

Los productos basados en sistemas son los medios que permiten recopilar, recibir, registrar, almacenar y utilizar información. Proporcionan los métodos por los que se recogen, obtienen y analizan los datos. Según el MNI, las unidades de inteligencia eficaces necesitan tener acceso a una serie de sistemas de datos nacionales, expedientes de la policía local, registros de delitos e inteligencia, y una amplia variedad de información procedente de fuentes abiertas.<sup>72</sup>

### **Seguridad**

La integridad del MNI requiere normas adecuadas de seguridad física, medioambiental, técnica y del personal. La política de Clasificaciones de Seguridad del Gobierno establece normas comunes para la protección de documentos sensibles y otros materiales en todos los organismos gubernamentales. Sus principios se aplican también a los datos guardados en sistemas informáticos y de registro electrónico.

### **Protección de datos**

Los directores generales son responsables de que se desarrollen y apliquen procedimientos y sistemas adecuados que garanticen que la información privada de las personas se mantenga de conformidad con lo estipulado en la Ley de protección de datos del Reino Unido de 1998 y en cualquier otra norma jurídica pertinente. La gestión de la información debe ser conforme con el Código de Prácticas sobre gestión de la información policial.

## **8.2.2 Renania del Norte-Westfalia (Alemania): elaboración de políticas y planificación estratégica**

La Policía del Estado de Renania del Norte-Westfalia en Alemania aplica la ILP, incluso en la elaboración de políticas y en la planificación estratégica.<sup>73</sup> El sistema de gestión y control de la estrategia se basa en cuatro pilares que representan las tareas centrales de la Policía Regional:

- Prevención de riesgos y respuesta a emergencias (PR)
- Lucha contra la delincuencia (investigaciones)
- Seguridad vial (tráfico)
- Servicios administrativos (SA)

Las 47 Autoridades Policiales Regionales (APR) de Renania del Norte-Westfalia tienen, a pesar de sus diferentes dimensiones, una estructura organizativa idéntica, que consta de cuatro direcciones que corresponden a dichas tareas principales, así como personal adicional encargado de brindar apoyo al jefe de la autoridad policial.

<sup>72</sup> Para obtener más información sobre los productos basados en sistemas para las unidades de inteligencia consúltese el NCIS (2000).

<sup>73</sup> Autoridad responsable: *Landesamt für Zentrale Polizeiliche Dienste NRW*, Duisburg (Alemania).

Como base estratégica, el Ministerio del Interior identifica las prioridades estatales en cada uno de los cuatro pilares antes mencionados (estrategias de campo). Dos organismos públicos se encargan de su elaboración, evaluación periódica y adaptación mediante el análisis de información y datos, así como su cotejo y comprobación. Este proceso también fija una asignación de recursos en función del volumen de trabajo y el presupuesto para las APR.

Ejemplos de posibles prioridades:

- (PR) Disponibilidad y accesibilidad de la Policía;
- (Investigaciones) Reducción de la delincuencia juvenil;
- (Tráfico) Reducción de los accidentes de personas mayores;
- (SA) Disponibilidad de personal dentro de las APR.

Para cada una de las prioridades, el Ministerio del Interior define los **Factores de Éxito Generales (FEG)**, que comprenden un conjunto de normas, procedimientos e indicadores cuya aplicación es obligatoria para todas las APR. Los FEG deben incluirse en el **Programa de Seguridad** anual de las APR, que también define sus prioridades y objetivos locales, así como las medidas y responsabilidades conexas. Las normas, procedimientos e indicadores regionales vinculantes se denominan **Factores de Éxito Específicos (FEE)**. En general, cada una de las direcciones de las APR está obligada a contribuir a la consecución de los objetivos de las otras tres.

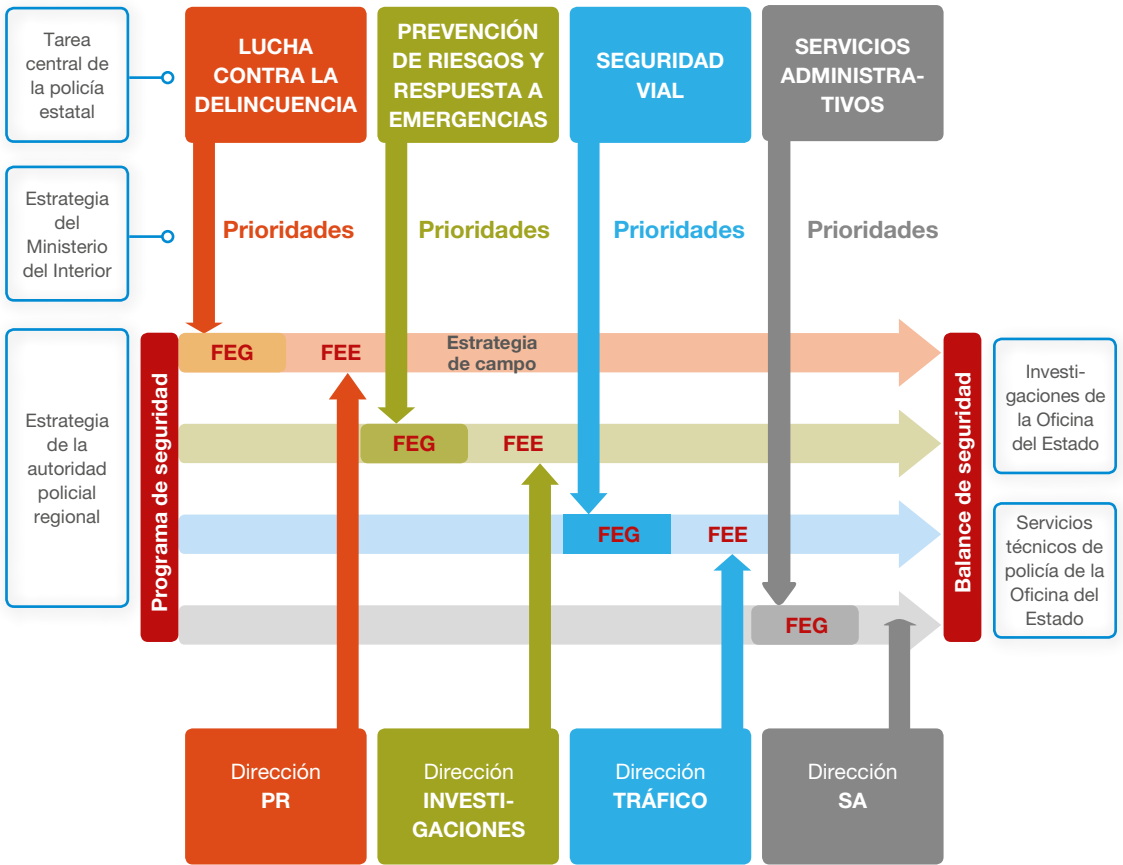
En nombre del Ministerio del Interior, los dos organismos regionales (la Oficina Regional de Investigaciones y la Oficina Regional de Servicios Técnicos de la Policía) se encargan de controlar y evaluar periódicamente las actividades de campo de las APR, que aparecen también documentadas en el Balance de Seguridad de fin de año de las APR. El diseño y la estructura del Programa de Seguridad y del Balance de Seguridad están prescritos y son idénticos para todas las APR. Constituyen la base de un proceso de “información de retorno” e intervención que incluye, entre otras cosas, el fomento y el apoyo de ejemplos de mejores prácticas. En el ámbito de la asistencia, se han creado grupos de comparación de las APR con los datos estructurales correspondientes para hacer posible y mejorar el intercambio de experiencias.

**Ventajas del modelo descrito:**

- concentración en las tareas principales con unos recursos y un presupuesto limitados;
- mejora de la implicación y responsabilidad de las APR a nivel local, teniendo en cuenta al mismo tiempo los objetivos a nivel estatal;
- normalización de un sistema de información y control a nivel estatal; y
- mejor comparabilidad entre las APR.

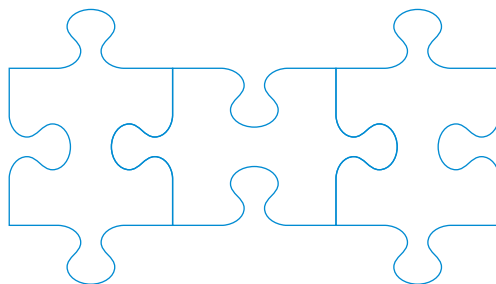
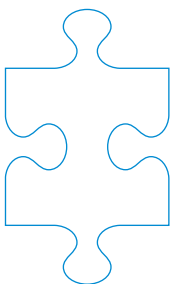
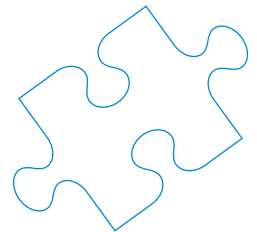


## PREVENCIÓN DE RIESGOS Y RESPUESTA A EMERGENCIAS



FEG: Factores de Éxito Generales  
 FEE: Factores de Éxito Específicos

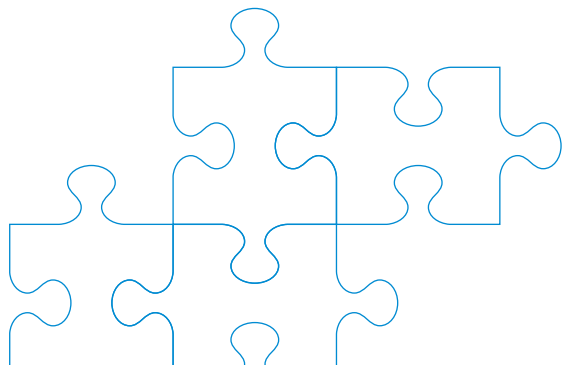
Figura 8.4 **Elaboración de políticas y planificación estratégica basadas en la inteligencia de la Policía Regional de Renania del Norte-Westfalia (Alemania)**



### 8.2.3 Suecia: estructuras organizativas y decisorias de la ILP

En 2015, se llevaron a cabo importantes reformas en la Policía Sueca, que pasó de tener 21 Direcciones de Policía independientes, cada una de ellas dirigida por una estructura de gobierno de la Junta de la Policía Nacional de Suecia, a tener una única Autoridad de la Policía Nacional, dirigida por un Jefe de la Policía Nacional y dividida en siete regiones policiales y el Departamento de Operaciones Nacionales. Estos cambios organizativos incluyeron la creación de una nueva estructura y de procesos de cooperación y coordinación de la ILP en Suecia en los planos estratégico nacional, operativo nacional, estratégico regional, operativo regional y operativo local. La estructura organizativa del modelo sueco de ILP es una estructura de mando y control descendente. En todas las reuniones de los grupos de gestión de cada nivel está presente un representante del nivel inferior siguiente, a fin de garantizar la coordinación y el intercambio de información entre los diferentes niveles.

El *Grupo Nacional de Gestión Estratégica* (SLG) está presidido por el Jefe Nacional de Policía. Otros representantes son los siete comisarios regionales de policía, el jefe del Departamento de Operaciones Nacionales y los jefes de otros departamentos nacionales, entre ellos los de finanzas, comunicaciones y recursos humanos. El SLG mantiene videoconferencias cada dos semanas y reuniones convencionales una vez al mes. Sus principales responsabilidades son examinar y tomar decisiones sobre las directrices y los planes estratégicos nacionales, y decidir las esferas prioritarias a largo plazo, incluida la asignación de recursos, sobre la base de decisiones gubernamentales, informes y evaluaciones estratégicos.



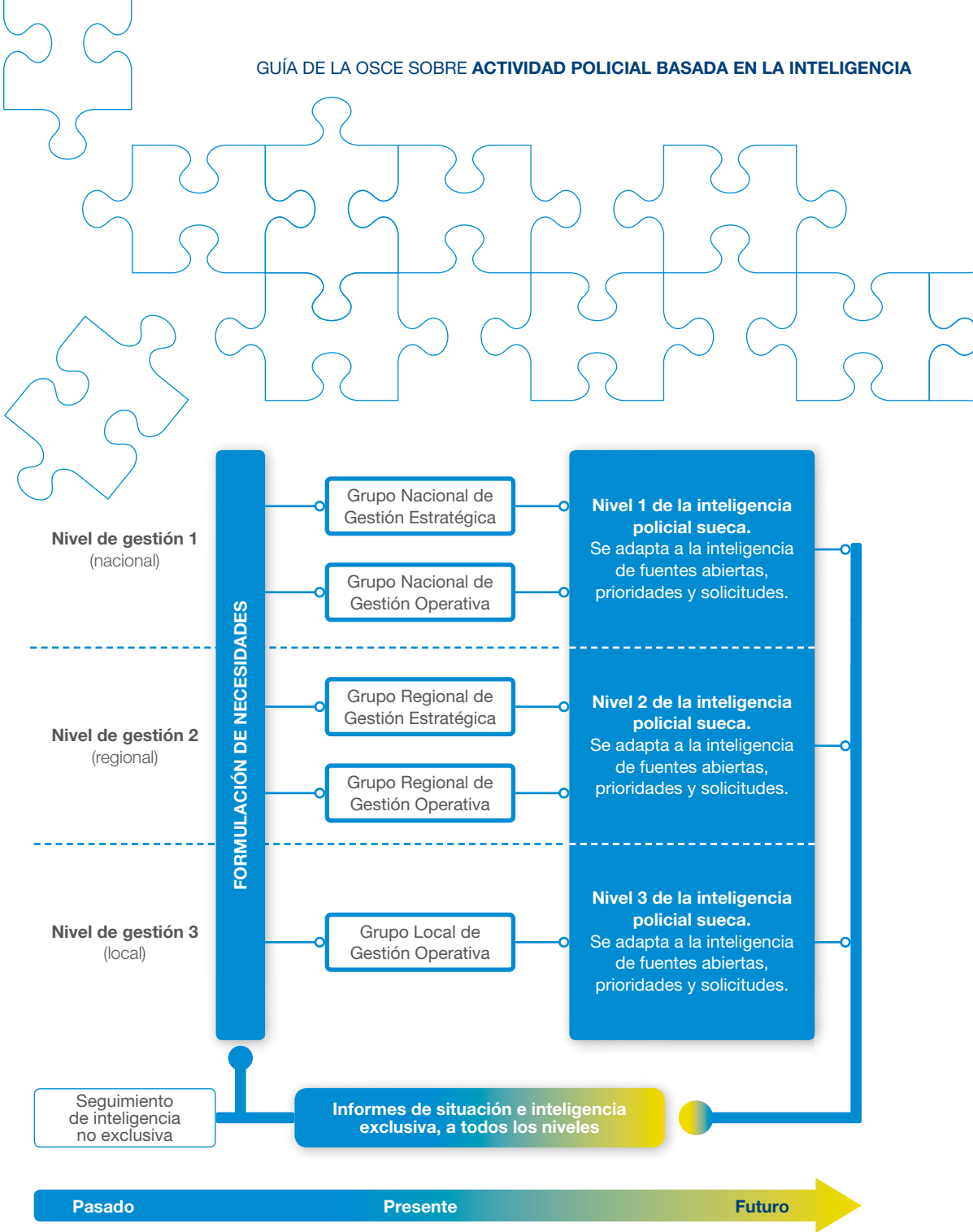


Figura 8.5 Estructuras organizativas y decisorias del modelo sueco de ILP

## 8. LA ILP EN LA PRÁCTICA

El *Grupo Nacional de Gestión Operativa* (NOLG) está presidido por el jefe del Departamento de Operaciones Nacionales. Otros representantes son los jefes adjuntos de las siete regiones policiales, el jefe de la División de Planificación Operativa Nacional y el jefe del Departamento Forense Nacional. El Jefe de Operaciones del Servicio de Seguridad de Suecia y el Jefe del Departamento Nacional de la Fiscalía General, de la Autoridad de Fiscales de Suecia, asisten a las reuniones en calidad de observadores. El NOLG mantiene videoconferencias cada dos semanas y reuniones convencionales una vez al mes. Sus principales responsabilidades son dar prioridad a las medidas, operaciones e investigaciones nacionales, sobre la base de los informes de inteligencia de la Unidad Nacional de Inteligencia Criminal situada en el Departamento de Operaciones Nacionales de la Dirección Nacional de Policía de Suecia.

Los *Grupos Regionales de Gestión Estratégica* (RSLG) están presididos por los comisarios de policía regionales de cada una de las siete regiones policiales. Otros representantes son los jefes de cada una de las áreas policiales de la región y los jefes de las unidades regionales de recursos humanos, finanzas, comunicaciones, desarrollo, investigación y operaciones, entre otras. Los RSLG se reúnen cada dos semanas. Sus principales responsabilidades son debatir y adoptar decisiones sobre directrices y planes estratégicos regionales, y decidir las áreas prioritarias a largo plazo, incluida la asignación de recursos, sobre la base de las decisiones nacionales del NOLG, los informes estratégicos y las evaluaciones.

Los *Grupos Regionales de Gestión Operativa* (ROLG) están presididos por los jefes adjuntos de cada una de las siete regiones policiales. Otros representantes son los presidentes de los Grupos Locales de Gestión Operativa (POLG) en cada una de las áreas policiales de la región y los jefes de las unidades regionales de investigaciones y operaciones, entre otras. El jefe de cada unidad de inteligencia regional actúa de relator de los ROLG, que se reúnen cada dos semanas. Las principales responsabilidades de los ROLG son dar prioridad a las medidas, operaciones e investigaciones regionales, basadas en la información disponible y en los informes de inteligencia de las unidades de inteligencia regionales. Los ROLG pueden tomar la decisión de dirigir a nivel local las medidas propuestas y pueden solicitar apoyo operativo y de inteligencia por parte del nivel nacional (NOLG).

Los *Grupos Locales de Gestión Operativa* (POLG) están presididos por los comisarios de policía locales. Otros miembros son los jefes de las áreas policiales sublocales y los jefes de investigaciones y operaciones locales. Los jefes de los grupos de inteligencia locales actúan de relatores de los POLG, que se reúnen una vez por semana. Las principales responsabilidades de los POLG son adoptar decisiones sobre las medidas, operaciones e investigaciones locales basadas en los informes de la Unidad de Inteligencia local. Los POLG pueden solicitar apoyo operativo y de inteligencia al nivel regional (ROLG).

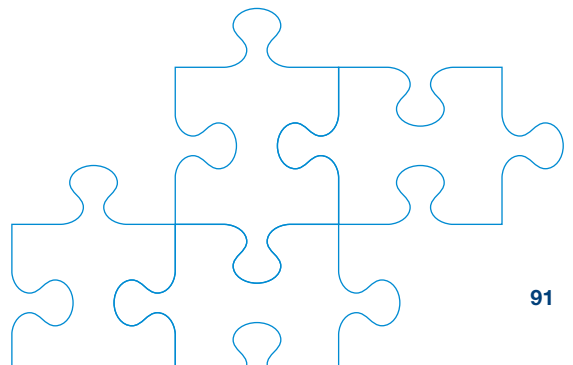
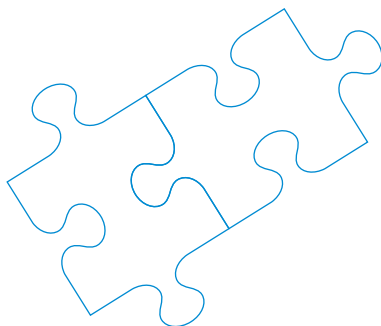
## Actividades nacionales conjuntas de inteligencia y operaciones en Suecia para hacer frente a la delincuencia organizada

En 2009, nueve autoridades públicas suecas firmaron un acuerdo de cooperación para poner en marcha actividades conjuntas de inteligencia y operaciones destinadas a prevenir y combatir la delincuencia organizada. Esta iniciativa nacional se amplió en 2016 aplicándose a nivel regional y local. Funciona en paralelo y está directamente relacionada con las estructuras de aplicación de la ILP descritas anteriormente.

Estas actividades conjuntas son medidas específicas de inteligencia, operativas y de investigación, aunque solo representan una parte de las iniciativas generales de la Dirección de Policía de Suecia y de las autoridades colaboradoras en la lucha contra la delincuencia organizada.

Los siguientes 12 organismos/autoridades nacionales participan y contribuyen a las iniciativas conjuntas contra la delincuencia organizada:

- Policía Nacional de Suecia
- Oficina Nacional de Empleo
- Autoridad de Delitos Económicos
- Organismo de la Seguridad Social
- Servicios Penitenciarios y de Libertad Vigilada
- Autoridades encargadas del cumplimiento de la ley
- Junta de Migración
- Guardia Costera de Suecia
- Agencia Tributaria
- Servicios de Seguridad
- Aduanas
- Fiscalía General



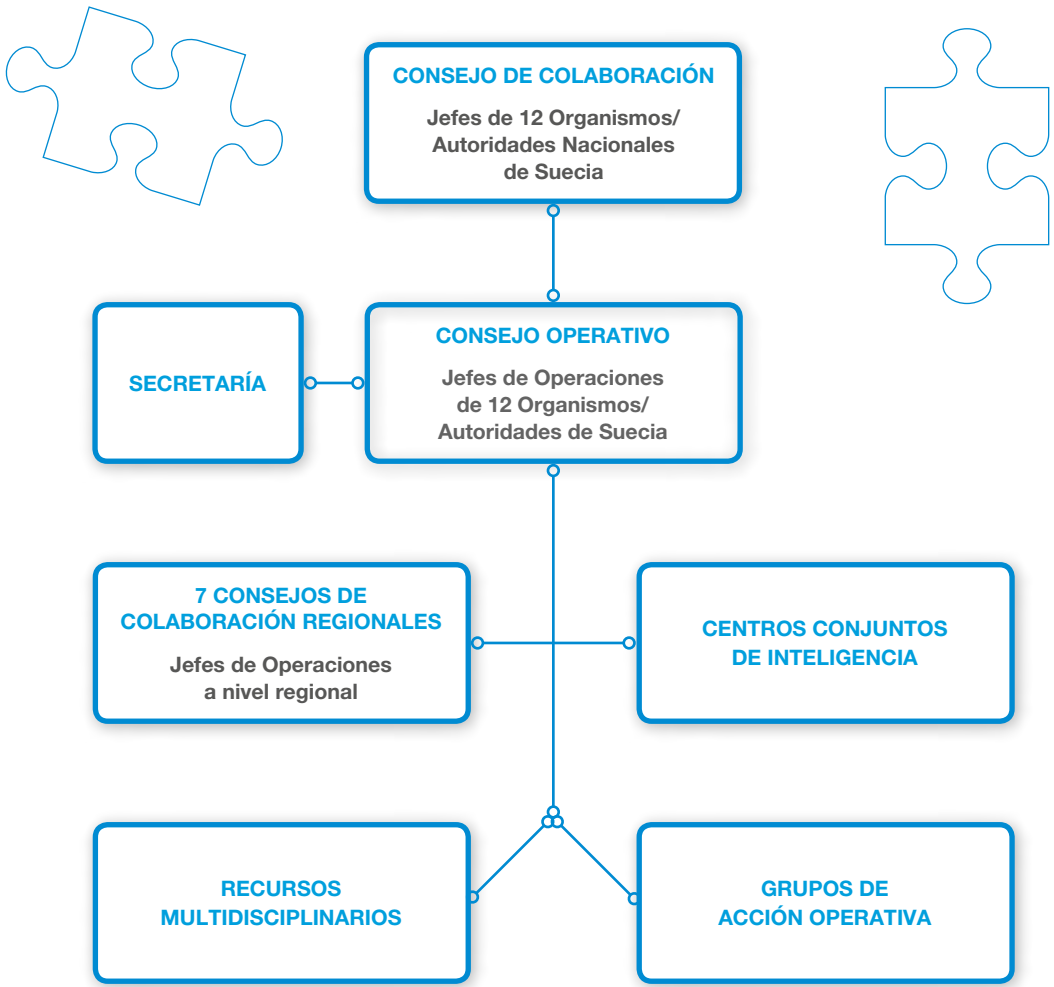


Figura 8.6 **Actividades conjuntas nacionales de inteligencia y operaciones en Suecia para hacer frente a la delincuencia organizada**

Estos 12 organismos nacionales participan y cooperan en un foro interinstitucional, el *Consejo de Colaboración*, compuesto por los jefes de cada organismo/autoridad colaboradora y presidido por el Jefe de la Policía Nacional Sueca. El cometido principal de este Consejo es adoptar decisiones sobre una estrategia conjunta para hacer frente a la delincuencia organizada en Suecia. El Consejo se reúne dos veces al año. A efectos de coordinación e intercambio de información, el jefe de la siguiente estructura inferior (Consejo Operativo) actúa de relator.

Por debajo del Consejo de Colaboración se encuentra el *Consejo Operativo*, cuyas tareas principales son dar prioridad y poner en práctica las decisiones estratégicas adoptadas por el Consejo de Colaboración. El Consejo Operativo, que se reúne todos los meses, también toma decisiones sobre el uso de los Grupos de Acción Operativa y otros recursos en tareas conjuntas de investigación u operativas. Cada uno de los 12 organismos/autoridades tiene un representante en el Consejo Operativo, que está presidido por el jefe del Departamento de Operaciones Nacionales de la Dirección Nacional de Policía, conectando así las dos estructuras y garantizando la circulación de la información.

La *Secretaría* presta apoyo a los Consejos Operativo y de Colaboración, así como a sus procesos. Sus tareas principales son la planificación, preparación y presentación de proyectos de decisión, la redacción de actas y el seguimiento de las reuniones de ambos Consejos. La Secretaría también tiene una función de coordinación y es responsable del proceso relativo a los grupos de acción.

Los *Consejos Colaboradores Regionales* de las siete regiones del país tienen como tareas principales el establecimiento de iniciativas conjuntas a nivel local y regional. Se reúnen cada cuatro semanas e informan al Consejo Operativo a través de la Secretaría.

Todas las entidades que participan en las actividades conjuntas cuentan con el apoyo de estructuras de inteligencia formadas por *Centros Regionales de Inteligencia* interinstitucionales situados en las siete regiones policiales y un *Centro Nacional de Inteligencia* interinstitucional ubicado en el Departamento de Operaciones Nacionales. Estos centros, representados por 11 de los organismos/autoridades colaboradoras<sup>74</sup>, aportan servicios analíticos y productos de inteligencia a las actividades conjuntas. De acuerdo con la ley de 2016, todos esos organismos/autoridades no solo están autorizados, sino que están obligados a compartir los datos, la información y la inteligencia que poseen sobre las tareas de inteligencia realizadas en el marco de este foro, a la hora de abordar actividades delictivas de carácter grave que lleve a cabo un grupo de personas de manera organizada y sistemática.

Los *Grupos de Acción Operativa* están compuestos por unos 200 agentes del orden. Están divididos en secciones de 20 o 30 agentes, destinados en las siete regiones policiales y en el Departamento de Operaciones Nacionales. Cada unidad cuenta con un jefe o jefe de grupo, investigadores, analistas y gestores. Los grupos de acción también colaboran diariamente con otros *recursos multidisciplinarios* de otras autoridades cooperantes, en calidad de equipos conjuntos, en intervenciones decididas por el Consejo Operativo.

---

74 La fiscalía sueca no está representada en los Centros de Inteligencia Conjunta, ya que no posee ni maneja inteligencia.

### 8.2.4 República de Serbia: estructuras operativas y de inteligencia de la ILP

El Ministerio del Interior de la República de Serbia decidió poner en práctica la actividad policial basada en la inteligencia en Serbia para mejorar el cumplimiento de la ley y lograr mejores resultados en la lucha contra la delincuencia y otras amenazas a la seguridad, así como para armonizar la labor policial con las normas, la estructura, la calidad y la terminología de las fuerzas policiales de los países desarrollados de Europa y del mundo. A este respecto, Serbia aprobó una nueva Ley de policía en 2016, en la que se define el concepto de la actividad policial basada en la inteligencia y se dan instrucciones sobre la forma de aplicarla en la práctica policial serbia.

#### Ley de policía serbia

##### Artículo 34

##### Modelo de inteligencia policial

“En el desempeño de las tareas policiales, la Policía aplicará el modelo de actividad policial basada en la inteligencia (ILP). La actividad policial basada en la inteligencia es un modelo de gestión de la labor policial basada en la inteligencia criminal. La inteligencia criminal es un conjunto de datos recopilados, evaluados, procesados y analizados, que sirven de base para tomar decisiones fundamentadas relacionadas con el desempeño de las tareas policiales”.

– **Ministerio del Interior de la República de Serbia. “Decreto sobre la promulgación de la Ley de policía”. PR núm. 1, Belgrado, 28 de enero de 2016.**

La Ley de Policía serbia también define y especifica las funciones y responsabilidades de las diferentes estructuras y niveles de la policía en la gestión de los elementos clave del modelo de ILP, incluida la elaboración de una Evaluación Estratégica de la Seguridad Pública, así como planes estratégicos y operativos que definen las prioridades y los objetivos de la labor policial, sobre la base de la Evaluación Estratégica.<sup>75</sup>

Tras un estudio a fondo de los modelos de ILP ya en vigor, como por ejemplo los del Reino Unido, Estados Unidos, Canadá, Australia y Suecia, el Ministerio del Interior elaboró un modelo de ILP serbio, que se adapta plenamente a las particularidades del sistema policial de la República de Serbia. El modelo serbio de ILP se expone en el Manual Nacional Serbio de

---

<sup>75</sup> Ley de policía serbia (2016): Art. 24 (función y responsabilidades de la Dirección de Policía en el Ministerio serbio del Interior); Art. 25 (tareas y actividades principales de los departamentos de policía).



ILP<sup>76</sup> e incluye los siguientes capítulos:

- Estructura del Modelo de ILP en la República de Serbia
- Liderazgo y dirección a niveles estratégico y operativo
- Proceso y prácticas de la inteligencia criminal
- Labor de la inteligencia criminal (planificación, recopilación, procesamiento, análisis y difusión de la inteligencia)
- Planificación del trabajo policial operativo (ejecutivo)
- La seguridad y el modelo de ILP
- Empleados y unidades responsables de asuntos de inteligencia criminal
- Desarrollo y capacitación del personal
- Sistemas de información y comunicación

En el Manual serbio, el término “actividad policial basada en la inteligencia” se refiere a un sistema y una metodología para gestionar la inteligencia criminal y la labor policial operativa prevista, en el que la inteligencia es la base para definir las prioridades y los objetivos estratégicos y operativos en la prevención y la represión de la delincuencia y otras amenazas para la seguridad. También es la base para tomar decisiones adecuadas sobre la labor y las medidas operativas de la policía, el compromiso racional de los recursos humanos disponibles y la asignación de recursos materiales y técnicos.

El Ministerio del Interior serbio está aplicando actualmente el modelo de ILP en las prácticas policiales de Serbia. La Dirección de Policía de Suecia y la Agencia Sueca de Cooperación Internacional para el Desarrollo han prestado apoyo a la policía serbia desde que comenzó el proceso de aplicación. Con el fin de diseñar el modelo serbio de ILP descrito, se llevó a cabo un análisis de las deficiencias para identificar las actividades concretas que deben llevarse a cabo en los ámbitos de adaptación del marco jurídico, la estructura organizativa, y el desarrollo de capacidades humanas y de tecnologías de la información. Se han adaptado varios documentos normativos relativos a las actividades policiales basadas en la inteligencia. La Evaluación Estratégica de la Seguridad Pública, que abarca un período de cinco años, y la Evaluación de la Amenaza de la Delincuencia Grave y Organizada (SOCTA) a nivel nacional, ya han sido adaptados. También se han asignado recursos humanos para que se encarguen de la aplicación de la ILP. Está previsto que el Ministerio del Interior de la República de Serbia logre la plena aplicación del programa en 2018.

La ILP serbia es un modelo diseñado para gestionar la labor policial en su totalidad, y no solamente las actividades policiales centradas en la prevención y la represión de la delincuencia organizada.

Las *condiciones necesarias* para que el modelo de ILP funcione de manera eficaz, según el Ministerio del Interior serbio y el Manual de ILP serbio, son las siguientes:

1. *Liderazgo y dirección* – Esta es una función clave del modelo que se establece a nivel estratégico y operativo, y que se ejerce de acuerdo con una metodología y un sistema de responsabilidad establecidos.

---

76 Ministerio del Interior de la República de Serbia (2016).

2. *Proceso de inteligencia criminal sistematizado* – En la práctica, el proceso completo de inteligencia criminal debe estructurarse en subprocesos (tareas), funciones y actividades que están conectadas entre sí o tienen lugar simultáneamente.
3. *Estructura organizativa eficaz* – Las unidades y subunidades organizativas que se dedican a la inteligencia criminal y al trabajo policial operativo se establecen de manera que sean compatibles con procesos y funciones definidos (en las mismas unidades organizativas se llevan a cabo procesos y funciones similares).
4. *Fuentes de datos e información* – Todas las fuentes abiertas y cerradas disponibles deben ser localizadas y utilizadas eficientemente con el objetivo de recopilar datos e información.
5. *Especial atención a los problemas de seguridad más complejos* – Se debe dar prioridad a la delincuencia organizada, la corrupción y otros hechos delictivos graves, y a sus autores (organizadores y ejecutores).
6. *Productos de inteligencia criminal* – De conformidad con la metodología definida para llevar a cabo la labor de inteligencia criminal y con los criterios de calidad definidos, la Unidad de Asuntos de Inteligencia Criminal elabora productos de inteligencia criminal, que son un requisito previo para definir adecuadamente los objetivos, fijar las prioridades y tomar decisiones a fin de ejecutar la labor policial.
7. *Marco jurídico* – Se debe definir un marco jurídico adecuado para que la actividad policial basada en la inteligencia funcione con éxito.
8. *Recursos humanos* – Los agentes de policía deben ser seleccionados específicamente (de conformidad con criterios y procedimientos especiales) e instruidos para llevar a cabo actividades de inteligencia criminal.
9. *Recursos técnicos* – Bases de datos y tecnología de la información bien desarrolladas, así como locales, equipos y herramientas técnicas adecuados, son elementos necesarios para el modelo de ILP.
10. *El tiempo como recurso* – Se necesita tiempo y paciencia para cambiar la cultura institucional y la forma de trabajar.

Como se muestra en la figura 8.7, el proceso de aplicación de la ILP consta de tres subprocesos, que representan el flujo de actividad utilizando la forma del número ocho. Estos subprocesos son: i) liderazgo y dirección (azul); ii) tareas de inteligencia criminal (blanco); y iii) labor policial operativa prevista (rojo). El subproceso de nivel medio, liderazgo y dirección, desempeña un papel de gestión (dirección y coordinación) con respecto a los otros dos subprocesos. *En primer lugar*, en el subproceso de liderazgo y dirección, gestores competentes inician (solicitan) la aplicación de la labor de inteligencia criminal. Sobre la base de sus encargos y sus solicitudes, se planifican y se llevan a cabo actividades concretas de inteligencia, y los resultados se presentan en un informe. *En segundo lugar*, sobre la base de este informe, los gestores competentes toman decisiones sobre la ejecución de la labor policial operativa prevista. *En tercer lugar*, sobre la base de esas decisiones, se planifican y se llevan a cabo actividades policiales operativas concretas, y a continuación se elabora un informe de evaluación. El flujo descrito del proceso de inteligencia criminal (blanco) puede terminar después de un ciclo o repetirse (completado con nuevas adiciones) en varios ciclos, dependiendo de la tasa de éxito logrado en la resolución de un delito concreto y de otras circunstancias.

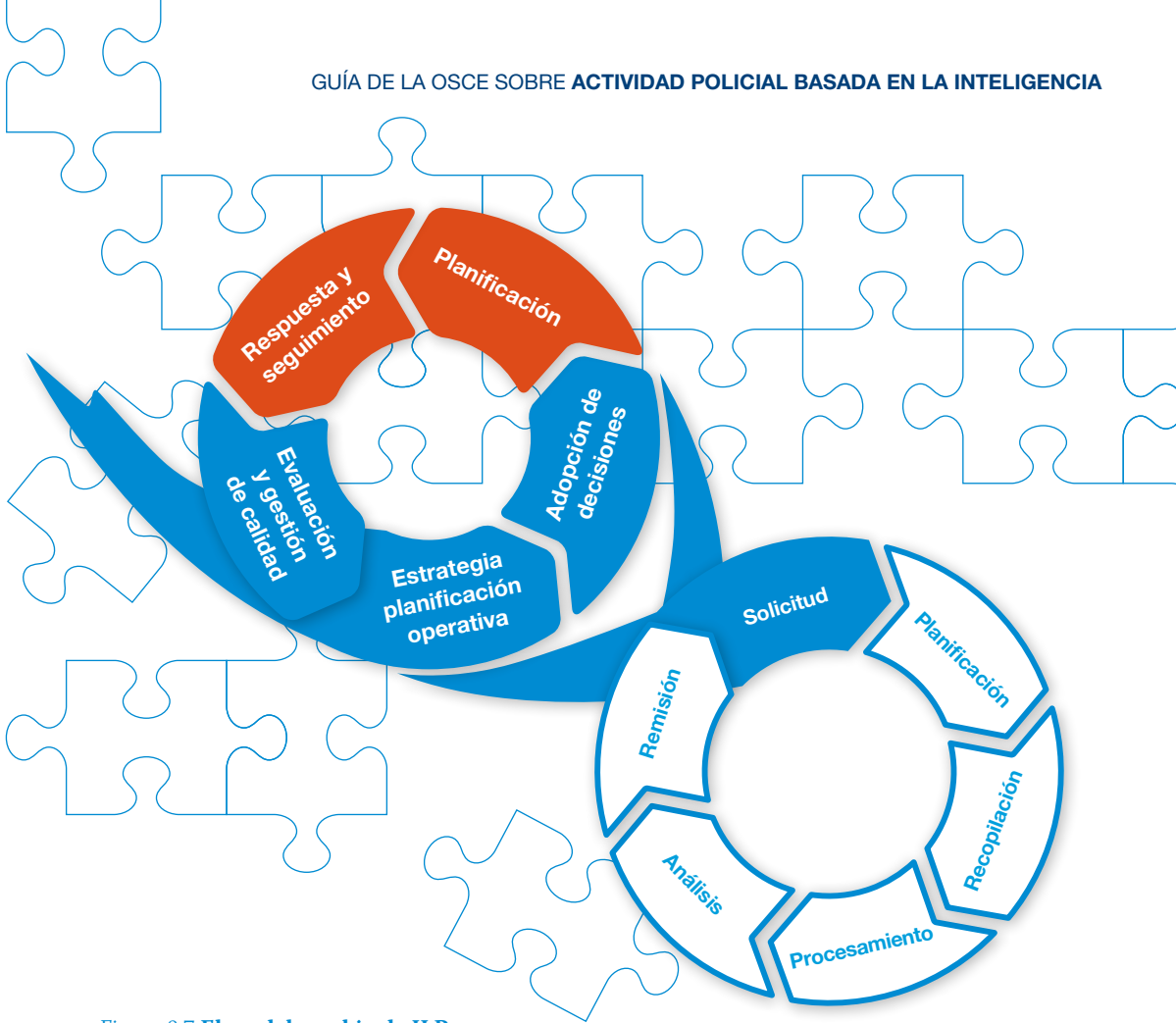


Figura 8.7 El modelo serbio de ILP

Fuente: Ministerio del Interior. República de Serbia..

Las estructuras organizativas de la ILP serbia dividen la toma de decisiones, el liderazgo, la dirección y la coordinación en tres niveles: nacional, regional y local. De acuerdo con los principios de la ILP, cada nivel tiene su propio mecanismo de toma de decisiones basado en productos de inteligencia criminal estratégicos y operativos, incorporando así el análisis y las evaluaciones en toda la planificación y gestión de la aplicación de la ley:

- *El Grupo de Dirección Estratégica (GDE)* a nivel nacional de la Dirección de Policía del Ministerio del Interior está presidido por el Director de la Policía Nacional de Serbia. Sus principales funciones y responsabilidades corresponden a las siguientes categorías: encargar o solicitar una evaluación estratégica para la seguridad pública y otros productos nacionales de inteligencia criminal; planificar estrategias, adoptando decisiones y asignando recursos, entre otras cosas, sobre la base de la evaluación estratégica y de otros productos concretos de inteligencia criminal; y supervisar y verificar la aplicación de los planes estratégicos.
- *El Grupo de Dirección Operativa de la Policía Criminal* a nivel nacional (GDO PC) está presidido por el Jefe de la Policía Criminal, y desempeña las siguientes funciones principales: elaborar un Plan Operativo Anual, a nivel nacional, para la prevención

- y represión de la delincuencia, basado en los planes estratégicos del GDE; asignar recursos para cumplir los objetivos clave del Plan Operativo Anual; y asignar tareas/ presentar solicitudes y adoptar decisiones sobre la base de productos concretos de inteligencia criminal en las esferas de la delincuencia grave y organizada.
- *Los Grupos de Dirección Operativa* a nivel regional (GDO DPR) están presididos por cada uno de los 27 Jefes de las Direcciones Regionales de Policía y desempeñan las siguientes funciones principales: planificar operaciones a nivel regional para la prevención y represión de la delincuencia, sobre la base de los planes estratégicos del GDE; encargar y coordinar las actividades operativas a nivel de los DPR; adoptar decisiones sobre la base de productos concretos de inteligencia criminal a nivel regional; y evaluar las tareas, operaciones e investigaciones policiales ya concluidas en el plano regional.
  - *Los Grupos de Dirección Operativa* a nivel local/de Comisarías de Policía (GDO CP) están formados por la dirección de las comisarías de policía y presididos por los comisarios. Sus funciones principales son las siguientes: planificar operaciones a nivel local y de comisarías para la prevención y represión de la delincuencia, sobre la base de los planes estratégicos del GDE, el Plan Operativo Anual de los GDO DPR y los productos de inteligencia criminal; adoptar decisiones, encargar y coordinar a nivel local y de comisarías las actividades operativas, incluida la investigación.

Además de ser un modelo para gestionar la labor policial operativa sobre la base de la inteligencia criminal, el modelo de la ILP también pretende integrar la gestión de la calidad. En el Manual serbio de ILP, se hace hincapié en el término “calidad” en relación con el proceso de la ILP, los recursos humanos, la capacitación, los productos de inteligencia criminal, las normas y los criterios de calidad, así como en lo tocante a la relación entre los grupos de liderazgo y dirección estratégica y operativa, por una parte, y el servicio de análisis, por otra. Todo esto pone de manifiesto el reconocimiento de que la calidad es una característica importante del modelo de ILP.

### 8.2.5 Montenegro: evaluaciones de la amenaza de la delincuencia grave y organizada

Siguiendo las recomendaciones formuladas en la Evaluación de la Amenaza de la Delincuencia Grave y Organizada en Montenegro (SOCTA MNE), una autoridad competente encargada del cumplimiento de la ley decide sobre la elaboración de una lista de prioridades nacionales e interinstitucionales para luchar contra la delincuencia grave y organizada. Estas prioridades quedan reflejadas en el establecimiento de tareas operativas y de investigación específicas prioritarias y en la coordinación interinstitucional.

Como se explica en la figura 8.8, la Evaluación SOCTA MNE abarca un período de cuatro años y corre a cargo de un equipo interinstitucional compuesto por representantes de los servicios de inteligencia y del sector de la seguridad montenegrinos.

## DOCUMENTOS ESTRATÉGICOS Y PRIORIDADES



Figura 8.8 **Evolución y planificación estratégica de la evaluación SOCTA en Montenegro**

Las prioridades de la Evaluación SOCTA MNE para 2013-2017 incluyen las siguientes esferas:

- *los delitos graves contra la vida y la integridad física* cometidos como consecuencia de conflictos entre grupos delictivos organizados;
- *el terrorismo y extremismo religioso*<sup>77</sup>, principalmente en relación con la participación de ciudadanos montenegrinos en fuerzas armadas extranjeras, así como con la intensificación del extremismo religioso en la zona de la península de los Balcanes;
- *la corrupción de alto nivel* cometida por personas que ocupan cargos públicos;
- *el tráfico de drogas*, que es una actividad delictiva dominante de la mayoría de grupos delictivos organizados;
- *los préstamos a intereses abusivos*, que se reconocen como un problema particular que da lugar a otros hechos delictivos graves;
- *la migración ilegal y la trata de seres humanos*, que se caracteriza por el abuso del procedimiento de asilo, así como por la explotación laboral y sexual; y
- *el blanqueo de capitales y las investigaciones financieras*, reconocidos como medios eficaces en la lucha contra la delincuencia organizada.

77 En la terminología de la OSCE se utiliza el término "extremismo violento".

*El Equipo Operativo Interinstitucional Nacional*<sup>78</sup> es un grupo de trabajo para la lucha contra la delincuencia grave y organizada, que fue establecido en 2015. Se trata de un órgano interinstitucional formado por representantes de los siguientes organismos:

- Ministerio de Justicia
- Policía
- Organismo de Seguridad Nacional
- Aduanas
- Departamento de Ingresos Públicos
- Administración para la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo

El Equipo Operativo Institucional tiene las siguientes tareas:

- sugerir prioridades nacionales en la lucha contra la delincuencia grave y organizada;
- proponer objetivos estratégicos y planes estratégicos plurianuales en la lucha contra la delincuencia grave y organizada;
- proponer un Modelo Nacional de Inteligencia, basado en la evaluación SOCTA MNE, para establecer prioridades, y gestionar y asignar tareas en la lucha contra la delincuencia grave y organizada;
- adoptar y poner en práctica planes operativos anuales en el ámbito de la lucha contra la delincuencia grave y organizada, basándose en las prioridades estratégicas establecidas;
- garantizar la cooperación interinstitucional en la realización de actividades específicas a nivel operativo en la lucha contra la delincuencia grave y organizada;
- estudiar medidas para la aplicación eficaz del Modelo Nacional de Inteligencia, estableciendo prioridades, y gestionando y asignando tareas basadas en la evaluación SOCTA MNE;
- presentar informes trimestrales sobre su labor a la Oficina de Coordinación Operativa; y
- realizar otras tareas para dirigir las actividades de lucha contra la delincuencia grave y organizada.

Montenegro ha modificado ligeramente la metodología de evaluación *Sleipnir* de la Real Policía Montada de Canadá, que se está utilizando para evaluar las amenazas de los grupos delictivos organizados identificados y para comparar las clasificaciones de las amenazas entre grupos, así como para identificar deficiencias en materia de inteligencia que es preciso subsanar. La versión montenegrina modificada del modelo *Sleipnir* incluye 14 criterios de amenaza que son objeto de evaluación, como se presenta en el cuadro 8.3.

---

78 Boletín Oficial de Montenegro. "Law on Basis of the Intelligence and Security Sector of Montenegro" (Ley sobre la base del sector de la inteligencia y la seguridad de Montenegro). N° 28/14: Art. 17.

Cuadro 8.3 Versión montenegrina de la herramienta de evaluación Sleipnir

Grupo ID	Puntuación de la amenaza	Corrupción	Violencia	Negocios legítimos	Blanqueo de capitales	Cooperación con grupos delictivos	Protección de líderes	Monopolio	Territorio de actuación	Medidas de prevención	Diversidad (delito)	Disciplina/orden	Cohesión	Dimensión	Experiencia
N-RV01-00	230.3	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
N-RA03-00	226.0	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
N-BK02-06	215.4	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
N-BK06-09	212.1	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-BS01-92	209.3	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-BS01-90	206.8	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-NI04-08	202.9	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-NI01-95	193.5	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-HI02-08	191.7	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-BK01-06	189.1	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-HI01-08	184.1	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
R-UR07-09	183.7	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-UK02-05	180.2	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-IA01-97	177.9	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-PG02-00	174.2	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-BS06-11	172.7	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-BS04-00	172.1	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-BS08-00	171.2	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-HI04-10	161.1	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
L-HI03-10	143.2	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta

Amenaza	Alta	Media	Desconocida	Baja	Nula
Valor del atributo en la matriz	Alta	Media	Desconocida	Baja	Nula

### 8.3 La ILP y la actividad policial de proximidad

La actividad policial de proximidad se centra en resolver problemas de manera colectiva, prevenir el delito y fomentar la confianza entre la policía y las comunidades a las que sirve. Las prácticas y principios de dicha actividad ayudan a crear y fortalecer asociaciones entre la policía y los ciudadanos, en las que la policía, los organismos gubernamentales y las comunidades locales colaboran activamente para resolver conjuntamente los problemas y atender las reclamaciones de la comunidad.<sup>79</sup> La labor policial de proximidad se basa en la noción de que una mayor participación de la comunidad mejorará las operaciones policiales y la eficacia organizativa, así como la legitimidad de la policía a ojos de los ciudadanos.

La actividad policial de proximidad centra su atención concretamente en incrementar y mejorar las relaciones entre la comunidad y la policía, lo que representa un cambio fundamental a la hora de identificar delitos y disturbios locales conjuntamente con la policía y, cuando sea posible, abordarlos y resolverlos conjuntamente. Se basa en la convicción de que con un enfoque más coordinado y colaborativo se pueden resolver los problemas actuales y prevenir los futuros. Este enfoque también implica trabajar de una manera más multidisciplinaria y con la posibilidad de que otros socios, incluidos los gobiernos municipales, otros organismos o departamentos gubernamentales, o asociaciones comunitarias, participen en un programa.

La actividad policial de proximidad también puede conllevar que la comunicación con los ciudadanos y por parte de estos sea mejor y más fiable. Aunque no se debería asignar a los agentes de policía de proximidad la tarea de recopilar información de inteligencia, el aumento de la confianza puede representar para la policía una fuente inestimable de información y concienciación acerca de la comunidad. Eso puede convertirse en información valiosa para que la policía pueda planificar y dirigir sus operaciones contra la delincuencia y el terrorismo de manera más eficaz y de ese modo la actividad policial de proximidad y la actividad policial basada en la inteligencia pueden apoyarse directamente la una en la otra.

La actividad policial de proximidad ha tratado de ampliar los mandatos de la policía, pasando de un enfoque limitado a la lucha contra la delincuencia y a la investigación, a otro vinculado más directamente con la comunidad, a fin de generar a menudo opiniones y preocupaciones de la comunidad sobre una amplia gama de cuestiones: entre ellas, el temor a la delincuencia, la prevención del delito, los disturbios con daños materiales y otros problemas sociales y de vecindad. Los principios básicos que se reflejan en la actividad policial de proximidad incluyen un enfoque más orientado al servicio, construido en torno a los temas de “visibilidad”, “accesibilidad” y “familiaridad”, con especial atención a la resolución colectiva de problemas.<sup>80</sup> También proporciona los medios para que la policía pueda interactuar más eficazmente con los ciudadanos, e identificar y resolver sus problemas prioritarios.<sup>81</sup>

---

79 OSCE (2008a: 89).

80 Innes, Martin: *Why 'soft' policing is hard: on the curious development of reassurance policing, how it became neighbourhood policing and what this signifies about the politics of police reform*. *Journal of community applied social psychology*, Vol. 15, No. 3 (2005: 156–169); y Quinton, Paul y Morris, Julia: *Neighbourhood policing: the impact of piloting and early nation implementation*. (Informe en línea del Ministerio del Interior, 01/2008) [<http://webarchive.nationalarchives.gov.uk/20110314171826/>; <http://rds.homeoffice.gov.uk/rds/pdfs08/rdsolr0108.pdf>] Consultado el 2 de junio de 2017.

81 Bullock (2013: 126-127).



De acuerdo con los principios clave de la actividad policial de proximidad, la policía debería:

- *comprometerse*, movilizarse y asociarse con las comunidades;
- *escuchar* las preocupaciones de las comunidades;
- *participar* en la resolución conjunta de problemas con la comunidad;
- *ser visible y accesible* para los ciudadanos;
- *conocer* a los ciudadanos y que estos la conozcan;
- *responder* a las necesidades de las comunidades;
- *respetar y proteger* los derechos de todos los miembros de la comunidad; y
- *responsabilizarse* de sus acciones y de los resultados de las mismas.<sup>82</sup>

Como se señala en el Capítulo 3, la actividad policial basada en la inteligencia fue desarrollada para desafiar el modelo policial dominante, tradicionalmente reactivo y basado en respuestas. La ILP es a la vez un marco y un enfoque descendente de adopción de decisiones relativas a la gestión, y tiene consecuencias tanto para la forma en que se organiza la labor policial como para su funcionamiento. Desde el punto de vista organizativo, a diferencia de la actividad policial de proximidad, que permite a los agentes un amplio margen de maniobra para desarrollar sus relaciones con las comunidades locales, la ILP está necesariamente más centralizada. La recopilación y el análisis sistemáticos de datos e información proporcionan la base para adoptar decisiones de gestión fundamentadas.

La ILP y la actividad policial de proximidad son enfoques complementarios que se apoyan entre sí pero que tienen algunas características diferentes con respecto a su orientación, enfoque jerárquico y mecanismos de adopción de decisiones, tal y como se describe en el cuadro 8.4.

**Cuadro 8.4 Comparación de las dimensiones principales en la actividad policial de proximidad y en la actividad policial basada en la inteligencia**

	ACTIVIDAD POLICIAL DE PROXIMIDAD	ACTIVIDAD POLICIAL BASADA EN LA INTELIGENCIA
¿A quién va dirigida?	Comunidades locales y barrios	Grupos delictivos, delincuentes reincidentes y peligrosos, lucha contra el terrorismo y el extremismo violento y la radicalización que conducen al terrorismo
¿Cómo es su enfoque jerárquico?	Ascendente	Descendente
¿Quién establece las prioridades?	Las preocupaciones y reclamaciones de la comunidad	Los responsables de la formulación de políticas y los mandos policiales encargados del análisis de inteligencia criminal

82 OSCE, BIDD/NTD (2014: 76).

Los criterios de ambos enfoques para alcanzar el éxito y los beneficios esperados son similares, en tanto que apuntan a:

- una mayor eficacia policial basada en una mayor circulación de la información;
- un aumento de la seguridad y la protección de la comunidad, que se traduce en una mayor satisfacción por parte de la ciudadanía.

La recopilación de inteligencia nunca debe ser el objetivo principal de la actividad policial de proximidad, pero sí puede ser un resultado colateral de una actividad policial de proximidad eficaz. Complementando y apoyando a la ILP, la actividad policial de proximidad puede facilitar el intercambio de información entre los ciudadanos y la policía, mediante el fomento de la confianza de los ciudadanos en la policía y el aumento de las posibilidades de interacción entre ambos.

A su vez, las actividades de asignación de tareas y coordinación de la ILP pueden fortalecer los efectos de la actividad policial de proximidad a través de los procesos de análisis de la información y de sus estructuras jerárquicas. El carácter más positivo de la relación policía-ciudadano promueve ahora un intercambio de información más continuado y fiable entre ellos.

“La actividad policial de proximidad ha contribuido a mejorar las aptitudes de muchos agentes del orden, que apoyan directamente las nuevas responsabilidades de la ILP: el enfoque científico en la resolución de problemas, la exploración medioambiental, la comunicación eficaz con los ciudadanos, la reducción del miedo y la movilización de la comunidad a la hora de abordar problemas son algunos de los atributos importantes que la actividad policial de proximidad aporta a este desafío”<sup>83</sup>

Por lo tanto, existe la posibilidad de que las iniciativas de la actividad policial de proximidad sirvan de puerta de acceso para que la información local pueda prevenir y combatir todas las formas de delincuencia, incluidos el extremismo violento y el terrorismo (véase el subcapítulo 8.4). Al mismo tiempo, la ILP puede ayudar a los agentes de la policía de proximidad a identificar, dar prioridad y abordar con mayor eficacia cuestiones de interés público.

---

83 Carter (2009: 86-87).

“La actividad policial en los barrios debe tratar de generar información y esa información debe ser incorporada y ayudar a alimentar el proceso del Modelo Nacional de Inteligencia. Existen orientaciones que llaman la atención sobre las diferentes maneras de generar información procedente de las comunidades. Esto puede incluir las observaciones de ciudadanos; la información obtenida por agentes en el desempeño de sus funciones en los barrios; y la información procedente de otros funcionarios del sector público como maestros y médicos. Se ha asumido que con este proceder, se aumenta el conocimiento sobre riesgos y vulnerabilidades, se consiguen mejorar las oportunidades de participación ciudadana y aumenta la confianza por parte de la comunidad. Además, como hemos visto, uno de los objetivos de la actividad policial en los barrios es identificar y abordar de forma proactiva los problemas de delincuencia que son prioritarios para las comunidades locales. Los agentes de policía deben considerar estas prioridades como ‘inteligencia’ e incorporarlas a los sistemas del Modelo Nacional de Inteligencia”.

– **Bullock (2013: 128-131).**

Un enfoque y un interés más locales también apoyan la prevención del terrorismo y la lucha contra el extremismo violento y la radicalización que conducen al terrorismo (VERLT), en las que las comunidades se han convertido en un centro clave de atención a la hora de formular y aplicar políticas antiterroristas. Esto se basa en la idea de que el terrorismo y el extremismo violento y la radicalización que conducen al terrorismo constituyen amenazas, no solo para la seguridad del Estado sino también para la seguridad comunitaria, y que, por lo tanto, las comunidades son también partes interesadas y socios en la lucha contra el terrorismo. La lucha contra el terrorismo, y en particular contra el VERLT, también requiere un enfoque multidisciplinario y coordinado, en el que participen una amplia gama de autoridades públicas, además de los sectores de la seguridad y la justicia penal. Al colaborar con un número más amplio de personas e involucrarlas en diversos temas que no se limitan al empoderamiento contra el terrorismo, el Estado puede disminuir el riesgo de que se estigmatice a ciertas comunidades.<sup>84</sup>

---

84 OSCE, OIDDH/TNTD (2014: 74).

## 8.4 La ILP en la prevención y lucha contra el terrorismo y el VERLT

Una buena actuación policial equivale a una buena prevención del terrorismo; así pues, una actuación policial profesional es fundamental para revelar información de inteligencia relacionada tanto con actividades terroristas como con delitos convencionales. Fomentar esta perspectiva permite a los departamentos de policía locales involucrar más activamente a los agentes de primera línea y reforzar el hecho de que el cumplimiento de la ley, la prevención del delito y la prevención del terrorismo están interrelacionados. Este enfoque ayuda a equilibrar el énfasis que se pone actualmente en las actividades antiterroristas con iniciativas tradicionales contra el delito. Muchos agentes de primera línea quieren asumir un papel en la lucha contra el terrorismo. La ILP puede ayudar a aclarar sus contribuciones al respecto.<sup>85</sup>

Con una orientación administrativa y una formación adecuada, la práctica de la ILP puede proporcionar a todos los agentes del orden una visión clara de su papel en la prevención y la lucha contra el terrorismo y el VERLT. Si los canales de la ILP en materia de estructuras y procedimientos están establecidos y funcionan bien, recopilar y presentar información y sospechas se convierten en parte integrante de los deberes diarios de todas las fuerzas del orden, incluida la actividad policial general, la gestión de fronteras y los servicios aduaneros.

Las políticas y los programas destinados a generar contactos y confianza con las comunidades locales, incluidas las empresas, las comunidades religiosas, los líderes educativos, los jóvenes dirigentes y los centros culturales, pueden ayudar a prevenir y combatir el extremismo violento y el terrorismo. Así, algunos países han redefinido la actividad policial de proximidad enmarcándola dentro de la ILP con fines antiterroristas, creando estructuras y procesos adaptados a los ordenamientos jurídicos nacionales, para obtener y analizar información de los ciudadanos y de los entes (o instituciones) locales.<sup>86</sup>

Como se menciona en el subcapítulo 8.3, la policía y las comunidades deben entender claramente que la actividad policial de proximidad no solo se ocupa de recopilar inteligencia, sino también de proteger las necesidades de las comunidades. Sin embargo, su principal tarea sigue siendo crear y mantener asociaciones entre la policía y los ciudadanos, basadas en el respeto y la confianza mutuos.<sup>87</sup>

---

85 Peterson (2005: 15-16).

86 Ratcliffe (2016: 115).

87 OSCE, OIDDH/TNTD (2014: 179).

“Hay un ámbito en el que la actividad policial de proximidad podría ser la única opción viable para recopilar información útil de la comunidad. En un escenario antiterrorista, numerosos analistas han argumentado que dicha actividad de proximidad será más efectiva en la recopilación de información local y posiblemente de inteligencia, y también más acorde con las expectativas ciudadanas con respecto a la policía en una nación democrática que las tácticas encubiertas y otras técnicas de inteligencia”.

– **Innes (2006: 229).**

Cuando tanto la policía como las comunidades comparten la idea de que el objetivo de la policía y de los organismos asociados en la lucha contra el VERTL es, en primer lugar, proteger a las personas vulnerables de las influencias radicalizadoras, es más fácil fomentar la confianza. La preocupación de que la policía espíe y seleccione como objetivo a las comunidades puede mitigarse en gran medida cuando las comunidades entienden que el papel de la policía es protegerlas y cuando el VERTL se explica en el contexto de la protección de la comunidad, por ejemplo, previniendo la explotación sexual de los niños o la trata de personas. Es innegable que la experiencia del Reino Unido ha demostrado que las dudas en torno a su estrategia y actividad política de prevención se pueden mitigar cuando la policía y los organismos gubernamentales centrales y locales trabajan juntos para transmitir un mensaje coherente de que la estrategia de prevención tiene por objeto lisa y llanamente proteger a las personas vulnerables de los radicalizadores, independientemente de su comunidad de origen.

Para facilitar el importante papel que desempeña la policía de proximidad, sus agentes deben recibir formación sobre dónde buscar y cómo identificar indicios de planificación de terrorismo o de VERLT, y cómo transmitir la información en consonancia con los procedimientos operativos normalizados nacionales, a través de los canales pertinentes, a una entidad de análisis centralizada. Los agentes también deberían recibir una formación especializada en materia de derechos humanos a fin de realizar esas tareas respetando plenamente las normas de derechos humanos<sup>88</sup>. También es imprescindible que los agentes locales que remiten dicha información reciban comentarios sobre su actividad en este sentido.

A fin de apoyar el papel central que desempeña la actividad policial de proximidad en la creación de asociaciones entre la policía y los ciudadanos y en la prevención de la delincuencia a todos los niveles, incluidos los delitos graves y las actividades presuntamente relacionadas con el terrorismo, o en la prevención y la lucha contra el VERLT, algunos países han designado a agentes especialmente capacitados en VERLT, que han sido desplegados para apoyar a los agentes de policía de la comunidad local. Las decisiones sobre la ubicación de

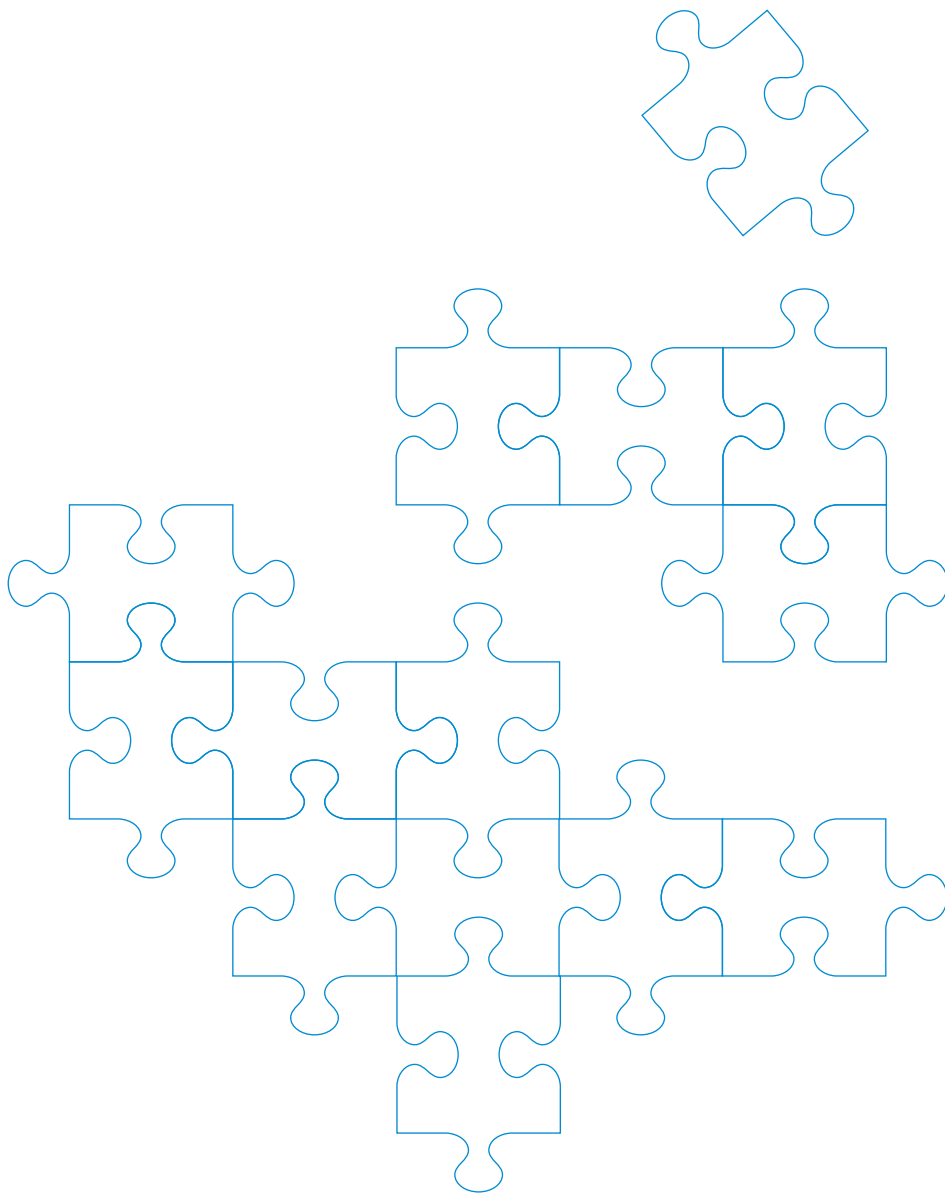
88 OSCE, OIDDH/TNTD (2014: 106-107).

este despliegue de recursos a largo plazo se basan en análisis de inteligencia que proporcionan una evaluación del riesgo y la amenaza de VERLT sobre una base geográfica. Dentro de una estructura predefinida y basada en decisiones oficiales arraigadas en la legislación nacional, estos agentes se relacionan con las comunidades como lo harían los agentes de la policía de proximidad, pero con el propósito específico y explícito de trabajar abiertamente con las comunidades y los grupos de la sociedad civil para crear confianza y minimizar el riesgo y la amenaza asociados con el VERLT. Al igual que los agentes de la policía de proximidad, estos agentes especializados envían información para su evaluación y valoración a una entidad central de análisis, a través de canales de comunicación oficiales, o la introducen directamente en las bases de datos nacionales. El objetivo de esta función especializada es, como siempre, trabajar en la comunidad y con las comunidades, e involucrar a todos los interesados en la prevención del VERLT; no se trata de espiar a estas comunidades.

Como se indica en el Capítulo 7, la ILP se basa en estructuras organizativas y sistemas de comunicación que funcionan correctamente y que pueden facilitar el intercambio de información en ambos sentidos entre las comunidades, los agentes de policía de la comunidad y otras fuentes locales, y una entidad central de análisis. Una vez más, hay que subrayar que el principal objetivo de la actividad policial de proximidad no es espiar a las comunidades, sino establecer vínculos positivos y aumentar la confianza entre la policía y el ciudadano para facilitar el intercambio de información e inteligencia. La participación de la comunidad en el contexto del VERLT debe basarse en una relación policía-comunidad que funcione y en el apoyo de la propia comunidad, que no hay que darlo por supuesto, hay que ganárselo. Es necesario desarrollar relaciones de confianza entre la policía y los diversos sectores de la comunidad mucho antes de que se puedan abordar cuestiones delicadas como el VERLT en iniciativas conjuntas.<sup>89</sup> Cuando los agentes de la policía de proximidad han establecido una relación de confianza y unos canales de comunicación saludables con sus comunidades locales, estos pueden ser la fuente de información más sólida, o incluso la única, procedente de la comunidad, con la que identificar los factores impulsores de la radicalización terrorista y que podría ayudar a prevenir incidentes terroristas o a identificar a las personas que pueden ser vulnerables frente a la radicalización terrorista.

---

<sup>89</sup> OSCE, OIDDH/TNTD (2014: 85-87).



## Referencias

*Australian Criminal Intelligence Management Strategy 2012-2015* (Commonwealth de Australia, 2012). [[www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2012-15.pdf](http://www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2012-15.pdf)] Consultado el 27 de abril de 2017.

Bell, Peter y Congram, Mitchell. *Intelligence-Led Policing (ILP) as a Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC)*. *International Journal of Business and Commerce*, Vol. 2, No. 12 (2013): 15-28. [[www98.griffith.edu.au/dspace/bitstream/handle/10072/64598/98685\\_1.pdf;sequence=1](http://www98.griffith.edu.au/dspace/bitstream/handle/10072/64598/98685_1.pdf;sequence=1)] Consultado el 5 de abril de 2017.

Bullock, Karen. *Community, intelligence-led policing and crime control. Policing and Society*, Vol. 23, No. 2 (2013): 125-144.

Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2ª edición (Washington, DC: Ministerio de Justicia de Estados Unidos, 2009).

Conferencia sobre la Seguridad y la Cooperación en Europa, *Acta Final de Helsinki* (Helsinki: 1975). [[www.osce.org/es/mc/39506?download=true](http://www.osce.org/es/mc/39506?download=true)]

Consejo de Europa, *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales* (CEDH), (4 de noviembre de 1950). [[www.echr.coe.int/Documents/Convention\\_SPA.pdf](http://www.echr.coe.int/Documents/Convention_SPA.pdf)]

Consejo de Europa, *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, Serie de Tratados Europeos, Núm. 108 (Estrasburgo: 28 de enero de 1981). [[rm.coe.int/16806c1abd](http://rm.coe.int/16806c1abd)]

Consejo de Europa, *The European Code of Police Ethics* (Estrasburgo: Publicaciones del Consejo de Europa, marzo de 2002). [[www.bak.gv.at/cms/BAK\\_dt/download/downloads/files/Verhaltenskodex/CoE\\_FRA\\_RPT\\_2687\\_EN\\_500.pdf](http://www.bak.gv.at/cms/BAK_dt/download/downloads/files/Verhaltenskodex/CoE_FRA_RPT_2687_EN_500.pdf)] Consultado el 27 de abril de 2017.

Tribunal Europeo de Derechos Humanos. Caso de Shimovolos contra Rusia. Demanda núm. 30194/09 (Estrasburgo: 21 de junio de 2011). [[hudoc.echr.coe.int/eng#{"appno":\["30194/09"\],"itemid":\["001-105217"\]}](http://hudoc.echr.coe.int/eng#{)] Consultado el 28 de abril de 2017.

Tribunal Europeo de Derechos Humanos. Caso de Roman Zakharov contra Rusia. Demanda núm. 47143/06 (Estrasburgo: 4 de diciembre de 2015). [[lovdata.no/static/EMDN/emd-2006-047143.pdf](http://lovdata.no/static/EMDN/emd-2006-047143.pdf)] Consultado el 28 de abril de 2017.

Tribunal Europeo de Derechos Humanos. Caso de Szabo y Vissy contra Hungría. Demanda núm. 37138/14 (Estrasburgo: 12 de enero de 2016). [[www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf](http://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf)] Consultado el 28 de abril de 2017.



Consejo de la Unión Europea. “Council conclusions on intelligence-led policing and the development of the Organized Crime Threat Assessment (OCTA)”. [“Conclusiones del Consejo sobre las funciones policiales basadas en la inteligencia y el desarrollo de la evaluación de la amenaza de la delincuencia organizada (EADO)”] Doc. 10180/4/05, REV 4, (Bruselas: 3 de octubre de 2005). [[register.consilium.europa.eu/doc/srv?l=ES&f=ST%2010180%202005%20REV%204](http://register.consilium.europa.eu/doc/srv?l=ES&f=ST%2010180%202005%20REV%204)] Consultado el 27 de abril de 2017.

Consejo de la Unión Europea. “Decisión Marco del Consejo de 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea”. *Diario Oficial de la Unión Europea* (2006/960/JHA, 18 de diciembre de 2006). [[eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32006F0960&from=EN](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32006F0960&from=EN)]

Consejo de la Unión Europea. “Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime.” [“Conclusiones del Consejo sobre la creación y aplicación de un ciclo de actuación de la UE para la delincuencia internacional organizada grave”] Sesión no. 3043 Justicia y Asuntos de Interior, (Bruselas: 8 y 9 de noviembre de 2010). [[www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/jha/117583.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf)] Consultado el 6 de abril de 2017.

Consejo de la Unión Europea. “Serious and Organised Crime Threat Assessment (SOCTA) – Methodology”. Doc. 9992/2/12, REV 2, COSI 28, (Bruselas: 19 de junio de 2012). [[www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/p24\\_soctamethodology\\_/p24\\_soctamethodology\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/p24_soctamethodology_/p24_soctamethodology_en.pdf)] Consultado el 6 de abril de 2017.

Consejo de la Unión Europea. “EMPACT Terms of Reference”. [“Términos de referencia de la plataforma EMPACT”] Doc. 14518/12, COSI 82, (Bruselas: 3 de octubre de 2012). [[www.statewatch.org/news/2012/oct/eu-council-cosi-empact-tor-14518-12.pdf](http://www.statewatch.org/news/2012/oct/eu-council-cosi-empact-tor-14518-12.pdf)] Consultado el 6 de abril de 2017.

Consejo de la Unión Europea. “Council conclusions on setting the EU’s priorities for the fight against serious and organised crime between 2014-2017”. [“Conclusiones sobre la determinación de las prioridades de la UE para la lucha contra la delincuencia organizada y grave durante el ciclo de actuación 2014-2017”] Reunión del Consejo de Justicia y Asuntos de Interior, (Luxemburgo: 6 y 7 de junio de 2013). [[www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/jha/137401.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137401.pdf)] Consultado el 6 de abril de 2017.

Consejo de la Unión Europea, *The EU Policy Cycle to tackle organized and serious international crime* (Bruselas: 2014).

Consejo de la Unión Europea, “Serious and Organised Crime Threat Assessment 2017 – Revised methodology”. Doc. 14913/15, CRIMORG 128, Bruselas: 11 de diciembre de 2015. [[www.statewatch.org/news/2015/dec/eu-council-socta-2017-methodology-14913-15.pdf](http://www.statewatch.org/news/2015/dec/eu-council-socta-2017-methodology-14913-15.pdf)] Consultado el 6 de abril de 2017.

Servicio de Inteligencia Criminal de Canadá, *Integrated Threat Assessment Methodology, Version 1.0* (Ottawa, Ontario: Servicio de Inteligencia Criminal de Canadá, 2007).

Eck, John E., Clarke, Ronald V. y Petrossian, G. *Intelligence Analysis for Problem Solvers* (Washington, DC: Departamento de Estado de los Estados Unidos, Servicios de Policía Orientados a la Comunidad, 2013).

Servicio Europeo de Acción Exterior, *Handbook on Intelligence Led Policing (ILP) for civilian CSDP Missions* (Capacidad Civil de Planificación y Ejecución, Ministerio belga de Asuntos Exteriores, Policía Federal de Bélgica, 2013).

Europol, *EU Policy Cycle SOCTA Empact* (Europol, 2010). [<https://www.europol.europa.eu/publications-documents/eu-policy-cycle-socta-empact>] Consultado el 27 de abril de 2017.

Europol, *SOCTA 2013 – EU Serious and Organised Crime Threat Assessment* (La Haya: Oficina Europea de Policía, 2013). [<https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013>] Consultado el 27 de abril de 2017.

Europol, *Exploring Tomorrow's Organized Crime* (La Haya: Oficina Europea de Policía, 2015). [<https://www.europol.europa.eu/publications-documents/exploring-tomorrow's-organised-crime>] Consultado el 27 de abril de 2017.

Europol, *SOCTA 2017 – European Union Serious and Organised Crime Threat Assessment 2017* (La Haya: Oficina Europea de Policía, 2017) [<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>] Consultado el 28 de abril de 2017.

Flood, B. y Gaspar, R. "Strategic aspects of the UK National Intelligence Model". En: "The path to enlightenment: Limiting costs and maximizing returns from intelligence-led policy and practice in public policing". *Policing: A Journal of Policy and Practice*, ed. Adrian James (Oxford University Press, 2017).

Centro de Ginebra para el Control Democrático de las Fuerzas Armadas (DCAF), *Criminal Intelligence Manual* (Liubliana: Instituto DCAF de Liubliana, 2014). [[dcaf-ljubljana.si/116](https://dcaf-ljubljana.si/116)] Consultado el 27 de abril de 2017.

Innes, Martin. "Why 'soft' policing is hard: on the curious development of reassurance policing, how it became neighbourhood policing and what this signifies about the politics of police reform". *Journal of community applied social psychology*, Vol. 15, No. 3 (2005): 156–169).

Innes, Martin. "Policing uncertainty: Countering terror through community intelligence and democratic policing". *The Annals of the American Academy of Political and Social Science*, Vol. 605, No. 1 (2006): 222-241.

Asociación Internacional de Jefes de Policía. “Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels”. IACP Intelligence Summit, Alexandria, Virginia (2002).

Interpol. “Análisis de información policial”. *Fact Sheet* (2014). [<https://www.interpol.int/es/Internet/Especialidades/Análisis-de-información>]

James, Adrian D.; Phythian, Mark; Richards, Julian y Wadie, Fiona C. ‘*What works?*’ in *police intelligence practice?* (The National Police Chiefs Council, 2016).

James, Adrian. “The path to enlightenment: Limiting costs and maximizing returns from intelligence-led policy and practice in public policing”. *Policing: A Journal of Policy and Practice* (Oxford University Press, 2017).

Karn, Jacqui, *Policing and Crime Reduction: The evidence and its implications for practice* (Londres: The Police Foundation, 2013).

Kelling, George L., and Bratton, William J. “Policing terrorism”. *Civic Bulletin* 43, No. 12 (2006).

Policía de Kosovo, *Handbook Intelligence led policing* (Pristina: 2016). [No publicado].<sup>90</sup>

Murdoch, Jim y Roche, Ralph, *The European Convention on Human Rights and Policing: A Handbook for police officers and other law enforcement officials* (Estrasburgo: Consejo de Europa/Unión Europea, 2013).

Ministerio del Interior de la República de Serbia, *Handbook on the police intelligence model* (2016). [[www.mup.gov.rs](http://www.mup.gov.rs)] Consultado el 28 de abril de 2017.

Ministerio del Interior de la República de Serbia. “Decree on the Promulgation of the Law on Police”. PR No. 1, (Belgrado: 28 de enero de 2016). [[arhiva.mup.gov.rs/cms\\_eng/home.nsf/Law-on-Police-adopted-01-03-2016.pdf](http://arhiva.mup.gov.rs/cms_eng/home.nsf/Law-on-Police-adopted-01-03-2016.pdf)] Consultado el 3 de mayo de 2017.

Servicio Nacional de Inteligencia Criminal (NCIS), *The National Intelligence Model* (NCIS Corporate Communications, 2000[[www.intelligenceanalysis.net/National%20Intelligence%20Model.pdf](http://www.intelligenceanalysis.net/National%20Intelligence%20Model.pdf)]) Consultado el 27 de abril de 2017.

National Policing Improvement Agency, *Practice Advice on Analysis* (Association of Chief Police Officers, 2008). [[library.college.police.uk/docs/npia/practice\\_advice\\_on\\_analysis\\_interactive.pdf](http://library.college.police.uk/docs/npia/practice_advice_on_analysis_interactive.pdf)] Consultado el 27 de abril de 2017.

O’Neill, Maria, Swinton, Ken y Winter, Aaron, *New Challenges for the EU Internal Security Strategy* (Newcastle, Reino Unido: Cambridge Scholars Publishing, 2013).

<sup>90</sup> Todas las referencias a Kosovo que figuran en este texto, ya sea al territorio, las instituciones o la población, se entenderá que están en plena consonancia con la resolución 1244 del Consejo de Seguridad de las Naciones Unidas.

*Boletín Oficial de Montenegro* “Law on Basis of the Intelligence and Security Sector of Montenegro”, No. 28/14. [[www.sluzbenilist.me/PravniAktDetalji.aspx?tag=%7B65668A19-BB7B-4029-BDC4-1D46FE9208E2%7D](http://www.sluzbenilist.me/PravniAktDetalji.aspx?tag=%7B65668A19-BB7B-4029-BDC4-1D46FE9208E2%7D)] Consultado el 3 de mayo de 2017.

OSCE, *Documento de clausura de la Reunión de Viena de 1986 de los representantes de los Estados participantes en la Conferencia sobre la Seguridad y la Cooperación en Europa, convocada sobre la base de las disposiciones del Acta Final relativas a la continuidad de la Conferencia* (Viena: 1989). [[www.osce.org/es/mc/40886?download=true](http://www.osce.org/es/mc/40886?download=true)]

OSCE, *Documento de la Reunión de Moscú de la Conferencia sobre la Dimensión Humana de la CSCE* (Moscú, 3 de octubre de 1991). [[www.osce.org/odihr/elections/14310](http://www.osce.org/odihr/elections/14310)].

OSCE, *Good Practices in Building Police-Public Partnerships by the Senior Police Adviser to the OSCE Secretary General* (Viena: OSCE, 2008a). [[www.osce.org/spmu/32547?download=true](http://www.osce.org/spmu/32547?download=true)] Consultado el 28 de abril de 2017.

OSCE, *Guidebook on democratic policing, by the Senior Police Adviser to the OSCE Secretary General*, 2a edición (Viena: OSCE, 2008b). [[www.osce.org/spmu/23804](http://www.osce.org/spmu/23804)] Consultado el 6 de abril de 2017.

OSCE, *Human rights in counter-terrorism investigations – A Practical Manual for Law Enforcement Officers* (Varsovia: Oficina de Instituciones Democráticas y Derechos Humanos (OIDDH) y Departamento de Amenazas Transnacionales (TNTD), 2013). [[www.osce.org/odihr/108930?download=true](http://www.osce.org/odihr/108930?download=true)] Consultado el 6 de abril de 2017.

OSCE, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach* (Viena: OIDDH y TNTD, 2014). [[www.osce.org/atu/111438](http://www.osce.org/atu/111438)] Consultado el 27 de abril de 2017.

OSCE. “Assessments of OSCE Field Operations’ engagement in national intelligence- led policing programmes in OSCE participating States”. Viena: OSCE, Unidad de Asuntos Policiales de Carácter Estratégico/Departamento de Amenazas Transnacionales (SPMU/ TNTD), 17 de febrero de 2016. [No publicado/interno].

OSCE. “Status of Intelligence-Led Policing Concepts in International Security and Law Enforcement Organizations”. *Interoffice Memorandum* (Viena: OSCE, 26 de abril de 2016). [No publicado/interno].

Reunión de Jefes de Policía de la OSCE, *Brussels Statement* (24 de noviembre de 2006). [[www.osce.org/spmu/23260?download=true](http://www.osce.org/spmu/23260?download=true)] Consultado el 6 de abril de 2017.

Consejo Ministerial de la OSCE, Declaración Ministerial. “Declaración Ministerial de Sofía sobre prevención y lucha contra el terrorismo” (Sofía: MC(12).JOUR/2, 7 de diciembre de 2004). [[www.osce.org/es/mc/41818?download=true](http://www.osce.org/es/mc/41818?download=true)]

Consejo Ministerial de la OSCE, Declaración Ministerial. “Declaración Ministerial de Bruselas sobre el apoyo y la promoción del marco jurídico internacional contra el terrorismo” (Bruselas: MC.DOC/5/06, 5 de diciembre de 2006). [[www.osce.org/es/mc/23034?download=true](http://www.osce.org/es/mc/23034?download=true)]

Consejo Ministerial de la OSCE, Decisión N° 5/06. “Delincuencia organizada” (Bruselas: MC.DEC/5/06, 5 de diciembre de 2006). [[www.osce.org/es/mc/23065?download=true](http://www.osce.org/es/mc/23065?download=true)]

Consejo Permanente de la OSCE, Decisión N° 1049. “Marco Estratégico de la OSCE para actividades relacionadas con la policía” (Viena: PC.DEC/1049, 26 de julio de 2012). [[www.osce.org/es/pc/94963?download=true](http://www.osce.org/es/pc/94963?download=true)]

Pajevic, Maid. “Application of the Theory of Criminal Intelligence in Police Work”. *E-Journal of Police Studies (Ijps), Internacionalna asocijacija policijskih akademija (INTERPA)* (2014).

Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (Canberra Comisión Parlamentaria Mixta de Canberra sobre Aplicación de la Ley, Commonwealth de Australia, 2013).

Peterson, Marilyn, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: Departamento de Justicia de los Estados Unidos, Oficina de Asistencia Judicial, 2005).

Quinton, P. y Morris, J. “Neighbourhood policing: The impact of piloting and early national implementation”. (Informe en línea del Ministerio del Interior, 01/2008) [<http://webarchive.nationalarchives.gov.uk/20110314171826/http://rds.homeoffice.gov.uk/rds/pdfs08/rdsolr0108.pdf>] Consultado el 2 de junio de 2017.

Ratcliffe, Jerry H., *Intelligence-Led Policing* (Cullompton, Reino Unido: Willan Publishing, 2008).

Ratcliffe, Jerry H., Strang, Steven y Taylor, Ralph. “Assessing the success factors of organized crime groups”. *Policing: an International Journal of Police Strategies & Management, Vol. 37, No. 1* (2014: 206-227).

Ratcliffe, Jerry H., *Intelligence-Led Policing*, 2ª edición (Londres/Nueva York: Routledge, 2016).

Renard, Thomas. “Counterterrorism in Belgium: Key Challenges and Policy Options”. *Egmont Paper 89* (Bruselas: Egmont Institute, 2016).

Inteligencia Criminal de la Real Policía Montada de Canadá. “Sleipnir Version 2.0, Organized Crime Groups Capability Measurement Matrix”. (Ottawa: RCMP, 2011). [[www.yumpu.com/en/document/view/51586046/sleipnir-version-20-organized-crime-groups-capability-](http://www.yumpu.com/en/document/view/51586046/sleipnir-version-20-organized-crime-groups-capability-)] Consultado el 27 de abril de 2017.

Stevens, John, "Intelligence-Led Policing". Ponencia presentada en la conferencia internacional del Instituto de Estudios de Derechos Humanos y Justicia Penal, Durban, 3-7 de diciembre de 2001.

Departamento de Operaciones de Mantenimiento de la Paz de las Naciones Unidas (PNUDKO). "Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions". Ref. 2015.15, 1 de enero de 2016. [[www.un.org/en/peacekeeping/sites/police/documents/Guidelines\\_Operations.pdf](http://www.un.org/en/peacekeeping/sites/police/documents/Guidelines_Operations.pdf)] Consultado el 27 de abril de 2017.

Asamblea General de las Naciones Unidas. "Pacto Internacional de Derechos Civiles y Políticos". *Núm. 14668, Serie de Tratados de Naciones Unidas, Vol. 999* (Nueva York: 16 de diciembre de 1966). [[www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx](http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx)]

Asamblea General de las Naciones Unidas, resolución 34, "Código de conducta para funcionarios encargados de hacer cumplir la ley". A/RES/34/169, 17 de diciembre de 1979. [[www.ohchr.org/SP/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx](http://www.ohchr.org/SP/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx)]

Asamblea General de las Naciones Unidas, resolución 45/95, "Guidelines for the regulation of computerized personal data files." ["Principios rectores sobre la reglamentación de los ficheros computerizados de datos personales"]. A/RES/45/95, 14 de diciembre de 1990. [[www.un.org/en/ga/search/view\\_doc.asp?symbol=A/RES/45/95&Lang=S](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/95&Lang=S)] Consultado el 27 de abril de 2017.

Asamblea General de las Naciones Unidas. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin." Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 4 de febrero de 2009, A/HRC/10/3. [[www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx](http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx)] Consultado el 27 de abril de 2017.

Asamblea General de las Naciones Unidas. "Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo. Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión". Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 17 de mayo de 2010, A/HRC/14/46. [[https://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/a.hrc.14.46\\_sp.pdf](https://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/a.hrc.14.46_sp.pdf)] Consultado el 28 de abril de 2017.

Asamblea General de las Naciones Unidas. "Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Maina Kiai, Addendum, Misión al Reino Unido de Inglaterra y del Norte de Irlanda". Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 17 de junio de 2013, A/HRC/23/39/Add.1. [[undocs.org/es/A/HRC/23/39/Add.1](http://undocs.org/es/A/HRC/23/39/Add.1)]

Asamblea General de las Naciones Unidas. “Informe del Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes, Juan E. Méndez”. Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 10 de abril de 2014, A/HRC/25/60. [[undocs.org/es/A/HRC/25/60](http://undocs.org/es/A/HRC/25/60)]

Asamblea General de las Naciones Unidas. “Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo”. Informe Anual presentado a la Asamblea General de las Naciones Unidas, 23 de septiembre de 2014, A/69/397. [[undocs.org/es/A/69/397](http://undocs.org/es/A/69/397)]

Asamblea General de las Naciones Unidas. “Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emmerson”. Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 16 de junio de 2015, A/HRC/29/51. [[undocs.org/sp/A/HRC/29/51](http://undocs.org/sp/A/HRC/29/51)]

Asamblea General de las Naciones Unidas. “Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo”. Informe presentado al Consejo de Derechos Humanos de las Naciones Unidas, 21 de febrero de 2017, A/HRC/34/61. [[undocs.org/sp/A/HRC/34/61](http://undocs.org/sp/A/HRC/34/61)]

Comité de Derechos Humanos de las Naciones Unidas, *HRC Observación general N° 16 (General Comment): Art. 17 (Derecho a la intimidad), Derecho al respeto de la intimidad, la familia, el hogar y la correspondencia, y la protección del honor y la reputación* (8 de abril de 1988). [[www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf](http://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf)]

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Convención de las Naciones Unidas contra la Corrupción* (Viena: Publicaciones de las Naciones Unidas, 2004). [[www.unodc.org/documents/treaties/UNCAC/Publications/Convention/04-56163\\_S.pdf](http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/04-56163_S.pdf)]

UNODC, *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos* (Viena: Publicaciones de las Naciones Unidas, 2004). [[www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf](http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf)]

UNODC, *Sistemas policiales de información e inteligencia. Manual de instrucciones para la evaluación de la justicia penal* (Viena: Publicaciones de las Naciones Unidas, 2006). [[www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Police\\_Information\\_and\\_Intelligence\\_Systems\\_Spanish.pdf](http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Police_Information_and_Intelligence_Systems_Spanish.pdf)]

UNODC, *Current Practices in Electronic Surveillance in the Investigation of serious and organized crime* (Viena: Publicaciones de las Naciones Unidas, 2009). [[www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic\\_surveillance.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf)] Consultado el 27 de abril de 2017.

UNODC, *Criminal Intelligence – Manual for Front-line Law Enforcement* (Viena: Publicaciones de las Naciones Unidas, 2010a). [[www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal\\_Intelligence\\_for\\_Front\\_Line\\_Law\\_Enforcement.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Front_Line_Law_Enforcement.pdf)] Consultado el 27 de abril de 2017.

UNODC, *Guidance on the preparation and use of serious and organized crime threat assessments. The SOCTA Handbook* (Viena: Publicaciones de las Naciones Unidas, 2010b). [[www.unodc.org/documents/organized-crime/Law-Enforcement/SOCTA\\_Handbook.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/SOCTA_Handbook.pdf)] Consultado el 27 de abril de 2017.

UNODC, *Criminal Intelligence – Manual for Analysts* (Viena: United Nations Publication, 2011a). [[www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal\\_Intelligence\\_for\\_Analysts.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf)] Consultado el 27 de abril de 2017.

UNODC, *Criminal Intelligence – Manual for Managers* (Viena: United Nations Publication, 2011b). [[www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal\\_Intelligence\\_for\\_Managers.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf)] Consultado el 27 de abril de 2017.

Ministerio de Justicia de los Estados Unidos, *Reducing Crime Through Intelligence-Led Policing* (Washington, DC: Ministerio de Justicia de los Estados Unidos, Oficina de Asistencia Judicial, 2009).

Ministerio de Justicia de los Estados Unidos, *Law Enforcement Analytic Standards*. 2ª edición (Washington, DC: Ministerio de Justicia de los Estados Unidos, Oficina de Asistencia Judicial, 2012).

Weisburd, David y Eck, John E. “What can the police do to reduce crime, disorder and fear?” *Annals of the American Academy of Social and Political Sciences*, Vol. 593 (2004): 42–65.

Wells, Ronald, “Intelligence-Led Policing: a new paradigm in law enforcement.” *Public Agency Training Council (PATC), E-Newsletter* (2009). [[www.patc.com/weeklyarticles/intelligence\\_policing.shtml](http://www.patc.com/weeklyarticles/intelligence_policing.shtml)] Consultado el 6 de abril de 2017.



## **Páginas web**

Center for Problem-Oriented Policing  
**[www.popcenter.org/about/?p=whatispop](http://www.popcenter.org/about/?p=whatispop)**.

International Association of Law Enforcement Intelligence Analysts (IALEIA)  
**[www.ialeia.org/](http://www.ialeia.org/)** [Consultado el 27 de abril de 2017].

Problem Oriented Policing  
**[www.popcenter.org/about/?p=whatispop](http://www.popcenter.org/about/?p=whatispop)** [Consultado el 27 de abril de 2017].

Oficina de las Naciones Unidas contra la Droga y el Delito – Delincuencia Organizada:  
**[www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside](http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside)** [Consultado el 27 de abril de 2017].

## Colección de publicaciones de la SPMU/TNTD

Vol. 1 Guidebook on Democratic Policing by the Senior Police Adviser to the OSCE Secretary General [Guía sobre la actividad policial democrática, por el Asesor Superior de Policía del Secretario General de la OSCE], Vol. 1 de la colección de publicaciones de la SPMU, 2ª edición, Viena, mayo de 2008.

Vol. 2 Reference Guide to Criminal Procedure [Guía de referencia del procedimiento penal], Vol. 2 de la colección de publicaciones de la SPMU, Viena, diciembre de 2006.

Vol. 3 Enhancing cooperation among police, prosecutors and judges in the fight against transnational organized crime [Fortalecimiento de la cooperación entre la policía, los fiscales y los jueces en la lucha contra la delincuencia organizada transnacional]. Informe de proyecto, Vol. 3 de la colección de publicaciones de la SPMU, Viena, diciembre de 2007.

Vol. 4 Good Practice in Building Police-Public Partnerships by the Senior Police Adviser to the OSCE Secretary General [Buenas prácticas en la creación de asociaciones entre la policía y los ciudadanos, por el Asesor Superior de Policía del Secretario General de la OSCE], Vol. 4 de la colección de publicaciones de la SPMU, Viena, mayo de 2008.

Vol. 5 Good Practices in Basic Police Training – Curricula Aspects by the Senior Police Adviser to the OSCE Secretary General [Buenas prácticas en la formación policial básica: aspectos de los planes de estudios por el Asesor Superior de Policía del Secretario General de la OSCE], Vol. 5 de la colección de publicaciones de la SPMU, Viena, octubre de 2008.

Vol. 6 Прекурсоры наркотических средств [Manual de Precursores], Vol. 6 de la colección de publicaciones de la SPMU, Viena, noviembre de 2008.

Vol. 7 Implementation of Police-Related Programmes. Lessons Learned in South-Eastern Europe [Aplicación de programas relacionados con la policía. Lecciones aprendidas en Europa sudoriental], Vol. 7 de la colección de publicaciones de la SPMU, Viena, diciembre de 2008.

Vol. 8 Controlled Delivery Guidebook for South-East European Countries, [Guía sobre entregas vigiladas para los países de Europa sudoriental], Vol. 8 de la colección de publicaciones de la SPMU, Viena, enero de 2009.

Vol. 9 Police and Roma and Sinti: Good Practices in Building Trust and Understanding [La policía y los romaníes y sinti: Buenas prácticas para crear confianza y buen entendimiento], Vol. 9 de la colección de publicaciones de la SPMU, Viena, abril de 2010.

Vol. 10 Trafficking in Human Beings: Identification of Potential and Presumed Victims. A Community Policing Approach [Trata de personas: Identificación de víctimas potenciales y presuntas. Un enfoque de la actividad policial de proximidad], Vol. 10 de la colección de publicaciones de la SPMU, Viena, junio de 2011.

Vol. 11 Police Reform within the Framework of Criminal Justice System Reform [La reforma policial en el marco de la reforma del sistema de justicia penal], Vol. 11 de la colección de publicaciones de la SPMU/TNTD, Viena, julio de 2013.

Vol. 12 OSCE Resource Police Training Guide: Trafficking in Human Beings [Guía de la OSCE sobre recursos para la capacitación policial: la trata de personas], Vol. 12 de la colección de publicaciones de la SPMU/TNTD, Viena, julio de 2013.

Vol. 13 Guía de la OSCE sobre la actividad policial basada en la inteligencia, Vol. 13 de la colección de publicaciones de la SPMU/TNTD, Viena, julio de 2017.

## Otras publicaciones del TNTD relacionadas con la policía

*Human Rights In Counter-Terrorism Investigations. A Practical Manual For Law Enforcement Officers* [Los derechos humanos en las investigaciones antiterroristas. Un manual práctico para los encargados de hacer cumplir la ley]. Publicación conjunta de la Oficina de Instituciones Democráticas y Derechos Humanos (OIDDH) y el Departamento de Amenazas Transnacionales (TNTD) de la OSCE, Varsovia, 2013.

*Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism. A Community-Policing Approach* [Prevención del terrorismo y lucha contra el extremismo violento y la radicalización que conducen al terrorismo. Un enfoque de la actividad policial de proximidad]. Publicación conjunta de la OIDDH y el TNTD, Viena, febrero de 2014.

Las publicaciones pueden solicitarse directamente a la SPMU/TNTD ([spmu@osce.org](mailto:spmu@osce.org)) o descargarse del sitio web de POLIS en: [polis.osce.org/library](http://polis.osce.org/library)





**Sigue a la OSCE**



