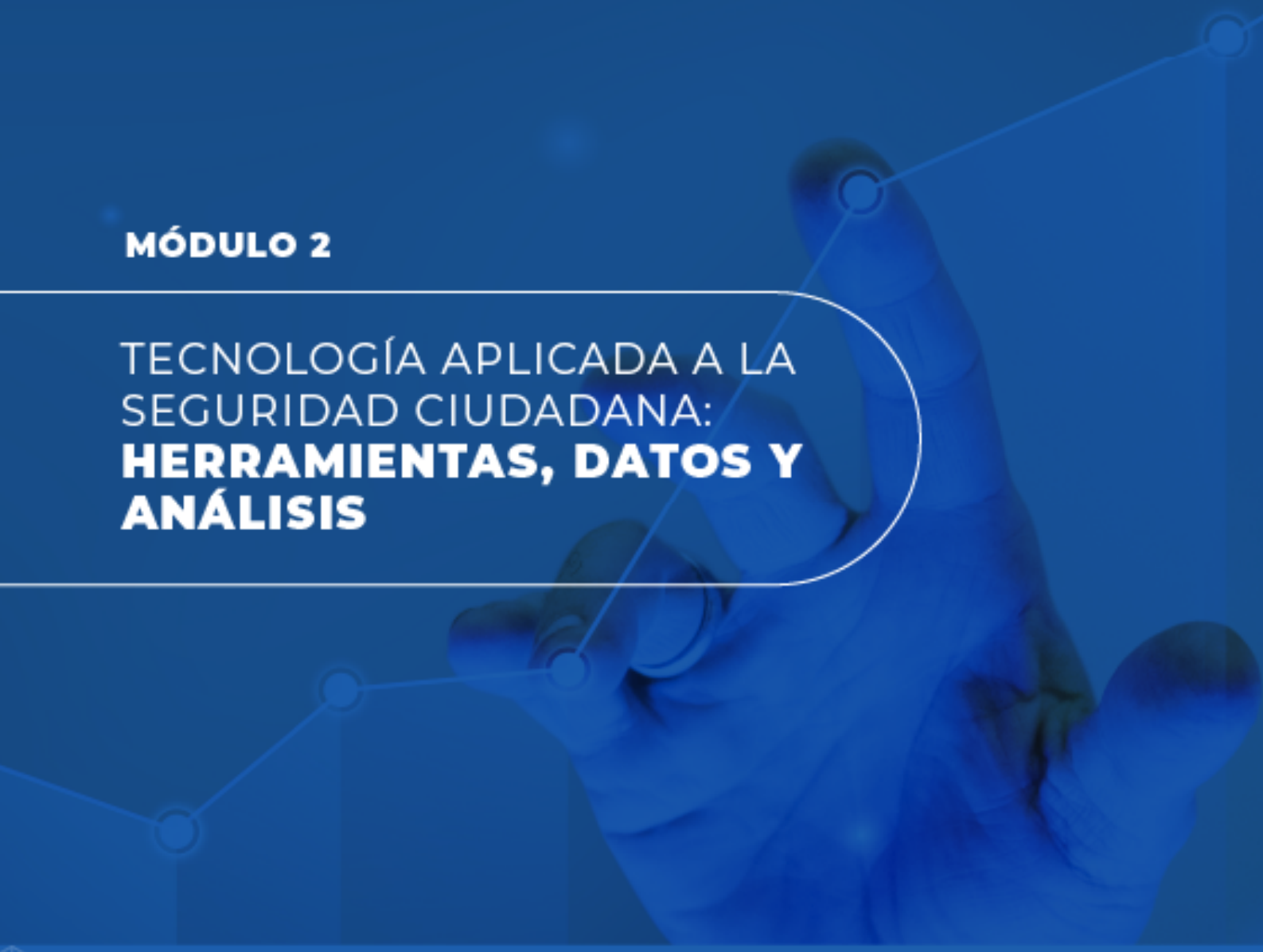
CURSO INICIAL DE FORMACIÓN **EN SEGURIDAD CIUDADANA, JUSTICIA Y COHESIÓN SOCIAL**



MÓDULO 2

TECNOLOGÍA APLICADA A LA SEGURIDAD CIUDADANA: **HERRAMIENTAS, DATOS Y ANÁLISIS**

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

PNUD

infoSEGURA

TECNOLOGÍA APLICADA A LA SEGURIDAD CIUDADANA: HERRAMIENTAS, DATOS Y ANÁLISIS

Contenido

Objetivo especifico

Conocer los tipos de información en la gestión de seguridad ciudadana, Identificar los puntos de dolor en la manipulación de datos y estrategias de fortalecimiento de gestión de los mismos. Conocer los tipos de análisis de información y sus usos en la gestión de la seguridad ciudadana. Identificar las principales herramientas tecnológicas disponibles, sus beneficios y limitaciones.

Estructura del módulo

Cada sección contiene información conceptual y metodológica sobre la temática específica. Cada apartado incluye un cuadro de "guía práctica" cuyo objetivo es orientar acciones prácticas de diagnóstico de la temática mediante preguntas e interrogantes que cada participante podrá aplicar a medida que avanza en los contenidos. Las guías prácticas no son exhaustivas, no obstante, funcionan como patrón de interrogantes básicos al momento del replanteo o implementación de un proceso o herramienta. Se incluyen además "links de interés" a fin ampliar, profundizar o acceder a un conjunto de fuentes y sitios relevantes para la consulta de los participantes.

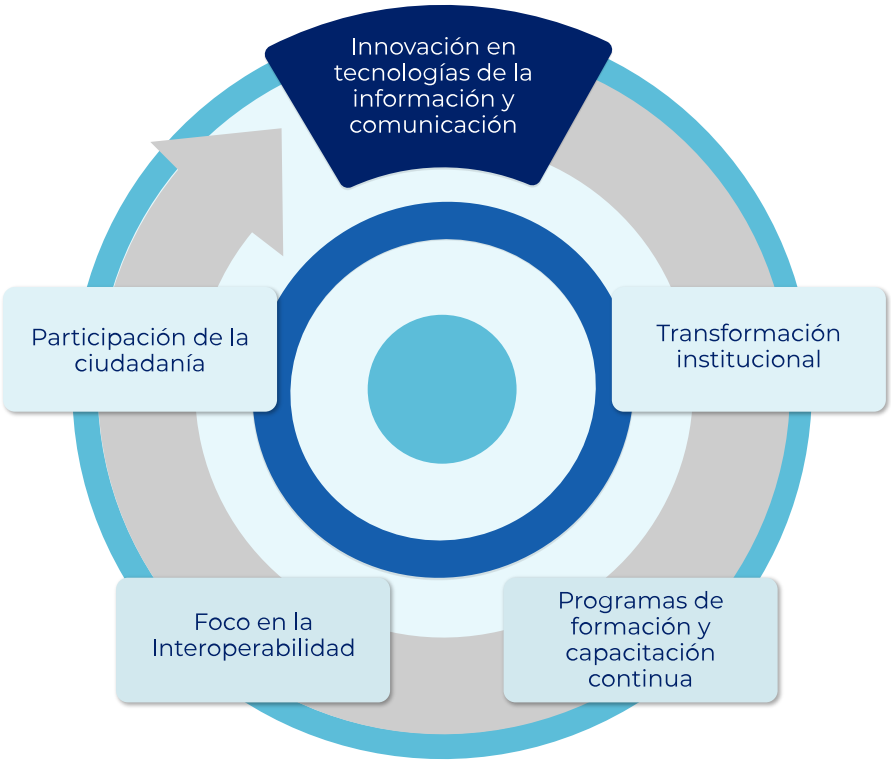
1. La incursión de la tecnología en la seguridad ciudadana

La innovación tecnológica transforma la manera en que se comportan, relacionan y organizan las personas y desarrollan los procesos, esta transformación alcanza ámbitos personales, empresariales, educacionales, estatales, incluso criminales. En las últimas décadas, en el ámbito de la seguridad se han tenido resultados positivos en la disminución de delitos mediante estrategias preventivas basadas en análisis de información, resolución de investigaciones por análisis de grafos, detención de criminales por reconocimiento de sistemas biométricos, análisis balístico y genéticos, entre otros. Sin embargo, aún queda un largo camino a recorrer.

La innovación tecnológica es una herramienta para la prevención y persecución del delito y el fortalecimiento de la seguridad ciudadana. Las instituciones relacionadas a la seguridad son parte del entorno en que trabajan y deben de ser permeables y adaptadas al contexto, un contexto de creciente presencia de tecnología. El camino de la innovación tecnológica es, como muchos otros, un camino de mejora continua donde los procesos involucrados deben encontrarse en revisión permanente.

En este módulo nos referiremos principalmente a la innovación tecnológica referente a las tecnologías de la información y la comunicación. Una de las principales características de este tipo de tecnología es que es generadora y consumidora de

grandes volúmenes de datos. Es por esto que nos enfocaremos en sus métodos y herramientas de recolección, almacenamiento, control, análisis y difusión. No obstante, la adopción de este tipo de herramientas es parte de una transformación más amplia que penetra en la cultura organizacional. Dicho esto, podemos advertir que al considerar la adopción de cualquiera de las herramientas que encontraremos en este módulo tendremos que considerar también que, además de la financiación correspondiente y la voluntad política, para explotar sus beneficios, deberán ser acompañadas por:



- **Transformación institucional:** Acciones proactivas para la gestión del cambio al interior de la institución. (Revisión de estructuras y procesos organizacionales, incorporación de marcos de trabajo ágiles como scrum y metodologías como desing thinking y otros mecanismos que fomenten el enfoque de solución de problemas y la resiliencia de la institución)

Guía práctica:
¿Existe un mecanismo de testeo de la iniciativa previo a la implementación? ¿Existe un área responsable de la tarea? ¿Existe un relevamiento de los puntos de dolor en la implementación y un canal de gestión de esos puntos de dolor? ¿Existe un análisis transversal de las necesidades? ¿Existe un espacio de puesta en común de las problemáticas? ¿Existen canales de comunicación formales entre las áreas involucradas?

- **Programas de formación y capacitación continua:** la formación debe ser inclusiva al interior de las instituciones y no limitarse solo a altos rangos. Debe brindarse también al personal técnico y administrativo. (Las capacitaciones deben ser enfocadas al rol que se cumple con respecto a la iniciativa, no obstante, todo el personal que tenga algún tipo de injerencia en la adopción debe conocer su función y objetivo)

Guía práctica:
¿Quién ingresa datos tiene nociones básicas de sistematización de información? ¿Quién ingresa datos cuenta con definiciones conceptuales de los campos a completar? ¿Conocen los analistas los objetivos específicos de la institución para con la temática? ¿Existe personal capacitado para la mantención de la infraestructura tecnológica? ¿Los mandos medios tienen el andamiaje conceptual para la lectura de resultados?

- **Foco en la Interoperabilidad:** La adopción de estrategias basadas en la innovación tecnológica se nutre de la interrelación de herramientas. Cuanto más interconectada se encuentra esta red de herramientas, mayor será el impacto de la adopción (El foco de la interoperabilidad se encuentra en todos los niveles: desde la necesidad de criterios normalizados para una comparación estadística, hasta la necesidad de interoperabilidad entre sistemas de instituciones judiciales y de registro de personas, que puede nutrir una base policial que alimenta un software de reconocimiento biométrico, para luego la captura de prófugos en línea mediante un sistema de videovigilancia, por ejemplo)

Guía práctica:
¿Las definiciones conceptuales de los sistemas son consecuentes con los de otras instituciones estatales y/o internacionales? ¿Las plataformas implementadas son compatibles con otras plataformas existentes? ¿Existe un canal automático para la alimentación de datos entre sistemas? ¿Existe esta tecnología o estos datos en otro organismo estatal? ¿Conocen otros organismos estatales las necesidades en términos de información e infraestructura tecnológica de mi institución o área? ¿Conoce mi organización las necesidades de información e infraestructura tecnológica de otras instituciones o áreas?

- **Participación de la ciudadanía:** Ya sea como generadores de información o como sujetos de derechos, al analizar cualquier tipo de adopción de herramientas de innovación tecnológica, debe ponerse el foco en las necesidades de la ciudadanía. (Las herramientas adoptadas debe tener consideración de la privacidad de los ciudadanos y el impacto en el ejercicio de sus derechos a la vez que mejorar las condiciones de seguridad ciudadana)

Guía práctica:
¿Qué impacto tiene en la cotidianeidad del ciudadano la herramienta? ¿Existen mecanismos para comunicar los derechos sobre su información? ¿Cuenta la institución con la infraestructura de seguridad para proteger los datos?

2. Sobre los datos, la información y el conocimiento

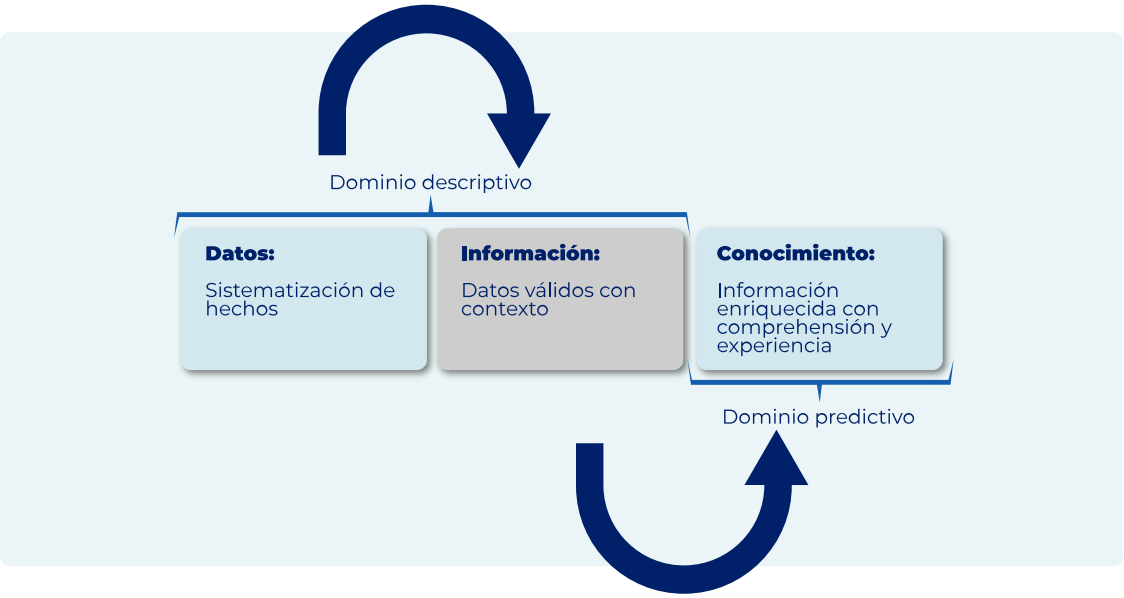
La bibliografía en diseño de políticas públicas nos lleva, cada vez más, a la implementación de políticas basadas en evidencia a fin de incrementar la eficacia de las medidas efectuadas. Para esto es esencial el conocimiento de los hechos. Anteriormente se mencionó que una característica de la innovación en tecnología de la información y comunicación es la producción de grandes volúmenes de datos. Ligado a la generación de políticas basadas en evidencia, los datos generados por las tecnologías de la información y la comunicación son la representación de estos hechos, los mismos, una vez sistematizados (mediante la estructuración y almacenamiento) deben ser analizados, otorgándoles sentido para la creación de información.

Guía práctica:
Interrogantes para la conversión de datos en información:
- Corregir: ¿Fueron revisados los datos? ¿Tienen sentido con la realidad?
- Contextualizar: ¿Para qué se generaron estos datos? ¿Qué temáticas impactan?
- Categorizar: ¿Cuáles son las unidades de análisis de estos datos?
- Calcular: ¿Pueden aplicarse análisis matemáticos o estadísticos que me permitan entender mejor los datos?
- Condensar: ¿Cuáles son las conclusiones principales de los datos recabados?

Hasta esta etapa tendremos un análisis descriptivo de la realidad, este es el momento de transformar la información en conocimiento, otorgándole a la información capacidades predictivas. El conocimiento, excede el análisis de los hechos contenidos en los datos, enriqueciéndolos con experiencia, valores, información y *"saber hacer"*. El conocimiento no se encuentra únicamente en bases de datos, es parte de los procesos organizacionales, sus prácticas y normas.

Guía práctica:
Interrogantes para la conversión de información en conocimiento:
- ¿Conozco hechos comparables? ¿Cuáles son las causas y consecuencias de los hechos que me presenta la información? ¿Con que otro ámbitos, organizaciones y temáticas se relaciona la información que estoy viendo? ¿Estoy incorporando diferentes miradas de otros rangos o especialistas en las conclusiones a las que llego?

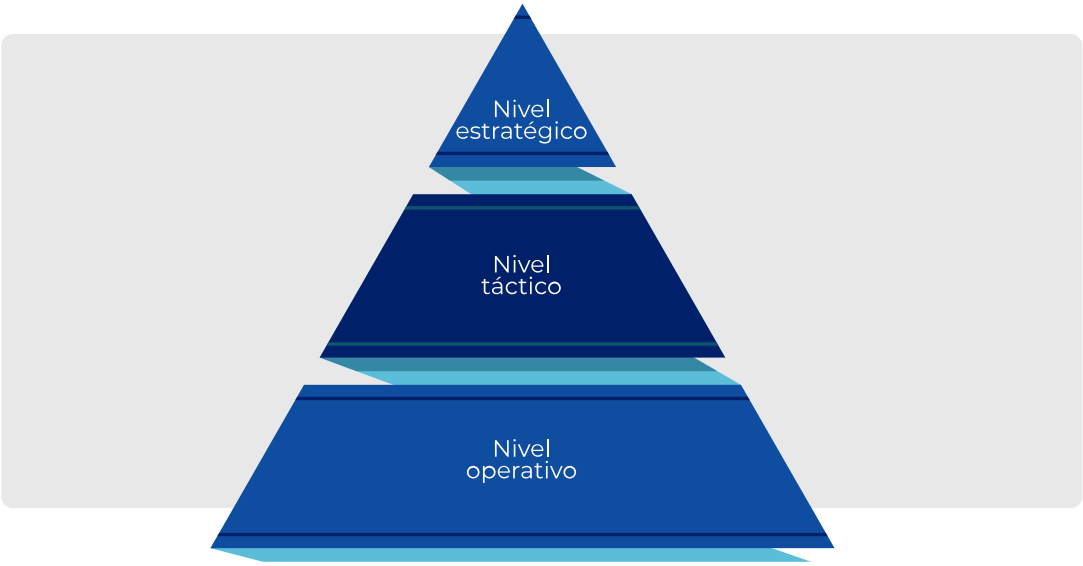
Cuando hayamos transcurrido este camino con los datos recabados, estaremos en condiciones de diseñar políticas públicas basadas en evidencia.



a) Niveles de la información

Es usual que el afán de recabar información nos lleve a generar reportes que se elevan a los altos mandos de la institución o a informes estadísticos que, en muchos casos, no se traducen en planes institucionales concretos. Una de las problemáticas que lleva a esta situación es que la planificación debe verse de manera integral. Hay tres niveles de gestión involucrados en la planificación: el nivel operativo, el táctico y el estratégico. Si bien los reportes a nivel estratégicos son relevantes en una organización, no debe ser el único destino y funcionalidad de la información dentro de la institución.

Para la traducción en planes institucionales concretos, la información debe ser generada para y utilizada por los tres niveles de gestión.



Nivel estratégico	En este nivel se definen los objetivos a largo plazo y se distribuyen los recursos para el cumplimiento de estos objetivos.
Nivel táctico	Este es el nivel donde se desarrolla detalladamente la planificación a partir de los objetivos planteados por la dirección estratégica.
Nivel operativo	En este nivel se realiza el monitoreo en tiempo real de las tareas definidas en el nivel táctico en línea con los objetivos estratégicos.

Guía práctica:

¿Qué tipo de información se ve en cada nivel?

Nivel estratégico	Este tipo de reportes debe incluir la evolución de los principales indicadores de la institución, sean estos delictuales u operativos.
Nivel táctico	Este tipo de reportes debe estar centrado en detallar la problemática para distribución de recursos. A este nivel, no es suficiente la evolución de indicadores principales. Si estamos tratando una problemática, por ejemplo: los homicidios, entonces tendremos que desagregar las variables que lo componen: • ¿Qué tipos de violencia están desencadenando los homicidios? ¿Qué participación tiene el crimen organizado? ¿Qué participación tiene la violencia juvenil? ¿Qué participación tienen los delitos contra la propiedad? ¿Qué participación tiene la violencia de género? ¿Qué rol tienen los flujos migratorios? ¿Cuáles son las modalidades del delito? En este punto vamos a encontrar que la problemática se complejiza aún más: • ¿Qué comportamiento tienen los barrios dentro de cada ciudad con cada tipo de violencia? O incluso ¿Cuáles son los principales focos, tipos de lugar arterias de escape? ¿Qué meses tiene los peores índices? O incluso ¿qué días y horarios? Pero el rol de la información no termina en la caracterización del delito y es momento de analizar la reacción de la institución para con este: • ¿Cómo es el patrullaje en estas zonas? ¿Cuáles son los recursos destinados actualmente? ¿Existen recursos adicionales para destinar? ¿Qué programas serían afectamos por la redirección de recursos? Y por supuesto, las respuestas a nivel estatal no deben ser unilaterales por lo que se debe conocer además los datos que hacen a la problemática de forma indirecta • ¿Qué servicios tiene la zona? ¿Cómo es la prestación de servicios de salud? ¿Dónde se encuentran las instituciones educativas? ¿Cómo es el transporte? ¿Hay instituciones sociales que intervengan en la zona? Este tipo de problemáticas tienen en general un factor territorial fuerte, por lo que los niveles departamentales y municipales deben desagregar la información al máximo posible a fin de encontrar las respuestas con mayor probabilidad de eficacia y eficiencia posible.
Nivel operativo	En este tipo de reporte la información es semanal, diaria e incluso en tiempo real: • ¿Qué zonas reportan disturbios? ¿Qué tipo de disturbios se reportan? ¿Se relaciona usualmente este tipo de disturbio a una escalada de violencia? ¿Es un día de particular riesgo en relación con sucesos anteriores? ¿Las condiciones ambientales o climáticas del momento propician algún tipo de violencia? • ¿Dónde está asignado el personal en este momento? ¿En qué condiciones se encuentra el equipamiento? ¿Hay aglomeraciones que dificulten la tarea?

Como vimos hasta ahora, la información debe ser generada para y utilizada por los tres niveles de gestión, de lo contrario, no es posible llevar la planificación estratégica a un resultado positivo.

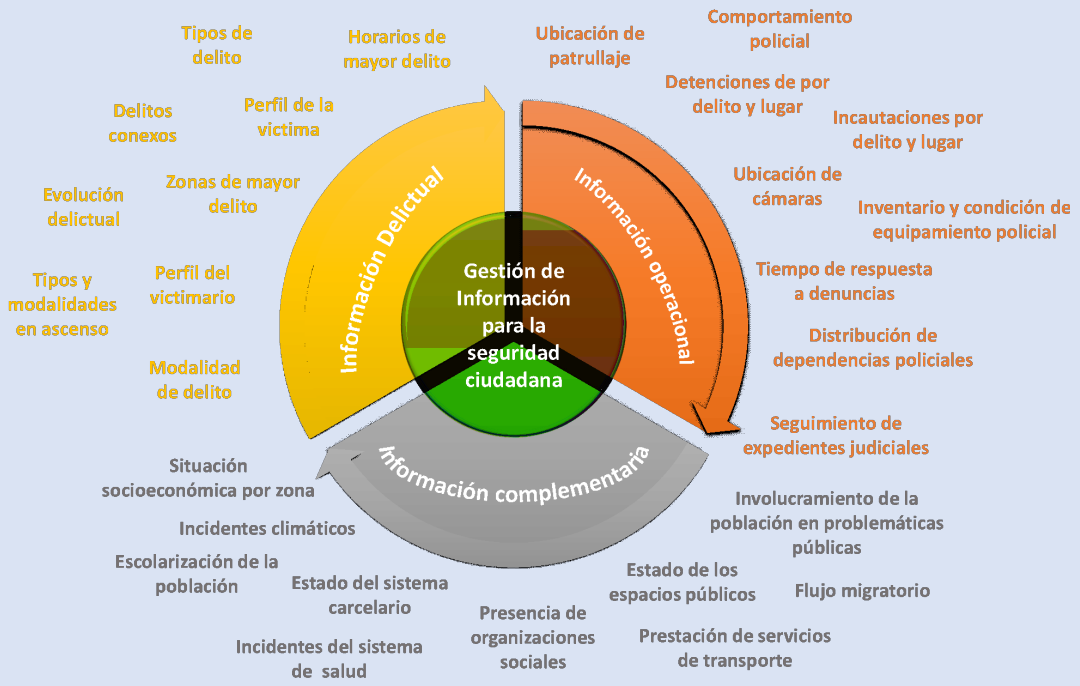
b) Tipos de información

Cuando pensamos en información destinada a la seguridad ciudadana, pensamos en **información delictual**. Es decir, el registro de hechos delictivos asociados a una temporalidad y a un territorio, desagregado en unidades de medición y caracterizados por patrones de ocurrencia. No obstante, la gestión de la seguridad ciudadana requiere nutrirse de otros tipos de datos para conocer las problemáticas en profundidad.

Para esto se deben enriquecer los datos mediante **información complementaria** obtenida de los vínculos interinstitucionales, esto es producto del foco en la interoperabilidad institucional. Cuando se caracteriza una zona delictualmente, no debe olvidarse la prestación de servicios estatales en la zona, la condición socioeconómica de la población, la tendencia a la participación ciudadana, las condiciones ambientales, y toda variable que afecte de forma directa o indirecta a la problemática delictual. De esta forma, las políticas implementadas desde un sector público se conectan con las políticas de otros sectores, transformando la intervención estatal en una intervención eficaz y eficiente.

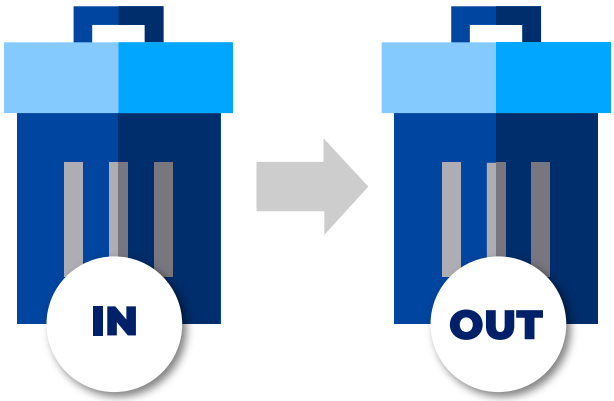
Por último, pero no menos importante, la gestión de la seguridad ciudadana es también la gestión de recursos que a su vez conllevan resultados. Por esto debe mapearse la disponibilidad de los recursos, materiales y humanos, sus intervenciones, los resultados de esas intervenciones y el seguimiento posterior de la mismas. Llamaremos a este tipo de información, **información operacional**. Mediante este tipo de información seremos capaces de conocer los puntos fuertes y débiles de institución para la intervención en la problemática y corregir a tiempo los desvíos de los planes implementados.

Guía práctica:
A continuación, vemos un mapa de tipos de información según la anterior categorización. Si bien la lista no es exhaustiva nos ubica en relación a los tipos de datos necesarios para la gestión de la seguridad ciudadana.



3. Gestión de datos:

Como vimos anteriormente, para llegar a la implementación de políticas basadas en evidencia, el primer paso es contar con datos, y para que los datos se conviertan en información lo que debemos hacer es controlar que los datos tengan la calidad suficiente para llegar a conclusiones sobre los hechos. Es posible que estemos familiarizados con una expresión común en el mundo de la información: *"Si entra basura, sale basura"*



Para evitar esta consecuencia, los datos deben acercarse lo más posible a la realidad. A continuación, veremos desde el origen de los datos, posibles situaciones que disminuyen su calidad, y algunas formas de evitarlo.

a) Recolección, almacenamiento y control

Podemos categorizar dos grandes ramas de la recolección de datos: la recolección automática y la recolección manual.

- **Recolección automática:** Este tipo de recolección de datos está asociada al concepto *"Internet de las cosas"*, es decir, dispositivos electrónicos conectados a una red. Estos dispositivos (en seguridad ciudadana), provienen principalmente de sistemas de geolocalización, videovigilancia, dispositivos móviles de comunicación. Mediante la recolección automática tendremos tipos de datos estructurados y los mayores riesgos en términos de recolección para la consistencia de los datos, es la fiabilidad de redes de conexión y el almacenamiento. En secciones posteriores se mencionarán diferentes herramientas disponibles y sus limitaciones.

Guía práctica:
Al implementar un dispositivo de recolección automática se debe considerar:
¿Cuenta la zona en con señal de red para el flujo de información en tiempo real? ¿Es necesaria la recolección en tiempo real o es suficiente con recepción y envío por lotes?

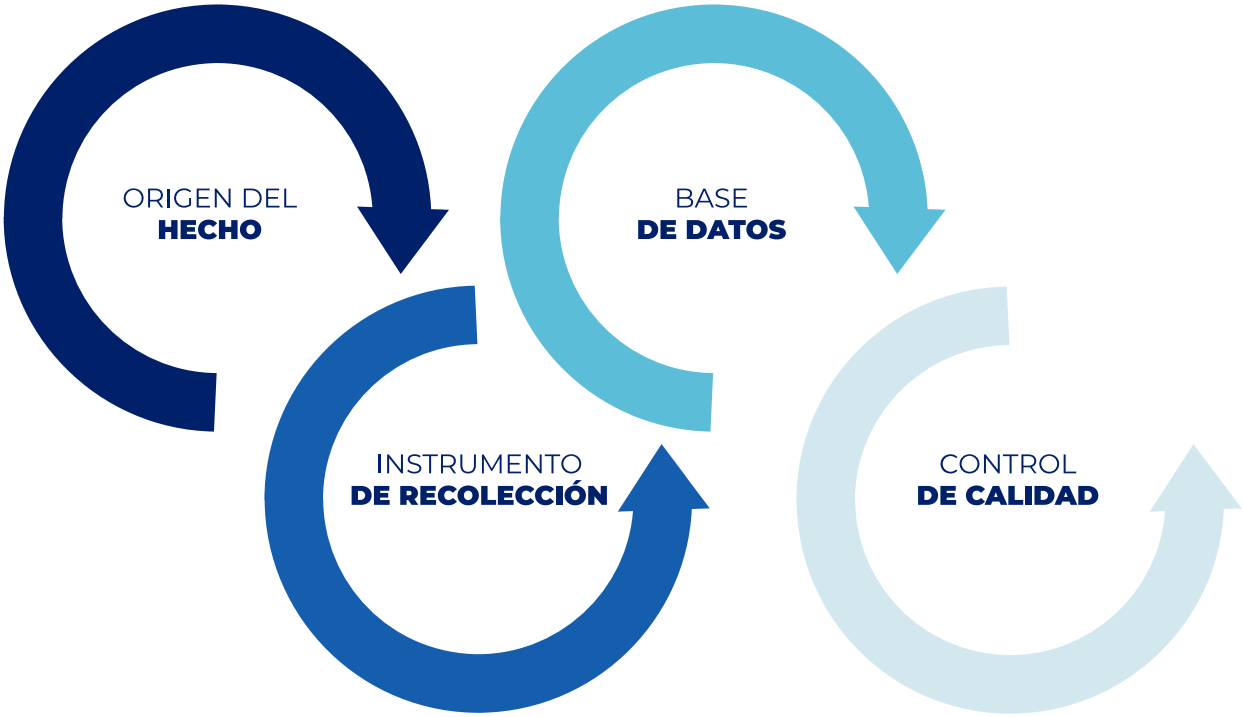
- Si consideráramos un sistema de geolocalización en equipos de comunicación policiales para patrullaje pedestre, probablemente queramos conocer la ubicación en tiempo real, mientras que la actualización de patentes con pedido de secuestro dentro de un sistema de videovigilancia puede soportar la actualización de patentes por lotes diarios.

  ¿Qué tipo de información estoy almacenando? ¿tengo capacidad para el resguardo histórico de información? Si bien se suele considerar deseable almacenar la mayor cantidad de información posible, este tipo de herramientas genera un importante volumen de datos y la conservación de los mismos requiere una fuerte inversión en infraestructura para su almacenamiento.

- De tener sistemas de videovigilancia, uno de sus principales usos será pericial, para esto, debe asegurarse el almacenamiento de imágenes en condiciones de seguridad propicias por un periodo de tiempo determinado. Cuanto más amplio sea el sistema de videovigilancia, mayor será la infraestructura requerida para el correcto almacenamiento. Por otro lado, si el tipo de datos que estamos generando es, como en el ejemplo anterior, un registro de ubicaciones de patrullaje pedestre, las obligaciones en términos de almacenamiento son menores y podemos reducir la cantidad de datos almacenados, ya sea registrando con una frecuencia baja la ubicación o disminuyendo el periodo histórico almacenado.

- **Recolección manual:** Este tipo de recolección de datos es aquella asociada a la intervención directa del personal de la institución con el entorno, que luego es estructurada para la generación de información. Incluye la sistematización de denuncias, hechos, intervenciones, detenciones, incautaciones incluso datos de la operatoria administrativa.
  La mayor parte de los insumos utilizados para el análisis provienen de este tipo de recolección, y es de suma importancia para la organización. No obstante, es en la recolección manual donde se encuentra la mayor deficiencia en la calidad de los datos. Datos faltantes, datos erróneos, duplicidad de datos, valores anormales y resolución deficiente de entidades en estructuras de bases de datos, son problemas regulares en todas las instituciones que recolectan y almacenan información manualmente.

  A continuación, veremos el camino de la recolección de datos con algunas de las buenas prácticas que mejoran su calidad.



Origen del hecho	Instrumento de recolección	Base de datos	Control de calidad
Cuanto más cercana temporal y espacialmente sea la sistematización al origen del hecho, mayor será la posibilidad de reducir la cantidad de datos faltantes. Es recomendable contar con instrumentos de carga digital en el origen del hecho o en la dependencia más cercana a la ocurrencia. Los mismos deben contar con el formulario estructurado definido y simplificar al máximo posible la carga. La transcripción de datos desde boletas de papel a digital suele resultar en perdida de datos y da lugar a interpretaciones erróneas por esto, siempre que sea posible, debe ser evitada.	Por instrumento de recolección, nos referimos al formulario de carga de información. La confección de este formulario de carga tiene dos aristas principales: el contenido y la forma. En cuanto al contenido, cada campo de información relevado debe estar definido estratégicamente para recolectar información rica para el análisis, a su vez debe recordarse que al incluir demasiados campos la carga se vuelve pesada y es posible que terminemos con múltiples datos faltantes. En cuanto a la forma, es lo que nos permite corregir los errores antes de que se trasladen a los registros, debemos contar con campos obligatorios, máscaras para el reconocimiento de formatos, límite de caracteres según tipo de dato y listas de selección. En suma, se deben evitar los campos abiertos de libre escritura ya que posteriormente será difícil categorizar la información para su análisis.	El uso de bases de datos relacionales no solo mejora la integridad de la información, sino que también facilita el manejo de entidades y sus dependencias. De esta forma cada hecho tendrá sus propias variables, comparables y agrupables entre sí, asociados a su vez a personas, con distintos roles en el hecho, también comparables y asociables, y de esta misma forma a entidades geográficas, vehículos, armas, elementos o cualquier tipo de información que desee registrase. Un correcto diseño de la estructura de la base de datos facilitará y enriquecerá en última instancia el análisis realizado. Al acompañar esto con software diseñado a los efectos, facilitaremos también el uso de máscaras para la estructuración de datos, la imposición de campos obligatorios y la agilidad en la carga.	La correcta ejecución de las etapas anteriores facilitará el control de calidad de los datos, pero aun así deberán realizarse análisis de consistencia sobre la información. Este tipo de análisis debe comenzar desde la unidad descentralizada de carga. Si una dependencia registra su propia información antes de elevarla a un nivel más alto, debe revisar si la carga del día tiene alguna anormalidad, si todas las terminales u oficiales registraron datos o si la información que está enviando es consistente. A nivel centralizado una buena práctica es la construcción de indicadores de validación de consistencia para lo que resultan útiles los softwares de análisis estadísticos donde puedan construirse programas de ejecución automática que alerten al analista de los faltantes o desvíos en la información. Un segundo control de información a nivel centralizado puede darse mediante la comparación de fuentes. Si bien es usual que la definición de categorías no sea exactamente igual en sistemas diferentes, -sobre una misma temática-, las variaciones temporales similares en las mismas unidades territoriales nos dan indicios de que el dato tiene sentido con la realidad.

Guía práctica:

Origen del hecho	Instrumento de recolección	Base de datos	Control de calidad
No siempre es posible la carga de datos en el lugar del hecho, ya sea por recursos limitados de la institución para la adquisición de terminales de carga o por la falta de disponibilidad de redes. En estos casos, también puede haber mejoras. Si los registros se recolectan en boletas de papel puede disminuirse el tiempo entre el hecho y el registro y/o no trasladar la boleta entre dependencias para su carga.	Algo esencial en la elaboración de formularios es la revisión conceptual de cada campo y categoría. Por ejemplo, para asegurarnos de un análisis con visión de género, es importante que las categorías relevadas sean definidas en conjunto con especialistas en la materia. Un aporte en el armado de formularios es que el responsable del diseño conozca los procesos realizados por el responsable de carga, para identificar la viabilidad del requisito. Y en todos los casos es recomendable contar con un documento de metadata donde se encuentren definidas todas las variables y categorías, conceptual y operacionalmente.	Algo muy común en las instituciones estatales es el manejo de bases de datos en Excel, pero la misma flexibilidad que colabora a su usabilidad, la vuelve vulnerable para la estructuración de información. Resulta complejo manejar consistentemente las limitaciones de campos y aún más el diseño de una estructura con diferentes entidades. A su vez, a la hora de manipular datos el volumen puede generar problemas y las vulnerabilidades en materia de seguridad de la información son mayores. En caso de usar esta herramienta, sería deseable una revisión permanente. Existen incluso softwares libres que nos permiten solucionar la mayor parte de los puntos de dolor. En caso de ya se encuentre en uso una base de datos relacional, suele ser deseable la revisión de estructuras y entidades en relación a nuevas necesidades de la organización	Algo deseable para asegurar un control de calidad es la confección y documentación de procesos de revisión. Esto es esencialmente una lista de controles, y cuanto mayor sea la automatización de este control mayor será el cumplimiento del mismo. En el segundo paso, la comparación con otras fuentes de información es esencial. La colaboración con otras entidades, por ejemplo. Por último, contar con la colaboración de establecimientos de educación superior, tanques de pensamiento y otras organizaciones sociales en el control de los datos también tiene efectos positivos en la calidad.

Guía práctica:

Hasta ahora listamos estrategias que colaboran al incremento de la calidad de los datos, pero independientemente de la estrategia que usemos, las preguntas que debemos hacernos para controlar la información serán las mismas:
¿Son completos los datos? ¿Están al día? ¿Podemos confiarnos en ellos? ¿Son influidos por el prejuicio, suposiciones o una perspectiva limitada? ¿Son exactos? ¿Son pertinentes? ¿Son verdaderos? ¿Los rendimientos reflejan las expectativas (y si no, ¿por qué no?)? ¿Son contraintuitivos (y si la respuesta es sí, ¿por qué?)? ¿Podemos comprobar de nuevo usando otros métodos? ¿Podemos usar los resultados con confianza?

b) Enriquecimiento de datos y foco en la interoperabilidad

Antes que adentrarnos en cuestiones técnicas de la interoperabilidad, como repositorios de datos interinstitucionales conectados en tiempo real, o compatibilidad de sistemas, vemos deseable comprender el objetivo de la interoperabilidad: el intercambio y cooperación efectiva entre entidades, ya sea para el control o para el enriquecimiento de datos. Para esto identificamos una serie de pasos que nos conducen hacia el camino de la interoperabilidad.

Guía práctica:

Crear vínculos	Para esto son útiles las mesas de trabajo interinstitucionales, y la formalización de canales de intercambio de información.
Analizar datos	La primera pregunta que contestar es ¿qué registra esta institución? ¿Las mismas variables tienen las mismas categorías? ¿Cuál es la diferencia entre las categorías y unidades de registro de las instituciones?
Comparar y dar sentido a las conclusiones	Una vez que notamos las diferencias y las podemos dimensionar tenemos que comprender la correlación de los datos. Por ejemplo ¿Cómo se relaciona la cantidad atenciones de salud de violencia sexual con la cantidad de denuncias? La cantidad de registros nunca será la misma, dado que el origen de la información es distinto, pero incluso la diferencia puede explicar la realidad. ¿Puede que al sistema de salud llegue una mayor cantidad de víctimas que a las instituciones policiales o judiciales? ¿La variación temporal de hechos coincide? ¿Puede notarse un aumento en las denuncias luego de un suceso público de relevancia?
Encontrar identificadores únicos	En este sentido hay muchas herramientas que nos pueden ayudar a relacionar datos. Hay normas y estándares internacionales hacia los que podemos migrar para encontrar un terreno común en temáticas de geografía y ubicación, nomenclatura de objetos. En términos delictuales contamos con la Clasificación Internacional de Delitos con fines Estadísticos de UNODC, además de los propios códigos penales. A nivel nacional podemos encontrar documentos únicos de identidad para las personas, pero también para el registro de vehículos, armas, entre otros. Si bien tarde o temprano esto deberá ser acordado para la compatibilización, cuantos más estándares comunes utilice nuestra organización, mayor será la posibilidad de enriquecer los datos.
Trabajar en la creación de bases de datos unificadas	Los proyectos de repositorios de información interinstitucionales deben ser pensados a largo plazo, la inversión a realizar será alta y las decisiones deberán ser reevaluadas en repetidas ocasiones, pero a fin de cuentas es innegable la necesidad de cooperación entre agencias estatales para la eficaz y eficiente locación de recursos.

Links de Interés

Clasificación internacional de delitos con fines estadísticos UNODC:
https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_SPANISH_2016_web.pdf

Ejemplo de repositorio de datos interinstitucional:
http://cead.spd.gov.cl/

4. Análisis de datos:

Una vez que contamos con datos y controlamos su calidad es momento de generar información y conocimiento para la gestión de la seguridad ciudadana. Antes de comenzar la siguiente sección donde veremos diferentes tipos de análisis aplicados a la temática y sus usos, vale mencionar: Los siguientes tipos de análisis pueden provenir desde modelos diseñados con base en estadística clásica, hasta modelos que incorporan el uso de redes neuronales pasando por rangos intermedios como la clusterización o árboles de decisión.

La elección del método debe estar relacionada con el tipo de datos que ofician de *input* y la finalidad del análisis, dicho esto, no es menor mencionar que el uso de redes neuronales (Conocido también como inteligencia artificial) es particularmente performante en el análisis de imágenes o sonido. En otros tipos de datos, aunque suele presentar un error estándar relativamente bajo a la hora de testear resultados, tiene la desventaja de ser un tipo de modelo de caja negra donde la parcialidad de los datos se replica sin posibilidad de reconocer las variables ponderadas e identificar los motivos de decisión.

a) Tipos de análisis para la gestión de recursos

- *Análisis basados en el lugar*

El policiamiento preventivo basado en datos y lugar es una herramienta que conlleva la identificación de patrones criminales en locaciones geográficas específicas para el despliegue de recursos policiales que disminuyan el riesgo de hechos delictuales. Este tipo de análisis tiene fundamento en el principio de que el delito tiende a agruparse en espacios observables y predecibles.

El tipo de análisis de mayor recurrencia en este sentido es el análisis de puntos calientes que consiste en la identificación de áreas (de limitada extención) que superan el número medio de delitos. También pueden encontrarse modelos con incorporación de variables socioeconómicas según geografía, identificación de tipos de lugares de mayor riesgo como parques, zonas comerciales, asentamientos, etc. A su vez este puede ser focalizado mediante la incorporación de franjas horarias, días de la semana o épocas del año.

Ejemplos de mapas de análisis de puntos calientes:

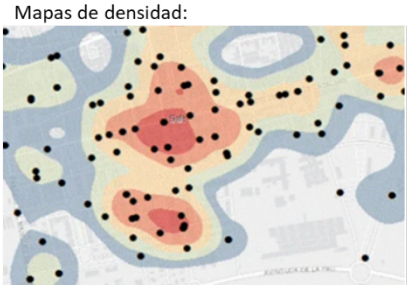
Mapas de puntos:

Mapas de búfer o zona de influencia:

Mapas interactivos:

Mapas graduados:

Mapas de densidad:



Mapas de segmentos de calles:

Link ejemplo de mapa delictual:

https://mapa.seguridadciudad.gob.ar/

Evaluación de programa implementado con uso de análisis de puntos calientes:

https://transparenciapresupuestaria.opp.gub.uy/inicio/registro-nacional-de-evaluaciones/evaluaci%C3%B3n-did-programa-de-alta-dedicaci%C3%B3n-operativa-pado

Guía práctica:

- **Tipos de datos:** Para la implementación de este tipo de análisis es requisito casi indispensable que la institución registre la geolocalización de hechos delictuales.
- **Limitaciones del análisis:**

  - **Tipo de delito:** este tipo de análisis suele ser enfocado a la persecución de delitos contra la propiedad y aún más a delitos como el robo automotor o robos con entrada ilícita. La razón de esto es que el grado de denuncias registradas es mayor, por los requisitos de las compañías aseguradoras mientras que el subregistro de denuncias (o cifra negra) en delitos como violencia intrafamiliar, agresiones sexuales, violencia de pandillas, posesión de armas o venta y consumo de drogas distorsiona los resultados del análisis para el policiamiento por lugar destinado a la reducción de estos tipos de hecho.

  - **Riesgo de profecía autocumplida:** una mayor presencia policial en una zona (destinada por medio de análisis de puntos calientes) puede llevar a un mayor registro de hechos en la misma, a causa de la intervención policial, lo que alimenta el riesgo de la zona, en detrimento de una recolección de datos imparcial.

- *Análisis basados en las personas*

El policiamiento preventivo basado en las personas tiene dos enfoques. El enfoque de la víctima y el enfoque del victimario, la ejecución de este tipo de análisis puede combinarse con el tipo de análisis basado en el lugar. Este tipo de análisis debe ser abordado con particular cuidado en términos de evitar la estigmatización, haciendo énfasis en la identificación de todo tipo de discriminación y distorsión de las protecciones constitucionales.

Enfoque del victimario: Una afirmación frecuente dentro de la criminología es que solo un pequeño porcentaje de las personas comete crímenes violentos.[1] Existen experiencias donde se identificaron personas sospechosas de homicidio tiroteos y crímenes violentos y se los notificó del riesgo involucrado ofreciendo el apoyo en servicios sociales a fin de evitar su intervención en delitos. Este tipo de iniciativa fue exitosa en la disminución de homicidios al inicio, más luego este indicador volvió a aumentar.

Experiencias parecidas se dieron asumiendo que posibles victimarios son también posibles víctimas, especialmente en crímenes violentos. En este tipo de experiencia, se notó un alto nivel de correlación entre las predicciones de los datos y la realidad, más los resultados en la reducción del delito no fueron alentadores. Este tipo de análisis enfocado en el victimario puede también puede realizarse mediante el estudio de

patrones de violencia de pandillas e incluso hay experiencias donde se utiliza información de redes sociales para el análisis. En estos casos los resultados, sino no determinantes resultan al menos más alentadores.

En todos los casos de análisis basados en el victimario, más allá de la actividad policial se debe enfocar el trabajo en brindar oportunidades a los ciudadanos identificados de riesgo, para generar cambios en su ambiente y de esta forma reducir la probabilidad de comisión de delitos.

Enfoque de la víctima: En este caso se busca la prevención desde la identificación de posibles víctimas. Este tipo de análisis realiza un perfilamiento de las víctimas de delitos identificando principales características ya sea desde una perspectiva integral (características de género, socioeconómicas, etarias, étnicas, etc) como ambientales (territoriales, institucionales, temporales, etc). La implementación de medidas en estos tipos de enfoque, al igual que en el anterior, suele exceder el ámbito del policiamiento

[1] The rise of big data police.

mediante el acercamiento a servicios sociales, el desarrollo de campañas de concientización o la modificación del entorno para la mejora del ambiente.

Guía práctica:

- **Parcialidad, discriminación y estigmatización:** Como se mencionó al principio de este apartado, este tipo de análisis suele reproducir las desigualdades de las sociedades que se analizan. Recurrentemente, el riesgo de conclusiones discriminatorias o estigmatizantes no es producto directo de las conclusiones del analista, sino que se encuentra embebido en los datos. Es por esto, que, a pesar de su innegable utilidad para el diagnóstico de problemáticas y posibles soluciones, los resultados deben tomarse con los recaudos necesarios para evitar la excesiva generalización y su consecuente impacto replicador de desigualdades.

- **El enfoque de género:** el análisis basado en las personas con enfoque en la víctima es utilizado frecuentemente para el análisis de delitos de género. Si bien es aplicable, no debe confundirse un análisis de la víctima de delitos de violencia de género con la producción de datos con enfoque de género.

  En la producción de datos con enfoque de género, no nos referimos a un delito en particular, sino a la identificación de las diferencias entre las personas, por el hecho de asumir roles masculinos o femeninos, que facilitan o dificultan la posibilidad de ejercer y reclamar derechos.

  Incluso es de remarcar que pensar en un enfoque de género implica superar las concepciones tradicionales sobre las mujeres como grupo vulnerable, promoviendo acciones afirmativas con fines correctivos que tengan como objetivo dar fin a las situaciones de discriminación y desigualdad atravesando la totalidad de la agenda institucional (donde las áreas específicas de género funcionen como veedoras de la efectivización de este impacto en la institución)

- *Análisis basado en el delito*

En este tipo de análisis, las características a definir serán aquellas asociadas al delito analizado. Desde la territorialidad, estacionalidad, modalidades, delitos conexos, organizaciones criminales cómplices y víctimas, hasta su integración con las actividades legales. Con este tipo de análisis podremos reconocer las rutas del delito, situaciones que lo propician, causas y consecuencias económicas, sociales, ambientales.

La forma de análisis difiere en dependencia del delito analizado y es aplicado desde delitos contra la propiedad hasta delitos de crimen organizado como la trata de personas. Por ejemplo, en el hurto, mediante la identificación de escenarios propicios,

en el caso del delito de robo de automotores, con el análisis de zonas y venta de autopartes y en el delito de trata de personas con el análisis del origen de las víctimas. Los análisis posibles son tantos como los delitos registrados.

Guía práctica:

- **Variables de enriquecimiento de datos y criterio experto:** Hasta este momento, cuando hablamos de enriquecimiento de datos nos referimos a temáticas que exceden el ámbito delictual. Para este tipo de análisis nos concentraremos en las variables de enriquecimiento propias del delito. Como ejemplo, si hablamos de narcotráfico podemos registrar cuestiones como pureza, sustancias de corte, marcas y sellos, métodos de ocultamiento, modalidad de venta, precio. Una característica tanto de este tipo de datos como del tipo de análisis en general es que requiere un grado mayor de manualidad, usualmente los campos que alimentan este tipo de información cuentan con un alto grado de datos faltantes, o incluso deben extraerse de campos no estructurados o de descripción, en estos casos los datos deben ser reconstruidos, se trabaja con un alto grado de inferencia de parte del analista, y requiere de una expertice mayor en criminología. A pesar de lo dicho, este tipo de análisis nos permite conocer en profundidad la problemática y llegar a conclusiones y soluciones enfocadas en la incidencia particular del entorno de estudio.

- *Análisis en tiempo real*

Este tipo de análisis tiene una estrecha relación con la implementación de dispositivos tecnológicos de conexión en tiempo real como aquellos contenidos por los sistemas de videovigilancia, sistemas de geolocalización o sistemas de comunicación para alerta temprana. Sobre este tipo de sistemas se montan modelos de análisis que facilitan la identificación de situaciones de riesgo.

Este tipo de modelos está fuertemente explotado en los sistemas de videovigilancia. Dentro de estos podemos encontrar modelos de análisis de comportamiento donde se catalogan conductas sospechosas y mediante el análisis de imágenes se disparan alertas

de posibles delitos en proceso. También sobre sistemas de videovigilancia se pueden encontrar sistemas de reconocimiento de patentes (para automóviles con denuncia de robo, por ejemplo) o incluso sistemas de reconocimiento biométrico para la identificación de personas prófugas de la justicia.

Los dispositivos como “botones de pánico” pueden agilizar el despacho policial en momentos de emergencia. Podemos encontrar también modelos de niveles de riesgos

montados sobre la ubicación de llamadas al 911, donde la concentración de llamadas por zonas tiende a indicar un riesgo mayor de ocurrencia de delito en tiempo real.

Guía práctica:

- **Adopción de modelos de análisis:** Normalmente este tipo de análisis requiere de la contratación de licencias de softwares preentrenados debido al componente técnico-tecnológico de su diseño, por lo que la adopción de este tipo de análisis requiere de una doble inversión: el hardware principal con su correspondiente software y el software adicional de análisis.

- **Limitaciones técnicas propias de la institución:** Previo a la adquisición de este tipo de herramientas se debe realizar una evaluación de factibilidad interna. A modo de ejemplo, la implementación de un software de reconocimiento de patentes requiere de la existencia de una base actualizada periódicamente (preferentemente interjurisdiccional) de patentes con denuncia de robo, misma situación se da en el caso de las personas prófugas de la justicia. Por otro lado, la implementación de "botones de pánico" requiere de un análisis de la factibilidad de respuesta principalmente en aquellos casos en que la disponibilidad sea ilimitada, como es el caso de los botones de alerta mediante aplicaciones en celulares. En suma, el paso previo a la compra de cualquier tipo de tecnología es un análisis pormenorizado del cumplimiento de condiciones para la adquisición del producto.

Link ejemplo de análisis de comportamiento sobre sistema de videovigilancia, veamos si les parece colocarlo.

https://www.youtube.com/watch?v=GKD_4xift3A

- *Análisis al interior de las instituciones policiales*

El análisis de datos puede permitirnos también evaluar los cuerpos policiales hacia el interior, ayudándonos a aumentar la efectividad de la institución e incrementar los mecanismos de rendición de cuentas.

Mediante la implementación de sistemas de geolocalización podemos monitorear a nivel operativo la ubicación de los efectivos, controlar y corregir el patrullaje en ejecución identificando en tiempo real zonas de bajo recorrido policial. A nivel singular la ubicación de cada efectivo y a nivel sistémico podemos evaluar la efectividad del

patrullaje en un periodo determinado y su relación con la disminución o aumento del delito en la zona. Con el mismo tipo de herramienta podemos medir el tiempo de respuesta a llamadas al 911.

Mediante el registro de información de intervenciones y sus resultados podemos medir la efectividad de cada cuerpo policial e incluso a nivel oficial. También podemos monitorear el uso de la fuerza e identificar situaciones de abuso de la autoridad policial. Este tipo de análisis puede ser acompañado por dispositivos de videovigilancia diseñados para la grabación de intervenciones policiales.

Guía práctica:

- Cuando se plantea este tipo de análisis, es deseable, además de generar una línea de base para la comparación histórica dentro de la institución, buscar parámetros o puntos de referencia de otros cuerpos policiales que oficien de objetivo para la institución.

b) Estadísticas

- *Consolidación de información y normalización*

Para la construcción de estadísticas, se requiere que los datos deben pasen por controles de calidad internos de procesamiento diario y en cada una de las dependencias involucradas, como se sugirió en apartados anteriores. Al consolidar la información por periodos de tiempo y regiones, se debe generar un nuevo proceso de control que audite la consistencia de la información según las desagregaciones de los informes estadísticos.

Anteriormente, en la sección de enriquecimiento de datos y foco en la interoperabilidad, mencionamos que resulta deseable la utilización de categorías e identificadores estándar en el registro de información. En los datos estadísticos es donde veremos el primer beneficio. El uso de categorías estándar nos permitirá comparar los datos de la institución con datos generados por otras instituciones o incluso datos a nivel internacional.

Si bien al interior de la institución puede resultar deseable la desagregación de un tipo de delito para la toma de decisiones operativas, una buena práctica es generar procesos de *ETL* (Extract, Transform, Load - Extraer, Transformar y Cargar) donde la carga de un tipo de delito autocomplete el equivalente en categorías estándar. Este mismo principio puede aplicarse a variables territoriales, mercadería incautada, autos secuestrados, etc.

Guía práctica:

- Ejemplo de ETL para delitos:

Categoría interna del delito	Categoría penal del delito	Categoría UNODC del delito
Homicidio de cónyuge	Art. En el Código Penal como homicidio agravado	0101 homicidio intencional

Caso hipotético: la institución decide implementar la categoría "Homicidio de cónyuge" con el objetivo de recolectar datos de este tipo particular de homicidio. Incorporar un proceso de ETL consiste en identificar que cada vez que sea registrado un "Homicidio de cónyuge" este es a su vez un "Art. 129 homicidio agravado" y un "0101 homicidio intencional". Esto permitirá por ejemplo comparar la categoría penal entre la institución policial y judicial y la categoría UNODC con datos de otros paises. Para lograr esto, la totalidad de las categorías deben ser mapeadas en los diferentes niveles, ganando en posibilidad de análisis y disminuyendo el tiempo de carga.

- *Participación, Colaboración interinstitucional, difusión y concientización*

Algo que nutre a las estadísticas de una institución es compartir los datos relevados. Esto debe darse en diferentes niveles:

- **Sector público:** una buena práctica es la formalización de canales para el envío de información periódica con otras áreas del Estado. Resulta aún más fructuoso si se acompaña con mesas de trabajo interinstitucionales que identifiquen las necesidades de información de cada institución. Es deseable también la generación de análisis interinstitucionales, ya sea para la validación de la información como para el diagnóstico de problemáticas comunes.

- **Asociaciones de la sociedad civil:** las instituciones de educación superior, tanques de pensamiento y ONGs son particularmente beneficiosas para el enriquecimiento y validación de estadísticas, para la auditoria de información y colaboración en el procesamiento y análisis de la información de la institución estatal. En este sentido pueden instituirse mesas de expertos o grupos consultivos que integren asociaciones de la sociedad civil.

- **Sociedad civil:** la información debe compartirse con la sociedad civil ya sea mediante boletines institucionales páginas web, medios de comunicación o plataformas de redes sociales. Una opción interesante es la publicación de datasets en la web institucional para abrir la posibilidad de análisis a la población general. Este tipo de acciones

colaboran a la transparencia estatal y al aumento de conciencia sobre las distintas problemáticas delictuales.

Guía práctica:

- Un ejemplo de colaboración exitosa entre instituciones del sector público (que incluye también instituciones educativas) es Mesa Técnica Interinstitucional para la Conciliación de Cifras de Víctimas de Homicidios y Feminicidios de El Salvador. Donde las instituciones se reúnen mensualmente para la comparación de datos institucionales.
  Enlace de referencia: https://www.seguridad.gob.sv/dia/acuerdo-interistitucional/

5. Herramientas de monitoreo y alerta temprana

En esta sección haremos una breve descripción de los dispositivos tecnológicos de mayor presencia en la gestión de la seguridad.

a) Videovigilancia

Los sistemas de videovigilancia, también conocidos como circuitos cerrados de televisión o CCTV consisten es la instalación de cámaras conectadas que generan un circuito de imágenes, el cual solo puede ser visto por un grupo determinado de personas. Inicialmente fueron utilizados en el ámbito privado y desde la década de los 90’ se expandieron exponencialmente al sector público para su uso en la seguridad ciudadana.

Este tipo de dispositivo se destacó inicialmente como herramienta de disuasión del delito en el marco del policiamiento preventivo. Los resultados de la implementación de sistemas de videovigilancia son materia de análisis con múltiples resultados según el territorio y delito focalizado puesto que no generan igual impacto en todos los delitos ni en todos los lugares. Es frecuente la crítica a los recursos humanos requeridos para el monitoreo, sin embargo, los avances tecnológicos en materia de análisis de imágenes en tiempo real, sobre los que comentamos en el apartado anterior, mejoran las oportunidades de monitoreo inteligente.

Otra funcionalidad de los sistemas de videvigilancia es la relacionada con los procesos judiciales al permitir la disponibilidad de evidencia oficial, para lo cual es necesario el correcto resguardo de imágenes. En una línea similar, se ha popularizado la incorporación de cámaras en móviles de patrulla e incluso cámaras corporales para oficiales de policías, ambos tipos de tecnología pueden incluir la grabación de audio y tienen como objetivo registrar la interacción entre el efectivo policial y la población civil

reduciendo la violencia entre los mismos y disminuyendo los actos de discriminación policial.

b) Geolocalización

Los sistemas de geolocalización se basan en el Sistema de Posicionamiento Global que permite mediante la tringulación de señales de satélite posicionar la altitud, latitud y longitud de objetos, localizados mediante mapas digitales. La utilización de este tipo de dispositivos se popularizó mediante la instalación en vehículos de patrulla como herramienta de control.

Actualmente este tipo de dispositivos puede ser incorporado en equipos de comunicación personales lo cual suma al control del patrullaje motorizado el control del patrullaje pedestre. Los datos generados por dispositivos de geolocalización pueden ser el *input* de modelos de control como los mencionados en la sección anterior. Los sistemas de geolocalización pueden ser potenciados en su uso aplicado a la seguridad ciudadana por la ampliación del alcance a vehículos de transporte público mediante regulación.

Guía práctica:

- **Cobertura y frecuencia de reporte:** para que los análisis de control rindan frutos, se debe tender a la cobertura total de móviles (si lo que queremos controlar es el patrullaje motorizado). Caso contrario, los análisis estarán sesgados por la cobertura de la herramienta. Lo mismo se replica en el control del patrullaje pedestre. En caso de que la implementación de la herramienta sea parcial, es conveniente que se definan zonas de completa cobertura de herramienta para sacar provecho de análisis consecuente a la herramienta implementada.

  Por otro lado, debe conocerse la frecuencia de reporte de la red, dependiendo del territorio sobre el que se esté trabajando puede que la frecuencia de reporte no sea la adecuada para el control de patrullaje. Esto ocurre principalmente en los dispositivos destinados al patrullaje pedestre.

c) Alerta temprana

En esta sección nos referiremos a los medios de comunicación de emergencias adicionales al 911 utilizados en la seguridad pública como botones de pánico o emergencia y alarmas vecinales.

Los botones de pánico son pulsadores conectados a un sistema de alarma que permiten a la víctima dar aviso automático y discreto de una emergencia. Este tipo de dispositivo

puede implementarse mediante diversas plataformas y cumplir múltiples propósitos. Con relación a las plataformas, -mientras que existen equipos con la finalidad única de funcionar como dispositivo de alarma- en la actualidad, existen experiencias de uso de aplicaciones para celulares inteligentes que cumplen el mismo fin. Por otro lado, los dispositivos suelen contar con tres tipos de alarmas: policial, médica y de bomberos. Las poblaciones objetivo de este tipo de dispositivo son múltiples. Se pueden otorgar a víctimas de violencia de género, establecimientos públicos, locales comerciales e incluso dar la opción de descarga de una aplicación para la población general.

Las alarmas vecinales se encuentran en el umbral entre la acción pública y privada, requieren de la organización vecinal, pero pueden ser incentivadas, apoyadas y financiadas desde el ámbito público. Existen distintos tipos de dispositivos de alarma vecinal, normalmente consisten en un mecanismo de activación de alarma que puede llevar a la comunicación con la institución policial y/o la activación de sonidos disuasorios. La característica distintiva de este tipo de herramienta es que cualquier vecino que note la ocurrencia de un hecho delictivo en su barrio puede activar la alarma, fomentando la empatía y sentido de unidad dentro de la comunidad.

Guía práctica:

Uno de los análisis previos a otorgar este tipo de dispositivos es el análisis de capacidad de respuesta policial, tanto en lo que concierne al funcionamiento de las plataformas de comunicación, como a la disponibilidad de recursos para acudir al hecho. El fomento de la alerta al cuerpo policial, de no tener respuesta, resultará en una fuerte disminución de la confianza en la institución. Es por esto que es recomendable que la implementación de este tipo de dispositivo sea paulatina para su correcto testeo.

6. Datos, confidencialidad y derechos.

El surgimiento de herramientas de la tecnología de la información y la comunicación representa la aparición de múltiples oportunidades para el fortalecimiento de la seguridad ciudadana, entre muchos otros ámbitos. Pero es innegable que, con estas oportunidades, surgen nuevas amenazas, particularmente las referidas a la vulnerabilidad de los derechos de los ciudadanos frente a la creciente digitalización del accionar público.

El uso de herramientas como los sistemas de videovigilancia y el análisis de redes sociales generan una constante tensión entre la seguridad pública y la privacidad. El almacenamiento y la manipulación de datos amenaza el derecho a la intimidad y el análisis que hace uso del perfilamiento y la categorización de víctimas y victimarios, desafía el principio de no discriminación. Por supuesto ninguna de estas herramientas es en si misma vulneradora de derechos, pero en ocasiones la línea que separa la manipulación de información y la vulneración de derechos es demasiado delgada. Después de todo, no debe olvidarse los datos no son solo registros dentro de una tabla,

están refereidos a personas, a ciudadanos y se debe velar por el cuidado de sus derechos.

Por eso, cuando trabajamos con datos debemos asegurarnos que los dispositivos y redes cuenten con los estándares necesarios de seguridad de la información para evitar fugas de datos y ataques informáticos. Todos los registros deben contar con la anonimización correspondiente al área que los manipula. Los ciudadanos deben ser informados de sus derechos de rectificación de información. Los estándares de seguridad deben ser protocolarizados dentro de la institución y siempre que generemos un análisis se debe contar con un marco metodológico tendiente a reducir al máximo la parcialidad de las conclusiones. En suma, la información es un aliado esencial para gestión estatal, siempre y cuando recordemos en todo momento que nuestro deber es velar por la seguridad ciudadana de manera integral.

infoSEGURA

Formación