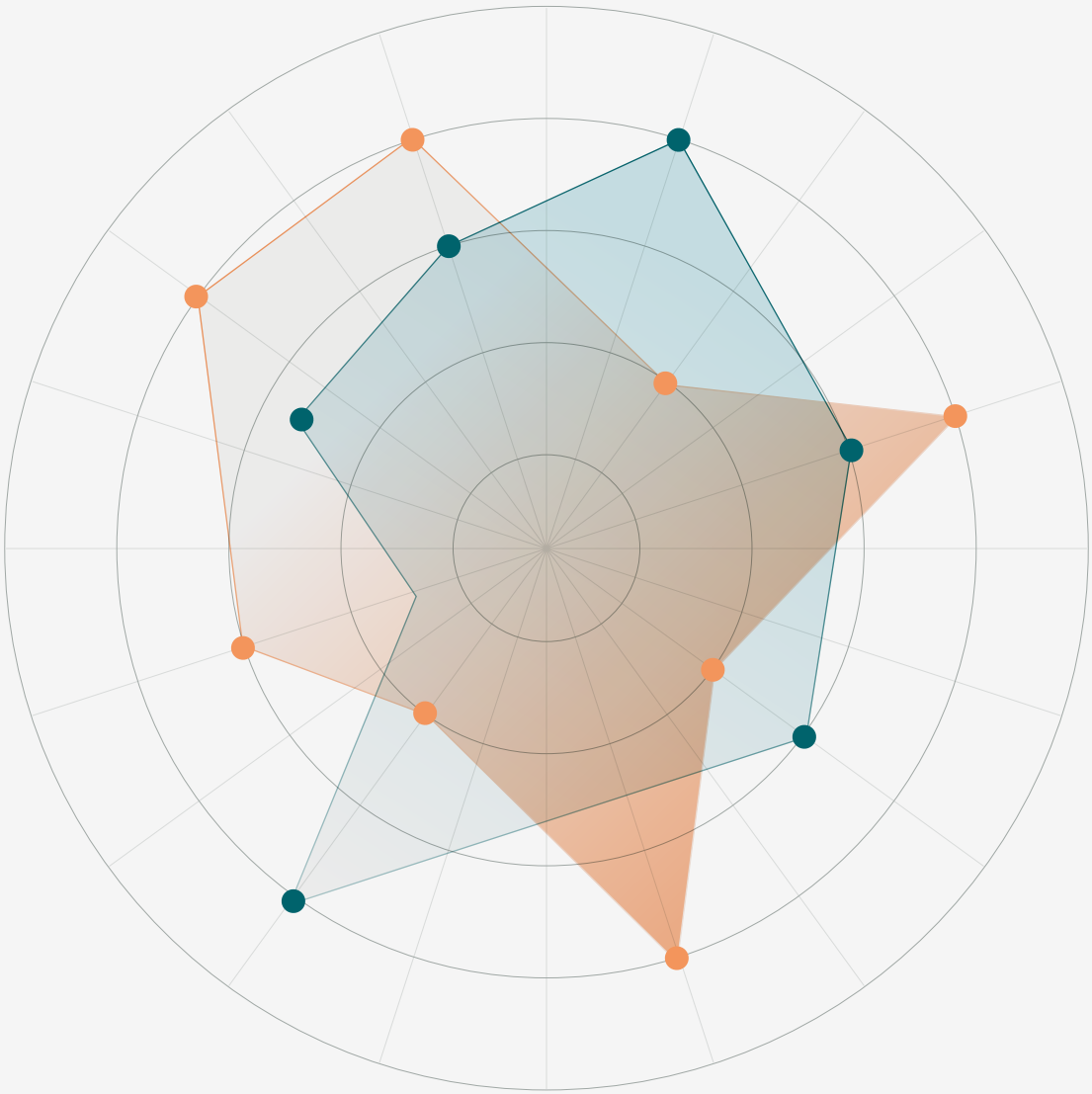
Blueprint

# Lineamientos para el desarrollo de sistemas de información para la prevención de crímenes contra personas defensoras de derechos humanos



CEJIL
CENTRO POR LA JUSTICIA Y EL DERECHO INTERNACIONAL

**Lineamientos para el desarrollo de sistemas de información para la prevención de crímenes contra personas defensoras de derechos humanos**

Julio de 2026

El Centro por la Justicia y el Derecho Internacional (CEJIL) tiene como misión contribuir al goce de los derechos humanos mediante un uso eficaz del Sistema Interamericano de Derechos Humanos (SIDH), y de otros mecanismos de protección internacional

**ISBN 978-987-23854-8-4**

**Elaboración y supervisión:**

**Viviana Krsticevic**
Directora Ejecutiva, CEJIL

**Johanna González**
Abogada, CEJIL

**Franco Albarracín**
Abogado, CEJIL

**Coordinación de diseño editorial:**

**David Romero,**
Director de Comunicaciones, CEJIL

**Nadia Ferrari,**
Oficial de comunicación, CEJIL

**Diseño y diagramación:**

**Julieta Melina Jiménez,**
Diseñadora Gráfica Editorial

**Cómo citar este material:**

CEJIL, Lineamientos para el desarrollo de sistemas de información para la prevención de crímenes contra personas defensoras de derechos humanos

Julio de 2026

Blueprint

# Lineamientos para el desarrollo de sistemas de información para la prevención de crímenes contra personas defensoras de derechos humanos

CEJIL
CENTRO POR LA JUSTICIA Y EL DERECHO INTERNACIONAL

# Prólogo



Quienes defienden derechos humanos en las Américas lo hacen, con demasiada frecuencia, a costa de su seguridad y de su vida. Las amenazas, la criminalización, la vigilancia, el desplazamiento y el asesinato se han convertido en una realidad cotidiana para miles de personas, comunidades y organizaciones que sostienen la democracia, el Estado de derecho y la vigencia de los derechos humanos en la región. Cada agresión contra una persona defensora no solo afecta a quien la sufre: también debilita la capacidad de las sociedades para exigir derechos, fiscalizar el poder y preservar un espacio cívico abierto.

Frente a esa realidad, el derecho internacional y constitucional han sido claros: los Estados tienen la obligación de prevenir, proteger, investigar, sancionar y reparar las violaciones de derechos humanos. El cumplimiento efectivo de estas obligaciones exige contar con sistemas capaces de producir, integrar, analizar y diseminar información sobre las agresiones contra personas defensoras. Sin información confiable, articulada y oportuna no es posible dimensionar la magnitud del fenómeno, identificar patrones de riesgo ni orientar respuestas eficaces de prevención, protección e investigación.

Y, sin embargo, el problema rara vez es la ausencia total de datos. Los Estados, los organismos internacionales, la academia y las organizaciones de la sociedad civil reúnen un acervo enorme de información valiosa. La principal carencia radica en la manera en que esta se articula, se relaciona y se utiliza para orientar políticas públicas. Estos Lineamientos buscan, precisamente, ofrecer una hoja de ruta —técnica, jurídica y metodológica— para recoger y transformar esos datos en un sistema de información capaz de fortalecer la prevención, la protección, la investigación y la rendición de cuentas frente a las agresiones contra personas defensoras.

Este documento es fruto de un trabajo profundamente colaborativo e interdisciplinario, y no habría sido posible sin la generosidad de muchas personas e instituciones.

Agradecemos de manera muy especial a la Global Rights Innovation Lab Clinic (GRIL) de la Universidad de California, Berkeley —en particular, Laurel Fletcher y Valentina Rozo Ángel—, cuyo aporte y el de un equipo brillante de estudiantes hicieron posible el abordaje interdisciplinario que distingue a este trabajo. Sus análisis sobre las taxonomías de criminalización, los distintos tipos de sistemas de información, las fuentes de datos disponibles y las herramientas estadísticas y de ciencia de datos ampliaron de manera significativa las perspectivas de análisis y enriquecieron el desarrollo de este *Blueprint*. Asimismo, expresamos nuestra gratitud a los expertos María Sol Espain y Ari Cunha por sus contribuciones invaluables al abordaje interdisciplinario.

Agradecemos a las instituciones del Estado colombiano que participaron en las mesas técnicas y aportaron su experiencia y sus observaciones, en especial a la Defensoría del Pueblo y a la Consejería Presidencial para los Derechos Humanos y el Derecho Internacional Humanitario, así como al Ministerio del Interior, la Fiscalía General de la Nación, la Jurisdicción Especial para la Paz (JEP) y la Autoridad Nacional de Licencias Ambientales (ANLA); y a los organismos internacionales que acompañaron el diálogo, ONU Mujeres y la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH). Reconocemos, asimismo, los invaluables aportes de instituciones del Estado brasileño —el Ministerio Público Federal, el Ministerio de Derechos Humanos y Ciudadanía, el Ministerio de Justicia y Seguridad Pública y el Consejo Nacional de Justicia— al debate sobre la protección integral de las personas defensoras y el enfrentamiento a la impunidad.

Resulta igualmente indispensable reconocer la contribución fundamental de las organizaciones de la sociedad civil, que, muchas veces de manera pionera, han documentado las agresiones contra quienes defienden derechos. Agradecemos de manera muy especial al Colectivo de Abogados «José Alvear Restrepo» (CAJAR) y al Programa Somos Defensores, cuya colaboración resultó particularmente valiosa a lo largo de todo este proceso. Un reconocimiento especial merece también la campaña “No es Hora de Callar” por su decisivo impulso al fortalecimiento de los sistemas de información en Colombia. Reconocemos, asimismo, los aportes de la Comisión Colombiana de Juristas (CCJ), la Fundación para la Libertad de Prensa (FLIP), el Instituto de Estudios para el Desarrollo y la Paz (INDEPAZ) y la Consultoría para los Derechos Humanos y el Desplazamiento (CODHES). En Brasil, agradecemos los intercambios con la Comissão Pastoral da Terra (CPT), la Articulação dos Povos Indígenas do Brasil (APIB), la Coordenação Nacional de Articulação das Comunidades Negras Rurais Quilombolas (CONAQ), la Justiça Global, el Consejo

Nacional de Derechos Humanos (CNDH) y el Consejo Nacional de Pueblos y Comunidades Tradicionales (CNPCT).

Expresamos nuestro agradecimiento, a la Agencia Suiza para el Desarrollo y la Cooperación, la Agencia Sueca para el Desarrollo Internacional y la Fundación Huneeus Quesney, cuyo apoyo hizo posible este trabajo.

Agradecemos también los aportes académicos del Dr. Jorge Roa Roa a esta investigación, así como los realizados por la Dra. Anna Luisa Walter de Santana y la profesora Andrea Robles Ustariz, y los comentarios del Dr. Gabriel Rojas Andrade. Además, este trabajo no habría sido posible sin la dedicación especial, dentro de CEJIL, de un equipo dedicado al estudio, la redacción y el desarrollo del documento que aquí se presenta, del que tuve el privilegio de formar parte junto con Johanna González y Franco Albarracín. En distintos momentos del proceso contamos, además, con el apoyo y el consejo de varias colegas, entre quienes destacamos, por su contribución sostenida, a María Noel Leoni, Florencia Reggiardo y Helena de Souza Rocha. Contamos también con la valiosa colaboración, en tareas logísticas y técnicas, de Dayana Mosquera, Vanessa Rossel y Juan Peltier.

Esperamos que estos Lineamientos sirvan a los Estados, a la sociedad civil y a la academia para fortalecer las herramientas, las prácticas y las políticas que protegen a quienes defienden los derechos de todas las personas. Porque, en última instancia, proteger a las personas defensoras es fortalecer la democracia, el Estado de derecho y la vigencia de los derechos humanos.

**Viviana Krsticevic**

Directora Ejecutiva, CEJIL

# Índice

# Glosario de siglas

**CADH.** Convención Americana sobre Derechos Humanos.

**CCC.** Corte Constitucional de Colombia.

**CEJIL.** Centro por la Justicia y el Derecho Internacional.

**CIDH.** Comisión Interamericana de Derechos Humanos.

**Corte IDH.** Corte Interamericana de Derechos Humanos.

**DDHH.** Derechos humanos.

**GRIL.** Global Rights Innovation Lab Clinic, Universidad de California, Berkeley.

**OACNUDH.** Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

**OEA.** Organización de los Estados Americanos.

**ONG.** Organización No Gubernamental.

**ONU.** Organización de las Naciones Unidas.

**PDDH.** Personas defensoras de derechos humanos.

**PIDCP.** Pacto Internacional de Derechos Civiles y Políticos.

**PIDESC.** Pacto Internacional de Derechos Económicos, Sociales y Culturales.

**RELE.** Relatoría Especial para la Libertad de Expresión de la CIDH.

**SIDH.** Sistema Interamericano de Derechos Humanos.

**SLAPP.** Demandas estratégicas contra la participación pública (por su sigla en inglés, Strategic Lawsuit Against Public Participation).

# Glosario de conceptos clave

**Alerta temprana.** Advertencia preventiva sobre una situación de riesgo. Puede ser de carácter estructural –referida a factores de riesgo de mediano plazo– o de inminencia –cuando el riesgo está próximo a materializarse– (en el caso colombiano).

**Anonimización:** Medida de protección que permite tratar o publicar información sin identificar a las personas, suprimiendo de forma irreversible los datos identificables.

**Base de datos estructurada / semiestructurada / no estructurada.** Tipos de bases de datos según su grado de organización: la estructurada se ordena en filas y columnas; la no estructurada comprende texto, audio o video sin formato tabular; la semiestructurada combina ambos. Los modelos predictivos pueden trabajar con las tres, aunque las no estructuradas requieren un procesamiento previo.

**Base de datos integrada.** Base analítica única que consolida la información de múltiples fuentes, previo proceso de deduplicación y permite estimar el subregistro. Es la opción más robusta para identificar patrones y tendencias –porque cruza toda la información en una sola base–, y también la más exigente en integración y homologación.

**Blueprint.** Literalmente, "plano" o "anteproyecto" (del inglés *blueprint*, los planos técnicos de arquitectura). En este documento designa un conjunto de lineamientos o arquitectura de referencia que traduce las obligaciones jurídicas y las necesidades operativas en parámetros mínimos y verificables para el diseño, el fortalecimiento y la armonización de los sistemas de información sobre agresiones contra personas defensoras. No constituye un sistema de información ni una propuesta cerrada de implementación tecnológica: es una guía que puede adoptarse, adaptarse o utilizarse como insumo en distintos contextos nacionales.

**Codebook (libro de códigos).** Documento auxiliar que define, para cada variable, su contenido conceptual y las reglas de codificación, de modo que dos personas que codifican la misma información de forma independiente lleguen al mismo resultado.

**Criminalización.** Uso indebido del derecho penal, civil u otras ramas del derecho por actores estatales y no estatales con el fin o la consecuencia de inhibir, restringir o silenciar la defensa de los derechos humanos por medio de la manipulación del poder punitivo del Estado.

**Deduplicación / vinculación de registros *(record linkage)*.** Proceso que evita contar dos veces un mismo hecho o una misma víctima cuando varias fuentes lo reportan, identificando cuándo distintos registros corresponden al mismo caso. Puede ser determinística (coincidencia exacta de identificadores) o probabilística (estima, a partir de varias variables, la probabilidad de que dos registros correspondan al mismo caso).

**Enfoque macrocriminal.** Aproximación que aborda los hechos no como eventos aislados, sino en función de las redes de responsabilidad, las cadenas de mando y los patrones que articulan a individuos, grupos e instituciones.

**Estimación por Sistemas Múltiples (ESM).** Método estadístico que permite estimar el subregistro –los casos no documentados por ninguna fuente– a partir del grado de solapamiento entre fuentes que registran los mismos casos.

**Homologación.** Establecimiento de reglas de equivalencia entre categorías preexistentes y nuevas variables, que permite armonizar información histórica registrada con definiciones o formatos distintos.

**Interoperabilidad.** Capacidad de distintos sistemas de información para intercambiar y utilizar datos entre sí, sobre la base de estructuras, definiciones y formatos comunes.

**Memorialización.** Procesos de construcción de memoria sobre graves violaciones de derechos humanos, reconocidos por los estándares internacionales como una garantía de no repetición.

**Metadatos.** Información técnica asociada a cada dato (origen, fecha de ingreso y actualización, método y nivel de verificación, sensibilidad, responsable de la carga, etc.) que asegura su trazabilidad.

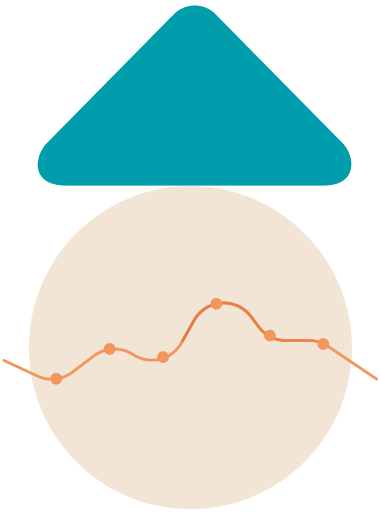
**Modelo predictivo.** Herramienta de la ciencia de datos que, a partir del comportamiento histórico de las variables, estima la probabilidad de hechos futuros o identifica patrones de escalada (por ejemplo, mediante regresión logística o agrupamiento de casos).

**Repositorio de datos.** Entorno común que centraliza información proveniente de múltiples fuentes preservando la identidad de cada base, sin consolidarlas en una sola base analítica.

**Subregistro.** Brecha entre los hechos efectivamente documentados y el universo real de casos. Su existencia fundamenta el uso de métodos estadísticos de estimación y de contrastación entre fuentes.

**Trazabilidad.** Posibilidad de conocer, para cada dato, su origen, el momento de su incorporación, quién lo registró y su estado de verificación, a lo largo de todo su ciclo de vida. Se sustenta en los metadatos asociados a cada dato.

**Transparencia activa.** Deber del Estado de producir y difundir información de oficio –sin que medie solicitud–, de forma completa, clara, veraz, actualizada y oportuna, y por canales accesibles.



# I. Introducción: sistemas de información para la prevención, protección y rendición de cuentas frente a los crímenes contra personas defensoras

El presente documento propone lineamientos para el desarrollo de sistemas de información para la prevención, protección, rendición de cuentas y reparación frente a las agresiones contra personas defensoras de derechos humanos (en adelante PDDH). Su desarrollo responde a la obligación de los Estados de producir información sistemática, confiable y útil sobre la situación, los ataques y los riesgos que enfrentan quienes ejercen el derecho a defender derechos. Esto constituye un elemento fundamental para fortalecer las políticas públicas de respuesta a los fenómenos de violencia y preservar un espacio cívico abierto para la defensa de los derechos humanos.

Este documento parte de una premisa central: la información sobre agresiones contra personas defensoras solo cumple una función protectora si permite pasar del registro aislado de hechos a la identificación de patrones, riesgos, respuestas institucionales y responsabilidades. Por ello, los sistemas de información no deben concebirse como simples repositorios de casos, sino como una herramienta fundamental de la política de Estado para cumplir con sus obligaciones de debida diligencia para la prevención, protección, investigación y rendición de cuentas.

La obligación estatal de producir información sobre la violencia contra PDDH deriva tanto de compromisos asumidos en el plano internacional como de mandatos de rango constitucional. Así, la Declaración de Naciones Unidas sobre los Defensores de los Derechos Humanos (1998) consolida el deber estatal de crear las condiciones para el ejercicio libre y seguro de la labor de defensa de derechos humanos[1]. En el mismo sentido, el Acuerdo Regional sobre el Acceso a la Información, la Participación Pública y el Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe (en adelante, Acuerdo de Escazú) reafirma la centralidad de la protección del entorno seguro y propicio para el ejercicio de derechos y de garantía de derechos de las personas defensoras de derechos humanos en asuntos ambientales[2]. En el plano interamericano, esta obligación se deriva del deber estatal de respetar y garantizar los derechos humanos, prevenir riesgos previsibles, proteger a personas y colectivos en situación de vulnerabilidad, investigar hechos de violencia, sancionar a los responsables y reparar las vulneraciones de derechos. La Corte Interamericana de Derechos Humanos (en adelante Corte IDH) ha reconocido expresamente el valor de la labor de las personas defensoras de derechos humanos para la democracia y el Estado de derecho, así como el derecho a defender derechos humanos. Asimismo, dicho tribunal corrobora la existencia de obligaciones reforzadas en cabeza de los Estados frente a personas defensoras de derechos humanos[3] y, como corolario de esas obligaciones, ha determinado desde 2021 la necesidad de crear sistemas nacionales de información sobre personas defensoras en los casos *Bedoya Lima y otra vs. Colombia* (2021)[4], *Sales Pimenta vs. Brasil* (2022)[5] y *CAJAR vs. Colombia* (2023)[6].

1 Asamblea General. Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, Resolución A/RES/53/144, 1998.

2 Acuerdo de Escazú, artículo 9.

3 Corte IDH. *Caso Escaleras Mejía y otros vs. Honduras*, Sentencia de 26 de septiembre de 2018, Serie C No. 361, párr. 54; Corte IDH. *Caso Defensor de Derechos Humanos y otros vs. Guatemala*, Sentencia de 28 de agosto de 2014, Serie C No. 283, párr. 142

4 Corte IDH. *Caso Bedoya Lima y otra vs. Colombia*, Sentencia de 26 de agosto de 2021, Serie C No. 431, párr. 193.

5 Corte IDH. *Caso Sales Pimenta vs. Brasil,* Sentencia de 30 de junio de 2022, Serie C No. 454, párr. 178.

6 Corte IDH. *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, Sentencia de 18 de octubre de 2023, Serie C No. 506, párr. 1047.

En el caso de Colombia, la Corte Constitucional ha reforzado estas exigencias en una sentencia significativa sobre la situación de personas defensoras de derechos humanos[7].

Estas obligaciones y órdenes convergen en una exigencia común: desarrollar sistemas de información capaces de fortalecer la protección de personas defensoras de derechos humanos y el espacio cívico. En este marco, los Estados deben producir, de manera proactiva, información sistemática y, cuando resulte pertinente, georreferenciada, que permita dimensionar la magnitud del fenómeno de hostigamiento, identificar patrones de agresión mediante datos adecuadamente desagregados, reconocer factores de riesgo y contextos territoriales, orientar medidas de prevención y protección, monitorear la respuesta institucional, apoyar investigaciones efectivas y contribuir a la no repetición. Asimismo, estos sistemas deben incorporar salvaguardas adecuadas para proteger la privacidad y confidencialidad de los datos personales; garantizar la integridad y seguridad digital de la información sensible; facilitar la interoperabilidad entre entidades; y asegurar mecanismos de participación efectiva de las personas defensoras y de la sociedad civil en su diseño, implementación y evaluación.

Los lineamientos que aquí se proponen buscan traducir las obligaciones y estándares internacionales en criterios concretos de diseño institucional, técnico y metodológico para los sistemas de información sobre agresiones contra personas defensoras. No pretenden reemplazar los sistemas de información existentes o imponer un único modelo ni definir una solución cerrada aplicable de manera uniforme a todos los contextos nacionales o todas las instituciones abocadas a la tarea de recoger información sobre el fenómeno. Por el contrario, la propuesta busca ordenar los elementos mínimos que un sistema de esta naturaleza debería

7 En el plano interno colombiano, la Sentencia SU-546 de 2023 de la Corte Constitucional colombiana (en adelante CCC) y su Auto aclaratorio 845 de 2024 ordenaron, en un pronunciamiento estructural sobre estado de cosas inconstitucional (en adelante ECI), la implementación articulada de una base de datos sobre la población líder y defensora y la puesta en marcha de un sistema informático de alerta temprana.

contemplar teniendo en cuenta los estándares internacionales[8], la revisión de las experiencias existentes a nivel nacional e internacional en la materia y un diálogo fructífero con instituciones, organizaciones sociales y personas expertas.

La satisfacción de estos estándares exige una arquitectura macro capaz de articular fuentes, generar relaciones lógicas y modelos de riesgo, y producir insumos útiles para la prevención, protección, investigación, sanción y reparación de las diversas formas de violencia contra PDDH. En ocasiones, ello deriva en múltiples bases de datos que enriquecen la comprensión del fenómeno, como los producidos desde espacios de sociedad civil y de instituciones internacionales, que ofrecen matices y contrapuntos con algunas de las bases y datos oficiales.

El desarrollo de un sistema de información sobre PDDH a nivel nacional mediante el uso de una multiplicidad de bases de datos o sistemas no está exento de desafíos. Es necesario definir en qué medida es posible articular esas fuentes teniendo en cuenta sus marcos legales y especificidad, preservar su autonomía, identificar solapamientos, reducir duplicaciones al combinar su uso y producir información útil sin generar una centralización forzada ni aumentar los riesgos para las personas defensoras. Las experiencias comparadas en el manejo de fuentes pueden brindar elementos de reflexión valiosos para abordar estos desafíos, especialmente considerando que, por razones normativas e institucionales, es frecuente que coexistan múltiples fuentes de información sobre el fenómeno y una pluralidad de bases de datos[9]. La discusión técnica sobre la arquitectura más adecuada para contextos con múltiples fuentes —incluida la opción de integración progresiva de bases de datos— se desarrolla más adelante, en la sección relativa a los elementos básicos de un sistema de información[10].

---

**8** Ver apartado 3 del documento. Por ejemplo, la CIDH sostiene que un sistema de información debe contener: "Datos sobre el número de condenas alcanzadas y grado de identificación de todos los responsables, incluidos autores materiales, intelectuales o inmateriales, así como partícipes, con estadísticas desagregadas por tipo de agresión (homicidio, desaparición, amenaza, desplazamiento) y por población (personas defensoras que sean mujeres, LGBTIQ+, indígenas y afrodescendientes, ambientales, comunales y de JAC), con metas anuales de incremento verificables". CIDH. *Segundo Informe de Seguimiento de Recomendaciones: Situación de personas defensoras de derechos humanos y líderes sociales en Colombia,* OEA/Ser.L/V/II, Doc. 7/26, 3 de febrero de 2026, párr. 242.

**9** En este sentido, es posible que los ministerios públicos o fiscalías, las instituciones nacionales de derechos humanos y organizaciones de derechos humanos cuenten con bases de datos relevantes.

**10** Ver apartado 5 del documento.

Estos lineamientos se nutren del estudio de algunos de los sistemas de información existentes. En particular, retoman la experiencia de Colombia, con una mirada complementaria sobre Brasil e insumos provenientes de experiencias globales y comparadas. El caso de Colombia es significativo para este ejercicio dado que el compromiso por responder a la gravedad y persistencia de la violencia contra personas defensoras en el país dio lugar a uno de los ecosistemas más desarrollados de la región en materia de registros, bases de datos y mecanismos de documentación producidos por entidades públicas, organizaciones sociales, observatorios independientes y organismos internacionales. También resultan relevantes las políticas, desarrollos institucionales e incluso supervisión judicial para responder al persistente fenómeno de agresiones contra personas defensoras, líderes sociales y periodistas[11]. Esta experiencia permite analizar con mayor precisión algunos de los desafíos relacionados con la articulación, interoperabilidad, trazabilidad, calidad de la información y uso legítimo de los datos, así como el tipo de procesamiento de datos, los productos e interfaces necesarios para maximizar su impacto, sin asumir que todos los países de la región tienen el mismo punto de partida.

La construcción de estos lineamientos se fundamenta en un proceso metodológico riguroso y colaborativo. El proceso incluyó investigación documental sobre estándares internacionales, revisión de información académica y de fuentes abiertas, la realización de entrevistas a instituciones y organizaciones, en mesas técnicas y en el involucramiento activo de personas expertas[12]. El diseño de las categorías y variables se basó en el análisis de fuentes de código abierto, en una investigación comparada realizada por la clínica jurídica *Global Rights Innovation Lab Clinic* de la Universidad de Berkeley (en adelante GRIL). Más aún, en el curso de la investigación contamos con un equipo y tres expertas/os en ciencia de datos que alimentaron las reflexiones e hicieron posible la elaboración de dos modelos. Este proceso incluyó la verificación empírica de la correspondencia entre la práctica actual de registro y los estándares jurídicos aplicables. Ello permitió identificar tanto las coincidencias

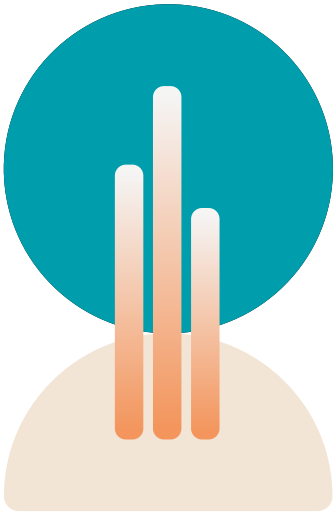
---

**11** CCC. Sentencia SU-546/23, 6 de diciembre de 2023. Orden número 24; CCC. Auto 845-24, 9 de mayo de 2024.

**12** Para esta investigación se analizaron –mediante entrevistas, derechos de petición, reuniones y fuentes primarias– las bases de datos pertinentes de Colombia de: Defensoría del Pueblo; Ministerio del Interior; Fiscalía General de la Nación (FGN); Autoridad Nacional de Licencias Ambientales (ANLA); Jurisdicción Especial para la Paz (JEP); Consejería Presidencial para los Derechos Humanos y el Derecho Internacional Humanitario; Programa Somos Defensores; Indepaz y Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH).

estructurales entre los sistemas existentes como los vacíos recurrentes que una arquitectura nueva debe tener en cuenta.

El *Blueprint* se organiza en 12 secciones. En primer lugar, se exponen las razones por las cuales un sistema de información de esta naturaleza resulta necesario y las funciones estratégicas que debe cumplir. A continuación, se desarrollan los objetivos de los Lineamientos. Luego, se precisa el fundamento jurídico que sustenta la propuesta. Más adelante, se presentan los elementos básicos de un sistema de información y, seguidamente, las categorías sustantivas que estructuran la arquitectura propuesta. Después, se abordan los aspectos a tener en cuenta para el manejo de datos y se señalan los usos analíticos y operativos del sistema de información. Posteriormente, se presentan los resultados o *outputs* posibles y se desarrollan las interfaces institucionales y con la sociedad civil. Hacia el final, se enuncian los principios éticos que deben orientar tanto el diseño como la operación cotidiana del sistema y se establecen las pautas de gobernanza necesarias para su implementación y sostenibilidad. Por último, se presentan las conclusiones.



## II. La necesidad de un sistema de información sobre personas defensoras

La violencia contra las PDDH constituye uno de los desafíos más graves para la democracia, el Estado de Derecho y la vigencia efectiva de los derechos fundamentales en la región. Los informes más recientes de organizaciones especializadas documentan, con metodologías y universos de cobertura distintos, una tendencia sostenida de agresiones letales y no letales en su contra, así como el cierre del entorno habilitante para la protección de los derechos[13].

Estos informes alertan sobre la aguda situación de Colombia, México, Guatemala, Brasil, Honduras y Perú, donde patrones persistentes de agresión letal y no letal se articulan con disputas por el control territorial, presencia de actores armados y economías ilegales, conflictos socioambientales, debilidad institucional y, en

**13** Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/61/40, 5 de enero de 2026, párr. 1; CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas*, OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 8; Global Witness, *Defenders Annual Report 2025 Roots of Resistance*, 2025. Disponible en: https://gw.hacdn.io/media/documents/Defenders_Annual_Report_2025_online_EN.pdf; Front Line Defenders. Global Analysis 2025/26, 2026. Disponible en: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf. El HRD Memorial es una iniciativa conjunta de una red de organizaciones de derechos humanos que incluye a Amnistía Internacional, FIDH, Front Line Defenders, Global Witness y el Programa Somos Defensores, entre otras.

determinados supuestos, acción u omisión estatal frente a riesgos previsibles[14]. Asimismo, dan cuenta de los pasos hacia el cierre del espacio cívico, la persistencia de la criminalización y la subsistencia de presos por motivos políticos en varios países del hemisferio, notablemente en Venezuela, El Salvador y Nicaragua[15].

Los sistemas de monitoreo del Sistema Universal y del Sistema Interamericano de Derechos Humanos (en adelante SIDH) confirman que el entorno para el ejercicio del derecho a defender derechos sigue fuertemente tensionado en América Latina —región que concentra la gran mayoría de los asesinatos de personas defensoras a nivel global—[16] por un conjunto de factores estructurales que se refuerzan mutuamente: la débil o ausente presencia integral del Estado en los territorios más afectados o frente a grupos significativos de la población[17]; la acción directa u omisión estatal como factor causal o agravante de la vulnerabilidad, incluida la insuficiencia de los mecanismos de protección existentes[18]; la estigmatización y criminalización de personas defensoras por parte de actores estatales y no estatales[19];

---

**14** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025; Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos, A/HRC/61/40, 5 de enero de 2026;* CIDH. *Segundo Informe de Seguimiento de Recomendaciones: Situación de personas defensoras de derechos humanos y líderes sociales en Colombia,* OEA/Ser.L/V/II Doc. 7/26, 3 de febrero de 2026; Global Witness, *Defenders Annual Report 2025 Roots of Resistance*, 2025. Disponible en: https://gw.hacdn.io/media/documents/Defenders_Annual_Report_2025_online_EN.pdf; Front Line Defenders. Global Analysis 2025/26, 2026. Disponible en: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf.

**15** Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *Situation of human rights in the Bolivarian Republic of Venezuela (advanced unedited version),* A/HRC/59/58, 26 de junio de 2025, párr. 33-52; Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *Situación de los derechos humanos en Nicaragua*, A/HRC/60/92, p. 4-5; CIDH. *Estado de excepción y derechos humanos en El Salvador*, 28 de junio de 2024, párr. 391; CIDH. *Situación de los derechos humanos en Guatemala*, OEA/Ser.L/V/II, Doc. 227/25, 2 de noviembre de 2025, párrs. 183-194.

**16** ONU. *The Sustainable Development Goals Report,* 2025, p. 41. Disponible en: https://unstats.un.org/sdgs/report/2025/The-Sustainable-Development-Goals-Report-2025.pdf; Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/46/35, 24 de diciembre de 2020, párrs. 5, 41.

**17** Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/58/53, 3 de enero de 2025, párrs. 5, 47.

**18** Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/46/35, 24 de diciembre de 2020, párr. 9.

**19** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas*, OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 8.

los altos niveles de impunidad frente a los ataques[20]; las formas crecientes de violencia digital, vigilancia y espionaje en línea[21]; los riesgos diferenciados que enfrentan las mujeres defensoras y las personas defensoras indígenas, afrodescendientes y campesinas[22]; la presencia de actores armados no estatales que ejercen control territorial mediante economías ilícitas[23]; y los conflictos vinculados al modelo de desarrollo extractivo y de la falta de resolución de disputas históricas sobre la tierra y el territorio, la desigualdad estructural[24], entre otros.

Ahora bien, la capacidad para documentar estos fenómenos presenta importantes asimetrías en la región. Mientras algunos países cuentan con bases de datos relevantes producidas por entidades estatales, intergubernamentales, organizaciones de la sociedad civil o la academia, otros carecen de registros básicos de información. Incluso cuando existen, algunas de las bases de datos operan como registros pasivos, concentrados mayoritariamente en eventos letales; mientras que otras registran crímenes sin identificar aquellos cometidos contra PDDH.

Documentar adecuadamente las agresiones contra personas defensoras y el cierre del espacio cívico es tan necesario como complejo. Sin información adecuada y oportuna no es posible comprender la magnitud del fenómeno, identificar patrones de riesgo, orientar medidas de prevención y protección ni evaluar la eficacia de la respuesta estatal. Parte de la complejidad se funda en al menos cuatro causas: i)

---

**20** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 7; Michel Forst, Relator Especial sobre la situación de los defensores de los derechos humanos. *Informe a la Asamblea General de las Naciones Unidas.* A/74/159, 15 de julio de 2019, párr. 23, 24

**21** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 134; Michel Forst, Relator Especial sobre la situación de los defensores de los derechos humanos. *Informe a la Asamblea General de las Naciones Unidas.* A/74/159, 15 de julio de 2019, párr. 21.

**22** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 8, 36, 47; Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/46/35, 24 de diciembre de 2020, párrs. 54, 66.

**23** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 7.

**24** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, p. 7, Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos,* A/HRC/46/35, 24 de diciembre de 2020, párrs. 10.

el subregistro; ii) la variedad de tipos de violencia; iii) la naturaleza colectiva de la defensa de los derechos humanos, y iv) la diversidad de definiciones, estrategias de documentación y producción de resultados.

Para comenzar, existe una alta complejidad a la hora de documentar cabalmente violaciones a los derechos humanos. Tanto las entidades estatales como las organizaciones de la sociedad civil cuentan con diferentes capacidades de documentación, redes territoriales y recursos económicos. Por lo anterior, es esperable que existan múltiples fuentes con resultados diferentes y que algunas ni siquiera registren los crímenes contra PDDH como una categoría específica, lo que dificulta poder identificar o asociar eventos, y contribuye al subregistro de este tipo de violaciones. En este marco, los ejercicios de contrastación y el uso de métodos estadísticos son necesarios para entender la dimensión de la problemática[25].

En segundo lugar, algunos de los sistemas existentes de documentación registran los homicidios, pero no captan necesariamente o con la misma rigurosidad el universo más amplio de violaciones que sufren las personas defensoras. Entre ellas, amenazas y ataques, desplazamientos forzados, confinamientos, detenciones arbitrarias, desapariciones, señalamientos y estigmatización, criminalización mediante el uso indebido del derecho penal, impunidad frente a las agresiones sufridas, violencia sexual y, de manera creciente, violencia simbólica y digital[26]. Tampoco capturan necesariamente la prevalencia territorial de los hechos, la diversidad de modalidades de violencia, las barreras de acceso institucional ni el uso de mecanismos formales e informales de persecución[27].

---

**25** Por ejemplo, para el caso colombiano, en el 2016, 6 entidades y organizaciones (Indepaz, Programa Somos Defensores, Cumbre Agraria, Front Line Defenders, OACNUDH y la Defensoría del Pueblo) monitorearon los asesinatos de líderes sociales en 2016, con cifras individuales que iban desde 61 hasta 133 casos. Al cruzar y consolidar las seis listas, sin contar dos veces un mismo caso –mediante un proceso de deduplicación–, se documentaron 160 asesinatos. Al utilizar métodos estadísticos para hacer la estimación del universo, se encontró que este podría ser de entre 160 y 180 con un intervalo de credibilidad del 95%. Es decir, podría haber hasta 20 líderes asesinados que no fueron documentados por ninguna organización. Ver: Patrick Ball, César Rodríguez Garavito y Valentina Rozo. *Asesinatos de líderes sociales en Colombia en 2016–2017: una estimación del universo.* Bogotá: Dejusticia, agosto de 2018.

**26** ONU Derechos Humanos. *Situación de las personas defensoras de derechos humanos en Colombia (2022-2025).* Bogotá: Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, marzo de 2026.

**27** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas,* OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025.

En tercer lugar, parte de los registros suelen documentar hechos individuales sin dar cuenta de las violaciones concatenadas ni su dimensión colectiva. Por ejemplo, pueden registrar el homicidio de un líder indígena sin considerar la secuencia de hostigamientos sufrida por su comunidad o por sus abogados/as. En consecuencia, la vulneración de derechos rara vez queda reflejada con la integralidad que el fenómeno exige[28]. En algunos casos, además, los registros disponibles capturan solo una fracción del problema o fueron usados en el pasado como herramientas de persecución[29]. Ello deriva en prevenciones para compartir información útil o necesaria con algunos actores estatales.

En cuarto lugar, en los casos donde sí se dispone de información relevante, la diversidad de definiciones y estrategias de documentación constituye, en sí misma, un rasgo valioso del ecosistema de información: responde a la pluralidad de mandatos, enfoques y vínculos territoriales de quienes documentan, y ha permitido visibilizar realidades que de otro modo habrían quedado fuera de registro. Así, el desafío no radica en la diversidad como tal, sino en que esta obstaculiza hacer las asociaciones necesarias entre los datos recabados para generar los análisis y productos que exigen las órdenes internacionales y nacionales –tanto a nivel individual como de manera agregada integrando las diversas bases–. Adicionalmente, aun en bases desarrolladas, el procesamiento y sus resultados podrían perfeccionarse para generar información y análisis más adecuados y oportunos para la toma de decisiones.

Al utilizar categorías diferentes, responder a finalidades diversas y aplicar métodos de verificación heterogéneos, los distintos sistemas enfrentan serios obstáculos de interoperabilidad, lo que dificulta construir series históricas consistentes, identificar patrones comunes y producir respuestas coordinadas entre autoridades con competencias concurrentes o con obligación de reserva. De este modo, aunque la multiplicidad de

---

**28** ONU Derechos Humanos. *Situación de las personas defensoras de derechos humanos en Colombia (2022-2025)*. Bogotá: Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, marzo de 2026.

**29** De allí que la CIDH indique que "(...) llama al Estado a atender las observaciones sobre posibles inconsistencias entre los datos de diferentes entidades y a fortalecer la articulación interinstitucional para superar estas brechas. Del mismo modo, insta a establecer mecanismos que eviten que la información sea utilizada para actividades de seguimiento o perfilamiento indebido de personas defensoras. En consecuencia, resulta indispensable avanzar hacia un registro unificado, confiable y con participación de la sociedad civil, en consonancia con los estándares interamericanos de debida diligencia, prevención y protección". CIDH. *Segundo Informe de Seguimiento*, OEA/Ser.L/V/II, Doc. 7/26, 2026, párr. 103.

registros es una condición necesaria para medir con rigor la magnitud del fenómeno, la ausencia de mecanismos que permitan integrarlos y hacerlos comparables impide aprovechar plenamente esa riqueza informativa para generar el conocimiento acumulado que la protección efectiva de las personas defensoras exige. A ello se suma que el fortalecimiento de las capacidades de procesamiento y la producción de resultados oportunos y adecuados pueden potenciar tanto a cada sistema en lo individual como al análisis agregado del conjunto. En ocasiones, la falta de atención a las interfases entre los sistemas existentes debilita los circuitos de protección y de justicia, con repercusiones para la capacidad preventiva o sancionatoria del Estado.

Estas dificultades se observan incluso en los sistemas de información más desarrollados de la región. Colombia ofrece, en este sentido, un caso ilustrativo. Precisamente por contar con uno de los ecosistemas de documentación más amplios y diversos del hemisferio, fue posible realizar allí un mapeo sistemático de un conjunto de bases de datos relevantes de nueve organizaciones de la sociedad civil e instituciones estatales. El estudio mostró que la información sobre personas defensoras existe, aunque de manera fragmentada: de las bases de datos analizadas, ninguna supera el 41% de variables con datos estructurados y cuantificables[30]. Entre las principales brechas identificadas se encuentran la

**30** En su investigación, GRIL analizó nueve fuentes de información: i) el *Sistema de Alertas Tempranas (SAT)* y el *Informe de Seguimiento a la Alerta Temprana 026-18* de la Defensoría del Pueblo; ii) el *Índice de Focalización de las Zonas Especiales de Garantías para el Liderazgo Social* del Ministerio del Interior; iii) los *Boletines de Defensores* y el *Informe público* que la Fiscalía General de la Nación presentó en cumplimiento del numeral 19 de la Sentencia SU-546 de 2023 de la Corte Constitucional; iv) la *Caracterización de Personas Defensoras de Derechos Humanos en Asuntos Ambientales y Organizaciones Socioambientales* de la Autoridad Nacional de Licencias Ambientales (ANLA); v) los informes *Análisis de la situación de Derechos Humanos y seguridad en Colombia: impactos de los ceses al fuego y la Paz Total* y *Gravedad de la situación de derechos humanos en Colombia* de la Jurisdicción Especial para la Paz (JEP); vi) el *Módulo de Información sobre homicidios de líderes/as sociales y personas defensoras de derechos humanos* de la Consejería Presidencial de Derechos Humanos; vii) los informes semestral y anual del *Sistema de Información sobre Agresiones contra Personas Defensoras de Derechos Humanos en Colombia (SIADDHH)* del Programa Somos Defensores; viii) el *Visor de Asesinato a Personas Líderes Sociales y Defensores de Derechos Humanos en Colombia* y el informe *Una tendencia que mata: el fracaso del Estado en la protección de los liderazgos sociales* de Indepaz; y ix) la *Situación de los derechos humanos en Colombia (Informe del Alto Comisionado)*, junto con la infografía y la presentación del *Informe Anual del Alto Comisionado 2021–2025* de la OACNUDH. Para el análisis se definieron 14 categorías (i) manejo de datos, ii) demografía, iii) presuntos perpetradores, iv) tipo de agresión, v) tipo de agresión – criminalización vi) salud, vii) factores de riesgo, viii) contexto territorial, ix) contexto socioeconómico y político, x) estado de derecho, xi) medidas de protección institucionales, xii) indicadores de judicialización, xiii) respuesta administrativa y de política pública, xiv) seguimiento y evaluación, con más de 80 variables.

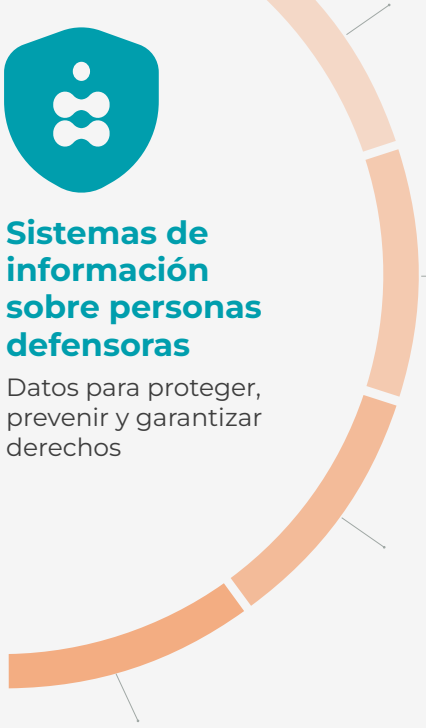
escasa cobertura de información sobre criminalización, salud mental y riesgo psicosocial de PDDH, represión digital, vigilancia tecnológica y uso de software intrusivo. Además, se observaron limitaciones en la información y la comparabilidad de los datos sobre presuntos perpetradores y niveles de responsabilidad, así como en la trazabilidad de las medidas de protección y de su eficacia y en la desagregación territorial y poblacional.

Las brechas identificadas en el caso colombiano ponen de relieve cómo la fragmentación de la información, las dificultades para integrarla y producir resultados adecuados pueden configurar una forma específica de impunidad informacional. Los lineamientos aquí propuestos buscan contribuir a superar estos desafíos y muestran por qué este esfuerzo resulta sumamente valioso e indispensable.

Ahora bien, conscientes de la necesidad de sistemas de información de personas defensoras y teniendo en cuenta sus desafíos, es importante precisar sus objetivos o funciones estratégicas. En primer lugar, el fortalecer la prevención temprana del riesgo mediante la identificación de tendencias, repeticiones y factores de alerta.

En segundo término, mejorar la protección individual, colectiva y territorial, permitiendo priorizar casos, ajustar medidas y monitorear su eficacia. Asimismo, debe contribuir a la investigación y judicialización de los hechos, facilitar el seguimiento de la impunidad e informar a la política criminal del Estado, y además, ofrecer evidencia para la formulación, monitoreo y evaluación de políticas públicas.

Finalmente, debe servir como herramienta de rendición de cuentas y como interfaz con la academia, la sociedad civil, las comunidades afectadas y los procesos de memoria, verdad y reparación. Todo ello bajo los principios de uso legítimo y de precaución, que eviten el registro con fines de persecución o estigmatización.



## Sistemas de información sobre personas defensoras

Datos para proteger, prevenir y garantizar derechos

1

### Prevención temprana del riesgo

Permite identificar escaladas, repeticiones y factores de alerta para actuar antes de que ocurran daños mayores.

2

### Mejora de la protección individual, colectiva y territorial

Ayuda a priorizar casos, ajustar medidas de protección y monitorear su eficacia para resguardar vidas y territorios.

3

### Investigación y judicialización de los hechos

Facilita la recolección y conservación de evidencia, fortalece las investigaciones y contribuye a la sanción de los responsables.

4

### Evidencia para políticas públicas y política criminal

Genera información para formular, monitorear y evaluar políticas públicas, y permite hacer seguimiento a los niveles de impunidad y respuesta institucional.

5

### Rendición de cuentas e interfaz social

Sirve como herramienta de rendición de cuentas y como interfaz con la academia, la sociedad civil, las comunidades afectadas y los procesos de memoria, verdad y reparación.

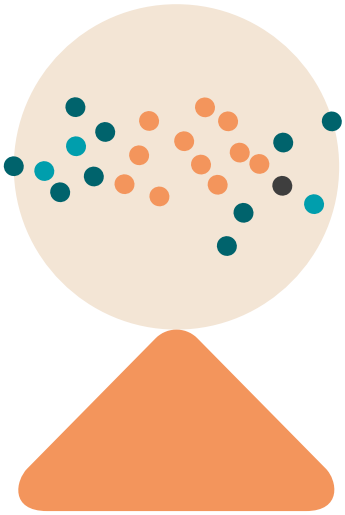
## Bajo principios de uso legítimo y de precaución

**Uso legítimo:**
solo para fines de protección, prevención, investigación y políticas públicas.

**Precaución:**
minimizar riesgos de exposición y daño.

**Confidencialidad**
y protección de datos personales.

**No discriminación,**
no estigmatización, no persecución.



## III. Los objetivos del Blueprint

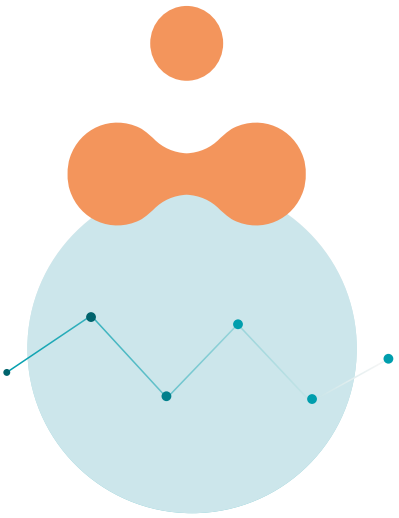
El *blueprint* constituye un conjunto de lineamientos destinados a orientar y apoyar los procesos de construcción, fortalecimiento y armonización de sistemas de información sobre agresiones contra PDDH, tomando como referencia las guías y estándares del derecho internacional de los derechos humanos. Ofrece una arquitectura de referencia que traduce obligaciones jurídicas y necesidades operativas en parámetros verificables de diseño institucional, y que puede ser adoptada, adaptada o utilizada como insumo por los Estados, los órganos de protección y las organizaciones de sociedad civil responsables de producir o articular información sobre el fenómeno. El *blueprint* no constituye un sistema de información ni una propuesta cerrada de implementación tecnológica. Por el contrario, busca identificar un conjunto de elementos mínimos comunes que permitan fortalecer la calidad, comparabilidad, interoperabilidad y utilidad pública de la información producida en distintos contextos nacionales. La estrategia es la armonización de estándares y propuesta de resultados para la mayor efectividad de los sistemas, y no la sustitución de los sistemas de información existentes ni la imposición de formatos únicos.

Teniendo en cuenta la pluralidad de fuentes estatales, independientes, comunitarias o multilaterales, el objetivo debe ser preservar esa diversidad y construir sobre ella una arquitectura capaz de relacionar fuentes, generar asociaciones significativas entre los datos y mejorar la interoperabilidad. Esto se observa con claridad en Colombia, donde coexisten múltiples registros con lógicas, metodologías, finalidades y alcances distintos, con vacíos que relevamos arriba y sin que existan mecanismos suficientes de articulación entre ellos. En otros contextos nacionales, el desafío puede ser diferente, pues antes que articular fuentes existentes puede ser necesario crear registros

básicos allí donde la violencia contra PDDH aún no se documenta de manera sistemática o no se registra teniendo en cuenta la calidad de la víctima u otros factores requeridos bajo el derecho internacional. En este sentido, en Brasil, por ejemplo, la documentación estatal de los homicidios y otras vulneraciones de derechos no suele identificar a las víctimas en función de su condición de personas defensoras, lo que dificulta dimensionar adecuadamente el fenómeno. Por ello, estos lineamientos deben poder leerse e implementarse de acuerdo con las condiciones, capacidades y necesidades de cada país y de las entidades que desarrollen la tarea.

En términos generales, este documento define los contenidos mínimos que deben integrar la arquitectura de datos y los sistemas de información. Asimismo, orienta la incorporación y articulación de fuentes diversas; propone reglas de calidad, verificación y no duplicación; identifica funcionalidades esenciales del sistema; precisa pautas para el análisis de la información y la elaboración de los productos mínimos de utilidad pública que este genera —estadísticas, informes periódicos, mapas, alertas tempranas y narrativas de casos—; incorpora salvaguardas adecuadas para la protección de la información sensible; y ofrece una base inicial para la gobernanza del sistema, incluidos los mecanismos de participación de las personas defensoras, las comunidades afectadas y la sociedad civil. Más que promover la mera recopilación de información, el *blueprint* busca generar condiciones para transformar datos en conocimiento útil para la prevención, la protección, la investigación y la formulación de respuestas institucionales basadas en evidencia.

De manera más específica, el diseño propuesto aspira a mejorar la comparabilidad regional de los registros, facilitar el análisis de riesgo, fortalecer la coordinación entre entidades públicas con competencias concurrentes, reducir la impunidad informacional y ampliar el acceso público a información pertinente para la participación, protección y ejercicio de derechos. Asimismo, busca que la información producida a partir del procesamiento y análisis de datos, así como los productos derivados de ella, resulten útiles para la prevención, la investigación de los hechos, los procesos de verdad, justicia y reparación, y la formulación de políticas públicas. Se trata de crear condiciones para que las decisiones estatales en materia de prevención, protección, investigación y reparación sean evaluables, y para que las comunidades afectadas puedan interactuar con herramientas más transparentes y útiles en la defensa de sus derechos. En último término, el objetivo es que el sistema de información deje de funcionar como un registro pasivo de eventos y se convierta en una infraestructura activa para la garantía efectiva del derecho a defender derechos.



# IV. La creación de sistemas de información es una obligación jurídica internacional de los Estados

El desarrollo de un sistema de información sobre agresiones contra PDDH no constituye solo una buena práctica de política pública, sino que encuentra respaldo en obligaciones jurídicas positivas derivadas del derecho internacional de los derechos humanos y de desarrollos nacionales en materia constitucional, como desarrollamos más arriba. Estas obligaciones definen los parámetros sustantivos y procedimentales que deben orientar el diseño y funcionamiento de las bases de datos destinadas a documentar, analizar y prevenir la violencia contra PDDH.

En el plano universal, la Declaración sobre Defensores de Naciones Unidas (1998) reconoce expresamente el derecho de toda persona, individual o colectivamente, a promover y procurar la protección y realización de los derechos humanos, y consolida el deber estatal de crear las condiciones para el ejercicio libre y seguro de la labor de defensa[31].

**31** Asamblea General. Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, Resolución A/RES/53/144, 1998.

Este instrumento recoge obligaciones ya plasmadas en numerosos tratados universales de derechos humanos vinculados al ejercicio del derecho a defender derechos humanos. Entre ellos, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC)[32].

En el plano interamericano, destacamos primordialmente la Convención Americana sobre Derechos Humanos (en adelante CADH) y el Acuerdo de Escazú de los cuales se derivan obligaciones estatales que expresan las protecciones reforzadas que ameritan las personas defensoras y la protección del entorno habilitante para el ejercicio de los derechos humanos.

Así, la jurisprudencia y doctrina emanada de la Corte IDH y los informes temáticos de la Comisión Interamericana de Derechos Humanos (en adelante CIDH) han consolidado estándares específicos aplicables a la protección de personas defensoras y al derecho a defender derechos. En particular, la Corte IDH ha desarrollado progresivamente estándares sobre la producción, sistematización, difusión y salvaguarda de información relativa a agresiones contra personas defensoras, especialmente a través de las garantías de no repetición ordenadas en los casos *Bedoya Lima, Sales Pimenta* y *CAJAR*, así como en lo establecido en el caso *Zapata* y la *Opinión Consultiva No. 32/25*.

En la Sentencia *Bedoya Lima y otra vs. Colombia*, la Corte IDH ordenó al Estado diseñar e implementar, en el plazo de un año, un sistema de recopilación de datos y cifras sobre violencia contra periodistas, con énfasis en la violencia basada en género contra mujeres periodistas. La medida incluyó la recopilación de indicadores de judicialización —acusaciones, condenas y absoluciones— y la difusión periódica de esa información con las salvaguardias necesarias para proteger la identidad de las víctimas[33]. En el Caso *Sales Pimenta vs. Brasil*, el tribunal interamericano replicó y amplió la medida para defensores ambientales y de tierras, exigiendo evaluar "el tipo, la prevalencia, las tendencias y las pautas de violencia" y desglosar

---

**32** Comité de Derechos Humanos, *Observación General 34: Libertad de opinión y libertad de expresión (artículo 19 del PIDCP)*, CCPR/C/GC/34 (2011), párrs. 21–36 y Comité de Derechos Humanos, *Observación General 36: Derecho a la vida (artículo 6 del PIDCP)*, CCPR/C/GC/36 (2019), párr. 7; Comité de Derechos Económicos, Sociales y Culturales, *Declaración: Defensores de los derechos humanos y derechos económicos, sociales y culturales*, E/C.12/2016/2, 29 de marzo de 2017, párr. 5.

**33** Corte IDH. *Caso Bedoya Lima y otra vs. Colombia*, Sentencia de 26 de agosto de 2021, Serie C No. 431, párr. 193.

los datos por Estado, origen étnico, militancia, género y edad[34]. Asimismo, dispuso la creación de un grupo de trabajo para identificar las causas de la impunidad estructural asociada a estas agresiones[35]. En la decisión *CAJAR vs. Colombia*, la Corte IDH consolidó el estándar en el marco de una sentencia estructural y vinculó de manera expresa la producción de información con los deberes de prevención, protección y no repetición. El Tribunal sostuvo que la ausencia de información integral impide dimensionar adecuadamente la magnitud de la violencia contra las personas defensoras, identificar patrones de riesgo y diseñar políticas públicas eficaces para enfrentar el fenómeno[36].

Esta línea fue profundizada por la *Opinión Consultiva 32/25* sobre emergencia climática y derechos humanos. Allí, la Corte IDH precisó que la producción de información constituye una obligación estatal derivada del derecho de acceso a la información[37]. En consecuencia, los Estados deben recabar y mantener actualizados datos desglosados sobre asesinatos, secuestros, desapariciones forzadas, detenciones arbitrarias, tortura y otros actos lesivos contra personas defensoras del ambiente[38]. Además, se ordena considerar factores socioeconómicos, de género, edad, sexo y etnia, y diseñar políticas orientadas a atender las causas estructurales de la violencia, incorporando un enfoque interseccional que permita identificar y responder a las afectaciones diferenciadas derivadas de situaciones de discriminación y vulnerabilidad[39].

**34** Corte IDH. *Caso Sales Pimenta vs. Brasil,* Sentencia de 30 de junio de 2022, Serie C No. 454, párr. 178.

**35** Corte IDH. *Caso Sales Pimenta vs. Brasil,* Sentencia de 30 de junio de 2022, Serie C No. 454, párr. 145.

**36** Corte IDH. *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, Sentencia de 18 de octubre de 2023, Serie C No. 506, párr. 1047.

**37** Corte IDH. *Opinión Consultiva OC-32/25*, 29 de mayo de 2025. Serie A No. 32, párr. 505.

**38** Corte IDH. *Opinión Consultiva OC-32/25*, 29 de mayo de 2025. Serie A No. 32, párr. 575.

**39** Corte IDH. *Opinión Consultiva OC-32/25*, 29 de mayo de 2025. Serie A No. 32, párr. 575.

Cabe señalar que, en el caso *Zapata* (2025), la Corte IDH reconoció el deber de los Estados de adoptar las medidas necesarias para proteger la integridad y la seguridad de los sistemas que almacenan datos personales frente a accesos no autorizados e interferencias indebidas, con especial atención a la recopilación y el almacenamiento de datos de personas defensoras[40].

El *Acuerdo de Escazú* añadió una dimensión especialmente significativa para la región al reforzar las obligaciones de acceso a la información, participación pública, justicia ambiental y protección especial de personas defensoras del ambiente. Este tratado reconoce en su articulado la importancia de asegurar un espacio cívico habilitante y la relevancia de las personas defensoras del ambiente, su protección y la investigación de los crímenes cometidos en su contra, para asegurar los derechos al desarrollo sostenible y al medioambiente.  El Plan de Acción sobre Defensoras y Defensores de los Derechos Humanos en Asuntos Ambientales, adoptado en el marco del *Acuerdo de Escazú,* incorpora la generación de conocimiento como uno de sus ejes prioritarios (eje A)[41]. El Plan obliga a los Estados a elaborar diagnósticos sobre la situación de quienes promueven y defienden derechos humanos en asuntos ambientales, incluyendo el número de víctimas y los tipos de vulneraciones, los instrumentos de prevención, protección y sanción, los sistemas de alerta temprana, y las prácticas y estrategias comunitarias de autoprotección[42]. Estas medidas adquieren especial relevancia en contextos donde las agresiones se vinculan con conflictos sobre tierra, recursos naturales, infraestructura o uso del suelo, y donde la asimetría informativa entre Estado, empresas y comunidades opera como factor agravante del riesgo.

**40** Corte IDH. *Caso Zapata Vs. Colombia*, Sentencia de 3 de octubre de 2025, Serie C No. 569, párr. 154.

**41** CEPAL. *Plan de Acción sobre Defensoras y Defensores de los Derechos Humanos en Asuntos Ambientales en América Latina y el Caribe y su programa de implementación*, LC/ESZ.2025/4, 2026, pág. 11-12, 14-16.

**42** CEPAL. *Plan de Acción sobre Defensoras y Defensores de los Derechos Humanos en Asuntos Ambientales en América Latina y el Caribe y su programa de implementación*, LC/ESZ.2025/4, 2026, pág. 11-12, 14-16.

A partir de la guía provista por los estándares interamericanos y el Acuerdo de Escazú se desprende un conjunto de pautas mínimas para el diseño de sistemas de información sobre agresiones contra personas defensoras en materia de contenido, propósito, productos y condiciones de operación[43].

En cuanto al contenido, estos sistemas deben registrar no solo homicidios u otras agresiones letales, sino también amenazas, desapariciones, desplazamientos, detenciones arbitrarias, tortura, hostigamientos, criminalización, violencia digital, vigilancia, ataques contra organizaciones y otras formas de violencia o restricción al ejercicio del derecho a defender derechos. Deben captar, además, no solo hechos individuales aislados, sino su dimensión colectiva, ya sea la pertenencia organizativa o comunitaria de la víctima y las secuencias de agresión dirigidas contra colectivos, comunidades u organizaciones. Esta información debe estar desagregada, como mínimo, por tipo de agresión, territorio, perfil de la víctima, género, edad, etnia, tipo de labor, pertenencia colectiva, contexto de riesgo, presunto perpetrador y posible acción u omisión estatal. La desagregación de la información no constituye un aspecto meramente metodológico, sino una exigencia sustantiva para visibilizar riesgos diferenciados y patrones específicos de violencia que afectan de manera desproporcionada a mujeres defensoras, pueblos indígenas, comunidades afrodescendientes, comunidades campesinas, personas defensoras ambientales, periodistas y otros grupos en situación de vulnerabilidad.

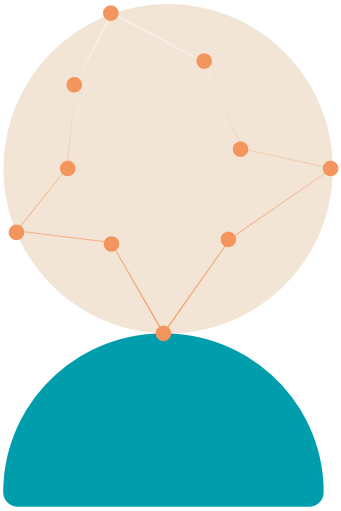
**43** Cabe señalar que la consolidación de estos estándares en el plano internacional encuentra hoy una expresión concreta en el caso colombiano. La CCC, en la Sentencia SU-546 de 2023 y en el Auto 845 de 2024, declaró un estado de cosas inconstitucional respecto a la situación de seguridad de la población líder y defensora de derechos humanos. La declaratoria se sustentó en la persistente y generalizada violación de sus derechos fundamentales, así como en la insuficiente capacidad institucional y presupuestal del Estado para garantizar su protección. Frente a ello, la Corte dispuso dos mandatos directamente vinculados con la producción y gestión de información. En primer lugar, dispuso la implementación articulada entre distintos organismos de una base de datos única, entendida como un sistema de información compuesto por diferentes bases de datos existentes, destinada al registro de la población líder y defensora de derechos humanos. Esta debe incluir una estadística única y un manejo articulado de la información acerca de los tipos de violencia sufridos por esta población, sobre la base de una definición uniforme de persona defensora y con sujeción a los principios del hábeas data. En segundo lugar, se ordenó la implementación, en un plazo de seis meses, de un sistema informático de comunicación ágil y expedito (tipo webchat, WhatsApp o aplicación móvil) que permita a la ciudadanía notificar amenazas y riesgos para su vida e integridad, con verificación inmediata y activación urgente de medidas de protección.

En cuanto al propósito, el uso de la información no debe limitarse al registro retrospectivo de hechos letales consumados. Debe permitir dimensionar la magnitud del fenómeno de las agresiones, identificar patrones de violencia, reconocer factores de riesgo, analizar causas estructurales, activar medidas de prevención y protección, evaluar su eficacia, orientar investigaciones, monitorear niveles de impunidad y contribuir a la verdad, la reparación y la no repetición.

En cuanto a sus productos, los sistemas deben generar información estadística, informes periódicos públicos, tableros de visualización, mapas, alertas, análisis de tendencias, estudios de patrones, modelos predictivos y otros insumos útiles para la toma de decisiones institucionales y sociales. La difusión de esta información debe realizarse con las salvaguardias necesarias para proteger la identidad, seguridad y privacidad de las víctimas cuando corresponda.

Finalmente, en cuanto a sus condiciones de operación, estos sistemas deben ser accesibles para distintos públicos —autoridades, sociedad civil, academia, comunidades afectadas y mecanismos de protección, justicia, verdad y reparación—, sin perder de vista los principios de seguridad, confidencialidad, participación, consentimiento, uso legítimo y no daño. La producción de información sobre personas defensoras solo cumple una función protectora si evita el perfilamiento indebido, la vigilancia, la estigmatización o cualquier uso que incremente los riesgos que precisamente busca prevenir.

| Eje / Estándar | Bedoya Lima y otra vs. Colombia | Sales Pimenta vs. Brasil | CAJAR vs. Colombia |
|---|---|---|---|
| **Tipo de víctima central** | Mujer periodista y defensora de la libertad de expresión. | Defensores ambientales y de la tierra. | Organización defensora de DD. HH. y sus integrantes. |
| **Patrón de violencia analizado** | Violencia sexual como mecanismo de censura indirecta y silenciamiento. | Violencia letal y no letal contra defensores en contexto de disputa territorial e impunidad estructural. | Vigilancia ilegal, estigmatización, amenazas y atentados como política sistemática. |
| **Calificación jurídica de la violencia** | Violencia sexual = violación grave de DD. HH. + restricción indirecta a la libertad de expresión. | Violencia contra PDDH = violación al derecho a la vida e integridad con deber reforzado de prevención. | Violencia y vigilancia estatal = violación múltiple con responsabilidad directa del Estado. |
| **Deber de investigación** | Debida diligencia reforzada con enfoque de género, hipótesis ligadas al ejercicio periodístico. | Investigación seria, en plazo razonable, orientada a desmantelar la impunidad. | Investigación reforzada, con análisis de patrones y responsabilidad estatal. |
| **Uso del poder estatal / fuerza** | Prohibición de tolerar o permitir violencia sexual como forma de control o castigo. | Responsabilidad por omisión estatal frente a riesgos previsibles. | Prohibición de uso del aparato estatal (inteligencia, vigilancia) para perseguir PDDH. |
| **Sistema de información (orden expresa)** | Orden expresa de crear sistema nacional de datos (1 año). | Orden expresa de crear sistema nacional de datos (2 años). | Orden expresa de crear sistema nacional de datos (1 año). |
| **Función del sistema de datos** | Derivada: registrar violencia sexual, censura indirecta y género para prevención. | Dimensionar magnitud real de la violencia y orientar políticas públicas. | Medir patrones, judicialización, control del poder estatal y no repetición. |
| **Desagregación exigida** | Enfoque de género (mujeres periodistas). | Territorio, etnia, militancia, género y edad. | Territorio, ámbito de acción, género y otros enfoques diferenciales. |
| **Indicadores de judicialización** | Implícitos (impunidad como forma de censura). | Acusaciones, condenas y absoluciones. | Investigaciones, acusaciones, condenas y absoluciones. |
| **Publicidad y datos personales** | Protección reforzada de la dignidad e intimidad de la víctima. | Difusión anual con reserva de identidad. | Difusión anual con salvaguardas de datos personales. |
| **Garantías de no repetición** | Sistema de datos + reformas estructurales, capacitación, enfoque de género | Sistema de datos + grupo de trabajo contra impunidad. | Sistema de datos + rendición de cuentas y control institucional. |
| **Aporte principal al estándar interamericano** | Reconoce la violencia sexual como censura indirecta y exige enfoque de género. | Establece que sin datos no hay prevención ni política pública. | Consolida el sistema de información como obligación autónoma y herramienta de control estatal. |



# V. Elementos básicos de un sistema de información

Los sistemas de información se basan en una arquitectura integrada por tres componentes esenciales: en primer lugar, la infraestructura física y los servidores (*hardware*); en segundo lugar, los programas y algoritmos (*software*) y, en tercer lugar, el equipo humano que diseña y opera los procesos. Las pautas desarrolladas en este documento están enfocadas primordialmente en el pilar de *software* o los programas del sistema que permiten gestionar el ciclo de vida de los datos[44].

Para que el sistema de información sobre personas defensoras cumpla su función debe contar con i) un mecanismo de ingreso de datos de calidad, ii) un procesamiento que permita organizar y analizar la información, y iii) productos útiles y oportunos que permitan transformar esos datos en conocimiento para garantizar el derecho a defender derechos, prevenir y proteger frente a riesgos y violencias, investigar eventos de hostigamiento, causas próximas y factores de riesgo, y mitigar y reparar los daños.

La efectividad de los sistemas de información depende directamente de la calidad de la información ingresada, de las decisiones tomadas en su procesamiento y de los resultados producidos. En el caso de las bases de datos relacionadas con violaciones a derechos humanos, es frecuente que estas presenten sesgos vinculados

**44** Agradecemos al equipo de GRIL de Berkeley por sus invaluables aportes al documento y en particular a las secciones interdisciplinarias y el desarrollo de la taxonomía sobre criminalización.

a enfoques o competencias institucionales diferenciadas, dificultades para recoger determinada información, perspectivas de quienes analizan los datos, entre otros factores. Los sesgos pueden ocurrir porque cada fuente –ya sea del Estado, de organizaciones de la sociedad civil u otros actores– posee un alcance de observación limitado, generando vacíos que impiden considerar la información disponible como una representación completa del fenómeno. Cuando ciertos campos faltan de manera sistemática o ciertos casos nunca se documentan, la base de datos deja de ser una representación neutral del fenómeno y pasa a reflejar desigualdades de acceso, visibilidad y poder. En este sentido, la interpretación de cualquier resultado exige comprender cómo las ausencias en la información ingresada pueden introducir sesgos que afecten los resultados obtenidos, y evaluar si el sistema elegido permite reducir esos efectos mediante el procesamiento de los datos o si simplemente los reproduce. Esto alerta sobre la importancia de recoger datos fiables de diversas fuentes y de brindar pautas relevantes para su procesamiento.

La multiplicidad de fuentes de información relevantes para entender los fenómenos que afectan a las personas defensoras también tiene implicancias para el diseño del sistema de información. En particular, obliga a definir una arquitectura capaz de trabajar con información proveniente de fuentes diversas de manera fiable, contrastable y metodológicamente robusta. Para ello, se identifican dos estructuras recomendadas: un repositorio de datos o una base de datos integrada de un repositorio.

> **La opción del repositorio de datos** consiste en centralizar información proveniente de múltiples fuentes, manteniendo la identidad original de cada base. El repositorio funciona como un entorno común de almacenamiento y consulta capaz de incorporar distintos tipos de datos –bases estructuradas, informes, mapas u otros documentos relevantes–, preservando la trazabilidad de la fuente original. Esta modalidad facilita el acceso, la comparación y el contraste de información proveniente de distintas entidades, permite incorporar indicadores y fuentes complementarias para enriquecer el análisis, y favorece la protección de información sensible mediante mecanismos de anonimización y controles diferenciados de acceso. No obstante, por sí sola esta opción no resuelve las duplicaciones entre fuentes ni permite estimar el subregistro, por lo que su capacidad analítica es limitada.

> Por otro lado, **la base de datos integrada de un repositorio** constituye un nivel más avanzado de integración de información. A diferencia del repositorio

de datos, no se limita a acopiar diversas fuentes, sino que las consolida en una única base analítica, deduplicando registros mediante técnicas de vinculación o deduplicación (*record linkage*). Esto permite identificar cuándo distintas fuentes se refieren al mismo hecho o a la misma persona (solapamientos), conservando la trazabilidad respecto de las fuentes originales, y estimar el subregistro mediante métodos estadísticos como la Estimación por Sistemas Múltiples[45]. Es la opción más robusta para el análisis de patrones y tendencias, pero también la más exigente en términos técnicos, operativos y de coordinación interinstitucional. En términos generales, permite ir más allá de lo reportado y estimar el universo de casos. Esta diferencia es clave en contextos donde la información es fragmentada y existen vacíos sistemáticos en el registro de violaciones a derechos humanos.

Cabe señalar que existe una opción más básica: **una nueva base de datos estructurada o semiestructurada,** es decir un sistema creado desde cero, con una estructura propia de recolección. Su ventaja es que permite estandarizar los datos desde el inicio y mantener el control total sobre las variables y los procesos de captura. Sin embargo, se limita a la información que la entidad logra documentar, reproduce sesgos de observación y no permite estimar el subregistro ni contrastar múltiples fuentes. Este tipo de base de datos puede resultar útil en contextos en los que no se cuenta con información, pero para una buena parte de las situaciones nacionales existen múltiples instituciones y organizaciones que recogen información relevante[46]. Por ello, si bien una base propia es fundamental para producir información oficial, la necesidad de contrastar datos y enriquecer el análisis con diversas fuentes hace recomendable optar por un repositorio o una base de datos integrada.

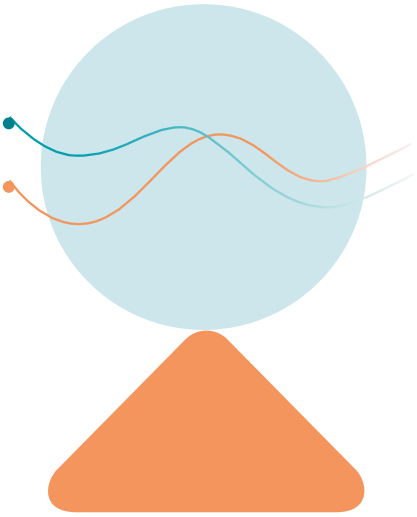
Sin embargo, vale la pena resaltar que estas opciones de estructura del sistema de información no son excluyentes entre sí. Es posible que una entidad u organización desarrolle una base de datos nueva, que esta sea incorporada a un repositorio

**45** Para ver ejemplos sobre el deber de los Estados de garantizar el derecho a la verdad y utilizar métodos estadísticos como este, ver: Alejandro Jiménez Ospina et al. *Contar la Verdad. Estadística en la Develación de Patrones de Violencia. Bogotá, Dejusticia. Diciembre 2022.*

**46** Por ejemplo, datos sobre homicidios, datos de lesiones, de procesos penales o judiciales en curso respecto de agresiones contra personas defensoras en cabeza de instituciones nacionales de derechos humanos, ministerios vinculados con temas de seguridad y justicia, fiscalías, comisiones de la verdad, organizaciones no gubernamentales, órganos y organismos internacionales, entre otros.

junto con otras bases, y que forme parte de una base integrada. Más aún, independientemente de la opción elegida, la utilidad del sistema dependerá de la calidad del *input*, de las decisiones metodológicas adoptadas durante su procesamiento y de la capacidad para identificar y mitigar problemas de sesgo y subregistro. Además, algunos de los posibles usos del sistema, así como su alcance y calidad, variarán en función del nivel de integración alcanzado. En este marco, teniendo en cuenta las funciones esperables del sistema de información para personas defensoras, resulta deseable avanzar progresivamente hacia una base integrada que permita comprender y abordar mejor el fenómeno de agresiones contra las PDDH, así como fortalecer las respuestas de prevención, protección, investigación y rendición de cuentas.

Teniendo en cuenta estas consideraciones, las secciones siguientes desarrollan algunos de los elementos centrales para el diseño de sistemas de información sobre personas defensoras, incluyendo las categorías sustantivas que deben estructurar el sistema, las reglas para la gestión y el procesamiento de los datos, y los productos analíticos y operativos que pueden derivarse de la información recopilada, a la luz de los estándares internacionales y la práctica comparada.



# VI. Las categorías que estructuran el sistema de información

A partir de los objetivos del sistema de información, esta sección presenta un estándar de referencia de las categorías y variables recomendadas. Su selección responde a una doble fuente: por un lado, los estándares internacionales, regionales y domésticos que identifican los elementos que todo sistema de esta naturaleza debe capturar; por otro, el mapeo comparado de un conjunto de sistemas de información, informes y bases de datos existentes en Colombia, así como de algunas experiencias regionales relevantes[47]. Este ejercicio permitió identificar tanto las coincidencias estructurales entre registros como los vacíos recurrentes que una arquitectura nueva puede y debe corregir[48].

> A partir de estas fuentes, el sistema se organiza en torno a seis categorías analíticas, que responden a preguntas distintas –i) quién es la persona defensora, ii) qué hechos u omisiones la afectan, iii) en qué términos se produce un uso abusivo del derecho en su contra, iv) cómo responde el Estado ante el hecho, v) quiénes son los presuntos responsables y vi) en qué contexto se inscribe

**47** Para más información sobre la metodología, ver sección 1 del documento.

**48** Es de esperar que no todas las bases de datos documenten todas las variables presentadas en esta sección. No obstante, este listado corresponde a las variables claves identificadas en la investigación para analizar y comprender el fenómeno de la violencia contra PDDH, a la luz de las obligaciones internacionales de los Estado.

> el riesgo–. Aunque cada una aborda un interrogante propio, están diseñadas para operar de manera relacional.

El valor del sistema de información no reside en la suma aislada de categorías o variables, sino en la posibilidad de relacionarlas entre sí. Estas categorías constituyen un piso mínimo que permite identificar patrones, establecer asociaciones relevantes y generar conocimiento útil para la prevención, la protección, la investigación, la reparación y las garantías de no repetición. Es precisamente esta lógica relacional lo que convierte un registro de eventos en una herramienta útil para la toma de decisiones y la formulación de respuestas institucionales basadas en evidencia.

Cabe remarcar que este estándar opera como un marco de referencia y no como un modelo rígido de implementación. No todas las jurisdicciones deberán implementar cada campo desde la fase inicial: el universo de variables propuesto busca cubrir las modalidades actualmente documentadas en los estándares internacionales, los registros comparados y las experiencias regionales mencionadas al inicio del documento, pero su adopción puede ser progresiva y adaptarse a las prioridades, capacidades y realidades de cada contexto nacional o local.

A continuación, se desarrollan cada una de las seis categorías analíticas, sus subcategorías y variables específicas. Éstas pueden aplicarse a diferentes tipos de datos, incluyendo datos estructurados, no estructurados o semiestructurados, tales como hojas de cálculo, informes narrativos o formularios de denuncia. El Anexo I, al final del documento, presenta una tabla consolidada con el conjunto de categorías, subcategorías y variables propuestas.

### a. Las personas defensoras

En primer lugar, el sistema se construye con base en una comprensión amplia de *quiénes son* las personas defensoras de derechos humanos. El punto de partida es la definición de la persona defensora que ha establecido la Corte IDH basada en los desarrollos de Naciones Unidas en la materia[49]. Allí se indica que:

**49** Asamblea General. Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, Resolución A/RES/53/144, 1998.

> "la calidad de persona defensora [...] está determinada por la naturaleza misma de las actividades desarrolladas, sin importar si se ejercen en forma ocasional o permanente, en el campo público o privado, de manera colectiva o individual, a nivel local, nacional o internacional, o si se contraen a específicos derechos civiles, políticos, económicos, sociales, culturales o ambientales, o se amplían al conjunto de estos"[50].

A partir de esta premisa, la categoría *PDDH o víctima* no busca construir un censo cerrado, sino registrar los eventos teniendo en cuenta aquellas características individuales y colectivas que permitan comprender los riesgos diferenciados e identificar las dinámicas y los patrones asociados al fenómeno, en función de los objetivos del sistema, incluida la prevención, la protección, la investigación de los hechos y la reparación de las víctimas. En el contexto de las Américas, resulta particularmente relevante identificar la pertenencia o asociación actual o previa a movimientos sociales, procesos organizativos, organizaciones no gubernamentales, entre otros.

El registro de cada evento de agresión contra personas defensoras requiere tomar en cuenta una serie de variables demográficas relativas a sus características personales e interseccionales, condiciones socioeconómicas, labor de defensa, antecedentes de riesgo y vínculos con procesos de defensa de derechos u organizaciones. Entre los parámetros determinados por los estándares de derecho internacional se identifican, entre otros, el sexo y género, edad, lengua, pertenencia étnica o racial, orientación sexual, discapacidad, nacionalidad, situación migratoria, ocupación, profesión, educación, estatus socioeconómico, lugar de residencia, lugar de trabajo, pertenencia organizativa, afiliación institucional, militancia, tipo de liderazgo, sector o temática vinculada a su labor[51]. Dado que varias de estas variables son datos sensibles, su incorporación al sistema debe acompañarse de las salvaguardas de privacidad, seguridad y no daño que se detallan en la sección siete.

Estas variables permiten registrar aspectos individuales y colectivos importantes para entender patrones de riesgo, modalidades de agresión e impactos. Desde

---

**50** Corte IDH. Caso *Zapata vs. Colombia*, Sentencia de 3 de octubre de 2025, Serie C No. 569, párr. 237.

**51** Ver sección 4 del documento. Corte IDH. *Caso Sales Pimenta vs. Brasil*, Sentencia de 30 de junio de 2022, Serie C No. 454, párr. 178; Corte IDH. *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, Sentencia de 21 de junio de 2023, Serie C No. 504, párr. 1047; Corte IDH. *Opinión Consultiva OC-32/35 (Emergencia Climática y Derechos Humanos)*, 29 de mayo de 2025, Serie A No. 32, párr. 512.

luego, la especificidad de las categorías y el nivel de desagregación deberán adaptarse a las realidades nacionales o locales. Por ejemplo, en Brasil resulta relevante identificar categorías de pueblos y comunidades tradicionales, como las comunidades *ribeirinhas,* cuya forma de vida se encuentra estrechamente vinculada a los ecosistemas fluviales y tienen un papel central en la defensa de las aguas, o las comunidades *quilombolas* –comunidades negras, rurales y urbanas, autoidentificadas y caracterizadas por vínculos históricos y colectivos con sus territorios, formas propias de organización social, cultural y política y trayectorias históricas de resistencia a la esclavitud–. De manera análoga, en Ecuador resulta pertinente reconocer como categoría al pueblo montubio, un pueblo campesino del litoral, con identidad cultural propia, formas asociativas de organización y reconocimiento constitucional como sujeto de derechos colectivos. La incorporación de estas categorías permite visibilizar riesgos, conflictos y formas de afectación que podrían permanecer ocultos bajo clasificaciones más generales. De igual manera, en países de la región caracterizados por una importante diversidad étnica y cultural, resulta fundamental reconocer las categorías propias de autoidentificación o las lenguas de los pueblos y comunidades tradicionales.

### b. Eventos y tipo de agresión

La segunda dimensión sustantiva corresponde al registro de los hechos y omisiones que constituyen *agresión* contra las personas defensoras, así como la determinación del tipo de agresión documentada.

La agresión no se agota en actos letales o físicamente violentos, sino que abarca un continuo de conductas que incluyen la estigmatización, la vigilancia, las amenazas y el desplazamiento, así como otros ataques directos y formas de hostigamiento administrativo, económico, legal y digital. Esta comprensión de las agresiones incluye, de manera expresa, acciones y omisiones estatales, porque solo así es posible capturar el rol del Estado como eventual perpetrador, ya sea por vulnerar directamente los derechos o por incumplir sus deberes de garantía cuando no actúa con la debida diligencia para prevenir, investigar, sancionar o reparar. El valor analítico del registro no reside únicamente en la identificación aislada del hecho o de la omisión, sino en la posibilidad de interpretarlos en clave relacional. Más adelante realizaremos algunas precisiones sobre manejo de datos, metadatos mínimos, deduplicación, sistemas de salvaguarda y procesamiento para asegurar su uso adecuado.

Las categorías utilizadas para registrar los diversos tipos de agresiones deben reflejar la diversidad de marcos normativos relevantes –incluidos el derecho internacional, el derecho penal y el derecho constitucional– así como los patrones emergentes de vulneración de derechos que afectan a las personas defensoras. Entre ellas: homicidio, tentativa de homicidio, desaparición forzada, desaparición temporal, detención preventiva arbitraria, criminalización, lesiones, tortura, tratos crueles o inhumanos, violencia de género, violencia sexual, tortura sexual, esclavitud, esclavitud sexual, reclutamiento forzado, confinamiento, desplazamiento forzado, desalojo forzado, exilio, amenazas, hostigamiento, intimidación, campañas de estigmatización, discriminación, difamación, instigación a la violencia, *doxxing*; vigilancia ilegal, interceptación de comunicaciones, uso de spyware o malware, apagones de internet (internet *shutdowns*), desactivación de tarjetas SIM, bloqueo o interrupción de servicios de mensajería instantánea, cierres o suspensiones de organizaciones, obstáculos administrativos, restricciones indirectas, multas, ataques a sedes, ataques a comunidades, daños a bienes colectivos, ataques a territorios, entre otros.

Ahora bien, uno de los patrones de vulneración de derechos que ha afectado de manera recurrente a defensoras ambientales, líderes indígenas y periodistas es la criminalización o el uso indebido de la capacidad punitiva del Estado promovido por diversos actores. Sin embargo, la documentación de esta categoría no es sencilla porque implica una valoración sobre el uso de un poder legítimo del Estado y porque hay discrepancias en su abordaje por diversas instituciones y organizaciones. Por ello, a continuación, se desarrolla con mayor detalle la categoría de criminalización, con el fin de contribuir a su adecuada conceptualización, documentación y análisis dentro del sistema de información.

### c. Criminalización

La criminalización de PDDH constituye una táctica frecuente para silenciar, desacreditar, tomar represalias o restringir la capacidad de las personas defensoras para ejercer su labor[52]. En esa misma línea, diversos órganos de protección y organizaciones especializadas reconocen dicho fenómeno como una de las formas

**52** La CIDH la ha caracterizado como "el uso indebido del derecho penal a través de la manipulación del poder punitivo del Estado por parte de actores estatales y no estatales con el objetivo de obstaculizar sus labores de defensa y así impedir el ejercicio legítimo de su derecho a defender los derechos humanos". Ver: CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas, OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, párr. 150.*

más relevantes de restringir el accionar de las personas defensoras de derechos humanos y el espacio cívico[53].

La Corte IDH afirma que: "el Estado tiene el deber de investigar denuncias, pero esta responsabilidad no se puede desviar de forma en que se utilice [su] poder punitivo [...] como herramienta de persecución, especialmente contemplando el contexto de violencia contra personas defensoras de derechos humanos"[54]. Ahora bien, la documentación de la criminalización puede ser más compleja que la de otros fenómenos porque implica generalmente evaluar el posible uso indebido de facultades que, en principio, constituyen expresiones legítimas del poder estatal para la protección de derechos de otras personas, corporaciones o de intereses públicos. Esta es una de las razones por las que el fenómeno es uno de los menos documentados dentro de las categorías de conductas inhibitorias del derecho a defender derechos.

En un esfuerzo para superar este subregistro, a continuación, se desarrolla una definición operativa de la categoría y proponemos un conjunto de subcategorías y variables destinadas a facilitar su documentación dentro del sistema de información sobre personas defensoras.

La formulación de la criminalización se encuentra asociada principalmente al ámbito penal. Sin embargo, en la práctica el uso punitivo del derecho puede operar también a través de la responsabilidad civil, del derecho administrativo, el tributario y de otras ramas del ordenamiento jurídico. Ahora bien, la literatura ofrece diversas definiciones de la criminalización. Estas abarcan desde enfoques que incluyen discursos estigmatizantes y campañas de desinformación hasta aquellos que consideran suficiente el inicio de cualquier proceso judicial contra una persona defensora, así como aproximaciones más amplias relacionadas con el litigio estratégico contra la sociedad civil y el litigio abusivo promovido por corporaciones. Con base en estos desarrollos y en

---

**53** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas*, OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025; CIDH y OACNUDH. Garantizar el espacio cívico es proteger el derecho a defender derechos, comunicado de prensa, 9 de diciembre de 2025; Mary Lawlor, Relatora Especial sobre la situación de las personas defensoras de derechos humanos. *Informe al Consejo de Derechos Humanos, A/HRC/61/40, 5 de enero de 2026;* Front Line Defenders. *Global Analysis 2025/26,* 2026. Disponible en: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf

**54** Corte IDH. Caso *Zapata vs. Colombia*, Sentencia de 3 de octubre de 2025, Serie C No. 569, párr. 198.

los patrones relevantes para las personas defensoras de derechos humanos, estos lineamientos adoptan una definición operativa de la criminalización más acotada, reservando otros fenómenos importantes en diversas categorías de agresiones.

A los efectos de estos lineamientos la criminalización consiste en el uso indebido del derecho penal, civil u otras ramas del derecho por actores estatales y no estatales con el fin o la consecuencia de inhibir, restringir o silenciar la defensa de los derechos humanos por medio de la manipulación del poder punitivo del Estado.

La falta de documentación sistemática de esta categoría en las bases de datos existentes sobre personas defensoras llevó a que este *Blueprint* otorgue especial atención a los campos necesarios para su adecuada identificación. En efecto, se propone organizar la categoría en tres ejes que responden a distintos matices del fenómeno: i) la criminalización *per se,* ii) los abusos del poder punitivo del Estado y iii) las demandas estratégicas contra la participación pública iniciada por actores privados o empresas.

En primer lugar, se distinguen una serie de supuestos que constituyen criminalización per se, en la medida en que su mera constatación permite clasificar el evento dentro de esta categoría sin necesidad de análisis adicional. En términos generales, se refiere a la aplicación de normas incompatibles con las obligaciones internacionales del Estado, o de actuaciones dirigidas contra conductas categóricamente protegidas por el derecho internacional. Se trata de casos claros, en los que no se requiere un análisis adicional del contexto para concluir que existe un uso abusivo del poder punitivo. Bajo esta categoría se agrupan cuatro subcategorías, con sus variables correspondientes. La primera comprende la criminalización de conductas protegidas por la libertad de expresión ya sea mediante la aplicación de figuras de desacato, calumnia o difamación[55], y otras conductas similares[56]. La segunda subcategoría refiere a la actuación punitiva del Estado sin sustento legal, esto es, los casos en que el Estado inicia o mantiene medidas punitivas sin una justificación jurídica adecuada. Su variable paradigmática es la detención arbitraria con posterioridad a

**55** CIDH, *Criminalización de la labor de las defensoras y los defensores de derechos humanos*, OEA/Ser.L/V/II, Doc. 49/15, 31 de diciembre de 2015, párr. 94.

**56** Asamblea General. Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, Resolución A/RES/53/144, 1998, art. 13. Allí, se plantea como criminalizante la formulación cargos por recibir financiación extranjera, en tanto la solicitud, recepción y uso de recursos para promover y proteger los derechos humanos constituye un derecho reconocido.

la culminación de una sentencia. El Grupo de Trabajo sobre la Detención Arbitraria (en adelante GTDA) califica como arbitraria toda privación de libertad respecto de la cual resulta evidentemente imposible invocar fundamento jurídico alguno, como ocurre cuando se mantiene a una persona detenida tras haber cumplido su condena o pese a una ley de amnistía que le sea aplicable[57]. Asimismo, el GTDA ha considerado que la detención secreta y la desaparición forzada constituyen privaciones de libertad arbitrarias *per se*, en tanto no admiten fundamento jurídico legítimo alguno. La tercera es el uso de fueros militares para juzgar a civiles[58]. Como variable, pueden considerarse los casos tramitados en la justicia militar en los que personas defensoras figuran como acusadas o testigos. Por último, la cuarta subcategoría comprende aquellos supuestos en los cuales un órgano internacional competente ya ha determinado la existencia de criminalización en el marco del examen de un caso o acción urgente, como puede ocurrir con decisiones de la Corte IDH, la CIDH, del GTDA o de otros procedimientos especiales u órganos de tratado.

En segundo lugar, se incorpora una serie de conductas bajo la categoría de abusos del poder punitivo estatal. Ellas comprenden situaciones frecuentes de posible uso ilegítimo de facultades que, en principio, constituyen expresiones legítimas del poder estatal. A diferencia de los supuestos de criminalización *per se,* estos casos suelen requerir una valoración contextual de la información disponible, ya sea a nivel individual o agregado, para determinar si efectivamente existe una criminalización. Esta categoría incluye actuaciones aparentemente válidas en el ejercicio de facultades penales, civiles o administrativas, pero que pueden operar como mecanismos de hostigamiento o restricción de la labor de defensa. Bajo esta categoría, es fundamental incluir: i) el uso abusivo de las facultades de investigación y acusación —por ejemplo, las investigaciones o los cargos múltiples, los procesos basados en la asociación o pertenencia, y los cargos vagos o agravados–; ii) la formulación de cargos falsos o infundados; iii) la dilación injustificada del proceso —demoras, secuenciación arbitraria, reprogramaciones o divulgación tardía de los cargos—; iv) la imposición de medidas cautelares desproporcionadas –como la detención preventiva arbitraria, la vigilancia y los allanamientos irrazonables, las fianzas excesivas, entre otras–; v) la imposición de

**57** Para esta categoría se siguen los criterios del Grupo de Trabajo sobre la Detención Arbitraria de Naciones Unidas (GTDA). Consejo de Derechos Humanos. *Métodos de trabajo del Grupo de Trabajo sobre la Detención Arbitraria*, U.N. Doc. A/HRC/36/38, 13 de julio de 2017, párr. 8 (categoría I).

**58** CIDH. *Informe sobre Terrorismo y Derechos Humanos*, OEA/Ser.L/V/II.116, Doc. 5 rev. 1 corr., 22 de octubre de 2002, párrs. 231-232; Corte IDH, *Caso Radilla Pacheco vs. México, Sentencia de 23 de noviembre de 2009, Serie C No. 209, párrs. 272-275.*

penas desproporcionadas –incluidas las multas excesivas y la disolución de organizaciones–; vi) las violaciones al debido proceso –limitaciones al derecho de defensa, obstrucción del acceso a la defensa técnica, retención de notificaciones o vulneración del *non bis in idem–;* y vii) el uso abusivo de procedimientos administrativos —como las prohibiciones de ingreso a terceros países—.

En tercer lugar, se incluyen las demandas estratégicas contra la participación pública (SLAPPs) en sentido estricto. Ellas constituyen litigios estratégicos iniciados por empresas u otros actores no estatales que, examinados a la luz de su propósito, buscan hostigar, desalentar o impedir la labor de las PDDH, y pueden dar lugar a una determinación de abuso del proceso judicial[59]. Este tipo de procesos ha prosperado en la región y en el mundo, acompañando estrategias corporativas orientadas a inhibir las conductas de denuncia o protesta y a generar un efecto amedrentador sobre el espacio cívico[60]. En ocasiones su poder inhibitorio está asociado a la posibilidad de imponer sentencias con indemnizaciones millonarias o de embargar bienes de personas y organizaciones. Entre algunas de las variables prevalentes para esta categoría se encuentran: las demandas por daños a la propiedad o la invasión de predios en el marco de la protesta o la defensa territorial; demandas por difamación y otras relacionadas con temas de libertad de expresión; los litigios derivados de protestas que afectan proyectos extractivos o de infraestructura; las demandas múltiples y simultáneas; y el uso abusivo de acciones de amparo de derechos fundamentales contra organizaciones o personas defensoras.

Dado que algunas manifestaciones de la criminalización pueden superponerse entre sí y con otras dimensiones del sistema, el diseño operativo deberá establecer criterios claros de clasificación y no duplicación. Esto resulta especialmente importante respecto de hechos susceptibles de ser registrados de manera simultánea como hostigamiento, vigilancia, estigmatización, agresión digital, sanción administrativa, judicialización abusiva o restricción al ejercicio de la labor de defensa. La utilidad del sistema dependerá, en definitiva, de su capacidad para preservar

---

**59** Business and Human Rights Resource Centre. *SLAPPS in Latin America: Strategic lawsuits against public participation in the context of business and human rights*, 2022. Disponible en: https://media.business-humanrights.org/media/documents/2022_SLAPPs_in_LatAm_EN_v7.pdf; Ver también: SLAPPs Database y recursos asociados. Disponibles en: https://www.business-humanrights.org/en/from-us/slapps-database/

**60** Business and Human Rights Resource Centre, SLAPPs Database y recursos asociados. Disponible en: https://www.business-humanrights.org/en/from-us/slapps-database/

la complejidad del fenómeno sin multiplicar artificialmente los registros ni perder consistencia analítica.

### d. Respuesta estatal frente al riesgo o al evento

#### i. Respuestas de prevención y protección

Un aspecto remarcado por el sistema interamericano consiste en solicitar que la *respuesta estatal frente al riesgo* sea plenamente observable en el sistema, no solo en cuanto a su existencia formal sino también en cuanto a su oportunidad, adecuación y eficacia material[61]. Esta categoría debe tener en cuenta varios aspectos relevantes en el desarrollo del sistema de información.

En la práctica la observación de la respuesta estatal supone un desplazamiento analítico. Es crucial constatar si el Estado actuó, pero también importa valorar si lo hizo a tiempo, si la medida adoptada fue proporcional y adecuada al riesgo identificado y a la persona o grupo a proteger, y si resultó idónea para neutralizarlo.

El seguimiento de los riesgos puede darse, además, a través de medidas individuales, colectivas o sistemas de alerta temprana que respondan a aquellos. Por ejemplo, en el caso de la Defensoría del Pueblo de Colombia, las alertas tempranas adquieren características diferenciadas según se emitan como alertas de inminencia o de carácter estructural[62].

El seguimiento de las respuestas de prevención y protección implica abarcar su ciclo completo y registrar de manera especialmente cuidadosa las agresiones o riesgos que originan las medidas, así como aquellos ocurridos durante la vigencia de esquemas de protección, pues tales eventos operan como indicadores de fallas del sistema y como prueba de que el deber de prevención no se satisface con la mera adopción formal de dispositivos.

A tal fin, el sistema debería registrar: la solicitud de protección y el estudio de riesgo correspondiente; el tiempo de respuesta; las medidas urgentes; los esquemas

---

**61** Corte IDH. *Caso Defensor de Derechos Humanos y otros vs. Guatemala*, Sentencia de 28 de agosto de 2014, Serie C No. 283, párrs. 157-158.

**62** República de Colombia. *Decreto 2124 de 2017*, 18 de diciembre de 2017, Diario Oficial de Colombia.

individuales, colectivos, territoriales o comunitarios; las medidas cautelares —internas o de la CIDH— y las medidas provisionales; la revisión periódica, modificación o terminación de los esquemas, con las razones de su retiro o levantamiento; el retorno seguro; y, transversalmente, la valoración de la suficiencia, adecuación y efectividad de tales medidas, incluidos los ataques ocurridos durante su vigencia.

En la misma lógica debe incorporarse el seguimiento de las alertas tempranas de carácter institucional, si están disponibles, tanto aquellas estructurales como las de inminencia. Dado que la información contenida en estos instrumentos no siempre se encuentra asociada a casos o personas individualizadas, el sistema debería prever un flujo de registro diferenciado para fuentes territoriales, contextuales y prospectivas de riesgo. Este flujo no debe forzar las alertas tempranas a la estructura del registro individual, sino permitir el análisis de unidades territoriales, temporales y contextuales, incluyendo el territorio cubierto, la población o colectivo potencialmente afectado, los factores de riesgo identificados, los repertorios de violencia advertidos, las recomendaciones emitidas, las entidades responsables de responder y las acciones efectivamente adoptadas. Así, las alertas tempranas no operarían como registros aislados, sino como información prospectiva correlacionable con la ocurrencia posterior de agresiones y con la oportunidad, suficiencia y efectividad de la respuesta estatal.

### ii. Justicia y la superación de la impunidad

El componente de *judicialización e impunidad* es central para valorar la eficacia de la intervención protectora o tutelar del Estado. Mientras la criminalización expresa un exceso del poder punitivo contra quienes ejercen la defensa de derechos, la impunidad expresa un déficit de ese mismo poder frente a quienes las agreden. Según la Corte IDH, ese déficit reiterado opera como factor de repetición y de consolidación de patrones de violencia[63].

Por ello, el sistema de información debe permitir registrar diversos aspectos de la respuesta judicial frente a las agresiones contra personas defensoras. En estos lineamientos se destacan tres de ellos: en primer lugar, los indicadores de avance y retrocesos procesales; en segundo lugar, aquellos que permiten registrar los distintos niveles y redes de responsabilidad criminal y, por último, la identificación de

**63** Corte IDH. *Caso Sales Pimenta vs. Brasil,* Sentencia de 30 de junio de 2022, Serie C No. 454, párr. 170.

garantías de acceso material y formal a la justicia. No obstante, dependiendo de los fenómenos que afecten a las PDDH puede resultar necesario generar categorías que trasciendan la respuesta penal y permitan evaluar otras vías de justicia o amparo de derechos, como el amparo constitucional de derechos o acción de tutela, la eficacia de la justicia civil, entre otros. Sin embargo, dada la importancia que los procesos penales suelen ocupar en la búsqueda de justicia, en estos lineamientos se desarrollan primordialmente las variables vinculadas a dicha categoría.

Para comenzar, resulta fundamental trazar el recorrido procesal completo de cada caso –sus avances y retrocesos– y asociar cada hito a los plazos procesales correspondientes, a fin de evaluar el cumplimiento del plazo razonable. Del estándar de debida diligencia y plazo razonable desarrollados por la Corte IDH se desprende la necesidad de registrar, como mínimo, una serie de categorías: las denuncias, las investigaciones abiertas o en curso, las acusaciones, las condenas, las apelaciones, la condena en firme, la prisión efectiva y las absoluciones. Cabe destacar nuevamente que, dependiendo de la naturaleza del caso, el curso del proceso puede no seguir las etapas del proceso penal, por ejemplo, en situaciones donde la protección depende de demandas civiles, tutelas u otras acciones constitucionales.

Adicionalmente, la jurisprudencia del tribunal interamericano generalmente ordena el establecimiento de diversos tipos de autoría y participación en las violaciones de derechos que constata. Ello comprende la determinación de autores materiales e intelectuales, la investigación de las cadenas de mando y la identificación de diversos actores que financian, auxilian o actúan con aquiescencia frente al crimen, así como los niveles de planificación[64]. Tales categorías deben expresarse conforme a las tradiciones del derecho penal nacional o comparado del país que corresponda[65].

Por último, un sistema más integral también debería incorporar indicadores capaces de identificar la accesibilidad de los mecanismos de justicia y las condiciones institucionales más amplias que inciden en la respuesta institucional frente a la impunidad. En este sentido, es posible evaluar si se consideró el posible nexo causal entre el hecho y la labor de defensa, si la investigación incorporó un análisis contextual de

**64** Corte IDH. *Caso Manuel Cepeda Vargas vs. Colombia*. Sentencia de 26 de mayo de 2010. Serie C No. 213, párr. 119, 216,

**65** Corte IDH. *Caso Manuel Cepeda Vargas vs. Colombia*. Sentencia de 26 de mayo de 2010. Serie C No. 213, párr. 216.

los riesgos y patrones asociados, o el tipo de pena impuesta. A ello deben sumarse indicadores agregados sobre el funcionamiento del sistema de justicia, tales como su independencia e imparcialidad, la autonomía de los órganos de investigación y juzgamiento, la existencia de fiscalías o unidades especializadas, la capacidad institucional —número y formación de investigadores, carga procesal y recursos asignados— y los niveles de corrupción[66]. A ello deben sumar indicadores de desempeño que sirvan como herramienta de rendición de cuentas frente a la impunidad estructural, tales como las demoras en los procesos y las estadísticas oficiales de esclarecimiento[67].

### e. Presuntos perpetradores

La identificación de los *presuntos perpetradores y redes de responsabilidad* es una categoría analítica indispensable para entender los riesgos afrontados por las PDDH y cerrar ciclos de impunidad. Su incorporación al sistema no constituye un juicio anticipado sobre responsabilidades individuales ni una determinación de culpabilidad. A los efectos del sistema, las redes de responsabilidad comprenden tanto a los presuntos perpetradores individuales como a las organizaciones o grupos —de carácter legal o ilegal— a los que pertenecen, así como a las instituciones que puedan estar vinculadas a crímenes u hostigamientos contra personas defensoras. Esto permite abordar las investigaciones con un enfoque macrocriminal cuando es pertinente.

El sistema de información debe permitir caracterizar patrones asociados a individuos, grupos e instituciones, distinguiendo entre agentes estatales, actores no estatales y actores empresariales, entre otros. Esta distinción es jurídicamente relevante porque, conforme a los estándares interamericanos y universales, el Estado responde no solo por la conducta directa de sus agentes sino también por los hechos de particulares cuando media aquiescencia, tolerancia o incumplimiento del deber de debida diligencia[68].

---

**66** CIDH. *Garantías para la independencia de las y los operadores de justicia. Hacia el fortalecimiento del acceso a la justicia y el estado de derecho en las Américas*, OEA/Ser.L/V/II, Doc. 44, 5 de diciembre de 2013, párrs. 15-37, 49; CIDH. *Corrupción y derechos humanos: estándares interamericanos*, OEA/Ser.L/V/II, Doc. 236, 6 de diciembre de 2019, párr. 288

**67** CIDH. *Tercer informe sobre la situación de las personas defensoras de derechos humanos en las Américas, OEA/Ser.L/V/II, Doc. 119/25, 15 de abril de 2025, párr. 183-185*

**68** Corte IDH. *Caso Velásquez Rodríguez vs. Honduras*, Sentencia de 29 de julio de 1988, Serie C No. 4, párrs. 172-174.

Entre las subcategorías que el sistema debería contemplar se encuentran, en primer lugar, los agentes estatales, como jueces, fiscales, integrantes de la fuerza pública, funcionarios públicos y autoridades locales, entre otros. En segundo lugar, los actores no estatales, incluidos los grupos armados organizados, diversos grupos ilegales, paramilitares u otras estructuras criminales a definir en función de dinámicas locales, nacionales, regionales y mundiales[69] y los actores no estatales individuales. En tercer lugar, las personas jurídicas o actores empresariales, entre ellos corporaciones, empresas, contratistas y terceros financiadores[70]. Por último, el sistema debería permitir identificar las formas de articulación entre actores, tales como los arreglos mixtos, la subcontratación criminal o la actuación conjunta de redes que combinan agentes estatales y no estatales.

El registro sistemático de estas variables permite identificar patrones de recurrencia por tipo de actor, reconocer territorios y sectores especialmente afectados por determinadas violencias y evaluar el cumplimiento de las obligaciones estatales de prevención y sanción.

### f. Contexto

El *contexto* constituye una dimensión indispensable del sistema porque muchos riesgos contra las personas defensoras solo adquieren sentido cuando se leen contra el trasfondo estructural en el que ocurren. Un homicidio, una amenaza o una agresión digital, considerados de forma aislada, pueden parecer hechos inconexos, pero al cruzarlos con otras variables –ruralidad, presencia de actores armados legales e ilegales, economías ilícitas, conflictividad socioambiental, megaproyectos extractivos o de infraestructura, procesos de licenciamiento ambiental, debilidad institucional, impunidad histórica o coyunturas electorales– revelan patrones sectoriales de persecución, impactos diferenciados en el territorio (municipios, regiones o dinámicas transnacionales) y su evolución en el tiempo.

---

**69** A modo de ejemplo, ver: Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Global Study on Homicide 2023. Homicide and organized crime in Latin America and the Caribbean, 2023*. Asimismo, en un ejercicio de mapeo de redes criminales con actuación regional, el proyecto *Amazon Underworld* —de InfoAmazonia, Armando.info y La Liga Contra el Silencio— identifica algunas de las relevantes para los fenómenos transnacionales, al cartografiar la presencia de grupos armados y economías criminales en las zonas fronterizas de la Amazonía (Bolivia, Brasil, Colombia, Ecuador, Perú y Venezuela). Disponible en: https://amazonunderworld.org/map/

**70** Al respecto, ver: Business and Human Rights Resource Centre, SLAPPs Database y recursos asociados. Disponibles en https://www.business-humanrights.org/en/from-us/slapps-database/

El sistema de información debe habilitar la conexión entre hechos individuales, distintos tipos de agresión y entornos estructurales de riesgo. Esta lectura relacional debería permitir identificar el impacto de tres tipos de elementos: las variables estructurales, los patrones y los predictores de violencia o vulnerabilidad.

Entre las variables estructurales podrían incluirse, a modo de ejemplo, las áreas de especial conflictividad, la ausencia estatal, la presencia de actores armados legales o ilegales, las economías ilícitas, los niveles de corrupción –medidos, por ejemplo, a través del Índice de Percepción de Corrupción[71]–, la información socioeconómica de la región, las tasas asociadas a la violencia –como el homicidio, feminicidio, lesiones, masacres, secuestro, violencia sexual, trata de personas, reclutamiento forzado, trabajo esclavo–, y los indicadores educativos, como la escolaridad y la deserción escolar.

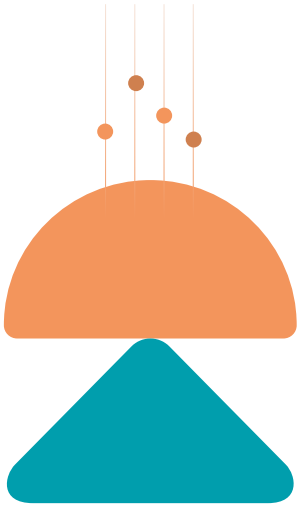
En cuanto a la identificación de patrones, el sistema debería tener en cuenta dinámicas relevantes para la labor de defensa en la zona, que pueden afectarla de manera directa o indirecta. Por ejemplo, los patrones de desaparición forzada, de persecución, confinamiento, reclutamiento forzado, deforestación, impunidad, entre otros. Pero también identificar patrones complejos que solo emergen del cruce de fuentes y variables distintas. Por ejemplo, la combinación de variables sobre presencia de grupos armados, economías ilícitas, tasas de homicidio y deserción escolar puede revelar riesgo de reclutamiento en zonas donde no existen denuncias directas. Del mismo modo, los datos de una fuente pueden evidenciar el subregistro de otra; mientras que el análisis de corredores territoriales, más allá de los límites municipales, puede mostrar dinámicas de expansión, control y disputa territorial que ayudan a identificar la victimización de personas defensoras en territorios específicos.

Adicionalmente, el conocimiento en profundidad de determinados fenómenos puede permitir identificar predictores de violencia: indicadores con valor prospectivo para esclarecer dinámicas, modular las respuestas institucionales y prevenir agresiones futuras. Algunos de estos indicadores dependerán de los fenómenos a documentar y de la información analítica producida mediante estudios cualitativos, pudiendo posteriormente alimentar modelos de predicción. Estos indicadores pueden expresarse tanto a través de hechos observables como de indicadores indirectos

**71** Para más información, ver: https://www.transparency.org/en/cpi/2025

o ausencias significativas de información. Así, por ejemplo, los cortes de internet han sido identificados como un predictor de escaladas de violencia, incluidas masacres y episodios de represión policial a nivel global. Otros posibles predictores incluyen los desplazamientos masivos y súbitos de poblaciones, los contextos electorales, los procesos de licenciamiento ambiental en países con debilidad institucional o las disputas entre grupos armados ilegales.

Esta capacidad de análisis contextual constituye una condición necesaria para que el Estado pueda prevenir riesgos previsibles, investigar los hechos, sancionar a los responsables y garantizar la reparación de las víctimas.



# VII. Manejo de datos

El manejo de datos es una condición central para la validez, la confiabilidad y la utilidad del sistema de información. Las decisiones sobre cómo se identifica, describe, vincula, protege y conserva cada registro determinan si el sistema será trazable, interoperable, confiable, seguro y, sobre todo, si será útil para la prevención, la protección, la investigación, la rendición de cuentas, la reparación y las garantías de no repetición. Esta sección precisa las reglas comunes que atraviesan todas las categorías: el codebook y las reglas de codificación, los metadatos mínimos, los criterios de deduplicación,  la homologación, normalización e interoperabilidad de datos, y las salvaguardas para proteger la información frente a usos indebidos o riesgosos.

A efectos del manejo de datos, conviene distinguir los diferentes tipos de información que el sistema procesa, que se corresponden con las categorías desarrolladas en la sección anterior. Cada tipo exige un tratamiento diferenciado en materia de metadatos, deduplicación y nivel de protección.

Las fuentes no siempre ofrecen información con el mismo nivel de detalle. El mapeo comparado muestra que algunas contienen registros individuales o de incidentes específicos, mientras que otras presentan información agregada, informes periódicos, reportes narrativos o documentos analíticos. Por ello, el sistema debe distinguir con claridad entre campos obligatorios, recomendados, condicionales y no aplicables. Cuando un campo no pueda diligenciarse, el sistema debe diferenciar la causa mediante estados como «No aplica», «No disponible» –el dato podría existir, pero no fue capturado– y «No verificable» –el dato existe pero no ha superado

el umbral de verificación–. Esta distinción ayuda a no confundir la falta de datos en una fuente con la ausencia del problema que se busca documentar.

### a. Codebook y reglas de codificación

El codebook es un documento auxiliar —típicamente una tabla o un conjunto de tablas— que define, para cada variable que el sistema captura, su contenido conceptual y las reglas para su codificación. Como mínimo, el codebook de cada sistema debería incorporar la definición conceptual de cada variable, su tipo de dato, los valores admitidos cuando la variable es categórica, las reglas para decidir entre valores ambiguos, ejemplos de casos típicos y casos límite, y los criterios específicos para distinguir, en cada variable, entre los estados "No aplica", "No disponible" y "No verificable" señalados más arriba.

A diferencia de la tabla consolidada presentada como Anexo I, que funciona como un catálogo de variables de referencia, el codebook es específico del sistema concreto que cada organización o entidad implemente y refleja sus decisiones operativas. Su función es doble: asegurar la consistencia interna durante la codificación —de modo que dos personas que codifican de forma independiente la misma información lleguen al mismo resultado— y servir de referencia para cualquier persona que posteriormente consulte la base de datos, permitiéndole entender qué representa cada variable, qué criterios se aplicaron y cómo interpretar los valores registrados.

En contextos donde el sistema combina fuentes diversas o donde la codificación es realizada por equipos distintos, el codebook es la condición que permite que la base de datos resultante sea coherente y comparable en el tiempo. Cuando las definiciones o categorías evolucionan, el codebook debe actualizarse de manera versionada, y esa información puede incorporarse como metadato del registro para preservar la trazabilidad histórica. Más aún, la existencia de un codebook en cada implementación es una condición para la comparabilidad regional que persigue este *Blueprint*: sin una documentación detallada de las reglas que cada sistema aplica, la interoperabilidad entre registros queda limitada a la mera coincidencia nominal de categorías.

### b. Metadatos mínimos

Los metadatos mínimos son la información técnica que asegura la trazabilidad del registro y, con ella, su auditabilidad y su capacidad de articulación con otras fuentes.

Como mínimo, cada registro del sistema debería incorporar: identificador único de registro, que permite distinguir cada entrada de cualquier otra en el sistema; identificador de evento, que permite asociar varios registros a un mismo hecho cuando distintas fuentes reportan la misma agresión; fuente del dato, entendida como el origen institucional, organizacional o comunitario del que proviene la información, preservando la trazabilidad hacia el documento o sistema original; fecha de ingreso y de última actualización, con control de versiones que registre correcciones posteriores sin borrar la cadena de procedencia; estado, método y nivel de verificación, que consigne no solo si el dato fue verificado, sino cómo y con qué grado de fiabilidad; autoría o responsable de la carga, que identifique a la persona o unidad que ingresó o modificó el registro; nivel de sensibilidad y clasificación de acceso del dato, como metadato asociado al registro y no solo a la categoría general, de modo que la regla de protección acompañe al dato a lo largo de todo su ciclo de vida; y método de captura, que indica si el registro se codificó manualmente, fue extraído automáticamente o se generó por vinculación de registros (*record linkage)* entre fuentes.

Conviene precisar que un mismo sistema puede tener más de una unidad de observación. Si bien el nivel de registro más frecuente es el hecho, también pueden serlo la persona defensora, las organizaciones, los procesos judiciales o las medidas de protección. Cada una de estas unidades debería contar con su propio identificador único persistente —por ejemplo, de víctima, de víctima-hecho, de proceso judicial o de medida de protección—, además del identificador único de registro y del identificador de evento ya mencionados. Estos identificadores son los que permiten vincular las distintas tablas entre sí y habilitan los análisis relacionales y longitudinales que se desarrollan más adelante.

Los metadatos cumplen una función técnica y jurídica. Permiten saber de dónde viene cada dato, cuándo fue incorporado, quién lo registró y cuál es su estado de verificación. Esta trazabilidad es clave para valorar la información en investigaciones, medidas de protección, procesos judiciales o trámites ante órganos internacionales, y también para revisar cómo opera el sistema y detectar posibles errores, sesgos o usos indebidos de la información.

### c. Llaves de deduplicación

La deduplicación es el proceso que evita el doble conteo de un mismo hecho o de una misma víctima cuando varias fuentes reportan el mismo evento. Las llaves de

deduplicación son las variables o combinaciones de variables que el sistema utiliza para realizar esa comparación, por ejemplo, nombre, fecha, municipio. Cuando la fuente es un índice agregado o un documento analítico sin registros individuales, este campo se marca como "No aplica", pues no existen unidades individuales que cotejar[72].

Cuando el volumen de registros es alto o existen errores tipográficos, nombres escritos de forma distinta o información incompleta, la coincidencia exacta de texto resulta insuficiente y se requiere vinculación de registros de carácter probabilístico, que evalúa en conjunto varias variables –por ejemplo, nombre, fecha, lugar y hecho victimizante– y estima la probabilidad de que dos registros correspondan al mismo caso. Por ello, la definición de las llaves de deduplicación debe adoptarse de la mano de las salvaguardas –seudonimización y control de acceso– y reconocerse como un campo condicional, dependiente del tipo de fuente y del modelo de sistema adoptado. Finalmente, como resultado del análisis de las llaves de deduplicación se obtienen identificadores únicos de víctimas y/o hechos victimizantes.

### d. Homologación, normalización e interoperabilidad de datos

La adopción progresiva de esta estructura requiere reglas de homologación y normalización para el manejo de la información histórica existente, dado que no todas las entidades registran las mismas variables, utilizan las mismas definiciones o conservan los datos en formatos comparables. Para ello, el sistema debería contar con diccionarios de datos, catálogos comunes, reglas de equivalencia entre categorías preexistentes y nuevas variables, criterios de calidad y metadatos mínimos que permitan conocer el origen, alcance, fecha de actualización, método de verificación y nivel de sensibilidad de cada dato. Asimismo, debería preverse una ruta institucional de actualización de parámetros, que permita incorporar, modificar o retirar variables cuando las dinámicas de violencia, conflicto o persecución lo requieran, preservando la trazabilidad de los cambios y la comparabilidad histórica[73].

---

**72** Comisión para el Esclarecimiento de la Verdad, la Convivencia y la No Repetición (CEV), Jurisdicción Especial para la Paz (JEP) y Human Rights Data Analysis Group (HRDAG). *Informe metodológico del proyecto conjunto JEP-CEV-HRDAG de integración de datos y estimación estadística*, 2 de agosto de 2022, Sección 3 "Vinculación de registros", pág. 23-24.

**73** DANE-SEN. *Recomendaciones de mecanismos, estándares y protocolos para la interoperabilidad en el intercambio, el uso y el reúso de datos en el SEN*, mayo de 2025, Dimensión 3 "Clasificaciones y vocabularios", pág. 37

La integración automatizada de información entre entidades con competencias en prevención, protección, investigación y judicialización depende de la existencia de estructuras de datos homologadas, diccionarios comunes, catálogos estandarizados, metadatos mínimos y protocolos seguros de intercambio. El desarrollo técnico de estos estándares —incluyendo vocabularios controlados, esquemas de metadatos, formatos de intercambio, identificadores comunes, reglas de calidad y criterios de actualización de variables— debería abordarse en lineamientos técnicos complementarios o en un anexo técnico de interoperabilidad, a desarrollarse en la fase de implementación de cada sistema nacional[74].

### e. Salvaguardas y protección de datos

Las salvaguardas y la protección de datos constituyen una condición esencial para la legitimidad, seguridad y utilidad del sistema. En ese sentido, la recopilación, el almacenamiento, el procesamiento y la difusión de datos nunca deben aumentar el riesgo de las personas defensoras, ni exponer a sus familias, comunidades, organizaciones, testigos o fuentes. La protección de datos opera, así, como expresión técnica de la debida diligencia reforzada y como salvaguarda frente a la persecución, la vigilancia, el perfilamiento indebido o la estigmatización.

El sistema debería distinguir, como mínimo, entre datos públicos, restringidos y confidenciales, asignando a cada nivel reglas diferenciadas de tratamiento, conservación y difusión. Categorías como la identidad de la persona defensora, su ubicación precisa, su estado de salud física o mental, su pertenencia étnica u organizativa, su orientación sexual o identidad de género, o la identidad de testigos y fuentes, deben tratarse en los niveles de mayor protección. Cabe señalar que esto rige el tratamiento y la difusión de los datos a nivel individual. No impide —y, de hecho, el sistema debe habilitarlo— el acceso a información estadística agregada desglosada por esas mismas variables –género, edad, etnia, tipo de labor, territorio, entre otras–, que es precisamente lo que permite visibilizar los riesgos diferenciados y los patrones de violencia.

La clasificación de los datos determina las medidas de protección aplicables. Entre ellas se encuentran la anonimización y la seudonimización, que permiten

**74** DANE-SEN. *Recomendaciones de mecanismos, estándares y protocolos para la interoperabilidad en el intercambio, el uso y el reúso de datos en el Sistema Estadístico Nacional (SEN)*, mayo de 2025, Sección 6.2 y Anexo A, pág. 43-50.

publicar información sin identificar a las personas y restringir el acceso a datos identificables a actores autorizados, mediante perfiles diferenciados y para finalidades legítimas, expresas y proporcionales. A ello se suman la minimización de datos, la reserva de identidad y, cuando corresponda, el consentimiento informado, entendido como una salvaguarda complementaria y no como un sustituto de las demás medidas de protección.

Por último, la seguridad del sistema debe poder demostrarse mediante mecanismos concretos de rendición de cuentas y control. Entre ellos se encuentran los registros de consulta (*logs*), que permiten conocer quién accede a qué información y con qué finalidad; los protocolos de respuesta frente a filtraciones o incidentes de seguridad; y las evaluaciones periódicas de impacto en derechos humanos y protección de datos, destinadas a verificar que las reglas de clasificación, acceso y difusión continúen siendo proporcionales a los fines del sistema. En esa misma línea, cuando el sistema incorpora herramientas de análisis o predicción, la supervisión resulta aún más importante. Los algoritmos pueden ayudar a orientar decisiones de protección o de política pública, pero estas deben considerar también la evaluación humana y otras fuentes de información relevantes.

# VIII. Usos analíticos y operativos de los sistemas de información

Como se planteó más arriba, el valor del sistema de información no reside en la suma de categorías o la magnitud de la información recabada, sino en la posibilidad de conectarlas para generar información y análisis útiles para responder a los objetivos del sistema. Así, la lógica relacional convierte un registro de eventos en un instrumento útil para la prevención, la protección, la investigación, la reparación y la no repetición. En este sentido, las decisiones que se adopten en el procesamiento de los datos y los resultados que se produzcan serán determinantes para que el sistema supere la condición de registro pasivo de eventos y se convierta en una infraestructura activa de garantía del derecho a defender derechos.

Ahora bien, el tipo de procesamiento posible y los resultados u *outputs* estarán marcados, en buena medida, por las decisiones de arquitectura del sistema de información, atendiendo a las capacidades institucionales, la fiabilidad de la información, la eliminación de sesgos y los contextos nacionales o institucionales.

En el capítulo sobre sistemas de información se remarcó la utilidad avanzar desde aquellos que compilan bases existentes hacia uno que permita integrar en mayor medida su información. Ello porque los sistemas integrados pueden mejorar los aprendizajes y resultados, de modo que la información cumpla un papel preventivo, de protección y de fortalecimiento de las respuestas individuales y colectivas para eliminar o mitigar riesgos y posibles daños.

En el estudio comparado de los sistemas de información y bases de datos se han registrado limitaciones –legales, fácticas o derivadas de exigencias de privacidad o seguridad– para compartir distintos tipos de datos demográficos, de eventos, o relativos a procesos judiciales o investigaciones en curso. Algunos de los desafíos que estas limitaciones generan pueden allanarse mediante pautas establecidas legalmente sobre acceso, uso restringido o interoperabilidad de los sistemas, teniendo en cuenta consideraciones de contexto y mandato legal. Lo cierto es que la existencia de múltiples fuentes de información y de bases de datos asociadas al fenómeno de agresiones contra personas defensoras de derechos humanos es un hecho de la realidad, y no un obstáculo a superar. A la información y bases de datos de la administración de justicia se suman las de entidades autónomas dentro del Estado, los registros temáticos o subnacionales y las bases de datos vinculadas al cumplimiento de las obligaciones frente a defensoras ambientales en virtud del Acuerdo de Escazú, entre otras. Más allá de estos esfuerzos se destacan otras iniciativas fundamentales desde la sociedad civil –organizaciones no gubernamentales, universidades, centros de pensamiento– orientadas a registrar y analizar diversos aspectos de las agresiones contra PDDH.

Las bases de datos de la sociedad civil fueron, en muchos casos, pioneras y contaron con información valiosa, sensible y oportuna que no fue documentada por fuentes estatales o intergubernamentales. Así, avanzaron de manera temprana en la documentación de procesos de vigilancia, seguimiento, desaparición forzada o impunidad frente a personas defensoras o frente a grupos especialmente afectados, como las mujeres defensoras o las personas defensoras ambientales o las personas en el exilio. En contextos adversos, de captura o desconfianza hacia los actores estatales clave para la protección, como fuerzas de seguridad o de la administración de justicia, han sido los espacios de la sociedad civil –organizaciones, iglesias, centros de investigación académicos— y las organizaciones internacionales quienes han ofrecido mayores garantías de imparcialidad, confidencialidad y seguridad a quienes denuncian. Ello ha derivado en sistemas robustos que acceden a información distinta de la que procesan las entidades estatales, como los del Programa Somos Defensores[75]; la Fundación para la Libertad de Prensa (FLIP)[76],

---

**75** Programa Somos Defensores. *Sistema de Información sobre Agresiones contra Personas Defensoras de Derechos Humanos en Colombia (SIADDHH). Disponible en:* https://somosdefensores.org/siaddhh/

**76** Fundación para la Libertad de Prensa (FLIP). *Periodistas asesinados. Disponible en:* https://flip.org.co/cifras/periodistas-asesinados

Justiça Global[77], Global Witness[78], CIVICUS[79], la Unidad de Protección a Defensoras y Defensores de Derechos Humanos, Guatemala (UDEFEGUA)[80] o la Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos (IM-Defensoras)[81], entre muchos otros. Adicionalmente desde los espacios internacionales –Naciones Unidas, los sistemas de protección de derechos previstos en la OEA, entre otros– se han generado informes valiosos a nivel nacional como también temáticos. Entre ellos, cabe destacar los desarrollos de la Relatoría Especial de las Naciones Unidas sobre la situación de los defensores de los derechos humanos, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH), la Relatoría Especial para la Libertad de Expresión (RELE) de la CIDH y el Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias.

Por ello, es necesario pensar cómo se cumple con el mandato internacional de asegurar un sistema de información estatal sobre personas defensoras de derechos humanos que articule o pueda beneficiarse de aquellas bases alojadas en diversas entidades, así como de la información complementaria que pueda surgir de otras fuentes, a fin de generar información útil para las políticas públicas y las prácticas en distintos niveles. Ya sea con el objetivo de comprender mejor los fenómenos individuales y colectivos para proteger a personas, grupos y comunidades; de perfeccionar las decisiones de política criminal atendiendo a factores relevantes o a posibles predictores de hechos de violencia letal; de orientar procesos de regulación del discurso de odio o de las amenazas por vía digital, entre muchos otros.

Adicionalmente, dados los patrones de violencia en la región y la importancia de los espacios de sociedad civil, incluidos los académicos, para el estudio de algunos estos fenómenos, es importante que la reingeniería de los sistemas de

---

**77** Justiça Global. *Protección de Defensoras/es de Derechos Humanos y de la Democracia*. Disponible en: https://www.global.org.br/es/blog/programa/proteccion-de-defensoras-es-de-derechos-humanos-y-de-la-democracia/

**78** Global Witness . *Latin America and the Caribbean.* Disponible en: https://globalwitness.org/en/regions/latin-america-and-the-caribbean/?page=2#listing

**79** CIVICUS (2024). *Violence targets journalists and human rights defenders without end*. Disponible en: https://monitor.civicus.org/

**80** Unidad de Protección a Defensoras y Defensores de Derechos Humanos - Guatemala (UDEFEGUA) *UDEFEGUA*. Disponible en: https://udefegua.org.gt/

**81** Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos (IM-Defensoras). *IM-Defensoras. Disponible en:* https://im-defensoras.org/

información tenga especialmente en cuenta a estos actores. Este enfoque implica no concebir a las instituciones gubernamentales como el único factor relevante para los aportes a la política pública y la práctica de prevención, sino considerar a la academia y a la sociedad civil como actores fundamentales para perfeccionar el análisis de información y el accionar de defensa de derechos del propio Estado. Más aún, hacerlo permite valorar su inmenso aporte a la democracia, al espacio cívico y al goce de derechos en el contexto de la región y promover sinergias virtuosas con dichos espacios. Por ejemplo, dejando la información disponible de un modo que facilite su acceso, así como generando las interfaces que permitan la alimentación de partes del sistema por entidades independientes, con el fin de ampliar el acceso a derechos, resolver sesgos, abordar temas o zonas silenciadas, facilitar el acceso a herramientas de protección, desarrollar medidas de autoprotección o apoyar la memorialización.

Ahora bien, las pautas brindadas por el derecho internacional para la elaboración de los sistemas estatales de información en la materia permiten delinear un mínimo de requisitos y de resultados relevantes para el procesamiento de datos. Así, la Corte IDH ha sostenido en sentencias relativas a varios países que es necesario contar con un sistema nacional de información sobre violencia contra personas defensoras[82]. El alto tribunal no solicita un censo de las personas defensoras, en virtud de la definición que el propio órgano de protección asume[83]. Lejos de ello, el tribunal requiere que se genere información conforme a las categorías y parámetros antes mencionados, desagregada a nivel subnacional o estatal, con el fin de producir estadísticas e información sobre patrones, eventos y contextos habilitantes relevantes para el ejercicio de derechos de las personas defensoras –individuos, grupos y organizaciones–, sobre la magnitud de las violencias de las que son objeto, así como sobre las causas últimas de las agresiones y la elaboración de al menos un informe anual público[84]. El objetivo del procesamiento de la información recogida consiste en alimentar las políticas públicas y prácticas de prevención y erradicación de las violencias y en apoyar el entorno habilitante para el ejercicio de los derechos[85].

**82** Ver sección 4 del documento.

**83** Ver sección 6.a. del documento

**84** Ver secciones 4 y 6 del documento.

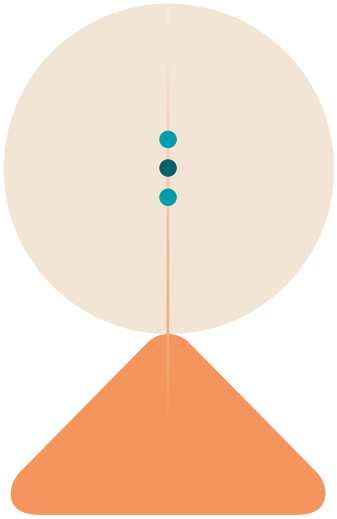
**85** Ver secciones 4 y 6 del documento.

Las pautas establecidas por el tribunal tienen consecuencias sobre el tipo de procesamiento de los datos exigido y sobre los resultados u *outputs*. En su nivel más básico, ese procesamiento permite producir información estadística desagregada —por ejemplo, números y porcentajes de amenazas, desplazamientos o tipos de violación asociados a ciertas características demográficas, así como la prevalencia y las tendencias según el espacio geográfico o el período temporal—. Pero entender la dimensión y la magnitud de los fenómenos que afectan a las personas defensoras de modo oportuno y adecuado, de cara a prevenir daños, exige cierta capacidad de asociar información y canalizarla hacia los diversos niveles del aparato estatal con fines de protección, prevención e investigación.

El procesamiento más complejo puede apoyarse en la estadística y en la ciencia de datos. Mediante diversas técnicas –la asociación de variables, la identificación de qué factores pesan más en la ocurrencia de un hecho, la agrupación de casos (*clustering),* la identificación de patrones o la proyección de escenarios de riesgo, entre otras– es posible generar conocimiento que no resulta visible en el dato aislado[86].

En la siguiente sección, se desarrollan algunos de los resultados o *outputs* posibles de un sistema de información sobre agresiones contra PDDH que podrían aportar a incidir de manera positiva sobre la protección de la labor de defensa de derechos.

**86** Cabe señalar que el aprovechamiento de estas técnicas depende, sin embargo, de contar con bases históricas normalizadas, información homogeneizada, reglas de calidad de los datos y metadatos suficientes para conocer el origen, el alcance, la confiabilidad y la fecha de actualización de la información



# IX. Selección de resultados o *outputs* previstos y posibles

Del procesamiento descrito y de las pautas fijadas por la jurisprudencia interamericana se desprende un abanico de resultados (*outputs*) posibles, de complejidad creciente que deben ser tenidos en cuenta a la hora de elaborar el sistema de información sobre personas defensoras.

Así, los resultados potenciales del sistema pueden organizarse de manera progresiva de acuerdo con el nivel de procesamiento de la información. Un primer nivel comprende producciones descriptivas, como estadísticas, informes periódicos, alertas y reportes. Un segundo nivel incorpora herramientas de visualización y síntesis, como índices, cartografías, geoportales y tableros, entre otros. Un tercer nivel, más avanzado, explora modelos analíticos y predictivos, incluyendo regresiones, modelos de clasificación y de extracción estructurada con modelos de lenguaje, entre otras posibilidades. No todos exigen el mismo nivel de capacidad técnica y conviene entenderlos como un repertorio escalable antes que como una lista cerrada[87].

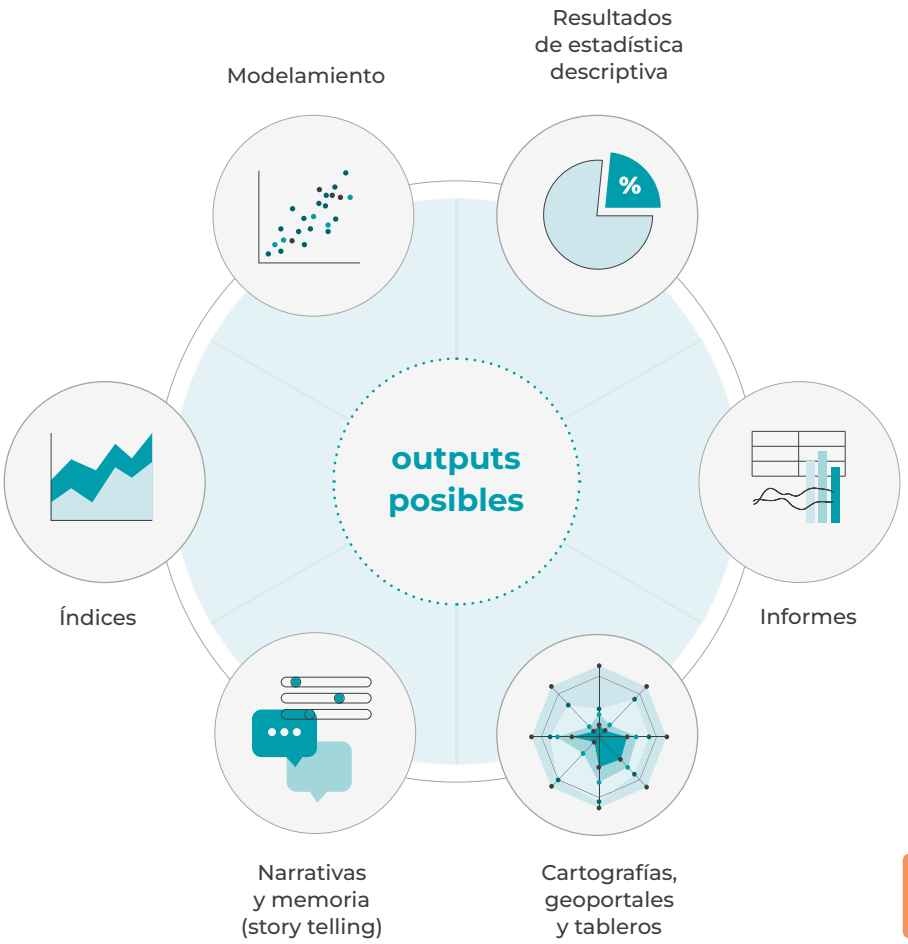
Cada uno de los resultados previstos, aún los de niveles de procesamiento menor, pueden generar mejoras en las políticas y prácticas de protección. Si bien

**87** Cabe notar que, si bien una parte de los resultados pueden y deben ser de carácter público, algunos de ellos –o la información producida o sus insumos– pueden tener carácter reservado, como la información pertinente para las medidas de protección individuales o relevante para la investigación penal.

remarcamos que el avance en los niveles de procesamiento de la información es un elemento clave de su eficacia, notamos una gran oportunidad de mejora en el desarrollo de *outputs*, así como su vinculación con las interfaces para las acciones de diversas entidades u organizaciones como planteamos más adelante en el texto.

A continuación, esta sección describe los principales *outputs* previstos para el sistema de información sobre personas defensoras, luego profundiza en dos ejemplos de modelos predictivos y concluye con pautas para su uso responsable.

**Principales *outputs* previstos**



### a. Resultados de estadística descriptiva

La sistematización de información permite generar estadísticas periódicas y desagregadas sobre diversos fenómenos, que a su vez posibilitan evaluar avances, retrocesos e hitos en el desarrollo de las políticas públicas. Algunos de estos ejemplos incluyen el número de víctimas y hechos victimizantes, así como el análisis bivariado con fecha, lugar o presunto responsable. Otras estadísticas de interés pueden ser el porcentaje de la población afectada y el enfoque diferencial según variables de género o pertenencia étnica, entre otras.

Una herramienta importante es el establecimiento de series temporales que permiten ver cómo evolucionan las agresiones o cómo se relacionan con las variaciones en la política, prácticas o eventos durante un periodo determinado (por ejemplo, trimestral, semestral, anual, etc.).

Cabe recordar que, la Corte IDH no solo exige que existan estadísticas, sino que señala algunas categorías y variables necesarias a relevar para comprender los diversos fenómenos de agresión, sus causas, impactos individuales y colectivos y la evolución de las tendencias.

### b. Informes

La Corte IDH plantea, como uno de los resultados necesarios, un informe anual sobre la temática y las respuestas del Estado. Este informe debe cumplir con el principio de transparencia y debe explicar temáticas como la o las bases de datos utilizadas, el procesamiento de la información, los modelos utilizados y las conclusiones. De manera fundamental, debe ser explícito en el porqué de las decisiones metodológicas y reconocer las limitaciones. Adicionalmente, para garantizar el acceso a la información, este informe debería contar con distintas versiones, que vayan desde el lenguaje técnico y metodológico hasta el lenguaje común para cualquier ciudadano/a. Asimismo, deben garantizarse mecanismos de participación para recibir sugerencias o críticas de la ciudadanía, de espacios académicos o de la sociedad civil.

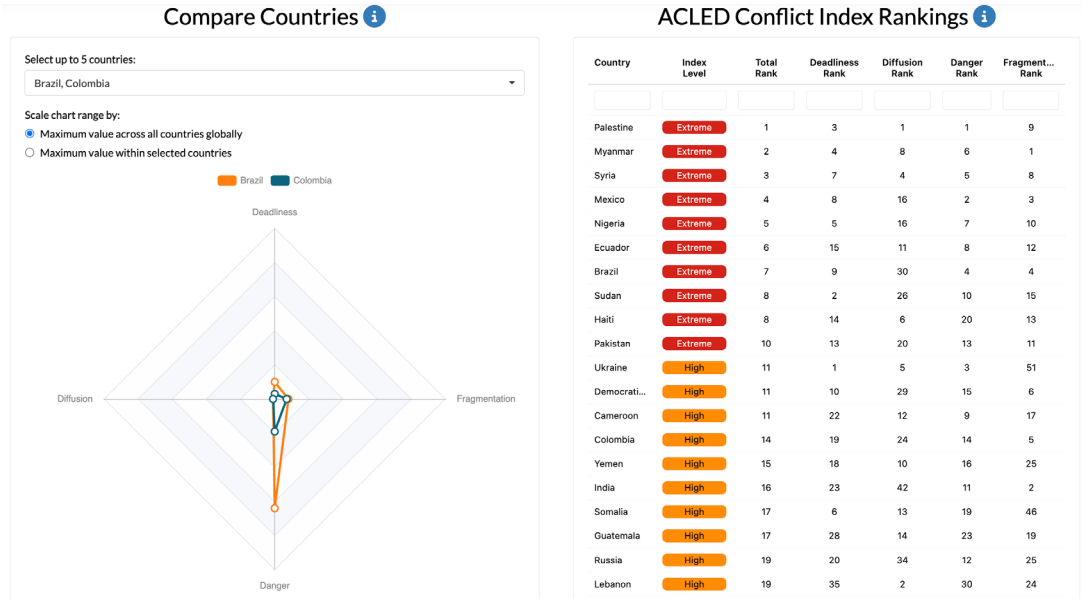
A su vez, la elaboración de informes trimestrales, con ciertos niveles de información, puede servir para evaluar de manera más ajustada y oportuna los fenómenos y los impactos de las medidas, políticas e iniciativas adoptadas. El uso en particular de tableros o *dashboards,* que expresen gráficamente parte de la información del informe y permitan mayores cruces de variables y temporales, puede ser de gran utilidad para hacer más accesible y útil la información del informe requerido.

### c. Cartografías, geoportales y tableros

Estas herramientas de visualización de la información facilitan la identificación de patrones, tendencias, factores de riesgo, actores involucrados y zonas de especial vulnerabilidad a lo largo del tiempo y contribuyen al diseño de medidas de prevención, protección y respuesta institucional. El verdadero poder analítico de estas plataformas radica en la capacidad de superponer distintas capas de información simultáneamente. Un análisis aislado ofrece una visión limitada, pero la combinación de múltiples factores puede revelar dinámicas ocultas. Por ejemplo, visualizar simultáneamente los niveles de deforestación (variable de patrones) con las amenazas (variable de agresión) puede evidenciar una posible correlación entre ambos fenómenos.

Estas herramientas deben ser accesibles para la población. Es decir, deben estar acompañadas de manuales claros, tutoriales intuitivos y diccionarios de datos que expliquen las variables presentadas con su respectiva metodología de documentación. Asimismo, deben tener un diseño centrado en el usuario, permitiendo que perfiles no técnicos puedan navegarla y comprenderla.

A manera de ejemplo, en la siguiente imagen se presenta un tablero de visualización de Armed Conflict Location & Event Data (ACLED). En el panel izquierdo, el usuario puede seleccionar distintos países para comparar el índice de conflicto en sus cuatro indicadores. De esta forma, es posible visualizar las fortalezas y debilidades de múltiples países y hacer comparaciones visuales. Mientras que en el panel derecho el usuario puede comparar los rankings de los indicadores para todos los países o algunos en particular.

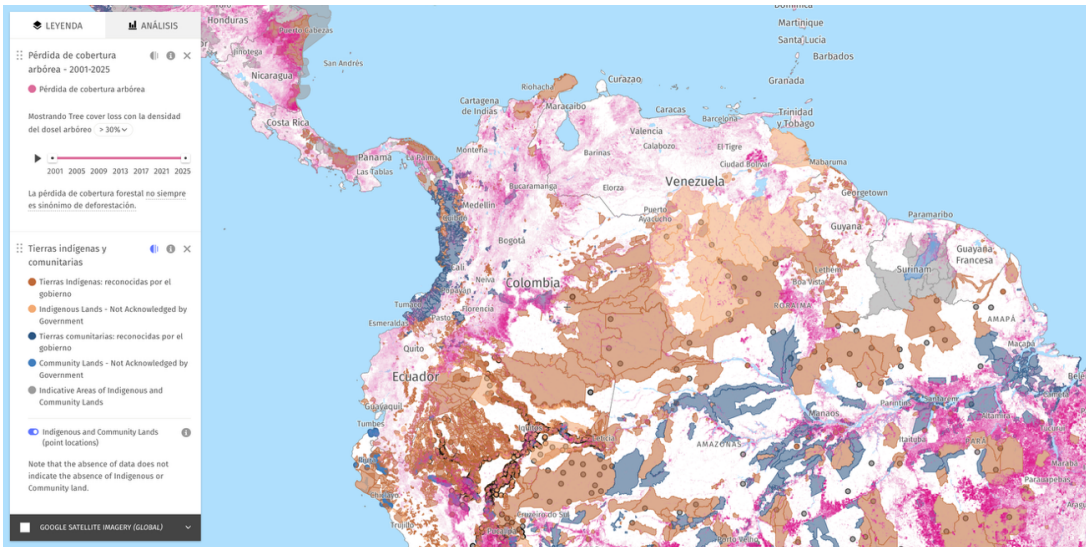



ACLED Conflict Index Rankings

| Country | Index Level | Total Rank | Deadliness Rank | Diffusion Rank | Danger Rank | Fragment... Rank |
|---|---|---|---|---|---|---|
| Palestine | Extreme | 1 | 3 | 1 | 1 | 9 |
| Myanmar | Extreme | 2 | 4 | 8 | 6 | 1 |
| Syria | Extreme | 3 | 7 | 4 | 5 | 8 |
| Mexico | Extreme | 4 | 8 | 16 | 2 | 3 |
| Nigeria | Extreme | 5 | 5 | 16 | 7 | 10 |
| Ecuador | Extreme | 6 | 15 | 11 | 8 | 12 |
| Brazil | Extreme | 7 | 9 | 30 | 4 | 4 |
| Sudan | Extreme | 8 | 2 | 26 | 10 | 15 |
| Haiti | Extreme | 8 | 14 | 6 | 20 | 13 |
| Pakistan | Extreme | 10 | 13 | 20 | 13 | 11 |
| Ukraine | High | 11 | 1 | 5 | 3 | 51 |
| Democrati... | High | 11 | 10 | 29 | 15 | 6 |
| Cameroon | High | 11 | 22 | 12 | 9 | 17 |
| Colombia | High | 14 | 19 | 24 | 14 | 5 |
| Yemen | High | 15 | 18 | 10 | 16 | 25 |
| India | High | 16 | 23 | 42 | 11 | 2 |
| Somalia | High | 17 | 6 | 13 | 19 | 46 |
| Guatemala | High | 17 | 28 | 14 | 23 | 19 |
| Russia | High | 19 | 20 | 34 | 12 | 25 |
| Lebanon | High | 19 | 35 | 2 | 30 | 24 |

Fuente: ACLED (s.f) Conflict Index Dashboard. Recopilado de: https://acleddata.com/platform/conflict-index-dashboard (24 de junio de 2026).

Adicionalmente, en la siguiente imagen se presenta un ejemplo de geoportal de Global Forest Watch. En este, el usuario puede seleccionar múltiples capas a visualizar, tales como la cobertura de árboles, plantaciones de soya, concesiones mineras o territorios indígenas y comunitarios. De esta forma, el usuario puede superponer distintas capas y hacer análisis visuales. En el ejemplo se muestra el mapa de Sudamérica con dos capas activadas: pérdida de cobertura arbórea (2001-2025) y territorios indígenas y comunitario, lo que permite identificar visualmente zonas donde ambos fenómenos coexisten geográficamente.




Fuente: Global Forest Watch (s.f) Map. Recuperado de: https://www.globalforestwatch.org/ (24 de junio de 2026).

### d. Narrativas y memoria (story telling)

Los sistemas también pueden dar lugar a productos centrados en las historias individuales y la memoria. En este sentido, parte de los ejercicios impulsados por la sociedad civil han sido pioneros en documentar y narrar estas historias, mediante relatos testimoniales, perfiles y semblanzas de personas defensoras, mapas de memoria, galerías y memoriales digitales y plataformas de visibilización, entre otros[88].

Estos formatos pueden integrarse al sistema; por ejemplo, mediante *storymaps* dedicados a las PDDH y organizaciones, en los que se relate su historia, trayectoria y aportes, de modo que el usuario final pueda conocer y reconocer su labor y fortalecer su visibilidad. Así, estos productos articulan la función documental del registro con su dimensión de memoria y reparación[89].

### e. Índices

Los índices son herramientas analíticas que sintetizan múltiples variables —por ejemplo, la frecuencia de ataques, el nivel de impunidad y la presencia de actores armados— en una sola métrica estandarizada y comparable entre regiones o períodos.

En un sistema de información sobre personas defensoras, los índices proporcionan métricas de referencia que permiten comparar el estado de la situación entre distintas regiones, construir rankings y, sobre esa base, priorizar alertas tempranas y orientar acciones de incidencia según la severidad del riesgo detectado. Su construcción puede combinar variables estructurales y territoriales (presencia de grupos armados, economías ilícitas, minería ilegal, desplazamiento, cultivos ilícitos,

---

**88** Véase, por ejemplo, la línea de productos narrativos y de memoria del Programa Somos Defensores, disponible en https://somosdefensores.org

**89** A continuación, se destacan algunos ejercicios de memorialización. Sobre las personas ejecutadas en Irán, el *Omid Memorial* del Abdorrahman Boroumand Center documenta y narra las historias de quienes fueron arbitrariamente privadas de su vida (disponible en https://www.iranrights.org/memorial). En materia de periodismo, la exposición «Periodismos (im)posibles: un oficio en medio del conflicto», del proyecto *Memorias del Periodismo en Colombia* de la FLIP, ofrece un recorrido por el pasado del oficio (disponible en https://memoriasdelperiodismo.co/periodismos-posibles/). En relación con las personas desaparecidas, en México se han creado sistemas para apoyar las investigaciones, encontrar indicios e identificar y localizar a las víctimas, como el sistema *Angelus* de la Comisión Nacional de Búsqueda (disponible en https://seguridad.conahcyt.mx/guerra-sucia/angelus) y la Consulta Pública del Registro Nacional de Personas Desaparecidas y No Localizadas (RNPDNO) (disponible en https://consultapublicarnpdno.segob.gob.mx).

entre otras), de modo que un fenómeno complejo pueda quedar expresado en valores que faciliten la identificación de patrones, comparación y seguimiento de tendencias. Además, permiten integrar múltiples fuentes de información sobre una misma problemática, lo que permite reconocer su variabilidad. Incluso pueden componerse de índices de otras entidades u organizaciones para enriquecer los análisis en caso de no poder acceder a información primaria.

Estos índices pueden ser integrados a herramientas de visualización o de modelamiento de datos para así evidenciar correlaciones ocultas, hacer pruebas de hipótesis o proyectar escenarios de riesgo futuro.

A modo de ejemplo, el índice de conflicto de ACLED presentado anteriormente se basa en cuatro dimensiones: fatalidad, peligro, difusión geográfica y fragmentación de grupos armados.

### f. Modelamiento

Una de las alternativas del sistema de información consiste en el uso de herramientas estadísticas y de aprendizaje automático para transformar los datos en evidencia que informe la toma de decisiones. Ello puede ser muy útil a la hora de abordar inmensas cantidades de información, pero también para explicar y resolver problemas de subregistro. Las aplicaciones de modelos pueden servir a distintos objetivos presentados a continuación.

Es importante resaltar que los modelos no requieren únicamente de información estructurada. Es decir, de información que pueda ordenarse en filas y columnas. Es posible utilizar información no estructurada, tal como audio, video y texto, para generar *outputs* como los presentados en esta subsección.

Además, vale la pena enfatizar que la capacidad analítica más avanzada de los modelos estadísticos o de *machine learning* no sustituye al juicio institucional ni a la intervención humana. Como se indica en las pautas de gobernanza del presente documento, ninguna decisión sobre medidas de protección debe adoptarse con fundamento exclusivo en un algoritmo. Sin embargo, los modelos pueden ser herramientas valiosas para priorizar la atención, detectar señales tempranas que escapan a la revisión manual y orientar el despliegue de recursos institucionales hacia las personas, grupos y territorios de mayor riesgo, entre otras funciones.

A nivel de gestión documental, los modelos de aprendizaje automático son fundamentales para la deduplicación de registros, garantizando que un mismo incidente o víctima no sea contabilizado de forma redundante. Una vez consolidada una macrobase de datos, esta información facilita el estudio de los patrones de documentación propios de cada fuente. Lo anterior ayuda a comprender las fortalezas y debilidades de distintas fuentes, así como a visibilizar posibles sesgos o vacíos.

En el ámbito del análisis causal, estas herramientas son capaces de medir el peso que tienen diferentes variables sobre una situación de vulnerabilidad. El sistema puede procesar múltiples factores simultáneamente para determinar cuáles de ellos influyen de manera más determinante sobre una variable de interés central, como lo es la fluctuación en los niveles de riesgo.

Asimismo, mediante pruebas de hipótesis, es posible comprobar estadísticamente cómo un mismo fenómeno afecta de manera desigual a diferentes poblaciones o áreas geográficas, aportando evidencia para justificar enfoques de protección diferenciados.

Por su parte, la implementación de modelos de agrupamiento automático o *clustering* permite la agrupación de víctimas o incidentes basándose estrictamente en sus similitudes intrínsecas, sin necesidad de imponer categorías predefinidas. Ello permite revelar patrones de comportamiento compartidos y dinámicas subyacentes que constituyen recursos esenciales para anticipar escenarios de riesgo, optimizar la asignación de recursos y mejorar sustancialmente el diseño de las políticas de prevención. Sin lugar a duda estos modelos pueden generar aportes importantes para un abordaje de política pública con una perspectiva macrocriminal, así como una política de protección que afine los criterios para abordar diversos factores de vulnerabilidad. Adicionalmente, el sistema puede integrar modelos predictivos que transforman el análisis histórico y contextual en inteligencia prospectiva. Al procesar el comportamiento pasado de las variables, estos algoritmos están diseñados para calcular la probabilidad de que ocurran futuros incidentes en el corto o mediano plazo, o identificar patrones de escalada que, de no atenderse oportunamente, desembocan en daños graves e irreversibles contra personas defensoras.

A continuación, se presentan dos ejemplos sencillos de posibles usos de modelos en información tanto estructurada como no estructurada, que muestran aplicaciones posibles de los sistemas de información para la prevención.

### i. Modelo predictivo con información estructurada

Existen múltiples modelos predictivos que pueden ser utilizados para apoyar la toma de decisiones y proteger a las PDDH. Si bien el objetivo del *blueprint* no es introducir todos los métodos posibles, en esta sección se introduce brevemente la regresión logística con un ejemplo hipotético en el que se busca predecir la probabilidad de que una persona defensora sea asesinada con base en amenazas previas y otras características individuales[90].

La regresión logística es un método estadístico estándar en el ámbito del aprendizaje automático, especialmente diseñado para predecir resultados binarios; es decir, situaciones donde solo existen dos respuestas posibles. Por ejemplo, determinar si una PDDH corre el riesgo de ser asesinada o no.

El modelo funciona estimando una probabilidad que oscila entre 0 y 1 para cada individuo, fundamentando su cálculo en un análisis riguroso de sus características observables a nivel individual. Para que este proceso sea posible, el algoritmo debe alimentarse de un conjunto de datos estructurados a nivel individual, donde cada registro o fila corresponde a la información detallada de una persona defensora, abarcando tanto la variable de interés o variable dependiente ("asesinado" vs. "no asesinado") como una serie de variables independientes que reflejan sus características, tales como el género, la etnia, el tipo de liderazgo que ejerce, la zona geográfica o el historial de agresiones previas.

El objetivo central de este algoritmo es procesar información histórica para aprender a identificar y cuantificar las relaciones existentes entre las distintas características y el desenlace fatal. Durante esta fase de entrenamiento, el modelo evalúa los datos del pasado y asigna un peso matemático específico a cada variable, el cual refleja

**90** Este apartado se nutre del trabajo realizado por GRIL, que desarrolló un prototipo de regresión logística a partir de datos sintéticos con el objetivo de introducir a un público no técnico un modelo predictivo. Su construcción se orientó a partir de estadísticas agregadas de informes públicos – como los Informes Semestrales del Programa Somos Defensores y el informe de la Misión de Observación Electoral sobre violencia contra liderazgos–. El modelo estimó la probabilidad de asesinato en función de variables como el tipo de labor de defensa, la etnia, el género y la existencia de agresiones previas. Con un conjunto de 5.000 registros simulados y una partición entre datos de entrenamiento (80%) y de prueba (20%), el modelo obtuvo un área bajo la curva ROC de 0.89, lo que indica una alta capacidad de discriminar entre casos de mayor y menor riesgo. El factor con mayor peso predictivo fue la existencia de agresiones previas documentadas, seguido del tipo de labor de defensa.

qué tan fuerte o determinante es su asociación con el resultado final. Una vez que el sistema ha consolidado este conocimiento y definido los pesos mediante una fórmula matemática, queda capacitado para recibir información completamente nueva y desconocida. Entonces, cuando el Estado o una organización ingresa datos de defensores cuyo nivel de peligro actual se ignora, el modelo es capaz de proyectar la probabilidad de riesgo basándose exclusivamente en los patrones que asimiló con anterioridad.

La adopción de la regresión logística es muy común en la fase inicial de proyectos predictivos debido a que ofrece ventajas operativas muy claras en comparación con otros métodos más complejos, destacando principalmente por ser un modelo relativamente fácil de interpretar. Su transparencia analítica permite a los tomadores de decisiones identificar con exactitud cuáles características específicas están vinculadas a los niveles de riesgo más altos, ya que dichas variables se verán reflejadas directamente con los pesos numéricos más elevados en la fórmula.

Además, tiene el mérito de traducir patrones históricos en estimaciones cuantificables y comparables, que pueden orientar la priorización de casos dentro de los mecanismos de protección o priorización en las investigaciones penales. De esta manera, el ejemplo desarrollado permite avanzar de manera significativa en medidas clave para prevenir daños fatales.

Ahora bien, estos modelos, que implican avances significativos para la situación existente en la mayor parte de los contextos, tienen límites que pueden ser superados por otras herramientas. Así, presentan una limitación estructural relevante para los fines del presente sistema: reduce la complejidad de la violencia contra personas defensoras a una única variable de interés (en este caso, un resultado binario de homicidio), ignorando el amplio espectro de violaciones que preceden, acompañan o sustituyen al homicidio. Por ejemplo, la detención arbitraria, el desplazamiento forzado, el confinamiento comunitario, el riesgo de reclutamiento de niños, niñas y adolescentes, y las violencias basadas en género en contextos de control armado. Todos ellos son resultados documentados y previsibles que un modelo exclusivamente centrado en la muerte no captura.

Por lo anterior, es posible utilizar modelos más complejos que permitan identificar múltiples variables de riesgo. Ello responde a que un sistema de información sobre personas defensoras debe orientarse a la prevención, lo que exige identificar las violaciones antes de que escalen hacia las formas más graves de agresión.

### ii. Gran Modelo de Lenguaje con información no estructurada

Los modelos de lenguaje natural resultan útiles para analizar información cualitativa presentada en textos. En específico, en este ejemplo se utilizó para extraer información estructurada (que puede ser ordenada en una tabla) a partir de documentos no estructurados. Esta capacidad resulta especialmente relevante para el sistema de información sobre personas defensoras, dado que una parte sustancial de la información disponible se encuentra en informes narrativos, alertas tempranas, registros de organizaciones de la sociedad civil y reportes institucionales que no están sistematizados en bases de datos.

En el presente apartado, se recurrió a un modelo de lenguaje con información no estructurada basado en las alertas tempranas de la Defensoría del Pueblo de Colombia. Esto permitió probar un modelo que asocia un mayor número de eventos y variables para lograr mejor información sobre posibles escaladas de violencia, consecuencias para diferentes personas y tiempos de respuestas institucionales. El modelo no tiene el objetivo de evaluar acciones institucionales frente a los eventos específicos incluidos en el ejemplo, sin embargo, podría ser perfeccionado para analizar algunos patrones que afectan a las personas defensoras, sus comunidades de pertenencia, las variaciones de aquellos en tiempo real como las escaladas y efectos a diversos grupos, los impactos de intervenciones institucionales de diferentes entidades o el accionar de otros actores.

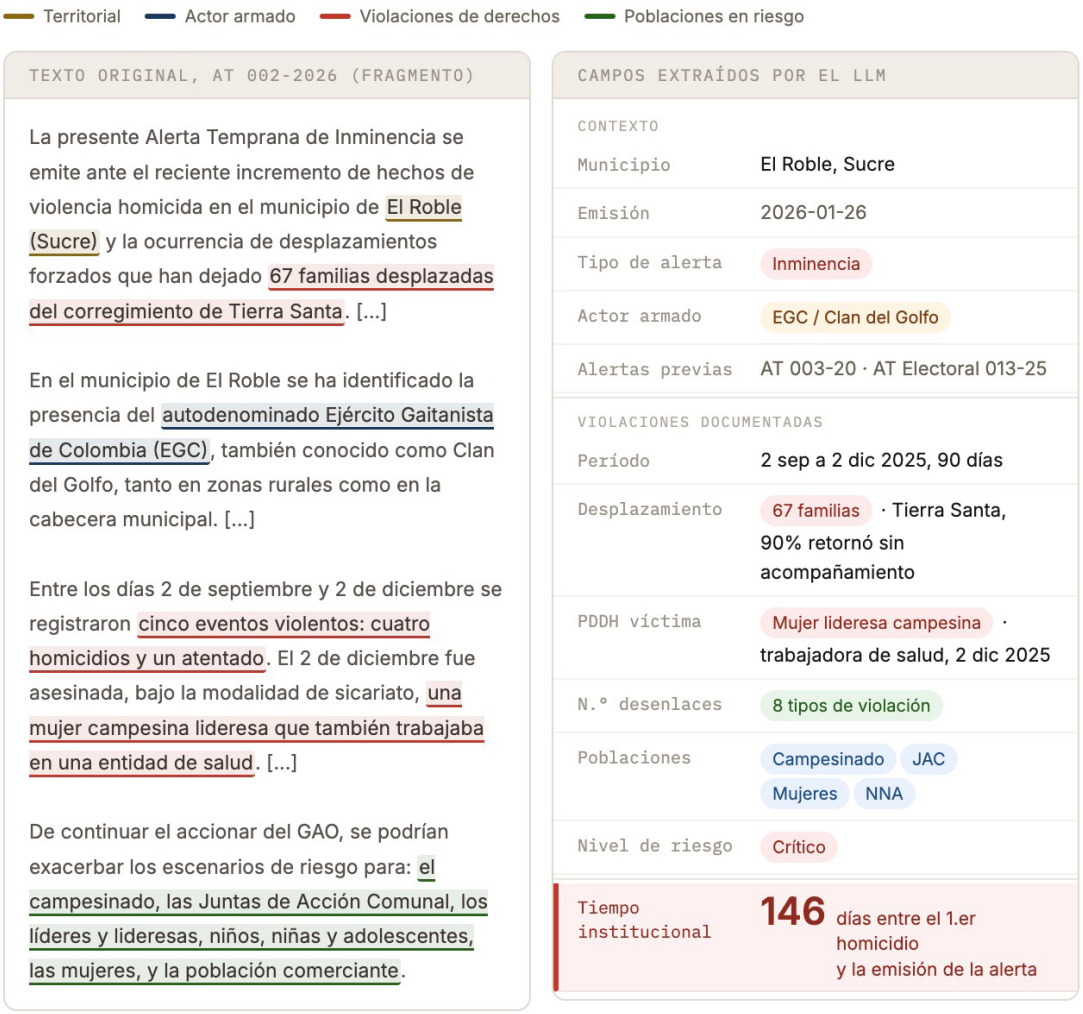
A su vez, los resultados de esta extracción estructurada constituyen el insumo de entrada para modelos de análisis causal, de agrupamiento (*clustering)* y de estimación de riesgo más sofisticados, descritos en las secciones anteriores de este capítulo. La lógica de su uso es acumulativa: la calidad del análisis depende de la calidad de la información estructurada disponible, y la extracción automática mediante modelos de lenguaje permite escalar esa estructuración a volúmenes de información que no podrían procesarse manualmente.

A modo de ejemplo, es posible tomar las Alertas Tempranas de Inminencia emitidas por la Defensoría del Pueblo de Colombia[91]. Estas alertas, que pueden descargarse del portal público del Sistema de Alertas Tempranas (SAT), son documentos de entre 10 y 20 páginas que describen el contexto territorial, los antecedentes del riesgo, los hechos violentos recientes, las poblaciones afectadas y las recomendaciones a las instituciones competentes. Su contenido es narrativo y heterogéneo, lo que dificulta su integración directa a bases de datos estructuradas.

Mediante un modelo de lenguaje, es posible transformar automáticamente el texto de estas alertas en un conjunto de campos estructurados: la secuencia temporal de eventos violentos con sus fechas y tipos, los grupos armados identificados y las acciones documentadas, las poblaciones en riesgo diferencial —incluidas las personas defensoras—, los indicadores de escalada del conflicto y la brecha entre los primeros eventos registrados y la respuesta institucional. Este proceso de extracción puede aplicarse sobre centenares de alertas de manera sistemática, generando una base de datos analítica que permite estudiar patrones a través del tiempo y el territorio.

Para ilustrar esta capacidad, se tomó específicamente la Alerta Temprana N° 002-2026 de Inminencia, emitida por la Defensoría del Pueblo el 26 de enero de 2026 para el municipio de El Roble, Sucre. Del texto de este único documento, el modelo registró ocho tipos de violaciones de derechos diferenciados, cinco indicadores de escalada, seis poblaciones en riesgo diferencial y una trayectoria temporal de noventa días antes del homicidio de una lideresa. La siguiente figura muestra esta extracción: a la izquierda, el texto original de la alerta con los fragmentos subrayados; a la derecha, los campos estructurados que el modelo deriva de ellos.

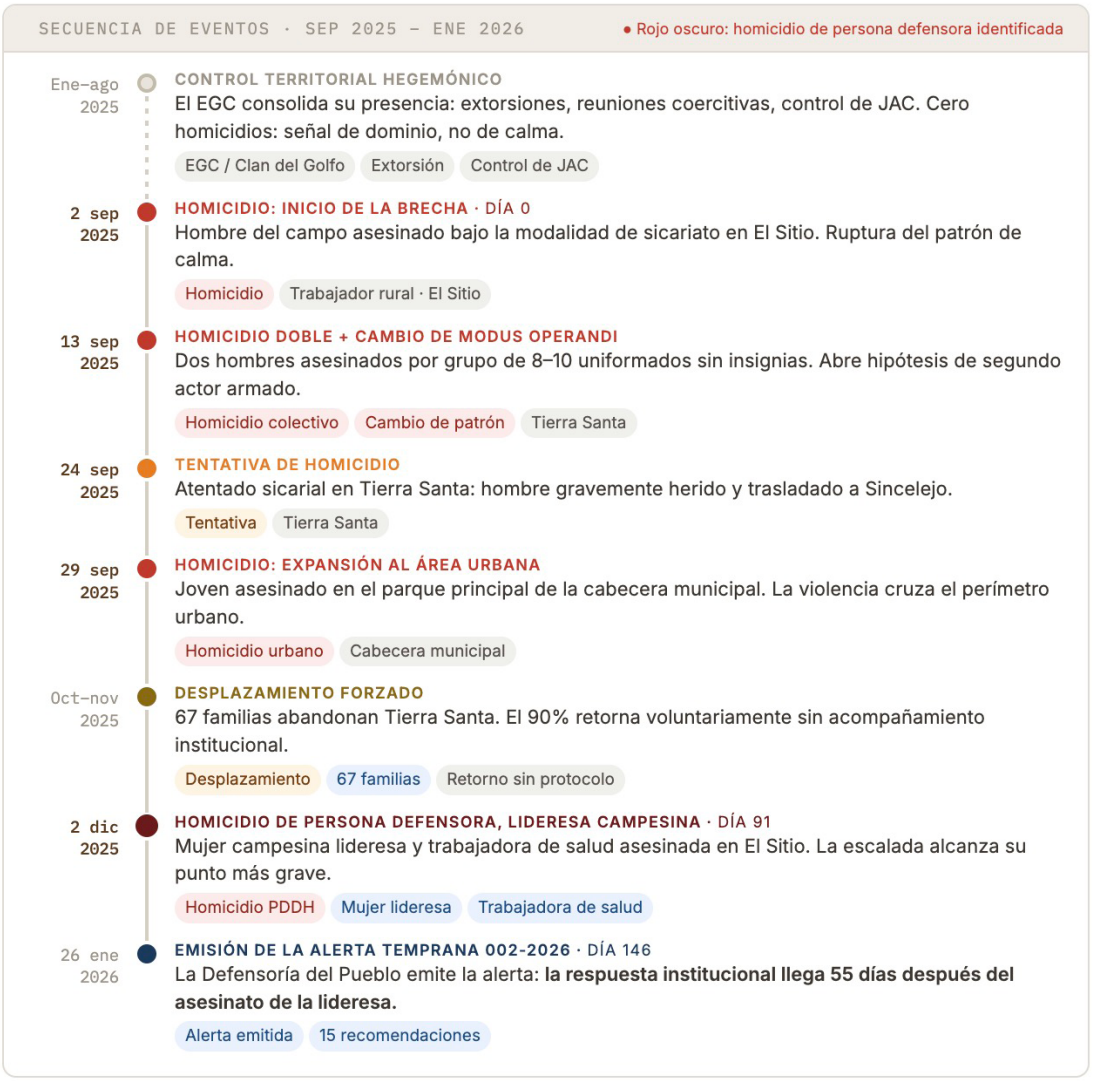
**91** Para más información, ver: https://alertastempranas.defensoria.gov.co/




Fuente: Alerta Temprana N.° 002-2026 de Inminencia, Defensoría del Pueblo de Colombia, 26 de enero de 2026. Extracción estructurada automatizada mediante modelo de lenguaje. Los fragmentos subrayados en el texto original corresponden a los campos extraídos; el color indica el tipo de información (territorial, actor armado, violaciones de derechos, poblaciones en riesgo).

Uno de los análisis que permitió la herramienta fue establecer una trayectoria de escalada. Así, entre el 2 de septiembre y el 2 de diciembre de 2025, el municipio registró cinco eventos violentos en una secuencia de noventa días: un primer homicidio en El Sitio; un doble homicidio en Tierra Santa cometido por un grupo de entre ocho y diez hombres uniformados sin insignias —modo de actuar atípico que generó la hipótesis de un posible segundo actor armado—; un atentado con herido grave en Tierra Santa; un homicidio en la cabecera municipal —con lo que la violencia cruzó hacia el área urbana—; y, finalmente, el asesinato de una mujer campesina lideresa que también se desempeñaba como trabajadora de salud en el corregimiento de El Sitio. Esta secuencia, invisible como patrón en un registro de eventos aislados, se vuelve analíticamente legible como trayectoria de escalada: ruptura de la calma aparente, cambio de modus operandi, expansión geográfica, y uno de los desenlaces se da con una víctima que es una persona defensora.

Esta secuencia se grafica en la siguiente imagen, que muestra cómo los eventos, leídos en el tiempo, configuran un patrón de escalada.




Fuente: Alerta Temprana N.° 002-2026 de Inminencia, Defensoría del Pueblo de Colombia, 26 de enero de 2026. Extracción estructurada automatizada mediante modelo de lenguaje

El modelo identificó, asimismo, cinco indicadores de escalada[92] y consiguió determinar ocho afectaciones: el homicidio de la lideresa; el desplazamiento forzado de 67 familias del corregimiento de Tierra Santa; el retorno sin acompañamiento institucional de aproximadamente el 90% de las familias desplazadas; las amenazas colectivas a quienes informaran a las autoridades; la extorsión sistemática

92 A saber: (i) ausencia prolongada de violencia letal en los ocho meses anteriores —que la Defensoría interpreta como consolidación del control hegemónico del grupo armado, no como paz—; (ii) ruptura abrupta del patrón con cinco eventos en noventa días; (iii) cambio en el modo de operar; (iv) progresión desde el área rural hacia la cabecera municipal; y (v) homicidio de una persona defensora como punto de cierre de la secuencia.

a funcionarios y comerciantes; la presión sobre las Juntas de Acción Comunal para actuar bajo las directrices del grupo armado; el riesgo de reclutamiento y utilización de niños, niñas y adolescentes en actividades de microtráfico; y los riesgos de violencias basadas en género en el contexto del control armado.

Adicionalmente permitió medir los tiempos de respuesta institucional: el modelo calculó un lapso de 146 días entre el primer evento letal documentado (2 de septiembre de 2025) y la emisión de la alerta (26 de enero de 2026). Este dato es analíticamente relevante: documenta el tiempo transcurrido entre la señal de alerta y la respuesta formal del sistema de alertas, y puede estudiarse de manera comparada sobre el conjunto del corpus de alertas o asociada a otras interfases con sistemas de protección de derechos. En este caso se aplicó frente a las alertas, pero podría hacerse de manera más compleja incluyendo otro tipo de datos de los sistemas de protección individual y colectiva, las medidas de seguridad pública, etc.

Aplicada sistemáticamente sobre el conjunto de las Alertas Tempranas de Inminencia disponibles en el portal público de la Defensoría del Pueblo[93], esta metodología permitiría construir una base de datos estructurada con información sobre trayectorias de escalada, patrones de actuación de grupos armados, distribución territorial de los resultados, brecha entre eventos y diversas respuestas institucionales, y modalidades de riesgo diferencial para personas defensoras. Este corpus podría enriquecerse con alertas de organizaciones de la sociedad civil o complementarse con las acciones de protección que provienen de procesos de sociedad civil.

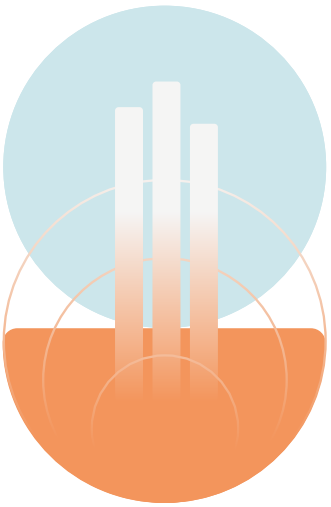
### g. Consideraciones de uso responsable

La aplicación de modelos en el contexto de sistemas de información sobre personas defensoras exige salvaguardas específicas, aunque algunas de ellas también son aplicables a la construcción de índices y otros sistemas de procesamiento de la información. En primer lugar, los resultados de los modelos deben tratarse como insumos para el juicio institucional y no como determinaciones autónomas: los *outputs* de los modelos —estimaciones de riesgo, identificación de patrones, cálculos de desfase— deben ser verificados y contextualizados por equipos humanos con conocimiento territorial y jurídico. En segundo lugar, la metodología

**93** A la fecha de elaboración de este documento suma más de 350 alertas emitidas entre 2017 y 2026. Para más información, ver: https://alertastempranas.defensoria.gov.co/

de extracción y los criterios de clasificación utilizados deben documentarse de manera transparente y estar disponibles para revisión, de modo que los resultados sean auditables y reproducibles. En tercer lugar, es necesario recordar que los algoritmos estadísticos simplifican la realidad y pueden perpetuar sesgos presentes en los datos históricos, lo que pueden llegar a revictimizar o excluir a poblaciones vulnerables. Por último, cualquier implementación a escala debe someterse a un análisis de riesgo que evalúe los posibles usos indebidos de la información consolidada, en línea con los principios de no daño y uso legítimo desarrollados en el capítulo de principios éticos del presente documento.

Con estas salvaguardas, los modelos analíticos descritos en esta sección representan un avance significativo respecto a los enfoques descriptivos existentes: no solo documentan lo que ocurrió, sino que hacen visible lo que estaba ocurriendo antes de que ocurriera, y lo hacen con la sistematicidad necesaria para orientar respuestas institucionales basadas en evidencia.



# X. Interfaces institucionales y con la sociedad civil

Los resultados del sistema deben estar diseñados para articularse con interfaces que aseguren impacto real en la prevención, protección, investigación y formulación de políticas públicas. El derecho internacional es muy claro en la definición de obligaciones de respuesta y debida diligencia frente a los riesgos previsibles y conocidos, que se trasladan en obligaciones de producción de información, diseminación y actuación desde diferentes entidades del Estado con competencia en la materia.

Sin embargo, no basta con producir informes, mapas, alertas, índices o modelos: estos deben poder llegar, con el nivel de detalle adecuado, a las autoridades responsables de adoptar medidas, activar rutas de protección, priorizar territorios o fortalecer investigaciones. Para ello, el sistema debería contemplar interfaces diferenciadas para entidades estatales, incluidas alertas orientadas a la protección y prevención, mecanismos de focalización territorial y productos específicos para órganos de investigación, administración de justicia y para diseminar la información de manera adecuada y oportuna a las personas o grupos en riesgo.

Estas interfaces deben diseñarse con estándares de interoperabilidad que permitan su integración con los sistemas de información de las entidades competentes y relevantes en el contexto nacional o local para abordar el fenómeno. Por ejemplo, entidades como Fiscalía, Unidad Nacional de Protección o mecanismos de protección de periodistas, Defensoría del Pueblo o instituciones nacionales de

derechos humanos, Ministerio del Interior, seguridad o justicia, u otras instituciones con funciones de prevención, protección, investigación o judicialización. Para ello, hay que contemplar estructuras de datos homologadas, metadatos comunes, protocolos seguros de intercambio, reglas de acceso diferenciado, mecanismos de trazabilidad sobre el uso de la información y pautas para su distribución o diseminación adecuada y oportuna a las entidades, organizaciones u organismos internacionales relevantes[94].

Dadas las realidades y características de la recolección de datos en la materia, el sistema de información sobre personas defensoras del Estado debe contemplar interfaces con espacios de sociedad civil. Ello puede ser especialmente útil para su contraste y análisis, la eliminación de sesgos y el potenciamiento de los fines de política pública a través de las sinergias con otros sistemas de información y garantía de derechos no estatales. En nuestro continente, y a nivel global, las organizaciones de sociedad civil, la academia y los espacios especializados cumplen un papel sustantivo en la documentación, contraste y uso público de la información y en la provisión de servicios de acompañamiento jurídico, psicosocial, médico, de asistencia humanitaria, entre otros. Su trabajo permite acompañar a personas y comunidades en riesgo, activar acciones de incidencia, fortalecer el monitoreo independiente, contribuir a la vigencia del Estado de Derecho, aportar a medidas de protección y autoprotección de individuos y comunidades y diseminar de manera oportuna y adecuada información clave, entre otras cuestiones. Por ello, el sistema estatal de información sobre personas defensoras debe prever la articulación posible con los datos que provengan de fuentes no gubernamentales –de modo de robustecer lo recogido y el análisis producido–, así como formas de acceso público o semipúblico a resultados, mediante niveles diferenciados que permitan aprovechar la información sin comprometer la seguridad de PDDH, víctimas, testigos, comunidades, fuentes ni de las políticas de seguridad o investigación penal. A ello se suma la previsión de productos específicos de transparencia activa sobre el desempeño institucional –estadísticas, informes, y otros de los señalados más arriba–, que puedan abrir la puerta a interfaces y sinergias con espacios de sociedad civil y académicos a nivel local, nacional, regional y global.

**94** DANE – SEN. *Recomendaciones de mecanismos, estándares y protocolos para la interoperabilidad en el intercambio, el uso y el reúso de datos en el SEN*, mayo de 2025, dimensión 4, pág. 39-40.

A continuación, enumeramos algunas de las posibles interfaces útiles para los sistemas de información sobre agresiones a personas defensoras que apoyan la prevención, protección, investigación, rendición de cuentas y la reparación. Ellas incluyen: i) interfaces de priorización individual, ii) alertas respecto a grupos en situación de riesgo, iii) interfaces con la administración de justicia y órganos de investigación, e iv) interfaces con espacios de protección de derechos y de memoria.

### a. Interfaces de priorización individual

Las interfaces pueden incluir canales de comunicación y respuesta individualizada, con niveles de información y acceso diferenciado para las distintas entidades competentes. Su finalidad es facilitar una respuesta coordinada frente a situaciones de riesgo individual o colectivo, de manera adecuada, oportuna y, cuando corresponda, consensuada. La definición de estas interfaces dependerá de los caminos institucionales que cada Estado prevea para responder a un riesgo identificado a partir de resultados individualizados que afectan a una persona o grupos de personas.

Como destacamos anteriormente, los canales y las interfaces deben contemplar una instancia de validación a cargo de personas con la experticia técnica y conocimiento del contexto necesarios para interpretar los resultados y definir las medidas de respuesta más adecuadas desde los distintos ámbitos institucionales. Estas pueden incluir las medidas de protección consensuadas, medidas de investigación reforzadas frente a amenazas o eventos asociados, medidas de apoyo familiar, médico o psicológico si fuera necesario, medidas de seguridad policial y otras acciones pertinentes según las características del caso.

Un ejemplo de este tipo de sistemas de información, basados en un uso dirigido de los datos, es la plataforma desarrollada por Impulso.gov para el Sistema Único de Salud del Brasil[95]. Esta combina datos, modelos basados en evidencia y accesos diferenciados para orientar la acción preventiva de los equipos de salud comunitarios mediante estrategias de micro-targeting, articulando la actuación de las entidades públicas y de los agentes de salud en las comunidades. Lo interesante de esta experiencia es la lógica de gestión diferenciada de la información y de los niveles de accesos para activar respuestas oportunas por parte de las instituciones competentes.

---

**95** Para más información, ver: https://www.impulsogov.org

### b. Interfaces de alerta respecto a grupos en situación de riesgo

Las obligaciones internacionales vinculadas a actuar frente a riesgos ciertos o inminentes se aplican tanto frente a individuos como a grupos afectados. En este marco, las obligaciones de debida diligencia implican adoptar medidas adecuadas y oportunas para informar de dichos riesgos a aquellas personas o colectivos potencialmente afectados, así como implementar acciones apropiadas para mitigarlos.

La dimensión colectiva de la labor de defensa de derechos no siempre es documentada o abordada de manera adecuada. Ello se debe, en parte, a que la literatura especializada y las políticas públicas han tendido a privilegiar el análisis de agresiones individuales y de eventos fatales. Sin embargo, muchas de las agresiones contra PDDH buscan silenciar, ralentizar o inhibir procesos colectivos de defensa de derechos. En efecto, buena parte del trabajo de defensa tiene una dimensión colectiva, tanto por la forma en la que se organizan los procesos de defensa de derechos como por los derechos, comunidades y personas involucradas. Por ejemplo, los integrantes de una organización no gubernamental que defienden a un pueblo indígena frente a una organización criminal que está ingresando a un espacio territorial específico.

La difusión oportuna y adecuada de información sobre situaciones de riesgo constituye, en sí misma, una medida de prevención y protección. El Estado tiene el deber de recopilar y difundir información de manera oficiosa sobre situaciones de riesgo en forma completa, clara, veraz, actualizada y oportuna, por canales accesibles y en un lenguaje comprensible para los distintos sectores de la población[96]. En consecuencia, el sistema debe contemplar reglas y flujos diferenciados para advertir, de manera oportuna y en un formato apropiado, sobre los riesgos identificados a las personas, organizaciones y comunidades concernidas, de modo que puedan adoptar decisiones informadas de prevención y autoprotección.

Asimismo, estas interfaces pueden habilitar medidas de prevención y autoprotección impulsadas desde la sociedad civil. En muchos contextos, las redes y organizaciones de sociedad civil cuentan con mecanismos propios de monitoreo, alerta y respuesta

**96** Corte IDH. *Opinión Consultiva OC-32/25 «Emergencia Climática y Derechos Humanos»,* párrs. 488-489, 503-504 y 521-523; CEJIL. *El acceso a la información climática y las obligaciones de derechos humanos. Guía temática para analizar la Opinión Consultiva OC-32/25*, enero de 2026, págs. 5 y 13-14.

–individuales y colectivos– y operan como canales de diseminación oportuna y adecuada de información en territorios y comunidades. Por ello, las interfaces del sistema deberían habilitar formas de acceso diferenciado y mecanismos de retroalimentación que permitan a estos actores tanto recibir alertas pertinentes como aportar información relevante para fortalecer las estrategias comunitarias de autoprotección.

En esta línea, desarrollar interfaces que permitan visibilizar esta dinámica puede resultar relevante, no solo para evidenciar actos colectivos de intimidación, estigmatización, hurto y otras agresiones, sino también para documentar los mecanismos de protección y autoprotección impulsados desde la sociedad civil como estrategias de prevención de futuros crímenes contra grupos sociales que defienden derechos (por ejemplo, amojonamientos, dotación de casas refugio, fortalecimiento de guardias comunitarias, entre otros). Registrar estas acciones también permitiría contrastar las acciones de prevención impulsadas por la ciudadanía con las políticas públicas existentes, evidenciando la necesidad de avanzar hacia modelos de protección con un mayor énfasis en las dimensiones colectiva y preventiva. De igual forma, las medidas colectivas implementadas a través de fondos de protección de la sociedad civil pueden ofrecer información valiosa sobre la incorporación de enfoques interseccionales, con el fin de reducir los riesgos que enfrentan las comunidades y las PDDH que las integran.

### c. Interfaces para la administración de justicia y órganos de investigación

El sistema de información sobre personas defensoras debería prever una interfaz especializada para órganos de investigación y administración de justicia, orientada a fortalecer la identificación, investigación y judicialización de agresiones contra PDDH. Como se señaló anteriormente, los resultados provistos por algunas de las herramientas de un sistema de información pueden ayudar a entender en mejor medida las redes criminales, las secuencias de crímenes, identificar individuos, zonas y grupos en riesgo, así como hacer lo propio frente a presuntos perpetradores. Adicionalmente, es posible modelar y entender en mayor medida las consecuencias y costos de la falta de intervención oportuna de las entidades estatales con responsabilidad de protección y los efectos de la impunidad.

Dado el carácter sensible de parte de esta información y la necesidad de preservar la integridad de las investigaciones, el acceso a los datos individuales y al detalle procesal debe operar bajo protocolos estrictos de seguridad de la información,

acceso controlado y trazabilidad de consultas, con especial reserva sobre la identidad de testigos y fuentes.

Una de las temáticas a las que puede abonar un sistema de información es al esclarecimiento de homicidios y crímenes asociados que tienen un impacto de tipos de violencia incluida la letal.

La información más desagregada de personas asesinadas, de los perpetradores y redes asociadas al crimen, desde una perspectiva macrocriminal, junto con herramientas que permiten asociar otros datos y delitos con el aumento de la violencia letal, pueden servir para fortalecer las investigaciones, asociar casos, determinar patrones, identificar posibles vínculos, a partir de variables relacionadas, y priorizar ciertos delitos. Así, por ejemplo, parte de los modelos usados más arriba y la experiencia de la comunidad que estudia la violencia contra personas defensoras muestran la relevancia de la persecución penal de las amenazas para esclarecer y prevenir homicidios, comprender patrones macrocriminales y vincular a diversas redes criminales.

Adicionalmente, es fundamental que en la interfaz las entidades vinculadas a la administración de justicia adopten una política de transparencia activa que permita acceder, de manera abierta o controlada, a parte de la información crítica sobre estado de casos –avances o retrocesos procesales, condenas, apelaciones, cumplimiento de la pena, etc.–. Ello supone una mayor transparencia y cooperación con organizaciones de la sociedad civil y la academia y entre las propias instituciones. Asimismo, deberían promoverse espacios de contrastación de datos o criterios en disputa respecto a la calificación de personas como defensoras de derechos humanos. Una interfaz que permita poner en diálogo estos ejercicios contribuiría, además, a visibilizar temas o zonas que permanecen silenciadas en los sistemas de información de la institucionalidad. Por ejemplo, en Colombia existen discrepancias y vacíos de información sobre los homicidios a personas defensoras y los procesos penales vinculados al esclarecimiento de estos, con datos variables entre entidades estatales, organismos internacionales, organizaciones de sociedad civil y academia.

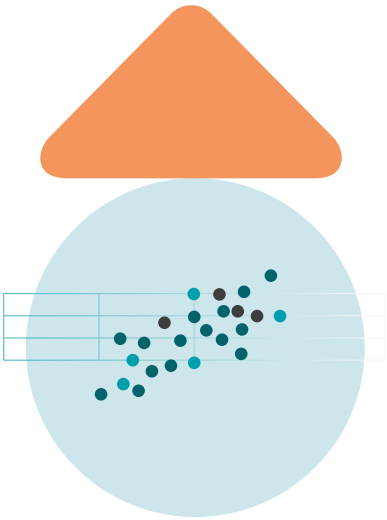
### d. Interfaces con espacios de protección de derechos y de memoria

Los espacios de la sociedad civil, los organismos internacionales, las defensorías del pueblo, las defensorías públicas y los mecanismos de verdad –como las comisiones de la verdad y los procesos de justicia transicional o de memorialización– cumplen un papel fundamental en la protección de los derechos de las personas defensoras

y en la construcción de memoria frente a las violencias que enfrentan. El sistema de información puede articularse con estos espacios para fortalecer la prevención, la protección, la investigación y la rendición de cuentas.

El valor de articularse con estos espacios reside en que un riesgo o un evento detectado por el sistema pueda canalizarse hacia la respuesta adecuada, que con frecuencia es multidimensional y excede la capacidad de una sola institución estatal. Así, la información del sistema puede ayudar a orientar y activar, según las necesidades de cada caso, el apoyo jurídico y la representación de las víctimas y los colectivos, las medidas de protección, el acompañamiento psicológico y psicosocial, la asistencia médica, la reubicación temporal o el refugio, y el apoyo cultural y lingüístico –incluida la adaptación a las lenguas de los pueblos y comunidades concernidas–. A su vez, por su cercanía con las personas y comunidades en riesgo, estos actores constituyen una fuente que retroalimenta al sistema. Para que esta articulación no genere nuevos riesgos, las interfaces deben prever formas de acceso reservado o controlado para las víctimas y sus representantes, preservando la confidencialidad y la seguridad de quienes intervienen.

Asimismo, la información sistematizada puede usarse e interactuar con la defensa de las víctimas y los colectivos —respaldando el litigio estratégico, las solicitudes de reparación y los procesos ante autoridades nacionales y órganos internacionales de protección— y con los procesos de verdad y memoria. En este último plano, los productos narrativos descritos más arriba pueden nutrir a las comisiones de la verdad, los archivos y los procesos de memorialización. Estas interfaces deben operar con el consentimiento de las personas y comunidades involucradas y bajo un enfoque centrado en las víctimas, de modo que la memoria fortalezca –y no comprometa– su seguridad.



# XI. Principios éticos de guía de las bases de datos o sistemas de información

Todo sistema de información, como el que aquí se propone, sobre agresiones contra PDDH debe regirse por principios éticos exigentes.

El primero de ellos es el principio de *no causar daño*. La recopilación, almacenamiento o difusión de datos nunca debe aumentar el riesgo de las personas defensoras ni exponer a sus familias, comunidades, fuentes u organizaciones o procesos de referencia. Las medidas de mitigación de riesgos como la trazabilidad de los accesos a información sensible deben estar al centro del diseño y la implementación de los sistemas de información.

A este principio rector se suman, de manera inseparable, los principios de *uso legítimo y de precaución*. Asimismo, cada registro debe estar orientado por una finalidad expresa, proporcional y conforme a los estándares interamericanos. Además, su diseño y operación deben incorporar salvaguardas que impidan que la información recopilada se emplee con fines de persecución, vigilancia, perfilamiento o estigmatización de las personas defensoras, sus familias, las organizaciones a las que puedan pertenecer o las comunidades por las que trabajen. La garantía de estos principios no es meramente declarativa, sino que exige mecanismos institucionales verificables de control interno y externo que permitan detectar y corregir usos desviados del sistema.

Adicionalmente, es imperativo considerar los principios de *privacidad*, *confidencialidad* y *seguridad digital*. La información debe ser tratada con criterios de minimización, acceso restringido cuando corresponda y protección frente a usos indebidos. En los casos pertinentes, deben existir mecanismos claros de *consentimiento informado* y de explicación sobre los usos posibles de la información recolectada.

También resultan esenciales los principios de *igualdad y no discriminación*. El sistema debe ser capaz de identificar impactos diferenciados sin reproducir sesgos estructurales ni exclusiones históricas. Uno de sus valores puede ser resolver o mitigar ausencias de información y sesgos en su recolección.

Finalmente, la *transparencia*, la *auditabilidad* y la *tutela efectiva de derechos* deben orientar tanto el diseño institucional como la operación cotidiana del sistema. La existencia de obligaciones de transparencia activa por parte del Estado debe asegurar la producción de información esencial para la política de protección de personas defensoras y para un entorno habilitante para el ejercicio de derechos de todas las personas. Adicionalmente, estas obligaciones se extienden al diseño institucional y su funcionamiento de modo de garantizar un escrutinio sobre la metodología de producción de información. A su vez, el sistema de información estatal sobre personas defensoras de derechos humanos debe estar orientado a la tutela efectiva de derechos reafirmando como vara para medir su valor, la capacidad efectiva de garantizar la vida y los derechos de personas, liderazgos sociales, organizaciones y comunidades vinculadas a la defensa de derechos.

# XII. Pautas para la gobernanza del sistema de información

La gobernanza responde a una pregunta que antecede a cualquier decisión técnica: quién administra el sistema, bajo qué reglas se adoptan las decisiones sobre su diseño y operación, cómo se distribuyen las competencias entre las entidades y actores que producen o articulan la información y cómo se comparte. En contextos caracterizados por la multiplicidad de fuentes, la gobernanza es precisamente el mecanismo que permite hacer operativa la estrategia de armonización y no sustitución, que garantiza la confiabilidad de la información y su uso para la protección de derechos[97].

Para que la gobernanza tenga efectos prácticos, debe expresarse en una estructura institucional mínima que determine quiénes intervienen, qué funciones cumplen, cómo usan y comparten la información y bajo qué reglas de control actúan. Esa estructura puede contemplar, al menos: una instancia coordinadora de carácter técnico, encargada de la operación y la continuidad del sistema; un comité técnico-metodológico responsable de las decisiones sobre variables, calidad e interoperabilidad; un comité de ética, seguridad y protección de datos que supervise el tratamiento de información sensible; un mecanismo permanente de participación

**97** Por ejemplo, el mandato de implementación articulada dispuesto por la Sentencia SU-546 de 2023 y el Auto 845 de 2024 de la Corte Constitucional colombiana, que ordenan la coordinación entre múltiples entidades (Mininterior, Mindefensa, Minjusticia, Minhacienda, DNP, Procuraduría, Defensoría y Fiscalía) bajo unificación conceptual y sujeción a los principios del hábeas data.

de las personas defensoras, las comunidades y las organizaciones de la sociedad civil, que intervenga en momentos clave del ciclo de vida del sistema –el diseño de categorías, variables, reglas de acceso y auditorías, la validación de riesgos y salvaguardas, la revisión de productos públicos y la evaluación periódica de su impacto–; protocolos de intercambio de información entre las entidades que producen o articulan datos; reglas de acceso diferenciado y trazabilidad según el nivel de sensibilidad; auditorías independientes a lo largo del ciclo de vida del dato; procedimientos accesibles para reportar usos indebidos, con mecanismos de reclamo y reparación; y reglas de suspensión del acceso ante riesgos, incidentes o filtraciones.

Esta arquitectura institucional es coherente con los Lineamientos Interamericanos de Gobernanza de Datos e Inteligencia Artificial de la OEA, que recomiendan establecer oficinas o entidades responsables con carácter técnico, definir con precisión los roles y responsabilidades en todo el ciclo de vida del dato y prever mecanismos de participación multiactor[98].

Un sistema de información sobre agresiones contra personas defensoras solo cumple su función protectora si incorpora mecanismos de participación significativa de las propias personas defensoras, las comunidades afectadas y las organizaciones de la sociedad civil en su diseño, implementación y evaluación. Este requisito no es meramente procedimental: enfrenta de manera directa la alta desconfianza que históricamente han manifestado quienes ejercen el derecho a defender derechos frente a la creación de bases de datos o registros estatales, desconfianza alimentada por antecedentes de uso de la información con fines de persecución, asesinato o perfilamiento. Un desafío significativo consiste en definir cómo integrar los datos estatales tomando en cuenta los registros de la sociedad civil sin comprometer la confianza ni la seguridad de las fuentes, preservando la autonomía de cada registro y garantizando que la participación opere como un control sustantivo sobre los usos legítimos del sistema.

La definición de roles y perfiles de acceso requiere un desarrollo específico, debido a su importancia para la seguridad, trazabilidad y uso legítimo de la información. En ese sentido, conviene diferenciar de forma explícita los permisos de registro, de consulta y de administración de la información, atendiendo tanto al nivel de

**98** OEA. *Lineamientos interamericanos de Gobernanza de Datos e inteligencia artificial*, 2024, disponible en: https://www.oas.org/ext/es/democracia/publicaciones/program/127

sensibilidad de los datos como a las necesidades de cada tipo de usuario. Esta diferenciación cumple una doble función: protege la información de las personas defensoras, las víctimas, los testigos y las fuentes, y fortalece la confianza de quienes aportan datos al sistema —confianza que, como se ha señalado, no puede darse por supuesta dada la histórica desconfianza frente a los registros estatales—. En coherencia con las salvaguardas previstas en la sección de manejo de datos de este documento, los perfiles deben asegurar que solo se acceda a datos identificables cuando exista una finalidad legítima, expresa y proporcional, y que ese acceso quede trazado. Adicionalmente, parte de la información puede ser anonimizada a efectos de limitar algunos de los riesgos de privacidad, seguridad o uso indebido. Los Lineamientos Interamericanos de la OEA antes mencionados respaldan este enfoque al recomendar la definición precisa de roles a lo largo del ciclo de vida del dato y la adopción de buenas prácticas de clasificación y categorización de la información para asegurar su protección[99].

Asimismo, este marco institucional debe cubrir no solo quién administra el sistema y cómo se recopilan los datos, sino también cómo se analizan y qué se hace con sus resultados, quienes acceden a que tipo de información y bajo que mecanismos de responsabilidad y trazabilidad, como se agrega o anonimiza, que es precisamente lo que distingue al sistema de un simple registro de hechos. A su vez, ninguna decisión sobre medidas de protección u otras políticas debe adoptarse con fundamento exclusivo en un algoritmo; por lo tanto, estas herramientas deben integrarse en una estrategia comprensiva que pondere también el contexto y las variables cualitativas, y deben someterse a supervisión humana permanente.

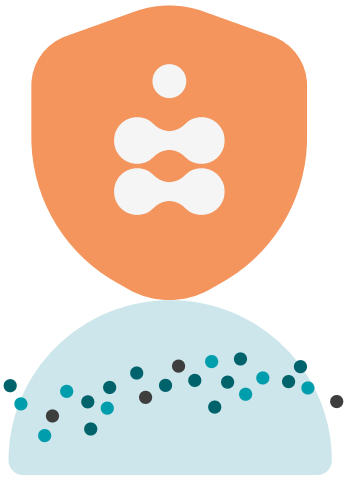
La gobernanza debe asegurar, en consecuencia, mecanismos verificables de auditabilidad, validación metodológica, trazabilidad de los resultados y rendición de cuentas sobre el acceso regulado a diversos tipos de datos y su uso, de modo que los productos analíticos sirvan a la protección sin reproducir sesgos, estigmatización, violaciones a la privacidad, ni nuevas formas de persecución, riesgo u exposición de las personas o grupos que el sistema busca proteger[100].

---

**99** OEA. *Lineamientos interamericanos de Gobernanza de Datos e inteligencia artificial*, 2024, lineamientos 5.4, 6.1 y 6.6

**100** OEA. *Lineamientos interamericanos de Gobernanza de Datos e inteligencia artificial*, 2024, lineamientos 5.4, 6.1 y 6.6.

Por último, la gobernanza no admite un diseño único, sino que debe adaptarse al punto de partida de cada país. Donde ya coexisten múltiples fuentes, el desafío es articularlas sin forzar su unificación ni suprimir su autonomía. Donde la violencia contra personas defensoras aún no se documenta sistemáticamente, la prioridad será crear registros básicos que incorporen desde su origen las salvaguardas y los mecanismos de participación necesarios. En ambos escenarios el objetivo es el mismo —convertir el sistema en una infraestructura activa de prevención y garantía—, pero la secuencia de las decisiones de gobernanza variará según cada realidad nacional.



## XIII. Conclusiones

Estos lineamientos buscan contribuir a la situación crítica que viven muchas personas defensoras de derechos humanos en el continente a través del cumplimiento de una obligación clara derivada del derecho internacional y constitucional: el establecimiento de un sistema nacional de información sobre agresiones contra personas defensoras de derechos humanos.

El camino de explorar las consecuencias de las guías provistas por el derecho internacional nos llevó a un proceso de estudio y aprendizaje junto a una comunidad interdisciplinaria, orientado a proveer elementos mínimos y desplegar el abanico de posibilidades de dichos sistemas. Y es que, en muchos casos, la información existe. De hecho, las entidades estatales, intergubernamentales, la academia y las organizaciones de la sociedad civil cuentan con un acervo significativo de datos relevantes. La carencia se marca primordialmente en la manera en que esa información se destila, articula, asocia y usa.

Por ello, este documento presenta una serie de recomendaciones mínimas sobre las categorías y variables a tener en cuenta, sobre los sistemas disponibles para procesar la información y los resultados necesarios para asegurar que esa información sea útil para la prevención, la protección individual y colectiva, la investigación de eventos –con un abordaje macrocriminal– y la rendición de cuentas.

En el ejercicio de no reinventar la rueda, realizamos investigaciones en profundidad sobre las bases existentes y encontramos una enorme riqueza de esfuerzos de sistematización. Sin embargo, las ausencias de información relevante, el escaso uso

de herramientas disponibles de mayor potencial y la falta de interfaces adecuadas son igualmente destacable. Procuramos desarrollar en el *Blueprint* el abanico de herramientas disponibles y posibles, atendiendo a las consideraciones técnicas, legales y de política pública basadas en una lectura aguda de la realidad y los obstáculos presentes en nuestro continente americano.

Como muchas iniciativas, esta tuvo un inicio y una serie de alianzas y contribuciones fundamentales de personas, instituciones y organizaciones vinculadas a la temática. El tiempo fue relativamente breve para la dimensión de la tarea. Esperamos continuar profundizando los debates, el aprendizaje conjunto y las aplicaciones de algunas de las innovaciones que se plasmaron en este documento.

El potencial de este trabajo es muy significativo para abordar un fenómeno persistente, de gran costo en vida, derechos y calidad de las democracias.

Anhelamos que este documento sirva para orientar la implementación de las obligaciones de diversos Estados en cumplimiento de sentencias y mandatos constitucionales e interamericanos bajo la CADH y el Acuerdo de Escazú. Asimismo, esperamos que estos lineamientos permitan discusiones más profundas e interdisciplinarias sobre la temática de modo de perfeccionar las herramientas, prácticas y políticas de quienes tienen la responsabilidad fundamental en el respeto y garantía del derecho a defender derechos y del entorno habilitante para su ejercicio. También, que permita amplificar y fortalecer el trabajo imprescindible que la propia sociedad civil y la academia hacen en desarrollo de su labor de defensa de derechos y de personas y comunidades vinculadas a la defensa de derechos humanos.

Nuevamente, agradecemos a quienes acompañaron el proceso de manera generosa, curiosa y práctica, sin perder nunca de vista que lo que está en juego es la posibilidad real de proteger, prevenir violencias y sostener sociedades más justas.

# Anexo

## Tabla de categorías analíticas del sistema de información

| Categoría y Definición | Subcategoría | Variables |
|---|---|---|
| **Personas defensoras / víctima**<br><br>Identificación funcional de la persona defensora o víctima, individual o colectiva, con las características que permiten comprender los riesgos diferenciados. No busca construir un censo cerrado. | **Perfil de la persona defensora** | Sexo y género; edad; lengua; pertenencia étnica o racial; orientación sexual; discapacidad; nacionalidad; situación migratoria; ocupación; profesión; educación; estatus socioeconómico; lugar de residencia; lugar de trabajo; pertenencia organizativa; afiliación institucional; militancia; tipo de liderazgo; sector o temática de la labor; antecedentes de riesgo; pertenencia o asociación, actual o previa, a movimientos sociales, procesos organizativos u organizaciones. |
| **Eventos y tipo de agresión**<br><br>Registro de los hechos y omisiones que constituyen agresión contra las personas defensoras y determinación del tipo de agresión. Incluye acciones y omisiones estatales. | **Tipo de agresión (acción u omisión)** | Homicidio; tentativa de homicidio; desaparición forzada; desaparición temporal; detención preventiva arbitraria; criminalización; lesiones; tortura; tratos crueles o inhumanos; violencia de género; violencia sexual; tortura sexual; esclavitud; esclavitud sexual; reclutamiento forzado; confinamiento; desplazamiento forzado; desalojo forzado; exilio; amenazas; hostigamiento; intimidación; campañas de estigmatización; discriminación; difamación; instigación a la violencia; doxxing; vigilancia ilegal; interceptación de comunicaciones; uso de spyware o malware; apagones de internet; desactivación de tarjetas SIM; bloqueo o interrupción de mensajería instantánea; cierres o suspensiones de organizaciones; obstáculos administrativos; restricciones indirectas; multas; ataques a sedes, comunidades, bienes colectivos y territorios. |
| **Criminalización**<br><br>Uso indebido del derecho penal, civil u otras ramas, por actores estatales y no estatales, con el fin o la consecuencia de inhibir, restringir o silenciar la defensa de los derechos humanos mediante la manipulación del poder punitivo del Estado. | **Criminalización per se** | Criminalización de conductas protegidas por la libertad de expresión (figuras de desacato, calumnia o difamación); actuación punitiva sin sustento legal (detención arbitraria, conforme al GTDA); uso de fueros militares para juzgar a civiles; determinación previa de criminalización por un órgano internacional competente (Corte IDH, CIDH, GTDA u otros procedimientos especiales u órganos de tratado). |
| | **Abusos del poder punitivo estatal** | Uso abusivo de las facultades de investigación y acusación (investigaciones o cargos múltiples, procesos basados en la asociación o pertenencia, cargos vagos o agravados); formulación de cargos falsos o infundados; dilación injustificada del proceso (demoras, secuenciación arbitraria, reprogramaciones, o divulgación tardía de los cargos); imposición de medidas cautelares desproporcionadas (detención preventiva arbitraria, vigilancia y allanamientos irrazonables, fianzas excesivas); imposición de penas desproporcionadas (multas excesivas, disolución de organizaciones); violaciones al debido proceso (limitaciones al derecho de defensa, obstrucción del acceso a la defensa técnica, retención de notificaciones, non bis in idem); uso abusivo de procedimientos administrativos (prohibiciones de ingreso a terceros países). |

| Categoría y Definición | Subcategoría | Variables |
|---|---|---|
| → **Criminalización** *(sigue)* | **SLAPPs (demandas estratégicas contra la participación pública)** | Demandas por daños a la propiedad o invasión de predios en el marco de la protesta o la defensa territorial; demandas por difamación y otras vinculadas a la libertad de expresión; litigios derivados de protestas que afectan proyectos extractivos o de infraestructura; demandas múltiples y simultáneas; uso abusivo de acciones de amparo (tutela) contra organizaciones o personas defensoras. |
| **Respuesta estatal frente al riesgo o al evento**<br>Reacción del Estado frente al riesgo y al hecho: medidas de prevención y protección y desempeño del sistema de justicia. | **Prevención y protección** | Solicitud de protección; estudio de riesgo; tiempo de respuesta; medidas urgentes; esquemas individuales, colectivos, territoriales o comunitarios; medidas cautelares (internas o de la CIDH); medidas provisionales; revisión, modificación o terminación de los esquemas, con sus razones; retorno seguro; suficiencia, adecuación y efectividad de las medidas; ataques ocurridos durante su vigencia; seguimiento de alertas tempranas institucionales |
| | **Justicia y superación de la impunidad** | Recorrido procesal (denuncias; investigaciones abiertas o en curso; acusaciones; condenas; apelaciones; condena en firme; prisión efectiva; absoluciones); niveles y redes de responsabilidad (autores materiales e intelectuales; cadenas de mando; financiadores, auxiliadores o actores con aquiescencia; niveles de planificación); garantías de acceso a la justicia y condiciones institucionales (independencia e imparcialidad; autonomía de los órganos de investigación y juzgamiento; fiscalías o unidades especializadas; capacidad institucional; corrupción); consideración del nexo con la labor de defensa; análisis contextual; tipo de pena; indicadores de desempeño (demoras procesales; estadísticas oficiales de esclarecimiento). |
| **Presuntos perpetradores**<br>Identificación de los presuntos perpetradores y redes de responsabilidad, sin que implique un juicio anticipado de culpabilidad; habilita un enfoque macrocriminal. | **Agentes estatales** | Jueces; fiscales; integrantes de la fuerza pública; funcionarios públicos; autoridades locales. |
| | **Actores no estatales** | Grupos armados organizados (diversos grupos ilegales, paramilitares u otras estructuras criminales, según dinámicas locales, nacionales, regionales y mundiales); actores no estatales individuales. |
| | **Actores empresariales (personas jurídicas)** | Corporaciones; empresas; contratistas; terceros financiadores. |
| | **Formas de articulación** | Arreglos mixtos; subcontratación criminal; actuación conjunta de redes que combinan agentes estatales y no estatales. |

| Categoría y Definición | Subcategoría | Variables |
|---|---|---|
| **Contexto**<br><br>Variables estructurales y territoriales que dan sentido al riesgo y permiten leer los hechos contra su trasfondo. | **Variables estructurales** | Áreas de especial conflictividad; ausencia estatal; presencia de actores armados legales o ilegales; economías ilícitas; niveles de corrupción; información socioeconómica regional; tasas de violencia (homicidio, feminicidio, lesiones, masacres, secuestro, violencia sexual, trata de personas, reclutamiento forzado, trabajo esclavo); indicadores educativos (escolaridad, deserción escolar). |
| | **Patrones** | Desaparición forzada; persecución; confinamiento; reclutamiento forzado; deforestación; impunidad |
| | **Predictores** | Cortes de internet; desplazamientos masivos y súbitos de poblaciones; contextos electorales; procesos de licenciamiento ambiental en países con debilidad institucional; disputas entre grupos armados ilegales. |

# Lineamientos para el desarrollo de sistemas de información para la prevención de crímenes contra personas defensoras de derechos humanos

Blueprint

Defendemos derechos
*para cambiar realidades*

**Con más de 30 años de experiencia,** trabajamos para reducir la desigualdad, la discriminación y la violencia, fortaleciendo la democracia, promoviendo y protegiendo los derechos humanos, y combatiendo la impunidad en la región. Nuestra misión es contribuir al pleno disfrute de los derechos humanos en las Américas mediante el uso eficaz de los mecanismos del Sistema Interamericano de Derechos Humanos (SIDH) y otros instrumentos internacionales de protección.

**Impulsamos estos procesos junto a víctimas, organizaciones y comunidades,** para que se traduzcan en justicia, garantías de no repetición y cambios reales en la región.

www.cejil.org

CEJIL
CENTRO POR LA JUSTICIA Y EL DERECHO INTERNACIONAL

ISBN 978-987-23854-8-4