MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Resolución PGN N° 56/2026

Buenos Aires, 14 de agosto de 2026.

VISTO:

El artículo 120 de la Constitución Nacional, las Leyes 24.946, 27.148, 26.734, 27.319 y 25.246, y las Resoluciones PGN n° 70/2018, 86/2018, 79/2023, 40/2024, 54/2024 y 51/2026.

Y CONSIDERANDO QUE:

Entre las atribuciones del Procurador General de la Nación se encuentra la de diseñar la política de persecución criminal para un ejercicio eficaz de la acción penal pública (artículos 33 de la ley 24.946 y 12 de la ley 27.148).

En ejercicio de esa atribución, y en atención a la grave amenaza que el terrorismo internacional representa para la paz y la seguridad, este Ministerio Público Fiscal ha venido desarrollando una política institucional sostenida de fortalecimiento de sus capacidades de prevención e investigación del fenómeno, entre cuyas manifestaciones se cuentan la creación de la Secretaría de Análisis Integral del Terrorismo Internacional (Resolución PGN n° 70/2018 y su complementaria n° 86/2018), la ampliación de atribuciones y reconversión de la Unidad Fiscal Especializada en Criminalidad Organizada (Resolución PGN n° 79/2023) y la incorporación del organismo al Centro Nacional Antiterrorismo (Resolución PGN n° 51/2026), entre otras.

La experiencia colectada en ese marco por la Secretaría de Análisis Integral del Terrorismo Internacional (SAIT) y la Unidad Fiscal Especializada en Criminalidad Organizada (UFECO), a partir de la colaboración y el trabajo sostenido con otras unidades especializadas de la Procuración General, con las fiscalías federales del país, con las agencias de las fuerzas de seguridad federales y con organismos internacionales, ha permitido advertir la necesidad de contar con un documento de referencia para la investigación de aquellos incidentes en los que el ataque terrorista aún no se ha producido, pero que presentan características distintivas vinculadas con procesos de glorificación, propaganda, radicalización, reclutamiento y movilización hacia la violencia.

Ello así por cuanto la diversidad de motivaciones, la utilización intensiva de ecosistemas digitales, la frecuente ausencia de estructuras jerárquicas y el carácter transnacional de muchas de estas actividades determinan que las investigaciones de esta naturaleza presenten un grado de complejidad

significativamente superior al de la criminalidad convencional y disímiles al de la criminalidad organizada, lo que exige un abordaje interdisciplinario y una coordinación permanente entre fiscales, fuerzas de seguridad, organismos de inteligencia financiera, especialistas en evidencia digital y en las restantes disciplinas conexas.

En esta dirección, la Secretaría de Análisis Integral del Terrorismo Internacional (SAIT) y la Unidad Fiscal Especializada en Criminalidad Organizada (UFECO) pusieron en consideración de este Despacho la *"Guía para la investigación de incidentes terroristas previos a un ataque"*, que desarrollaron de manera conjunta, tomando en cuenta, además, las instrucciones elaboradas por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) en materia de identificación de usuarios y preservación de la evidencia digital.

Se verificó que esta clase de incidentes se inicia, casi en su totalidad, mediante publicaciones de contenido extremista o amenazas difundidas en línea, respecto de las cuales la ausencia de criterios comunes de análisis conduce con frecuencia a que reciban un tratamiento propio de delitos comunes, sin atender al contexto en el que se inscriben, ni evaluar adecuadamente el riesgo que expresan.

El documento parte de la comprensión del terrorismo como proceso criminal organizado, continuo y permanente -conceptualizado por la doctrina especializada como *"Ciclo terrorista"*- en el que el atentado constituye únicamente el eslabón final y visible de una cadena previa de actividades interdependientes, y no como un hecho aislado o instantáneo. Esta concepción resulta consistente con el enfoque preventivo adoptado por la comunidad internacional a partir de la Estrategia Global de las Naciones Unidas contra el Terrorismo (Resolución A/RES/60/288 de la Asamblea General) y con las resoluciones del Consejo de Seguridad de las Naciones Unidas 1373 (2001), 2178 (2014), 2354 (2017), 2396 (2017) y 2462 (2019).

Sobre esa base, la Guía sistematiza los procesos de radicalización hacia el extremismo violento y la movilización, describe los mecanismos mediante los cuales los operadores de propaganda identifican y captan personalidades vulnerables -con particular atención a los entornos digitales, las plataformas de mensajería y los ecosistemas asociados a los videojuegos en línea- y propone una matriz de indicadores ideológicos, conductuales y sociales, ordenados en categorías progresivas relativas a teorías conspirativas y polarización social, identificación con ideologías extremistas, escalada discursiva, extremismo violento y movilización, clasificados según niveles de riesgo medio, medio-alto, alto y crítico, sugiriendo las medidas de investigación proporcionadas a cada nivel.

Asimismo, aporta una metodología de investigación integral estructurada en siete áreas complementarias de obtención y análisis de información, así como una lista de verificación destinada a ordenar la actividad investigativa.

Corresponde destacar que los indicadores y niveles de riesgo desarrollados en la Guía no constituyen tipos penales ni supuestos de imputación, tampoco importan atribución de responsabilidad penal y menos aún presunción de culpabilidad alguna. Se trata de una herramienta de gestión de riesgo y orientación de la actividad probatoria, cuya valoración deberá ser contextual, proporcional y acumulativa. Ningún indicador, considerado aisladamente, resulta suficiente para tener por acreditada la existencia de un delito ni habilita por sí la adopción de medidas coercitivas o intrusivas.

En igual sentido, la aplicación de las pautas contenidas en la Guía debe observar estrictamente el principio de legalidad, la libertad de expresión, de culto y de asociación, el derecho a la intimidad, la proporcionalidad y necesidad de las medidas de prueba y el debido proceso, con el control jurisdiccional que en cada caso corresponda, quedando excluida toda intervención fundada exclusivamente en la adhesión ideológica, la pertenencia religiosa, la nacionalidad, el origen étnico o el ejercicio legítimo de la crítica institucional.

Del mismo modo, la información proveniente de tareas de monitoreo de fuentes abiertas o suministrada por organismos nacionales o extranjeros con competencia en materia de inteligencia, seguridad o aplicación de la ley solo puede operar como "*notitia criminis"*, esto es, como dato inicial que habilita el despliegue de la actividad investigativa, debiendo el Ministerio Público Fiscal asumir la dirección del caso y validar tales datos mediante prueba independiente que resulte útil en un eventual juicio posterior, conforme a los mecanismos previstos en las Resoluciones PGN n° 40/2024 y n° 54/2024.

Teniendo en cuenta esas premisas, y de acuerdo con los fundamentos expuestos en el documento anexo que por la presente se aprueba, resulta conveniente poner a disposición de las y los magistrados y funcionarios de este Ministerio Público Fiscal criterios orientadores comunes para la investigación de incidentes terroristas previos a un ataque, sin perjuicio de la valoración que en cada caso concreto corresponda al representante del Ministerio Público a cargo de la investigación, conforme a las circunstancias comprobadas de la causa y a la estrategia procesal que estime adecuada.

En consecuencia, de acuerdo con lo normado por el artículo 120 de la Constitución Nacional y las leyes 24.946 y 27.148;

RESUELVO:

I. APROBAR la *"Guía para la investigación de incidentes terroristas previos a un ataque"*, presentada conjuntamente por la Secretaría de Análisis Integral del Terrorismo Internacional y la Unidad Fiscal Especializada en Criminalidad Organizada, que se agrega como anexo de la presente.

II. RECOMENDAR a las/los representantes del Ministerio Público Fiscal de la Nación que, en adelante, consideren la aplicación de esas pautas en la investigación de incidentes terroristas previos a un ataque, en particular en aquellos casos originados en publicaciones, manifestaciones de contenido extremista o amenazas difundidas en entornos digitales.

III. ENCOMENDAR a la Secretaría de Análisis Integral del Terrorismo Internacional y a la Unidad Fiscal Especializada en Criminalidad Organizada la difusión de la Guía, la asistencia y capacitación de las y los magistrados y funcionarios que así lo requieran, y su actualización periódica en función de la experiencia colectada y de la evolución del fenómeno.

IV. Protocolícese, hágase saber y, oportunamente, archívese.

2026

SAIT | Secretaría de Análisis Integral del Terrorismo Internacional
UFECO | Unidad Fiscal Especializada en Criminalidad Organizada

Guía para la investigación de incidentes terroristas previos a un ataque

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Guía para la investigación de incidentes terroristas previos a un ataque

---

Elaborado por la Secretaría de Análisis Integral del Terrorismo Internacional (SAIT) y la Unidad Fiscal Especializada en Criminalidad Organizada (UFECO)

Diseño: Dirección de Comunicación Intitucional
Publicación: agosto 2026

2026

SAIT | Secretaría de Análisis Integral del Terrorismo Internacional
UFECO | Unidad Fiscal Especializada en Criminalidad Organizada

Guía para la investigación de incidentes terroristas previos a un ataque

Contenido

La experiencia colectada por la Secretaría de Análisis Integral del Terrorismo (SAIT) y la Unidad Fiscal contra el Crimen Organizado (UFECO) a partir de la colaboración y el trabajo sostenido con otras Unidades Especializadas de la Procuración General, fiscalías federales del país, agencias de las Fuerzas de Seguridad Federal y organismos internacionales, ha permitido detectar la necesidad de producir un documento cuyo objetivo es servir de referencia para la investigación de incidentes terroristas en los que aún no se produjo el ataque terrorista pero que poseen ciertas características distintivas (glorificación, propaganda, radicalización, reclutamiento, movilización, etc).

Hemos observado que este tipo de incidentes se inician, casi en su totalidad, en forma de publicaciones de contenido extremista y/o amenazas en línea, respecto a las cuales no existe una conciencia judicial mínima que permita otorgarles un tratamiento jurídico adecuado dentro del contexto terrorista para evitar que sean investigadas como simples delitos comunes.

Mas allá del encuadre jurídico que, en definitiva, merezca cada hecho en particular, la investigación propiamente dicha debe primeramente responder cuestionamientos básicos que permitan determinar fehacientemente frente a qué clase de conductas nos enfrentamos y así evaluar el riesgo y el grado de peligrosidad del hecho y del/los investigados.

I. El ciclo terrorista

Actualmente hay consenso que el fenómeno terrorista no se reduce únicamente el atentado, el cual solo resulta ser el eslabón final de una larga cadena de concatenaciones previas. En efecto, el fenómeno del terrorismo contemporáneo presenta características propias que lo distinguen de manera cualitativa de otras formas de criminalidad grave. Debe quedar claro desde el inicio que no estamos en presencia de un delito aislado ni de un hecho instantáneo, sino de un proceso complejo, organizado y permanente, que se desarrolla a lo largo del tiempo y a través de múltiples fases funcionalmente coordinadas e intrínsecamente conectadas. La doctrina especializada ha conceptualizado este proceso como “Ciclo Terrorista”[1], para el cual la comisión de un atentado constituye únicamente la fase final y visible de una serie previa de actividades interdependientes que resultan indispensables para su concreción.

1. LASMAR, J. M. A legislação brasileira de combate e prevenção do terrorismo quatorze anos após 11 de Setembro: limites, falhas e reflexões para o futuro, Revista de Sociologia e Política, v. 23, n. 53, p. 47-70, mar. 2015. y LASMAR, J. M. As Dinâmicas Financeiras do Terrorismo Internacional In: Perspectivas do Terrorismo Transnacional Contemporâneo, ed.1. Belo Horizonte: Arraes, 2019, v.1, p. 135 - 165.

"United Nations Interregional Crime and Justice Research Institute. (2024). The nexus between transnational organized crime and terrorism in Latin America. UNICRI.

En efecto, la experiencia comparada y los estudios empíricos muestran que la mayor parte del tiempo y de los recursos de las organizaciones y los individuos vinculados al terrorismo se destinan a tareas de propaganda, adoctrinamiento, reclutamiento, radicalización, financiamiento, obtención de medios logísticos, inteligencia y selección de objetivos, siendo el acto violento final una mínima porción del fenómeno en su conjunto.

Todas y cada una de estas etapas constituyen una unidad de acción con un propósito único, lo que implica que cada fase del ciclo terrorista forma parte del fenómeno delictivo y no puede ser escindida, aun cuando las conductas individuales y específicas puedan no tener por sí solas relevancias penales directas e inmediatas.

En este sentido, debemos partir de la premisa de que el terrorismo no puede ser

comprendido como un simple “evento”, sino como una empresa criminal organizada, de carácter permanente, en la cual cada uno de los aportes funcionales cumple un rol específico y necesario para la producción del resultado final de violencia.

Así, las actividades de propaganda, radicalización, reclutamiento, financiamiento, provisión de medios, apoyo logístico o realización de tareas de inteligencia de una organización o individuo terrorista no son conductas neutrales, equívocas ni jurídicamente irrelevantes. Por el contrario, constituyen aportes objetivos y dolosos a un camino criminal destinado a la comisión de actos de extrema gravedad. Cada una de estas acciones incrementa de manera concreta la capacidad operativa de la entidad, grupo o individuo terrorista y, con ello, el riesgo para la población y para el orden institucional.

Por lo tanto, esperar a que ocurra un atentado o se encuentre en la fase inminente de su ejecución para que el derecho penal intervenga, no solamente resulta ineficaz sino negligente frente a la naturaleza preventiva que debe adoptarse frente al terrorismo y a la función protectora del Estado de Derecho.

Esta concepción filosófico-penal del terrorismo como un fenómeno progresivo y no como un hecho aislado encuentra un sólido respaldo en el derecho internacional. Desde la adopción de la “Estrategia Global de las Naciones Unidas contra el terrorismo”[2], la comunidad internacional abandonó definitivamente la visión exclusivamente reactiva del terrorismo para adoptar un enfoque integral basado en la prevención, en la interrupción temprana de los procesos de radicalización y en el fortalecimiento de las capacidades estatales para detectar e investigar todas las fases que conducen a un atentado.

Pilares de la Estrategia Global de las Naciones Unidas contra el Terrorismo

Hacer frente a las condiciones que propician la propagación del terrorismo	**Prevenir y combatir** el terrorismo	**Fortalecer la capacidad** de los Estados para prevenir el terrorismo y luchar contra él	**Asegurar el respeto** de los DDHH y el imperio de la ley

2. Resolución de la Asamblea General de las Naciones Unidas A/RES/60/288

Importancia investigativa

Desde la perspectiva investigativa, el concepto de “Ciclo Terrorista” posee una relevancia central para la actuación del Ministerio Público Fiscal, en tanto permite comprender que los atentados terroristas no constituyen hechos espontáneos, aislados o desvinculados de actividades previas. Por el contrario, y como se dijo los estudios académicos especializados y los informes elaborados por organismos internacionales sumados a la experiencia de la SAIT y la UFECO coinciden en señalar que los actos terroristas se encuentran precedidos de procesos graduales de radicalización, captación ideológica, propaganda, financiamiento, adquisición de capacidades técnicas, logística, inteligencia y planificación, los cuales pueden desarrollarse durante extensos períodos de tiempo.

Precisamente, una de las principales características del terrorismo actual consiste en que gran parte de las conductas relevantes para la concreción del acto violento se producen con anterioridad al ataque y, frecuentemente, en ámbitos digitales, descentralizados y transnacionales, donde los actores extremistas desarrollan tareas de propaganda, adoctrinamiento, reclutamiento y coordinación operativa.

Ello impone la necesidad de adoptar un enfoque investigativo integral que permita detectar tempranamente indicadores objetivos de radicalización y movilización hacia la violencia, identificar redes de apoyo, individualizar reclutadores, financistas y facilitadores logísticos, y reconstruir las dinámicas organizativas que sostienen el proceso criminal. En este sentido, la investigación no debe limitarse únicamente a reconstruir atentados ya consumados, sino también a desarticular estructuras, interrumpir procesos de captación y evitar la consolidación de ecosistemas extremistas capaces de generar actos de violencia.

Para ello, la investigación debe fundarse siempre en indicadores objetivos, verificables y jurídicamente relevantes, respetando estrictamente las garantías vinculadas con la legalidad, la libertad de expresión, la proporcionalidad y el debido proceso.

En definitiva, comprender que el terrorismo es un proceso criminal continuo, implica reconocer que la amenaza terrorista comienza a construirse mucho antes de la detonación de un explosivo, de un ataque armado o de la ejecución material de un atentado. Consecuentemente, la eficacia de la respuesta estatal dependerá, en gran medida, de la capacidad de las autoridades judiciales y de las fuerzas de seguridad de identificar, documentar y analizar aquellas conductas que permitan verificar riesgos, neutralizar amenazas y proteger de manera efectiva a la sociedad y al Estado de Derecho.

Lo que entendemos por radicalización

Generalmente el primer paso en un proceso de radicalización hacia el extremismo violento que conduce al terrorismo suele ser lo que en doctrina se conoce como "apertura cognitiva"[3], conceptualizada como el momento en que una persona comienza a cuestionarse las ideas, las normas y las instituciones que antes aceptaba y ahora rechaza. Muchas veces, esta apertura sucede mientras se transcurre una crisis identitaria, personal o espiritual, o cuando se perciben injusticias o agravios intolerables, ya sea hacia la propia persona o hacia ciertas comunidades o religiones. En la búsqueda de explicaciones o de un significado a esas inquietudes, el individuo se vuelve más receptivo a ideologías alternativas con las cuales toma contacto al iniciar investigaciones personales. En estas búsquedas una persona puede toparse con propaganda extremista e identificarse con una ideología o con una comunidad radical y comenzar a justificar el empleo de la violencia como método válido.

Seguidamente, el individuo puede transitar hacia una fase de búsqueda de sentido y encuadre ideológico, en la que comienza a adoptar narrativas que atribuyen causalidad a los agravios percibidos, frecuentemente mediante esquemas dicotómicos que oponen un "nosotros" frente a un "ellos". En este nivel se verifica una progresiva internalización de discursos radicales, que pueden ser reforzados a través de entornos sociales, redes digitales o vínculos interpersonales, consolidando así una identidad alineada con postulados extremistas.

En etapas ulteriores del proceso, se observa una intensificación del compromiso ideológico y una creciente aceptación de la violencia como medio legítimo para la consecución de los fines propuestos. En términos de la llamada "escalera hacia el terrorismo"[4], ello se corresponde con los niveles intermedios y superiores, en los cuales el individuo no solo justifica moralmente el empleo de la violencia, sino que también puede comenzar a identificar objetivos, legitimar a perpetradores de actos terroristas y deshumanizar a quienes son definidos como adversarios o enemigos.

El tramo final del proceso se caracteriza por la movilización hacia la acción, donde el sujeto puede involucrarse activamente en actividades de apoyo, facilitación o ejecución de actos violentos. Este estadio implica la superación de inhibiciones morales y sociales, así como la consolidación de mecanismos de racionalización que permiten al individuo percibir su accionar como legítimo, necesario o incluso obligatorio. La literatura especializada destaca que no todos los individuos que transitan etapas previas alcanzan este nivel, siendo el

3. "Apertura cognitiva" es un término acuñado por el sociólogo Quintan Wiktorowitz.
4. Ver Fathali Moghadam , "La Escalera al terrorismo".

pasaje a la acción un fenómeno relativamente infrecuente en términos comparativos.

El modelo de radicalización desarrollado por McCauley y Moskalenko[5] complementa esta visión al identificar mecanismos tanto individuales como grupales —como la victimización percibida, la polarización, la presión de pares o la competencia intergrupal— que pueden acelerar o profundizar el proceso. Dichos autores enfatizan el carácter multifactorial y dinámico de la radicalización, descartando explicaciones simplistas o unicausales y subrayando la interacción entre variables psicológicas, sociales y contextuales.

Desde una perspectiva jurídica, los modelos mencionados permiten estructurar un marco interpretativo útil para la identificación temprana de indicadores de radicalización, evaluación de riesgos y diseño de estrategias judiciales de detección oportuna del extremismo violento. No obstante, corresponde destacar que tales esquemas poseen carácter descriptivo y no determinista, en tanto la trayectoria de cada individuo puede verse interrumpida, revertida o desviada en función de intervenciones oportunas o de la concurrencia de factores protectores.

II. Matriz de riesgo a ser usada en investigaciones

Profusa evidencia ha dado cuenta que no existe un perfil único de terrorista individual y que resulta imposible detectar al individuo que cometerá el próximo acto terrorista a partir del estudio de características personales como edad, sexo, raza, ideología, creencias, nivel socio-económico, etc. Sin embargo, la construcción de indicadores ideológicos, conductuales y sociales plausibles que permitan examinar si una persona está en proceso de radicalización y movilización a la violencia, son herramientas indispensables para la prevención e investigación penal.

El posteo de un mensaje glorificando un atentado, efectuando propaganda de un individuo o una organización terrorista o incitando a la comisión de actos de esa naturaleza, podría indicar que la persona que lo publica estaría transitando un proceso de radicalización. Detectar ese proceso implica observar y registrar los cambios progresivos que experimenta esa persona que termina justificando la violencia como la única manera de hacer valer sus creencias o ideas. En ese tránsito, existen patrones ideológicos, conductuales y sociales que pueden ayudar a detectar la fase en la que se encuentra la persona investigada, su

5. McCauley, Clark y Moskalenko, Sophia, “How Radaicalization Happens to Them and Us”, Oxford University Press, New York, 2011 y “Understanding Political Radicalization: Two Pyramids Model”. American Psychologist, 2017.

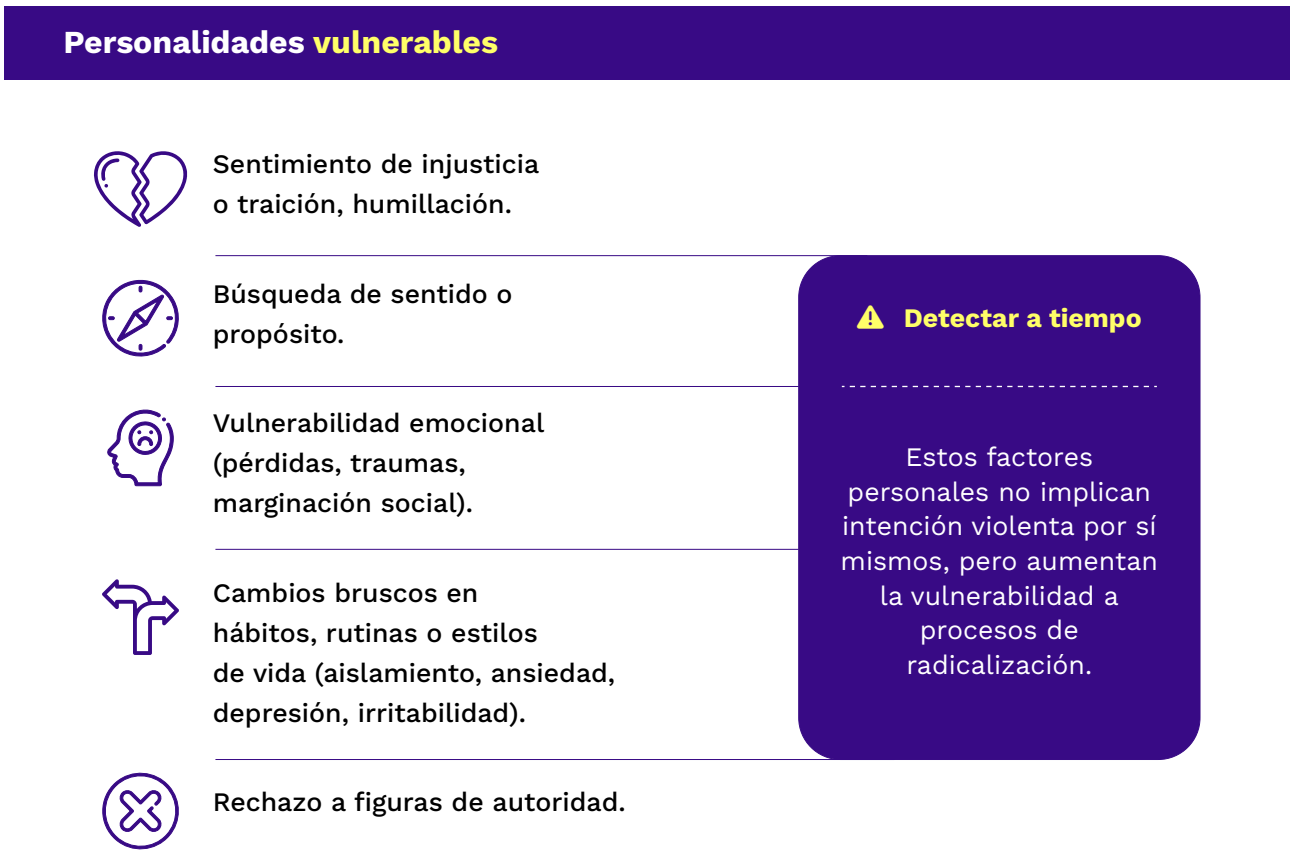
grado de peligrosidad y el riesgo que representa para la sociedad, todo lo cual incide en las decisiones a tomar en una investigación penal.

En base a lo expuesto presentamos una serie de indicadores, aclarando desde ya que deben ser entendidos como señales de alerta orientados a comprender procesos de radicalización, fortalecer su detección y establecer el nivel de amenaza y riesgo que debe atribuírsele a una determinada conducta, especialmente en investigaciones vinculadas con extremismo violento, amenazas híbridas o terrorismo. Creemos que la utilidad de estos indicadores reside principalmente en que permiten un adecuado análisis tendiente a orientar medidas de prueba, priorizando una estrategia de investigación basada en evidencia y facilitando la articulación con áreas especializadas, servicios de salud mental, entornos educativos o actores comunitarios, para evitar tanto la criminalización indebida de conductas ambiguas como el descarte de señales relevantes que, consideradas integralmente, podrían anticipar escenarios de riesgo.

Debemos advertir además que la evaluación de estos indicadores debe realizarse de manera contextual, proporcional y acumulativa. Ninguno de ellos constituye por sí mismo evidencia suficiente de criminalidad ni habilita automáticamente la adopción de medidas coercitivas. Sin embargo, su identificación puede resultar de alto valor, especialmente cuando converge con otros indicadores.

Ahora bien, la base sobre la cual se asientan los indicadores obliga a explicar previa y brevemente el concepto de “Personalidad vulnerable”, que en materia de prevención del extremismo violento y terrorismo[6] demuestra que determinados factores psicosociales pueden incrementar la susceptibilidad de una persona frente a procesos de captación ideológica y movilización hacia la violencia. Entre dichos factores suelen identificarse sentimientos persistentes de injusticia, humillación o exclusión; crisis de identidad; necesidad de pertenencia; vulnerabilidad emocional derivada de pérdidas, traumas o aislamiento social; así como síntomas de ansiedad, depresión o irritabilidad.

6. Véase reportes coincidentes de UNODC, CTED, Europol y la ICCT.



—

Gráfico número 1. Personalidades Vulnerables

Forma en que los reclutadores identifican personalidades vulnerables a su propaganda extremista:

En términos generales, los operadores de propaganda extremista suelen focalizarse en las personalidades vulnerables descriptas en el gráfico 1. Se trata de sujetos que manifiestan sentimientos de aislamiento social, frustración, resentimiento, pérdida de sentido vital, crisis de identidad o necesidad de pertenencia a un grupo. Estas características personales suelen exteriorizarse mediante publicaciones, comentarios o interacciones en entornos digitales donde los usuarios expresan emociones vinculadas con exclusión, discriminación, fracaso personal, enojo político o desconfianza hacia las instituciones estatales y sociales.

A partir de dichas manifestaciones los reclutadores identifican perfiles potencialmente receptivos a narrativas extremistas, particularmente aquellas basadas en discursos victimistas, conspirativos, apocalípticos o de confrontación contra determinados grupos sociales, religiosos, políticos o culturales.

Los procesos de captación suelen desarrollarse mediante una lógica gradual y relacional. Inicialmente, los actores extremistas difunden propaganda de manera masiva en espacios digitales abiertos —redes sociales, foros, plataformas de mensajería o comunidades virtuales— a fin de detectar usuarios que reaccionen positivamente o manifiesten afinidad ideológica con determinados contenidos. Posteriormente, una vez identificados dichos perfiles amistosos, los contactos se trasladan hacia espacios de interacción más cerrados y personalizados, donde el vínculo interpersonal adquiere centralidad. En esta etapa, el reclutador procura construir confianza, brindar contención emocional y reforzar narrativas dicotómicas de "nosotros contra ellos", promoviendo progresivamente la internalización de creencias extremistas y legitimando el uso de la violencia como herramienta política, religiosa o ideológica.

En este sentido, se ha señalado que el proceso de radicalización digital no depende exclusivamente de la exposición a propaganda, sino de la convergencia entre factores individuales de vulnerabilidad y dinámicas sociales de pertenencia y reconocimiento. Precisamente por ello, las organizaciones terroristas explotan necesidades psicológicas vinculadas con identidad, propósito, reconocimiento y comunidad, ofreciendo a los individuos una narrativa simplificada del mundo, una causa trascendente y un espacio colectivo donde sentirse aceptados o valorados.

En este punto conviene hacer traer a colación una teoría académica desarrollada por investigadores de la Universidad de Maryland denominada "Teoría de las 3N (Needs, Narratives y Networks)[7], que se traduce al idioma español como Necesidades, Narrativas y Redes.

Esta teoría parte de la premisa de que la radicalización no constituye el resultado de un único factor causal, sino de la interacción dinámica entre tres dimensiones fundamentales: una necesidad psicológica (Need), una narrativa ideológica (Narrative) y una red social de apoyo (Network). La convergencia de estos tres elementos explica por qué determinadas personas, expuestas a circunstancias similares, desarrollan procesos de radicalización mientras otras no lo hacen.

El primer componente, denominado Necesidad (Need), refiere a la existencia de una motivación psicológica vinculada con la búsqueda de significado personal, reconocimiento, dignidad o propósito vital. Según esta concepción, las personas experimentan la necesidad de sentirse valiosas y socialmente relevantes. Cuando dicha necesidad resulta frustrada —como consecuencia de experiencias de humillación, discriminación, fracaso personal, exclusión social, pérdida de estatus, acontecimientos traumáticos o percepciones de injusticia— puede

7. La teoría fue desarrollada principalmente por Arie Kruglanski, Jocelyn Belanger, y Rohan Gunartna para el Centro de Estudios del Terrorismo de la Universidad de Maryland.

surgir una intensa búsqueda de significado. Esta situación no conduce necesariamente al extremismo; sin embargo, incrementa la vulnerabilidad del individuo frente a narrativas capaces de ofrecer respuestas simples y emocionalmente satisfactorias a sus frustraciones.

El segundo componente corresponde a la narrativa (Narrative), entendida como el sistema ideológico que proporciona una explicación coherente acerca del origen de los agravios percibidos, identifica responsables, define enemigos y ofrece un mecanismo para recuperar el significado perdido. La narrativa extremista interpreta la realidad mediante categorías dicotómicas —"nosotros" frente a "ellos", "víctimas" frente a "opresores", "creyentes" frente a "enemigos"— y presenta a la violencia como una respuesta legítima, necesaria o incluso moralmente obligatoria para restaurar la justicia o proteger al grupo de pertenencia. Durante esta etapa se produce la denominada identificación ideológica, en la cual el individuo comienza a adoptar progresivamente símbolos, consignas, referentes históricos, discursos y valores propios de una determinada ideología extremista, fortaleciendo su sentido de pertenencia y redefiniendo su identidad personal en función de dicha causa.

El tercer elemento es la Red (Network), es decir, el conjunto de relaciones personales y sociales que validan, refuerzan y consolidan la narrativa previamente adoptada. Las investigaciones realizadas demuestran que las ideas radicales adquieren mayor estabilidad cuando son compartidas en un entorno social que proporciona reconocimiento, aceptación y apoyo emocional. En la actualidad, estas redes no se limitan a organizaciones terroristas tradicionales, sino que comprenden también comunidades virtuales, plataformas digitales, canales de mensajería cifrada, foros especializados, videojuegos en línea y otros ecosistemas donde los individuos encuentran referentes ideológicos, mentores y pares que fortalecen su identidad extremista. En este contexto, la presión grupal, el reconocimiento social y la validación permanente favorecen la progresiva normalización de discursos de odio, la deshumanización del adversario y la legitimación de la violencia como herramienta ideológica o religiosa.

Trajimos a colación esta concepción porque entendemos que posee una especial utilidad para la investigación penal de incidentes terroristas, al permitir comprender la radicalización como un proceso evolutivo susceptible de ser detectado e interrumpido en etapas tempranas. En lugar de centrar exclusivamente la atención en la preparación material de un atentado, el modelo invita a identificar indicadores vinculados con vulnerabilidades personales, cambios en la identidad ideológica y transformaciones en los vínculos sociales del individuo. En consecuencia, la detección de factores de vulnerabilidad, la adopción progresiva de narrativas extremistas y la integración en redes de validación ideológica constituyen elementos relevantes para la evaluación del riesgo, la priorización de investigaciones y el diseño de estrategias preventivas orientadas a impedir la transición desde la radicalización cognitiva hacia la movilización operativa.

Veremos a continuación en detalle la serie de indicadores que nos permiten evaluar el grado de radicalización y peligrosidad de una persona teniendo siempre en cuenta que la radicalización es un proceso dinámico y no lineal en el cual un sujeto puede avanzar, estancarse o retroceder en distintos momentos.

III. Indicadores

Teorías Conspirativas:

Uno de los indicadores tempranos de mayor relevancia dentro del proceso de radicalización hacia el extremismo violento son las llamadas “teorías conspirativas”, que conducen a la polarización social. Estas narrativas funcionan como estructuras de legitimación ideológica y predisponen a determinados individuos a justificar el uso de la violencia contra personas,

grupos o instituciones identificadas como responsables de supuestos agravios, ya sea personales o colectivos.

Tienen la particularidad de simplificar fenómenos políticos, económicos, sociales o religiosos complejos mediante construcciones bipolares y emocionalmente movilizadoras, en las cuales determinados actores son presentados como enemigos absolutos, ocultos o conspirativos y responsables de una amenaza existencial contra la propia comunidad.

En esa línea, comienza a tomar forma y adquirir especial relevancia la ya mencionada visión maniquea ("ellos y nosotros"), entendida como construcción lógica binaria donde el mundo queda dividido entre un "bien absoluto" —representado por el propio grupo ideológico, religioso, político o identitario— y un "mal absoluto", atribuido al adversario. Esta lógica elimina progresivamente los espacios de diálogo, complejiza la aceptación de mecanismos de resolución de conflictos y favorece procesos de deshumanización de aquellos a quienes se considera enemigos. La literatura académica especializada8 sostiene que la deshumanización constituye un componente recurrente en los procesos de radicalización, en tanto permite justificar moralmente agresiones contra individuos, grupos, etnias, razas, basados en que los destinatarios representan amenazas existenciales, o son traidores, invasores, enemigos internos o agentes de una conspiración superior.

A ello se suma que las teorías conspirativas suelen atribuir a actores ocultos, élites, gobiernos, minorías poderosas o determinados grupos religiosos o étnicos, la responsabilidad de acontecimientos políticos, económicos o sociales relevantes, aunque sin sustento fáctico verificable. En entornos extremistas, el consumo de dichas teorías funciona frecuentemente como "puerta de entrada" hacia narrativas radicales más complejas, dado que generan desconfianza institucional y favorecen la percepción de que los mecanismos legales o políticos tradicionales resultan inútiles para revertir la supuesta amenaza. Diversos estudios internacionales9 sobre extremismo en línea han demostrado que estos relatos poseen una elevada capacidad de viralización en plataformas digitales, especialmente cuando son acompañados por contenido emocional, desinformación, discursos de agravio colectivo o reinterpretaciones distorsionadas de hechos reales.

Asimismo, los discursos de odio y los procesos de polarización social extrema representan elementos centrales dentro de esta categoría. Los discursos de odio comprenden expresiones que promueven, justifican o incitan a la hostilidad, la discriminación o la violencia y suelen difundirse mediante memes, hashtags, videos, narrativas humorísticas o lenguaje codificado, dificultando su detección inmediata. La polarización extrema, por

8. Belanger J. & Kruglanski A. (2019), "Radicalization leading to violence: A test of the 3N model". Frontiers in Psychiatry. Reicher, Stephen. Cambridge Habdbook of the psychology of Violent Extremism (2025). "The Role of dehumanization". Cambridge University Press.

9. Radicalization Awareness Netowrk – The Impact of Conspiracy Narratives on Violent Right-Wing and Left-Wing Extremist Narratives (2021).

su parte, se manifiesta a través del rechazo sistemático a perspectivas divergentes, el aislamiento en comunidades ideológicamente homogéneas y una creciente hostilidad frente a quienes sostienen posiciones distintas. Este fenómeno favorece el cierre cognitivo y reduce la exposición a discursos moderadores o a contra-narrativas.

Un último elemento a considerar es la desconfianza sistemática en las instituciones y liderazgos democráticos, la cual puede expresarse mediante la deslegitimación del sistema judicial, los procesos electorales, las fuerzas de seguridad, los medios de comunicación, o autoridades legítimamente constituidas. Cabe aclarar que, si bien la crítica institucional constituye una manifestación legítima protegida por la libertad de expresión, su importancia en términos investigativos aumenta cuando se combina con llamados implícitos o explícitos a desconocer el orden democrático, justificar acciones violentas o promover la sustitución coercitiva de las instituciones por mecanismos de fuerza.

—

Gráfico número 2 representativo de Indicadores Tempranos

Ejemplos de Conductas asociadas a Teorías Conspirativas y Polarización Social.

- Creencia en narrativas o ideologías que justifican la violencia contra oponentes.
- Aparición de cambios en el círculo de amistades.
- Rechazo a figuras de autoridad.
- Expresión de sentimientos de injusticia, traición y/o humillación.
- Publicación de teorías conspirativas que justifican la violencia.
- Expresión de que personas con ideas o pensamientos distintos deben tener un escarmiento.
- Búsqueda de material ideológico.

Identificación con Ideologías Extremistas

El segundo nivel lo constituye lo que llamamos "Identificación con ideologías extremistas" y comprende el conjunto de indicadores vinculados con la adhesión progresiva, explícita o implícita, a narrativas, símbolos, comunidades o doctrinas que legitiman la violencia política, religiosa, racial o identitaria como mecanismo válido de acción. Existen publicaciones académicas[10] que sostienen que los procesos de radicalización suelen comenzar por una etapa de identificación ideológica, en la cual el individuo comienza a adoptar criterios extremistas que reorganizan su percepción de la realidad, redefinen sus amigos y enemigos y justifican mecanismos de confrontación violenta. Esta categoría permite detectar señales de profundización ideológica y consolidación de una identidad extremista previa a eventuales conductas operativas.

Uno de los indicadores centrales de este grupo es la adopción de símbolos, emblemas, consignas o referencias asociadas a organizaciones o movimientos extremistas[11]. Dicha adopción puede manifestarse mediante imágenes de perfil, banderas, iconografía, tatuajes, hashtags, memes, frases codificadas o referencias históricas utilizadas recurrentemente en entornos radicalizados. La literatura especializada[12] señala que estos elementos cumplen una doble función: por un lado, consolidan el sentido de pertenencia grupal e identidad colectiva; por el otro, facilitan el mutuo reconocimiento entre miembros o simpatizantes dentro de comunidades digitales cerradas o semiclandestinas. En los ecosistemas extremistas contemporáneos, particularmente en plataformas descentralizadas o foros cerrados, el lenguaje simbólico y los códigos visuales son crecientemente utilizados debido a su capacidad para evadir mecanismos

10. "Social Identity Theory and the Study of Terrorism and Violent Extremism", Anders Strindberg. Swedish Defense Research Agency.

11. Una conducta repetitiva que se ha observado en las causas estudiadas es la incorporación de palabras, nombres, simbología a cuentas personas tales como direcciones de correos electrónicos, contraseñas, etc. Es común encontrar, por ejemplo, correos del estilo 1488@gmail.com o dylanklebold@hotmail.com

12. Horgan, J. (2005). The Psychology of Terrorism. Radicalisation Awareness Network (2021). *Manifestations of Violent Right-Wing Extremism and Practices for P/CVE*.

automáticos de moderación y transmitir mensajes ideológicos de modo subrepticio.

Otro aspecto de alta relevancia investigativa es el consumo sistemático de propaganda o contenido extremista. Este fenómeno comprende la exposición frecuente y progresiva a materiales audiovisuales, manifiestos, discursos, publicaciones, podcasts o contenidos digitales que glorifican organizaciones extremistas, justifican atentados o promueven narrativas de odio y confrontación. Se ha demostrado que la repetición constante de propaganda extremista puede producir procesos de normalización cognitiva de la violencia, reforzar sesgos ideológicos y disminuir barreras morales frente a la agresión contra determinados grupos. Debemos también poner énfasis en la denominada "auto-radicalización digital", fenómeno en el cual individuos vulnerables consumen de manera autónoma contenidos extremistas sin contacto directo inicial con reclutadores ni miembros de organizaciones terroristas, desarrollando progresivamente una cosmovisión personal radicalizada.

Asimismo, la participación en grupos, foros o canales digitales que promueven ideologías extremistas constituye otro indicador significativo de esta categoría. Plataformas como Telegram, Discord, SoundCloud, redes descentralizadas y comunidades cerradas son utilizadas no solo para difundir propaganda, sino también para reforzar dinámicas de pertenencia, validación grupal y aceleración ideológica. En dichos espacios suelen desarrollarse mecanismos de presión social, reforzamiento mutuo, glorificación de ataques previos y deshumanización del adversario. La participación activa en estas comunidades, evidenciada cuando la persona comienza a interactuar recurrentemente, comparte contenido extremista, busca reconocimiento interno o establece vínculos con otros usuarios de perfil radicalizado revela una peligrosa aceleración en el proceso de radicalización.

Finalmente, y como ya hemos visto, la aceptación progresiva de narrativas que presentan a la violencia como necesaria, legítima o inevitable para alcanzar determinados objetivos ideológicos, expresada mediante discursos que niegan legitimidad, humanidad o derechos básicos a quienes sostienen posiciones ideológicas diferentes, es un indicador importante a tener en cuenta.

—

Gráfico número 3.

Ejemplos de Identificación con ideologías extremistas

- Aislarse de la familia y amigos, citando recurrentemente ideología o doctrinas extremistas.
- Cambiar de vocabulario, forma de hablar o comportamiento habitual para reflejar un nuevo punto de vista asociado a ideas radicalizadas.
- Rechazo al debate o lectura de ideas o personas con discursos no violentos.
- Búsqueda, investigación de atentados o atacantes del pasado.
- Consumo y difusión de contenido extremista violento.
- Expresiones de deseos de notoriedad o voluntad de morir a través de actos de extremismo violento y/o actos terroristas.

Escalada Discursiva

Se trata de una categoría central en la escalada hacia el extremismo violento, particularmente presente en entornos digitales. La experiencia de la SAIT, la UFECO y la colectada por organismos internacionales especializados demuestra que, antes de la movilización operativa hacia la perpetración de un ataque terrorista, suele producirse en la persona una transformación progresiva de su discurso, caracterizada por el incremento de expresiones hostiles, amenazas y legitimación de la violencia. La verbalización de esa violencia no solo refleja un fanatismo ideológico sino que puede constituir una señal de intenciones futuras.

Precisamente uno de los elementos principales de esta categoría es el incremento del lenguaje violento y de amenazas, usualmente reflejados en el uso recurrente de expresiones agresivas, intimidatorias o explícitamente hostiles contra aquellos considerados enemigos. Hemos visto que el camino es similar en todos los casos, ya que se evoluciona desde expresiones ambiguas o indirectas hacia formulaciones más concretas, explícitas y emocionalmente intensas. En contextos de radicalización, el lenguaje violento puede cumplir múltiples funciones: reforzar la identidad grupal, generar impacto emocional, intimidar adversarios, atraer reconocimiento dentro de comunidades extremistas o ensayar narrativas de confrontación futura. Su relevancia como indicador aumenta cuando el sujeto comienza a incorporar referencias recurrentes a castigos, eliminación, purificación, guerra, resistencia o venganza.

El uso de lenguaje violento tiene como consecuencia inmediata la normalización de la violencia como solución legítima. En esta etapa, suelen aparecer narrativas que describen la confrontación violenta como “defensa propia”, “respuesta necesaria”, “acto patriótico”, “guerra cultural”, “resistencia legítima” o “deber moral”, entre muchos otros. La legitimación de la violencia constituye uno de los puntos de inflexión dentro del proceso de radicalización, ya que implica el debilitamiento de barreras éticas y normativas frente al uso de la fuerza contra terceros.

Otro indicador que debe tomarse con especial consideración es la justificación o celebración de actos violentos, incluyendo atentados, ataques de odio, asesinatos ideológicos o acciones violentas cometidas por actores extremistas. Esta conducta que, como muchas otras, se manifiesta mediante publicaciones, comentarios, memes, videos, música, imágenes o referencias simbólicas, favorece procesos de imitación, identificación psicológica y validación colectiva de la violencia, dando lugar a los llamados actores

solitarios13 (“Lone actors, por sus siglas en idioma inglés”), donde la repetición sistemática de referencias positivas hacia terroristas, atacantes o ideólogos violentos constituye un antecedente observable antes de la movilización hacia ataques terroristas14. En efecto, la construcción de figuras heroicas alrededor de atacantes previos favorece dinámicas de “contagio” o inspiración, especialmente entre sujetos vulnerables, aislados o en búsqueda de reconocimiento personal.

Especial gravedad revisten los llamados a la violencia, directos o indirectos, razón por la cual hemos catalogado a este indicador como de nivel crítico. Como dijimos, dichos llamados pueden adoptar formas explícitas —por ejemplo, exhortaciones concretas a atacar personas, instituciones o grupos determinados— o modalidades indirectas en forma de insinuaciones, referencias simbólicas, memes violentos o expresiones que incentivan a terceros a “actuar”, “levantarse”, “responder” o “hacer justicia”. Este tipo de manifestaciones posee una elevada importancia porque puede funcionar como mecanismo de movilización individual o grupal, especialmente en ecosistemas digitales donde las dinámicas de viralización y refuerzo colectivo potencian la propagación del discurso extremista.

13. En los últimos 5 años los llamados “actores solitarios” llevaron a cabo el 93% de los ataques terroristas fatales en occidente y, estadísticamente, tienen 3 veces más posibilidades de llevar con éxito un ataque que grupos de 2 o mas personas. (Fuente: Terrorism Global Index 2026).

14. En numerosos casos recientes, los perpetradores consumieron manifiestos, videos o contenidos producidos por atacantes anteriores y reprodujeron parcialmente sus narrativas, símbolos y motivaciones.

—

Gráfico número 4. Escalada Discursiva.

Ejemplos de conductas de Escalada Discursiva

- Acceso de ataques de ira y/o invitaciones a peleas contra familiares, amigos, miembros de la comunidad o figuras de autoridad abogando ideología extremista.
- Justificación ideológica, religiosa o política realizada de manera pública de actos violentos cometidos por terceros
- Intentos de radicalizar otras personas (especialmente familiares o colegas).
- Expresiones de aceptación de la violencia como el medio necesario para el logro de objetivos ideológicos, políticos o religiosos.
- Sacarse fotos y/o videos con armas o parafernalia asociada a organizaciones terroristas o extremistas (presentes o del pasado), especialmente si van acompañadas con amenazas del uso de violencia.
- Amenazas contra grupos específicos (incluidos razas, religiones, personal de fuerzas de seguridad o militares, gobiernos) sin referencias concretas de tiempo, modo y lugar.
- Aparición de Mentores
- Uso de memes y hashtags extremistas, siglas radicales, lenguaje codificado.

Extremismo Violento

Los indicadores del cuarto escalón ya se identifican con el Extremismo Violento propiamente dicho y representan la fase de mayor gravedad dentro de los procesos de radicalización, en la medida en que dejan de reflejar únicamente adhesión ideológica o escalada discursiva y comienzan a evidenciar una aproximación concreta hacia la movilización, es decir, la materialización de actos violentos.

Los sujetos que transitan esta etapa suelen exhibir señales compatibles con preparación operativa de ataques y consolidación de vínculos con entornos extremistas capaces de facilitarles y/o resolverles cuestiones logísticas o incentivarlos a la comisión de acciones terroristas.

El interés en armas, explosivos o tácticas de ataque constituye un indicador de riesgo. Se manifiesta mediante búsquedas sistemáticas de información sobre armamento, fabricación de explosivos improvisados, tácticas militares, seguridad de objetivos, vulnerabilidades de infraestructura crítica o métodos para maximizar daño y letalidad. Numerosos actores extremistas desarrollan procesos de autoformación técnica a través de plataformas digitales consumiendo videos instructivos, videojuegos y manuales distribuidos clandestinamente. La relevancia de este indicador aumenta cuando las búsquedas técnicas aparecen acompañadas de otros factores concurrentes, como aislamiento ideológico, glorificación de ataques, contacto con actores extremistas o adquisición de materiales compatibles con acciones violentas.

Particular gravedad revisten los restantes tres indicadores de la fase, que han sido clasificados como de nivel crítico. La vinculación con individuos o grupos extremistas violentos permite facilitar procesos de adoctrinamiento, transmisión de instrucciones y eventual incorporación a redes de apoyo logístico u operativo. En consecuencia, la identificación de contactos recurrentes, la participación en espacios extremistas cerrados o la interacción sostenida con actores radicalizados constituye un elemento de alta relevancia para la evaluación del riesgo y es un indicador de intervención inmediata.

Especial atención merece también la intención manifiesta de cometer actos de violencia. La hemos valorado como de riesgo crítico. En la literatura especializada se la conoce como “fuga verbal” (“leakage”, en idioma inglés) previa al ataque. Se tratan de comunicaciones parciales o indirectas acerca de las intenciones del perpetrador a sus contactos personales, comunidades digitales o redes sociales y es un indicio fuerte del paso inminente al ataque que justifica una intervención oportuna en pos de prevenir hechos de extrema gravedad.

Finalmente, la eliminación de rastros digitales y físicos constituye un indicador de elevada

relevancia porque evidencia conciencia de ilicitud y voluntad de dificultar la identificación o reconstrucción investigativa posterior. Este comportamiento puede incluir borrado masivo de chats y cuentas de correo electrónico, destrucción de dispositivos, uso intensivo de cifrado, eliminación de historiales, cierre de cuentas bancarias, destrucción de documentación, cambios de identidad digital o empleo de mecanismos de anonimización. Este tipo de conductas suelen aparecer en etapas avanzadas de radicalización operativa, particularmente cuando el sujeto considera inminente una acción violenta, un desplazamiento clandestino o un eventual enfrentamiento con fuerzas de seguridad.

—

Gráfico número 5. Extremismo Violento

Ejemplos de conductas catalogadas como de Extremismo Violento

- Declaraciones personales o en línea de intenciones violentas que incluyan algunos objetivos específicos, tiempos de realización y rol a cumplir.
- Utilización de tácticas de evasión, adopción de medidas de contra-seguimiento, cambios recurrentes de números telefónicos, contraseñas o direcciones de correo electrónico.

- Salida de grupos en línea. Usualmente para el ingreso en otros grupos más seguros en términos de vigilancia exterior donde se discuten y analizan actividad violenta.
- Compra inusual de equipos tácticos militares o de fuerzas de seguridad, que podría indicar la planificación de actos violentos.
- Interés en investigar, probar, construir explosivos de forma casera.
- Comunicar su predisposición a involucrarse en hechos violentos justificando la acción como inevitable por razones ideológicas, políticas o religiosas.
- Adquisición o intentos de adquisición de armas, o municiones para ser usadas en actos violentos.
- Realización de entrenamientos estilo militar o prácticas de tiro con supuestas intenciones de cometer actos violentos.

Movilización[15]

Finalmente, corresponde hablar de la movilización, aclarando desde ya que muchas personas que exponen ideas extremistas nunca se movilizarán, es decir, no cometerán actos terroristas. La evaluación de cuándo una persona pasará de la instancia de extremismo a la acción violenta concreta debe necesariamente estar basada en evidencias.

A diferencia de los indicadores ideológicos, discursivos o de identificación extremista, que reflejan principalmente adhesión ideológica y convencimiento cognitivo, los indicadores de movilización evidencian el inicio de la transición concreta hacia la preparación, facilitación o eventual ejecución de actos terroristas. Esta fase se caracteriza por la reducción de las últimas barreras psicológicas frente a la violencia y la adopción de medidas orientadas a preservar clandestinidad, seguridad operativa y capacidad de acción.

Un primer indicador es la integración del individuo en células o grupos operativos. Ello supone un salto cualitativo desde la mera adhesión ideológica hacia la incorporación efectiva en estructuras organizadas con capacidad de coordinación, planificación o ejecución de acciones violentas. La integración puede producirse de manera presencial o virtual. La pertenencia a grupos operativos adquiere relevancia porque facilita el acceso a recursos, financiamiento, instrucciones, es decir, a la capacidad material de cometer atentados.

Justamente la recepción de instrucciones para actuar, que puede comprender órdenes directas, guías tácticas, manuales operativos, objetivos específicos o indicaciones logísticas destinadas a preparar o ejecutar actos violentos es un indicador crítico. Muchos actores

15. De acuerdo con el enfoque desarrollado por la Radicalisation Awareness Network (RAN), la movilización hacia la violencia constituye el proceso mediante el cual un individuo desarrolla simultáneamente la intención y la capacidad necesarias para involucrarse en acciones extremistas violentas, diferenciándose así de la mera radicalización ideológica o cognitiva. Radicalisation Awareness Network (RAN). *Protective and Promotive Factors Building Resilience Against Violent Radicalisation.* European Commission, 2018.

extremistas han operado bajo modalidades híbridas, donde organizaciones o referentes ideológicos brindaron orientación remota a individuos radicalizados sin necesidad de participación de las estructuras jerárquicas tradicionales.

Lógicamente, la planificación y preparación o el ensayo de ataques constituye uno de los indicadores más sensibles y de mayor relevancia. Este fenómeno comprende todas aquellas conductas orientadas a organizar materialmente una acción violenta, incluyendo reconocimiento de objetivos, vigilancia física o digital, adquisición de equipamiento, planificación logística, simulaciones, pruebas de rutas de escape, almacenamiento de materiales o ensayos operativos y su detección requiere intervención judicial inmediata. En numerosos casos a nivel internacional, este tipo de actos preparatorios fueron detectados por las autoridades con posterioridad a la comisión del atentado, y evidenciaron la importancia de interpretar estas conductas dentro de matrices integrales de evaluación de riesgo.

Justamente, el estudio de atentados internacionales que realiza SAIT demuestra que en la mayoría de los ataques terroristas existieron etapas previas de preparación detectables mediante análisis integrales del comportamiento, actividad digital y patrones de desplazamiento de sus perpetradores. En muchas oportunidades, la identificación temprana de estas conductas permitió frustrar ataques antes de su ejecución, lo que explica el alto valor preventivo de este indicador dentro de las estrategias modernas de contraterrorismo.

Otro indicador que suele históricamente marcar la inminencia de un ataque es la existencia de mensajes de despedida. Este tipo de mensajes puede adoptar formas explícitas (publicaciones de despedida o comunicaciones dirigidas a familiares y allegados) o modalidades indirectas, ambiguas o simbólicas. La investigación criminológica y contraterrorista internacional identifica este fenómeno como parte del ya mencionado “leakage conduct”, es decir, como se explicó en el punto anterior, el comportamiento mediante el cual un sujeto comunica parcial y/o indirectamente sus intenciones antes de atacar. En varios atentados recientes, especialmente aquellos perpetrados por actores solitarios, se detectaron publicaciones previas donde los autores publicaban despedidas, referencias apocalípticas, mensajes de cierre emocional o expresiones de inevitabilidad respecto a su actuación violenta futura.

—

Gráfico número 6 de Movilización

Ejemplos de conductas catalogadas como de Movilización.

- Despedidas inusuales o notas con instrucciones para proceder luego de la muerte.
- Deshacerse de elementos personales importantes de manera inusual o sin sentido. Puede incluir desembolsos dinerarios con urgencia, cierre apresurado de cuentas bancarias.
- Vigilancia reiterada de blancos potenciales.
- Comunicación directa o intención de desarrollar una relación personal con operativos extremistas violentos.
- Viajar o planear viajar (compra de pasajes) a zonas de conflicto, a participar de actividades de organizaciones terroristas.
- Amenazas concretas contra un blanco determinado.

Significado de los niveles de riesgo en la evaluación de Indicadores de Movilización hacia la Violencia

Hemos clasificado los indicadores en niveles de riesgo Medio, Medio-alto, Alto y Crítico. Su finalidad es proporcionar a fiscales, jueces y organismos de seguridad de una herramienta objetiva de gestión de riesgo para evaluar la evolución de un proceso de radicalización, una posible conducta delictiva y determinar la intensidad de la respuesta estatal requerida. La asignación de determinado nivel de riesgo a una conducta particular no es un mecanismo de atribución de responsabilidad penal ni implica, por sí mismo, la imputación de un delito y menos aún constituye presunción de culpabilidad alguna. Por el contrario, se trata de una metodología de valoración destinada, como adelantamos, a identificar señales tempranas para asignar recursos de manera eficiente y adoptar medidas probatorias proporcionales al nivel de amenaza detectado.

En consecuencia, la valoración del director de la investigación debe concentrarse en el desarrollo global del caso, la convergencia de indicadores, la evolución temporal de las conductas observadas, la existencia de factores externos y de elementos objetivos que permitan determinar si las conductas investigadas reflejan una adhesión ideológica, una radicalización más o menos avanzada o una movilización a la violencia.

Los indicadores clasificados como de riesgo MEDIO representan señales tempranas de vulnerabilidad o predisposición que pueden incrementar la susceptibilidad de una persona frente a narrativas extremistas pero que, por sí solos, no evidencian adhesión a ideologías violentas ni intención de cometer actos ilícitos.

Esta clase de indicadores posee un valor principalmente preventivo y analítico, permitiendo identificar contextos de riesgo que podrían ser explotados por reclutadores o propagandistas extremistas.

Desde nuestra perspectiva, la presencia exclusiva de indicadores de riesgo medio normalmente no justifica medidas intrusivas, aunque puede orientar actividades de análisis, monitoreo contextual o articulación con organismos especializados en prevención del extremismo violento.

En la práctica estamos frente a un perfil social de un individuo todavía integrado, donde las publicaciones son aisladas, exclusiva o mayoritariamente re-publicaciones que no tienen contenido original ni un patrón común, lo que indica que la persona podría tratarse más de un consumidor de propaganda o un simpatizante ideológico que de un organizador, reclutador o posible atacante.

En estos casos se recomienda proseguir la investigación, especialmente si redistribuye contenido (para determinar el origen del original), si tiene contacto con administradores de grupos cerrados, si recibe material de propaganda, instrucciones o dinero (toda la parte de investigación financiera clásica). Se sugiere realizar una investigación OSINT, el análisis de los vínculos y monitoreo digital.

Los indicadores de riesgo MEDIO-ALTO reflejan una evolución desde factores meramente predisponentes hacia conductas que evidencian una mayor exposición a entornos extremistas o una creciente internalización de narrativas radicales. En esta etapa suelen aparecer comportamientos vinculados con el consumo sistemático de propaganda extremista, la adopción de determinados símbolos o consignas, la participación ocasional en espacios digitales radicalizados o la profundización de discursos polarizantes.

Aunque todavía no se observan elementos claros de preparación operativa o violencia inminente, estos indicadores sugieren que el individuo podría estar atravesando una fase de consolidación ideológica que merece especial atención investigativa.

La detección de indicadores de riesgo medio-alto puede justificar un seguimiento más cercano de la evolución conductual del sujeto, especialmente cuando aparecen asociados a procesos de aislamiento social, cambios abruptos de conducta o interacción con comunidades radicalizadas.

En esta etapa las publicaciones se hacen más frecuentes, se crea contenido propio, se inician búsquedas sobre objetivos potenciales y/o publican fotos de posibles blancos.

La investigación deberá combinar un análisis de la personalidad del autor, verificando sus antecedentes penales, especialmente aquellos relacionados con violencia u odio, verificar si ha tenido cambios bruscos de comportamiento o rupturas sociales visibles (puede saberse a través de testimoniales o seguimientos) y cuáles son sus capacidades personales, especialmente si tiene formación militar o técnica, acceso a armas, recursos económicos.

Aquí debe ampliarse la investigación mediante vigilancia digital y real, un análisis financiero, testimoniales al entorno, eventualmente cooperación internacional.

Los indicadores clasificados como de riesgo ALTO evidencian una probabilidad significativa de progresión hacia escenarios de violencia extremista. En esta categoría se encuentran conductas que reflejan legitimación de la violencia, vinculación creciente con entornos radicalizados o manifestaciones compatibles con etapas avanzadas de radicalización.

La presencia de indicadores de riesgo alto exige una evaluación permanente y coordinada

entre fiscales, fuerzas de seguridad y analistas especializados (UFECO-SAIT), ya que probablemente refleje la existencia de procesos de radicalización avanzados susceptibles de evolucionar hacia conductas preparatorias o movilización operativa.

En términos investigativos, esta categoría supone un monitoreo intensivo en tiempo real que pueda dar lugar a una intervención urgente en caso necesario, con medidas intrusivas inmediatas. Justifica la intensificación de medidas de obtención de información, análisis de vínculos, preservación de evidencia digital y evaluación de posibles amenazas contra personas, instituciones o infraestructura crítica.

La experiencia judicial ha demostrado que en este tipo de investigaciones resulta frecuente que gran parte de la actividad criminal permanezca oculta dentro de comunidades cerradas, plataformas cifradas, foros privados o canales de comunicación restringidos, donde la evidencia difícilmente pueda obtenerse mediante técnicas tradicionales de investigación.

De ello se colige que la interceptación, captación, registro y análisis de comunicaciones telefónicas y digitales resultan esenciales para establecer la identidad real de los autores, reconstruir eventuales redes de apoyo, individualizar mentores, reclutadores o facilitadores, detectar canales de financiamiento y determinar si existen instrucciones, distribución de funciones, selección de objetivos o actividades de preparación logística. Asimismo, permiten conocer la evolución del discurso del investigado en ámbitos privados o restringidos, donde las manifestaciones pueden diferir sustancialmente de aquellas que realiza públicamente, y verificar si la aparente adhesión ideológica se corresponde con una voluntad concreta de participación, colaboración o ejecución de actos violentos.

La intervención de comunicaciones posee también una función central en la evaluación de temporalidad e inminencia. El análisis de la frecuencia, contenido y secuencia de los intercambios puede revelar cambios abruptos en la conducta, aceleración del proceso de radicalización, recepción de órdenes, fijación de fechas, adquisición de materiales, vigilancia de objetivos o adopción de medidas de seguridad y contrainteligencia. Estos elementos son relevantes para determinar si corresponde mantener la investigación bajo observación, profundizar las medidas de obtención de prueba o interrumpir de manera inmediata un proceso que pudiera encontrarse próximo a la ejecución de un ataque.

La intervención de comunicaciones no debe concebirse exclusivamente como un medio para documentar un delito ya consumado. En investigaciones por terrorismo constituye también una herramienta de prevención judicial, en cuanto permite conocer oportunamente el verdadero grado de radicalización del sujeto, comprobar la existencia de capacidades operativas y detectar señales que exijan una acción disruptiva. Su finalidad legítima consiste en transformar una hipótesis construida a partir de indicadores de riesgo en información

concreta, verificable y judicialmente controlada, evitando tanto una intervención estatal prematura como la pérdida de una oportunidad real de impedir un hecho violento.

De manera complementaria, en los supuestos en que la estructura investigada opere mediante comunidades cerradas, relaciones de confianza o canales de difícil acceso, deberá evaluarse la utilización del agente encubierto o del agente revelador, previstos en la Ley 27.319. La norma habilita estas figuras, entre otros supuestos, en los casos en que resulte aplicable el agravante terrorista del artículo 41 quinquies del Código Penal, y exige que su empleo se rija por criterios de necesidad, razonabilidad y proporcionalidad.

El agente encubierto permite una inserción sostenida en una organización o asociación delictiva con el objeto de identificar a sus miembros, impedir la consumación de delitos y reunir información y elementos de prueba. El agente revelador, en cambio, desarrolla una actuación puntual y no permanente, destinada a exteriorizar una actividad ilícita, identificar a los involucrados y recolectar material probatorio. La diferencia entre ambas figuras debe ser considerada al diseñar la estrategia: la primera resulta especialmente útil para conocer estructuras, jerarquías, roles y procesos prolongados de adoctrinamiento o preparación; la segunda puede ser adecuada para verificar una oferta, una entrega, una provisión de materiales, una instrucción concreta o una manifestación operativa específica.

En ambos casos, la actuación debe dirigirse a documentar conductas y decisiones criminales preexistentes, sin provocar artificialmente el delito ni inducir al investigado a realizar acciones que de otro modo no habría ejecutado. Su valor reside en obtener evidencia concreta sobre el grado de compromiso del sujeto, sus vínculos, sus capacidades y la posible proximidad de una acción violenta, aportando elementos indispensables para decidir la estrategia judicial más adecuada, es decir, si corresponde prolongar la investigación, escalar las medidas o disponer su interrupción urgente.

Finalmente, los indicadores clasificados como de riesgo CRITICO representan la fase de mayor peligrosidad. Son conductas que sugieren una proximidad temporal significativa con la posible ejecución de un acto violento o la integración efectiva en estructuras extremistas operativas.

La experiencia demuestra que muchos de estos indicadores aparecen en períodos relativamente próximos a la ejecución de atentados, razón por la cual requieren una valoración inmediata y prioritaria.

Desde la óptica del Ministerio Público Fiscal, la concurrencia de uno o varios indicadores críticos justifica la adopción urgente de acciones disruptivas, la detención preventiva del/los involucrados, el secuestro de todos los dispositivos personales y material relacionado

al ataque, una coordinación inter-agencial, y evaluación de riesgos para potenciales víctimas, siempre dentro del marco de legalidad, proporcionalidad y control jurisdiccional correspondiente.

Investigación de Incidentes Terroristas:

Presente el ciclo terrorista, radicalización, modos de reclutamiento e indicadores de riesgo, abordamos específicamente la investigación de publicaciones y/o manifestaciones de contenido extremista en línea que pueden derivar en incidentes terroristas, poniendo énfasis, dadas las características del fenómeno terrorista, en la adopción de un enfoque metódico, legalmente cuidadoso y técnicamente riguroso, que posibilita el estudio en detalle del mensaje publicado, el perfil digital del autor, sus conductas en línea, su conducta y entorno en la vida real y eventuales síntomas psicológicos.

El objetivo de la investigación será reunir, preservar y analizar evidencia para identificar procesos de radicalización, técnicas de reclutamiento, redes de apoyo, capacidades operativas y riesgos concretos del caso bajo estudio.

Dos líneas paralelas y simultáneas deben desarrollarse al inicio de la investigación. Por un lado, determinar fehacientemente quién es la persona física que se encuentra detrás de las publicaciones o mensajes que estamos analizando y, por el otro, estudiar detenidamente el posteo y/o mensaje.

Para la identificación de la persona detrás del “nickname digital”, y la preservación de la evidencia digital nos remitimos a las instrucciones publicadas por la Unidad Fiscal Especializada en Cibercrimen (UFECI), que son sumamente útiles e instructivas al respecto[16].

En relación al incidente en sí mismo, debe tenerse presente que el posteo y/o mensaje puede asumir la forma de texto, imágenes (fotos, memes, banderas, símbolos, tatuajes), videos (entrenamientos, discursos, atentados) o audios (podcasts, himnos, prédicas). En todos los casos, estudiaremos inicialmente si se trata de un manifiesto que justifica una acción terrorista, la violencia o la actividad de un grupo terrorista; si es un discurso que promueve ideología extremista; o si se trata de una amenaza concreta.

Asimismo, debemos responder las siguientes preguntas ¿Se replica contenido publicado por grupos terroristas conocidos? ¿Se replica atentado específico o un grupo determinado? ¿Se reivindica la lucha armada de grupos violentos? ¿Se usa simbología asociada a grupos

16. Ver Manual UFECI en https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

extremistas, tales como logos, íconos, frases, himnos? ¿Los mensajes contienen llamados a la incitación a cometer actos terroristas? ¿Se intenta deshumanizar al enemigo? ¿Se hacen amenazas concretas, como tiroteos, masacres? ¿Se individualizan objetivos?

Las respuestas a estos interrogantes aportarán los primeros datos valiosos para construir un perfil acertado acerca del autor y su intención, lo que orientará para determinar la estrategia procesal adecuada en el caso.

Pasos a seguir para construir prueba relacionada a la investigación

A modo introductorio corresponde aclarar que en un contexto caracterizado por la utilización intensiva de redes sociales, plataformas de mensajería, foros especializados y comunidades virtuales, resulta habitual que las primeras alertas relacionadas con procesos de radicalización, extremismo violento y terrorismo provengan de actividades de monitoreo y ciberpatrullaje, de entornos digitales realizados por organismos nacionales o extranjeros en materia de inteligencia, seguridad o aplicación de la ley.

Estos mecanismos permiten detectar publicaciones, interacciones, imágenes, videos, manifiestos, o comportamientos digitales que, analizados en su conjunto, pueden revelar la existencia de indicadores compatibles con etapas iniciales o avanzadas del ciclo terrorista. En ciertos casos, la información obtenida no constituye evidencia suficiente para acreditar la comisión de un delito, pero sí proporciona elementos objetivos que justifican el inicio de una investigación preliminar destinada a verificar la existencia de una amenaza concreta, identificar a los involucrados y preservar oportunamente la evidencia digital.

Su principal función consiste en aportar un dato inicial o una “notitia criminis” que habilita el despliegue de la actividad investigativa del Ministerio Público Fiscal y las fuerzas de seguridad, orientando la búsqueda de evidencia independiente que permitan confirmar o descartar la hipótesis investigativa. Este criterio resulta particularmente relevante en investigaciones sobre terrorismo, donde la intervención temprana constituye uno de los principales instrumentos para impedir la consumación de ataques y proteger eficazmente la seguridad pública.

De este modo, el Ministerio Público Fiscal asume la dirección del caso validando por medios probatorios independientes los datos de la investigación y habilitarlos para una eficaz utilización en un eventual juicio posterior.

Presente ello, se analizará el contenido del posteo/mensaje, para determinar cuál es su objetivo. En concreto analizaremos la terminología usada, consignas, hashtags, memes, etc. Al hacerlo, podremos determinar si se trata de una incitación a la acción mediante

convocatorias o instrucciones; si se intenta influir audiencias deshumanizando al enemigo; si se utiliza lenguaje específico extremista, Yihadista, palabras claves (88, 1488) o mensajes cifrados (por ejemplo, la utilización de números reemplazando a letras como modo de evadir las alertas de moderación de las plataformas digitales). Si hay llamados explícitos o implícitos a la violencia o referencias a organizaciones terroristas designadas[17]. Es importante prestar atención a la circunstancia de si se difunde material logístico o instructivo, (por ejemplo, cómo fabricar explosivos, cómo atacar instituciones, cómo hacer inteligencia, cómo seleccionar objetivos).

En líneas generales esto permite conocer el grado de información y conocimiento del autor respecto a la ideología extremista de que se trate o a las organizaciones terroristas, lo que, a su vez, es un indicio sobre su grado de compromiso.

En este punto es importante conocer el número de visualizaciones que tuvo el posteo, cantidad de veces que fue compartido, así como likes y comentarios que recibió la publicación.

La fecha de la publicación también puede aportar datos interesantes. Si coincide con algún atentado (nacional o internacional) y/o se produjo en fechas sensibles para determinar si se ha publicado en fechas simbólicas, coincide con eventos internacionales y/o reacciona a noticias recientes[18].

17. Para conocer las organizaciones terroristas que han sido designadas por la República Argentina debe consultarse el REPET (Registro Público de Personas y Entidades vinculadas a Actos de Terrorismo y su Financiamiento) en https://repet.jus.gob.ar/

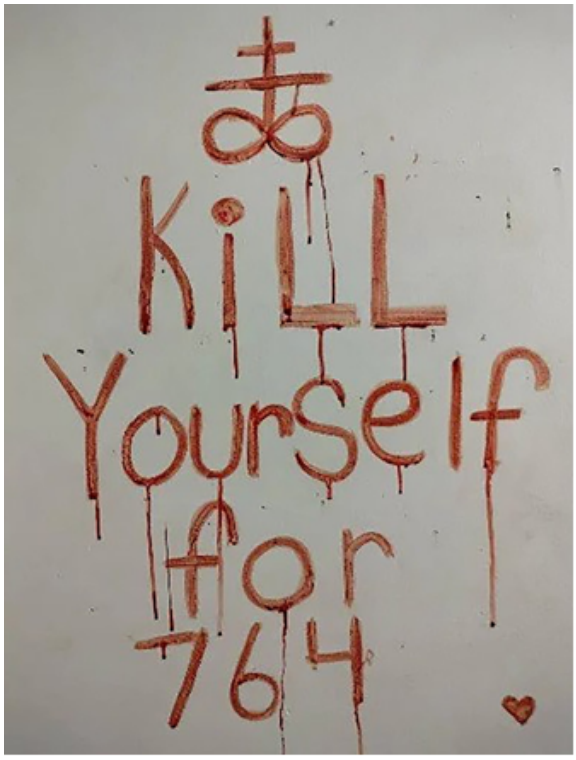
18. Es bastante común que, por la simbología específica que contienen los ataques terroristas, sus pepetradores se inclinen por atacar en fechas que tengan un significado particular. (Por ejemplo, los neonazis eligen el 20 de abril -fecha de nacimiento de Adolph Hitler- como día significativo).

Ejemplo de posteo en línea de una agrupación neonazi.[19]

Luego, se analizará qué plataforma digital se ha utilizado para la publicación, ya que el tipo de comunidad usada también otorga indicios para determinar el riesgo que enfrentamos. El nivel de exposición al que se somete una persona generalmente está relacionado con su intención y con la sofisticación de la amenaza. No es lo mismo publicar propaganda pública en una red abierta que ejercer una coordinación en canales de mensajería instantánea como Telegram o Signal o en foros anónimos al estilo 4chan o 8Kun.

De ello se colige que estudiar la plataforma digital o red social que se ha utilizado es importante, para conocer si permite mayor anonimato o bien tiene moderación activa. Redes masivas como YouTube, Instagram o X tienen mayores recursos para detectar y reportar contenido extremista, mientras que pequeñas como GAB, 4chan o BitChute toleran discursos de contenido extremista, reaccionan más lentamente a las denuncias y, por tales motivos, son deliberadamente utilizadas por grupos violentos. La elección de canales privados (Telegram, Discord) puede indicar etapas más avanzadas en el proceso de radicalización.

19. Imagen obtenida del diario Tiempo Argentino, edición del 16/11/2023.



Ejemplo de posteo en un canal privado.[20]

En este sentido, debemos tener en cuenta las características distintivas de los algoritmos de algunas plataformas. Por ejemplo, TikTok posee una velocidad algorítmica mayor. Telegram es usualmente u tilizada para profundización ideológica, mientras que Discord se usa para socialización entre extremistas. Este análisis permitirá colectar indicios objetivos para determinar el tipo de discursos que enfrentamos.

En este sentido, adquiere particular relevancia el ecosistema de videojuegos en línea y plataformas asociadas, que constituyen un ámbito particularmente propicio para la interacción social sostenida entre jóvenes y adolescentes. Cabe aclarar que los videojuegos, en sí mismos, no generan ni constituyen inherentemente herramientas extremistas; sin embargo, determinadas organizaciones y actores radicales han advertido el potencial de dichos espacios para identificar y captar personas vulnerables mediante dinámicas sociales desarrolladas dentro de comunidades virtuales de juego.

En efecto, los videojuegos que permiten múltiples jugadores simultáneos en línea (en especial Roblox y Minecraft) y las plataformas vinculadas a ellos, incluyendo sistemas de chat de voz, servidores privados, canales de streaming y aplicaciones complementarias de comunicación, permiten la creación de vínculos interpersonales continuos entre usuarios

20. Imagen obtenida del diario ABC. Noviembre, 2025"

que, muchas veces, permanecen fuera de la supervisión familiar o institucional. En dichos espacios, los reclutadores pueden detectar jóvenes que manifiesten aislamiento social, baja autoestima, frustración, necesidad de reconocimiento o fuerte dependencia emocional respecto de comunidades virtuales. En estos casos puntuales, el proceso de captación suele iniciarse mediante interacciones aparentemente informales vinculadas al juego, evolucionando progresivamente hacia conversaciones de contenido político, ideológico o identitario.

La academia[21] ya puso de manifiesto que las dinámicas propias de determinados entornos de juego —competencia, cooperación grupal, construcción de clanes o equipos, sentimiento de misión compartida y existencia de enemigos comunes— pueden ser aprovechadas por reclutadores extremistas para reforzar narrativas de confrontación y pertenencia colectiva. En este contexto, se aprovechan las relaciones de confianza construidas durante el juego para trasladar a los jóvenes hacia canales de comunicación externos, tales como Discord, Telegram o foros cerrados, donde la exposición propagandística se intensifica y adquiere mayor sistematicidad.

Asimismo, se ha verificado que ciertos movimientos extremistas utilizan elementos propios de la cultura digital juvenil —memes, humor irónico, referencias a videojuegos, lenguaje codificado y estética gamer— como mecanismos para normalizar discursos violentos o facilitar la aproximación inicial a potenciales simpatizantes. Tales estrategias permiten reducir las barreras de percepción frente al extremismo, presentando contenidos ideológicos bajo formatos aparentemente recreativos, humorísticos o contraculturales, especialmente atractivos para públicos adolescentes y jóvenes.

En consecuencia, el análisis de los ecosistemas digitales vinculados a videojuegos y plataformas de interacción asociadas reviste especial importancia para las autoridades judiciales y fuerzas de seguridad, no desde una lógica de criminalización de espacios recreativos, sino en función de comprender cómo determinados actores extremistas instrumentalizan dichos ámbitos para identificar vulnerabilidades, construir vínculos de confianza y desarrollar procesos graduales de radicalización ideológica, dirigidos principalmente hacia jóvenes expuestos a contextos de fragilidad emocional, social o identitaria.

Otro factor a considerar es la audiencia a la cual va dirigido el mensaje, es decir, a quien se intenta influenciar, reclutar o movilizar para determinar si está dirigido al público en general o a una audiencia determinada. En líneas generales invitaciones privadas buscan reclutar, propaganda constante busca radicalizar, llamados a la acción buscan movilizar,

21. Jessica White, Claudia Wallner, Petra Regeni. Extremism in Gaming Spaces, Policy for prevention and moderation. RUSI. 2025.

amenazas supone intimidación y publicación de discursos de odio generan polarización.

El tipo de posteo determinará si se trata de propaganda abierta dirigida al público en general, si tiene un contenido de fuerte carga ideológica dirigida a simpatizantes de determinada causa; si busca atraer jóvenes vulnerables, grupos ideológicos, comunidades marginadas o en conflicto para tomarlos como potenciales reclutas, o si se dirige a sujetos ya radicalizados.

Una de las formas para determinar estas cuestiones es analizar el lenguaje o los métodos audiovisuales utilizados. Palabras como ER[22], Red Pill[23], Chad[24], Stacy[25], Foids[26] remiten al ecosistema Incel[27]. Términos como 88[28], 1488[29], Great Replacement[30], White Genocide son típicos del supremacismo blanco; y expresiones como Shahid[31], Kuffar[32], Mujahiddin[33] se identifican con el extremismo Yihadista.

La frecuencia en las publicaciones también es un elemento a examinar para determinar si estamos frente a una publicación aislada, o el posteo forma parte de una estrategia más amplia y consistente.

Una vez identificada la persona física que realizó el posteo y/o publicó un mensaje, se deberá verificar si tiene muchos seguidores y, por ende, se advertirá si tiene capacidad de influencia. Seguidamente corresponde analizar sus otras redes sociales a efectos de identificar qué perfiles comenzó a seguir y cuándo. Verificar si tiene cuentas suspendidas previamente, si utiliza cuentas en espejo, si utiliza VPNs para enmascarar su ubicación,

22. En referencia a Elliot Roger, quién mató a 6 personas en Isla Vista, California, en mayo de 2014, para luego suicidarse. Antes de hacerlo envío un correo electrónico con una autobiografía a sus allegados. Ese manifiesto fue tomado por la comunidad Incel como referencia.

23. En el contexto de la manósfera la “Red Pill” es reconocer que el feminismo es dañoso para los hombres, que los hombres son víctimas de un mundo ginocéntrico y que los hombres tienen derecho a tener sexo y las mujeres deberían estar sexualmente disponibles para ellos. Este mensaje no es solamente conceptual sino que en el submundo Incel se utiliza como verbo que significa la diseminación del concepto a otras personas. El concepto contrario es la “Blue Pill”, que denota que una persona con esa ideología es ignorante acerca de cómo es el mundo en realidad.

24. Es lo opuesto al Incel. Son hombres hegemónica y convencionalmente lindos que tiene éxito entre las mujeres.

25. Es la versión femenina del Chad, aunque es utilizada en forma más despectiva. Las Stacies son caracterizadas como femeninas y hermosas pero estúpidas y promiscuas.

26. Forma despectiva de referirse a las mujeres.

27. INCEL (Involuntary Celibates), Célibes involuntarios.

28. 88. Es una expresión muy común en el ecosistema de supremacismo blanco y neonazismo. Significa que el 8 se corresponde con la octava letra del abecedario , que es la H. Por consiguiente, 88 es igual a HH o Heil Hitler.

29. En este caso se combina el numero 1488 para significar las 14 palabras y la simbología de 88 (Heil Hitler). Las 14 palabras son: “We must secure the existance of our people and a future for White kids”. “Debemos asegurar la existencia de nuestra gente y un futuro para nuestros niños blancos”.

30. Teoría del Gran Reemplazo. Narrativa que expresa que la población europea blanca está siendo deliberadamente reemplazada a nivel cultural y étnico por otras comunidades, a través de la inmigración y la mayor tasa de natalidad de las minorías.

31. Mártir, martirio.

32. En el Islam radical se refiere a los Infieles.

33. Se le denomina a toda persona que realiza la Yihad. Su significado original era definir a aquel que se esforzaba por la senda de Dios. En lenguaje moderno, pasó a utilizarse para designar a los combatientes islamistas que participan en una guerra considerada religiosa o de liberación.

cambia de alias o de nicknames, si modera grupos en línea, si tiene múltiples cuentas similares y, cronológicamente, que contenidos consumió (videos, manifiestos, libros, canciones), si utiliza patrones de lenguaje violento. Estas respuestas usualmente aportan información valiosa a la investigación.

Asimismo, debe intentarse determinar si recibió instrucciones, le propusieron acciones, le facilitaron material, elogiaron sus amenazas y/o accedió a tutoriales o manuales de ataque (tales como el Anarchist Cookbook[34], White Resistant Manual[35]).

Para ello, resulta útil determinar si su identidad digital se trata de un perfil real o falso. En este último caso, qué tipo de herramientas se utilizaron para enmascarar la IP u ocultar la verdadera procedencia de la publicación. Si se han utilizado técnicas de amplificación de mensajes, tales como bots o cuentas automatizadas, campañas con hashtags y/o coordinación entre múltiples perfiles. Si hubo intentos de evasión de la detección automatizada (como cambios sutiles, errores ortográficos intencionales, tipografías, sobreimpresiones), si el contenido fue borrado, o re-subido.

Este análisis ayudará a comprender la experiencia y conciencia de la persona investigada sobre la vigilancia y el patrullaje en línea; facilitará evaluar la intencionalidad del investigado y qué capacidad efectiva de daño posee, para, finalmente, conocer una cuestión de suma importancia, si actuó solo o es parte de una red organizada.

Con estos datos, es dable proceder a especificar si la investigación se encuentra ante: a) una mera expresión ideológica u opinión protegida constitucionalmente y sin relevancia penal, b) un indicio de radicalización activa, c) una amenaza concreta. De ese modo podremos determinar el aspecto legal del mensaje, si incurrió o no en un delito y proceder a la calificación jurídica del episodio.

La investigación debe, naturalmente, complementarse con verificaciones de vínculos off line. En este contexto, el objetivo central de la actividad investigativa consistirá en reunir, preservar, analizar e integrar evidencia proveniente de múltiples fuentes, permitiendo evaluar el nivel de riesgo existente y adoptar medidas preventivas y judiciales proporcionales dentro del marco constitucional y convencional vigente. Una serie de medidas, dividida en siete módulos, ha sido representada en el siguiente cuadro, aclarando que el orden es indistinto y la utilización de cada medida probatoria dependerá, en gran medida, de la situación fáctica del caso concreto y la estrategia procesal del director de la investigación.

34. Es un libro escrito por William Powell, publicado en 1971 que contiene instrucciones para el armado de explosivos, de armas y de dispositivos de vigilancia.

35. Es Manual escrito por Axl Hess bajo el seudónimo “Aquilifer” y distribuido anónimamente en 2001 en sitios extremistas como whitehonor.org como una guía de resistencia descentralizada para la supervivencia de la raza blanca. Fue tomado como referencia por ecosistemas supremacistas blancos y neonazis.

Finalmente, es importante destacar que, dadas las características de los hechos y los sujetos involucrados, las investigaciones relacionadas con procesos de radicalización, extremismo violento y terrorismo presentan un grado de complejidad significativamente superior al de la criminalidad convencional. La diversidad de motivaciones, la utilización de ecosistemas digitales, la frecuente ausencia de estructuras jerárquicas, la convergencia entre factores personales, psicológicos, sociales, ideológicos y financieros, así como el carácter transnacional de muchas de estas actividades, exigen que la investigación sea desarrollada mediante un enfoque interdisciplinario, capaz de integrar conocimientos provenientes de distintas áreas del saber.

En consecuencia, el Ministerio Público Fiscal debe apoyarse en equipos de trabajo conformados por profesionales que posean perfiles complementarios, cuya actuación permita comprender integralmente el fenómeno investigado y reducir el margen de error en la evaluación del riesgo. La experiencia comparada demuestra que la adecuada interpretación de los indicadores de riesgo depende, en gran medida, de la interacción permanente entre investigadores criminales, analistas de inteligencia, especialistas en evidencia digital, psicólogos, criminólogos, expertos financieros, y peritos informáticos, entre otros.

Este proceso colaborativo de producción de información es el que permite construir una comprensión global del caso investigado y transformar esa información en evidencia útil para la toma de decisiones procesales y de fondo adecuadas.

A continuación las técnicas de investigación sugeridas para aplicar a la investigación de incidentes terroristas previos a un posible ataque.

Técnicas de Investigación
Aplicables a incidentes terroristas precios a un ataque

Objetivo

Reunir, preservar y analizar evidencias pertinentes para identificar procesos de radicalización, redes de apoyo, capacidades operativas, y riesgos concretos, respetando derechos fundamentales y garantizando la cadena de custioda.

1. Inteligencia financiera

- Análisis de movimientos bancarios.
- Reportes UIF (ROS, RIFI, etc.)
- Seguimiento de flujos de dinero tradicionales y alternativos.
- Detección de estructuras de financiamiento y apoyo material.

2. Investigación digital

- Secuestro y preservación de dispositivos
- Análisis forense de telefonía, computadores y almacenamiento en la nube.
- Recuperación de chats, archivos, metadatos y actividad en línea.
- Análisis de plataformas, foros, redes sociales y aplicaciones cifradas.

3. Vigilancia y seguimiento

- Vigilancias físicas y electrónicas (ley 25.520 y CCyCN).
- Geoposicionamiento y análisis de patrones de movilidad.
- Seguimiento de comunicaciones con autorización judicial.
- Uso de tecnologías de monitoreo y sensores.

4. Fuentes Abiertas (OSINT)

- Recolección y análisis de información pública en internet.
- Monitoreo de medios, redes sociales, foros y comunidades en línea.
- Análisis de imágenes satelitales, registros públicos y filtraciones.
- Herramientas OSINT para vinculación de datos.

5. Técnicas especiales de Investigación

- Agentes encubiertos e infiltrados.
- Entregas vigiladas.
- Operaciones encubiertas digitales.
- Cooperación Internacional (Acuerdos MLAT/CSJN y 2775/96.

6. Evidencia física y forense

- Relevamiento de escena.
- Secuestros de elementos físicos y materiales.
- Análisis químico, biológico balístico y explosivístico.
- Cadena de custioda documentada y preservada.

7. Entrevistas e interrogatorios

- Entrevistas a testigos cláves.
- Interrogatorios a imputados y personas vinculadas.
- Técnicas de entrevistas cognitivas y análisis conductual.

Principios rectores

Legalidad	Proporcionalidad	Necesidad	Cadena de custodia	Enfoque integrado	Derechos fundamentales
Toda técnica debe contar con autorización judicial y respaldo normativo	Las medidas debe ser adecuadas, necesarias y razonables	Utilizar las técnicas menos lesivas para llegar al objetivo legítimo	Documentar cada paso para garantizar la validez de la evidencia	Coordinación entre áreas especializadas y organismos nacionales e internacionales	Respeto irrestricto a las garantías constitucionales

Finalidad última

Anticipar, prevenir e impedir la comisión de actos terroristas mediante una investigación profesional, estratégica y respetuosa del Estado de Derecho.

El modelo representado en el cuadro está basado en una metodología de investigación integral, donde convergen siete áreas complementarias de obtención y análisis de información. Ninguna resulta suficiente por sí sola para comprender adecuadamente un caso de radicalización o terrorismo; por el contrario, la fortaleza del enfoque reside en su capacidad de integrar información financiera, digital, física, testimonial y operativa para construir una visión completa del fenómeno investigado.

La primera dimensión corresponde a la inteligencia financiera, cuya finalidad es identificar flujos económicos, fuentes de financiamiento, estructuras de apoyo material y mecanismos de sostenimiento de actividades extremistas. La investigación financiera puede incluir el análisis de movimientos bancarios, reportes de operaciones sospechosas, transferencias nacionales e internacionales, uso de criptomonedas, plataformas de pago digital y eventuales mecanismos de ocultamiento patrimonial. En materia contraterrorista, la evidencia financiera resulta especialmente relevante porque permite detectar facilitadores, identificar redes de apoyo y reconstruir la dimensión logística de una organización o individuo radicalizado.

La segunda área comprende la investigación digital post-intervención, siendo que los allanamientos se transforman en una de las fuentes probatorias más relevantes en materia de terrorismo y extremismo violento. Esta actividad incluye el secuestro y preservación de dispositivos electrónicos, el análisis forense de teléfonos celulares, computadoras y servicios en la nube, la recuperación de archivos eliminados, el examen de metadatos y el análisis de comunicaciones mantenidas a través de plataformas digitales. Permite confirmar y/o identificar procesos de radicalización en línea, consumo de propaganda extremista, contactos con actores radicalizados y eventuales actividades de planificación o preparación de actos violentos, más allá de las medidas tomadas con anterioridad a la intrusión.

El tercer capítulo refiere a las actividades de vigilancia y seguimiento, destinadas a verificar conductas, vínculos, desplazamientos y actividades del sujeto investigado. Estas medidas pueden incluir observación física, vigilancia electrónica, geolocalización autorizada judicialmente, análisis de patrones de movilidad y utilización de tecnologías de monitoreo. Su finalidad es determinar si las expresiones ideológicas observadas evolucionan hacia comportamientos compatibles con fases avanzadas de radicalización, preparación logística o movilización operativa.

En cuarto lugar aparecen las fuentes abiertas de información (OSINT), entendidas como el conjunto de técnicas orientadas a recopilar y analizar información disponible públicamente. Ello comprende redes sociales, sitios web, foros, plataformas de mensajería abiertas, medios de comunicación, registros públicos y otras fuentes accesibles sin medidas intrusivas.

La explotación sistemática de fuentes abiertas permite detectar discursos extremistas, símbolos ideológicos, conexiones entre individuos, patrones de comportamiento digital y eventuales indicadores de radicalización o movilización hacia la violencia.

La quinta categoría engloba las técnicas especiales de investigación, herramientas particularmente relevantes para desarticular estructuras complejas vinculadas al terrorismo. Entre ellas pueden encontrarse agentes encubiertos, operaciones controladas, infiltraciones digitales, cooperación internacional, intercambios de información entre fiscales y otros organismos especializados. Estas técnicas permiten acceder a información que difícilmente pueda obtenerse mediante medios investigativos tradicionales y suelen resultar esenciales para identificar redes operativas, facilitadores o procesos avanzados de planificación de atentados. Un párrafo especial merece la figura del arrepentido colaborador por su capacidad para permitir a la investigación ascender a niveles superiores de la organización criminal y, así, profundizar y completar la investigación.

La sexta dimensión corresponde a la evidencia física y forense, que comprende el relevamiento de escenas, secuestro de elementos materiales, análisis balísticos, químicos, biológicos, documentales y cualquier otro examen técnico destinado a reconstruir actividades preparatorias o verificar la existencia de capacidades operativas. La correcta preservación de la cadena de custodia resulta indispensable para garantizar la validez probatoria de los elementos obtenidos y su posterior utilización en sede judicial.

Finalmente, la séptima área está constituida por pruebas testimoniales, esenciales para contextualizar la información obtenida por otras vías. Las declaraciones de familiares, allegados, testigos, compañeros de trabajo, contactos digitales o personas vinculadas al investigado permiten comprender cambios conductuales, procesos de radicalización, dinámicas relacionales y factores de riesgo que difícilmente se pueden identificar únicamente mediante evidencia técnica. Asimismo, pueden aportar información relevante sobre motivaciones, vínculos y actividades desarrolladas por los sujetos investigados.

Como ha podido advertirse el modelo enfatiza la importancia de un enfoque integrado e interdisciplinario, basado en la cooperación entre fiscales, fuerzas de seguridad, organismos de inteligencia financiera, especialistas forenses y socios internacionales. La complejidad de los fenómenos terroristas contemporáneos, especialmente aquellos desarrollados en entornos digitales y redes transnacionales descentralizadas, exige superar enfoques fragmentados y avanzar hacia modelos de investigación coordinados que permitan detectar tempranamente indicadores de radicalización, evaluar riesgos de movilización y prevenir la materialización de actos de violencia extremista.

Checklist investigativo

Para casos de radicalización y movilización hacia la violencia

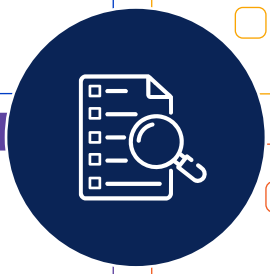
Detectar señales | **Evaluar** riesgos | **Analizar** contextos | **Actuar** con legalidad

1 Perfil del sujeto

- [ ] ¿Existen factores de vulnerabilidad personal?
- [ ] ¿Presentan cambios abruptos de comportamiento?
- [ ] ¿Experimenta cambios de humillación, injusticia o aislamiento?
- [ ] ¿Existe deterioro de vínculos familiares o sociales?

2 Entorno y factores de contexto

- [ ] ¿Existen factores de vulnerabilidad personal?
- [ ] ¿Presentan cambios abruptos de comportamiento?
- [ ] ¿Experimenta cambios de humillación, injusticia o aislamiento?
- [ ] ¿Existe deterioro de vínculos familiares o sociales?



3 Ideología y narrativa

- [ ] ¿Consume propaganda extremista?
- [ ] ¿Utiliza símbolos, consignas o lenguaje codificado?
- [ ] ¿Justifica la violencia como medio legítimo?
- [ ] ¿Deshumaniza a personas o grupos específicos?

4 Actividad digital

- [ ] ¿Participa en grupos cerrados (Telegram, Discord, foros?
- [ ] ¿Mantiene contacto con reclutadores o mentores?
- [ ] ¿Comparte propaganda, manifiestos o contenido radical?
- [ ] ¿Utiliza medidas de ocultamiento digital?

5 Capacidad operativa

- [ ] ¿investiga armas, explosivos o tácticas?
- [ ] ¿Realiza vigilencia de objetivos?
- [ ] ¿Adquiere materiales sospechosos?
- [ ] ¿Recibe instrucciones para actuar?

6 Indicadores de movilización

- [ ] ¿Planifica o ensaya o ataque?
- [ ] ¿Emitió amenazas?
- [ ] ¿Publicó mensajes de despedida?
- [ ] ¿Intentó viajar o contactar zonas de conflicos?
- [ ] ¿Se integró a celulas o grupos operativos?

Principios rectores

Legalidad
Toda técnica debe contar con autorización judicial y respaldo normativo

Proporcionalidad
Las medidas debe ser adecuadas, necesarias y razonables

Necesidad
Utilizar las técnicas menos lesivas para llegar al objetivo legítimo

Cadena de custodia
Documentar cada paso para garantizar la validez de la evidencia

Enfoque integrado
Coordinación entre áreas especializadas y organismos nacionales e internacionales

Derechos fundamentales
Respeto irrestricto a las garantías constitucionales

Usar esta Checklist como guía. Cada caso requiere análisis integral, coordinación interagencial y respeto pleno de los derechos y garantías constitucionales.

Ministerio Público Fiscal de la Nación
Procuración General de la Nación

–

Av. de Mayo 760 (C1084AAP)
Ciudad Autónoma de Buenos Aires, Argentina.
Tel.: (54-11) 4338-4300
www.mpf.gob.ar | www.fiscales.gob.ar