

UNIVERSIDAD CATÓLICA DE SALTA



FACULTAD DE CIENCIAS JURÍDICAS

LICENCIATURA EN RELACIONES INTERNACIONALES

TEMA DE INVESTIGACIÓN

“La inversión económica del gobierno de los Estados Unidos (mediante el FBI) para defenderse de los ataques terroristas, ambientales y religiosos, entre los años 2.002 y 2.005”

Alumno: OSCAR ANDRÉS PUCCI

Director: Lic. CAROLINA ROMANO.

Salta, Argentina 2025



UNIVERSIDAD CATÓLICA DE SALTA

TRABAJO FINAL DE INVESTIGACIÓN DE LA CARRERA DE LICENCIATURA
EN RELACIONES INTERNACIONALES

“La inversión económica del gobierno de los Estados Unidos (mediante el FBI) para
defenderse de los ataques terroristas, ambientales y religiosos, entre los años 2.002 y
2.005”

AUTOR: Oscar Andrés Pucci

DIRECTOR: Mg. Lic. Carolina Romano

SALTA – ARGENTINA 2025

AUTORIDADES DE LA UNIVERSIDAD

GRAN CANCELLER: SER Monseñor Mario Antonio Cargnello

RECTOR: Ing. Rodolfo Gallo Cornejo

VICERRECTORA ACADÉMICA: Mg Constanza Diedrich

VICERRECTOR DE INVESTIGACIÓN Y DESARROLLO: Dr. Federico Colombo

VICERRECTOR ADMINISTRATIVO: CPN Daniel Torres

VICERRECTOR DE FORMACIÓN: Pbro. Dr. Cristian Gallardo

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS

DECANO: Dr. Eduardo Jesús Romani

SECRETARIA ACADÉMICA: Dra. María Marta Argibay

DIRECTOR DE LA CARRERA DE RELACIONES INTERNACIONALES: Lic.
Federico de Singlau

TRIBUNAL EXAMINADOR

Fecha de defensa: 15 / 12 / 2025

Lic. Federico de Singlau

Lic. Víctor F. Toledo

Lic. Oscar Oñativia

CALIFICACIÓN FINAL:

DEDICATORIA

A Valentino, Agustín, Padres, Hermanos y Sobrinos.

EPÍGRAFE

*“La persona humanista y civilizada pide las cosas por favor, el terrorista las exige
por pavor.”*

Fernando Savater

INTRODUCCIÓN

El presente trabajo se fundamenta en la teoría realista desarrollada por Hans Morgenthau (1992), quien plantea las leyes del comportamiento de los Estados, los tipos de políticas, así como las configuraciones principales del poder. Asimismo, establece que los Estados tienen un deseo innato tanto de dominar o influir en el comportamiento de otros, llevándolos a conflictos de intereses en la lucha por la supremacía.

Desde esta perspectiva, el objetivo principal de la Política Exterior para el Realismo es la supervivencia del Estado, por lo tanto, los asuntos de seguridad serán primordiales para estos actores racionales que son principales en el sistema internacional. La existencia de amenazas a la supervivencia del Estado y las acciones de Política Exterior, tales como, por ejemplo, el tratamiento hacia el terrorismo, son asuntos de supervivencia que importan al Estado por el hecho de la racionalidad que comporta su accionar (Torres Rodríguez, 2017).

Por otro lado, se pretende examinar y articular con el punto anterior, la categoría conceptual objeto de estudio de terrorismo, así como las formas y dimensiones que dan alcance a este concepto. De acuerdo a Wardlaw (1986), el terrorismo se vincula a “la amenaza o el uso de la violencia con fines políticos cuando esa acción intenta influir en la actitud y comportamiento de un grupo distinto al de sus víctimas inmediatas y cuando sus ramificaciones trascienden las fronteras nacionales” (p. 106).

Si bien esta es una definición preliminar, en este estudio se pretende analizar los enfoques teóricos sobre el terrorismo. Concretamente, tras un repaso del continuo temporal en el que diferentes aproximaciones se han ido sucediendo, se indagará sobre sus variantes en términos de terrorismo religioso y terrorismo ambiental, así como los fondos económicos y presupuestarios de prevención destinados para combatirlos.

La preocupación por el terrorismo ha aumentado notablemente desde los ataques del 11 de septiembre de 2001, que no solo alteraron la perspectiva de seguridad nacional en Estados Unidos, sino que también transformaron la política internacional. En este contexto, se vuelve esencial analizar cómo el gobierno de Estados Unidos, a través del FBI, ha respondido a las diferentes amenazas terroristas, especialmente aquellas de naturaleza religiosa y ambiental. La relevancia de estudiar las inversiones económicas en la defensa contra el terrorismo radica en comprender cómo estas decisiones no solo reflejan respuestas a amenazas inmediatas, sino también cómo se gestionan y distribuyen los recursos en un entorno caracterizado por la incertidumbre global, ¿pero... ¿qué pasaba en el mundo en ese periodo en materia de terrorismo?

En el año 2002, hubo tres grandes atentados terroristas perpetrados por grupos vinculados a Al-Qaeda y a separatistas chechenos, uno en Indonesia, otro en Rusia y otro en Kenia, asesinando a más de 340 personas, sin contar con los atacantes.

En el año 2003 las actividades terroristas tuvieron como escenario principal Irak con un número no especificado de muertos, hay que recordar que fue el año del inicio de la invasión de dicho país. Luego tenemos otros atentados, tanto en Marruecos como en Turquía, matando a más de 90 personas y a los terroristas.

En el año 2004 se produjeron atentados en España, Indonesia y en Rusia, siendo este último uno de los más impactantes ya que se produjo en una escuela y resultó en la masacre de 186 niños. Ese año murieron un total de 531 personas, incluidos los niños. No se sabe el número de terroristas muertos ese año.

Por último, en el año 2005 tenemos atentados en Reino Unido, Egipto, Indonesia y Jordania matando a 220 personas y a un número no determinado de terroristas.

Los escenarios de todos esos ataques fueron escuelas, discotecas, sectores turísticos, iglesias y transporte público, mostrando una evidente planificación para causar el mayor impacto en la población.

Entonces este estudio es relevante por diversas razones. En primer lugar, ofrece un análisis crítico sobre cómo se priorizan las amenazas y se asignan los recursos en consecuencia. En segundo lugar, investigar los costos económicos de los ataques terroristas en comparación con la inversión preventiva puede proporcionar información valiosa sobre la efectividad de las políticas y estrategias de seguridad implementadas. Evaluar si los fondos destinados a la prevención realmente están logrando sus objetivos de reducción de la amenaza terrorista es fundamental. Además, explorar las diferencias entre el terrorismo religioso y ambiental permite una comprensión más matizada de la naturaleza de estas amenazas y su evolución en la conciencia pública y política.

Para abordar la investigación de manera efectiva, se han adoptado decisiones metodológicas que permiten una exploración integral del tema. En cuanto al tipo de investigación, se utilizará un enfoque cuanti-cualitativo que permitirá realizar un análisis exhaustivo que considere tanto las cifras de inversión económica del FBI como la interpretación y comprensión de las implicaciones de dichas inversiones en el contexto de la política de seguridad. A su vez, el enfoque será explicativo relacional, lo que facilitará investigar cómo la inversión se relaciona con los resultados en términos de prevención de ataques terroristas, buscando establecer conexiones entre las decisiones de gasto y sus impactos en la seguridad nacional. La recolección de datos cuantitativos se recopilarán cifras sobre el presupuesto del FBI destinado a la prevención del terrorismo entre 2002 y 2005, mientras que para la parte cualitativa se analizarán documentos relevantes que permitirán entender la efectividad de estas inversiones y su impacto en la seguridad.

El trabajo se estructurará en ocho capítulos que abordarán diferentes aspectos del terrorismo y la respuesta del gobierno de Estados Unidos a estas amenazas. La investigación comienza en el Capítulo I en donde se exploran las complejas definiciones de terrorismo a través de las perspectivas de diversos académicos y organizaciones oficiales. Revela cómo la comprensión del terrorismo varía según el contexto político, jurídico y lingüístico, y enfatiza que las definiciones se ven influenciadas por el contexto y la perspectiva. El capítulo clasifica los diferentes tipos de terrorismo y analiza las implicaciones de estas definiciones para las respuestas estatales y las relaciones internacionales.

En el Capítulo II, el trabajo se centra en los actores clave involucrados en la lucha contra el terrorismo, con especial atención al Buró Federal de Investigaciones (FBI), relatando su evolución histórica y las importantes reformas implementadas bajo la dirección de J. Edgar Hoover, también se examinan los métodos de la agencia para la recopilación de inteligencia y las investigaciones. Luego se analiza el surgimiento de actores no estatales, como el Frente de Liberación de la Tierra (ELF) y el Frente de Liberación Animal (ALF), ilustrando cómo sus motivaciones y acciones reflejan una nueva dimensión del terrorismo interno.

El Capítulo III empieza a profundizar los cambios presupuestarios tras los atentados del 11 de septiembre, detallando el aumento sustancial de la financiación federal para defensa e inteligencia, especialmente para reforzar al FBI, centrándose en asignaciones presupuestarias específicas para iniciativas antiterroristas, ajustes operativos y la introducción de nuevas medidas de seguridad destinadas a garantizar la seguridad nacional ante la evolución de las amenazas.

Continuando con este análisis, el Capítulo IV describe el presupuesto para 2003 e ilustra la ampliación del papel del FBI en la lucha contra el terrorismo. Destaca el

importante apoyo financiero destinado a las iniciativas de modernización, el desarrollo de capacidades de inteligencia y la formación de relaciones de colaboración con otras agencias, lo que refleja un enfoque integral de la seguridad nacional.

El Capítulo V se centra en el presupuesto para 2004, haciendo hincapié en la consolidación continua de las medidas de seguridad. Describe el aumento de la financiación para la lucha contra el terrorismo, la mejora de la infraestructura y el avance tecnológico, destacando el enfoque del FBI en la adaptación a un panorama complejo de amenazas. Este capítulo destaca la importancia de las respuestas integradas a los desafíos de seguridad nacional.

En el Capítulo VI, se analiza el presupuesto de 2005, año crucial en la evolución de las políticas de seguridad estadounidenses. El capítulo analiza la continua expansión del papel del FBI en el contexto de los conflictos globales, en particular en Irak y Afganistán, haciendo hincapié en el aumento de la financiación para operaciones de inteligencia, la modernización de las instalaciones y el aumento de los recursos para la lucha contra el terrorismo.

El Capítulo VII presenta los proyectos especiales del FBI, en particular las iniciativas Webhouse y Trilogy. Estos proyectos buscan modernizar las capacidades tecnológicas y operativas de la agencia para responder a las nuevas amenazas globales. El capítulo ilustra la transformación hacia un entorno operativo digital e interconectado que mejora la eficacia del FBI ante los desafíos de seguridad contemporáneos.

En el Capítulo VIII, la atención se centra en los incidentes terroristas nacionales ocurridos entre 2002 y 2005. El capítulo analiza el auge del terrorismo, especialmente las actividades de grupos ecoterroristas como el ELF y el ALF, junto con las amenazas que representan diversos grupos con motivaciones ideológicas. Analiza incidentes

específicos, sus motivaciones y las acciones preventivas del FBI, ilustrando el diverso panorama de amenazas al que se enfrentó la agencia.

A lo largo del desarrollo de los capítulos se podrá tener acceso a toda la información mencionada la cual nos llevará a responder tanto a las preguntas iniciales, como a las que fueran apareciendo.

CAPÍTULO I

Definiciones de terrorismo

1.1 Introducción

El estudio del *terrorismo* como fenómeno político, social y jurídico requiere una comprensión amplia que considere tanto sus dimensiones históricas como las perspectivas teóricas que intentan explicarlo. En el campo de las Relaciones Internacionales, el *terrorismo* se analiza como una amenaza transnacional que desafía la autoridad del Estado y el orden del sistema internacional. Desde la teoría realista, el Estado es concebido como el actor central y racional que busca asegurar su supervivencia en un contexto anárquico. En consecuencia, toda amenaza que comprometa su estabilidad o su poder constituye un asunto de seguridad nacional, y el *terrorismo* se inscribe dentro de ese marco de preocupación vital.

Hans Morgenthau (1992) sostiene que la política internacional está regida por leyes objetivas derivadas de la naturaleza humana y que los Estados actúan guiados por el interés definido en términos de poder. Bajo esta premisa, el *terrorismo* puede entenderse como una forma particular de violencia que afecta directamente el equilibrio de poder, al intentar modificar el comportamiento de los Estados mediante el miedo y la coacción. En términos realistas, el fenómeno terrorista pone en evidencia la vulnerabilidad del Estado frente a actores no estatales que logran proyectar poder sin poseer los atributos tradicionales de soberanía.

El análisis del *terrorismo* desde esta perspectiva permite comprenderlo no solo como un hecho criminal o moralmente condenable, sino como un instrumento político con fines estratégicos. El uso del terror —como medio para condicionar las decisiones de un gobierno o desestabilizar el orden establecido— se convierte en una herramienta que desafía la racionalidad estatal y el principio de autoridad. Por lo tanto, examinar las distintas definiciones de *terrorismo* resulta esencial para entender cómo los Estados conceptualizan la amenaza y justifican sus políticas de seguridad y defensa.

A lo largo de este capítulo se desarrollan tres perspectivas complementarias para abordar el concepto: la primera, basada en el aporte de diversos autores académicos que han intentado definir el fenómeno y sus características esenciales; la segunda, de naturaleza lingüística,

proveniente del análisis del *Diccionario de la Real Academia Española*; y la tercera, de carácter jurídico-operativo, elaborada por el *Federal Bureau of Investigation* (FBI) y el *Department of Homeland Security* (DHS) de los Estados Unidos. Cada una de estas aproximaciones contribuye a clarificar los distintos enfoques desde los cuales se entiende el *terrorismo*, así como las implicaciones políticas y normativas que surgen de su conceptualización.

En suma, el propósito de este capítulo es presentar un panorama ordenado de las principales definiciones existentes, exponiendo cómo el concepto ha evolucionado y cómo sus interpretaciones reflejan intereses, valores y contextos específicos. De este modo, se busca sentar las bases teóricas necesarias para comprender el papel del *terrorismo* en las Relaciones Internacionales contemporáneas, particularmente en lo que respecta a la securitización de las amenazas y al rol del Estado como garante de la seguridad y la estabilidad global.

1.2 Según algunos autores consultados

El *terrorismo*, como categoría de análisis dentro de las Ciencias Sociales y las Relaciones Internacionales, exige una aproximación teórica que permita comprender su naturaleza, sus motivaciones y su dinámica histórica. La dificultad radica en que no existe una definición única ni universalmente aceptada que abarque la totalidad de sus manifestaciones. Por ello, la literatura académica ha intentado, desde distintos enfoques, establecer criterios que orienten su comprensión conceptual y su tratamiento político y jurídico.

Carrillo Ramírez (2015) sostiene que una de las deficiencias persistentes desde la década de 1930 ha sido la falta de criterios compatibles para definir el *terrorismo*, generando ambigüedad en los marcos normativos y en la praxis política de los Estados. Manassero y Tello (2014) coinciden en que el fenómeno terrorista es antiguo, pero su conceptualización es problemática: si bien se reconoce su existencia y sus efectos, no hay consenso respecto de su significado preciso. Según los autores, esta falta de uniformidad impide construir una definición que sea aplicable a nivel internacional.

Por su parte, García Probert (2014) subraya que el *terrorismo* se asocia históricamente con actos de violencia sistemática destinados a infundir terror en la población, afectando derechos fundamentales como la libertad, la seguridad y la propiedad, además del orden institucional vigente. En este sentido, se entiende como una forma de violencia política orientada a desestabilizar estructuras de poder y alterar el equilibrio social. Carrillo Ramírez (2015) amplía esta noción señalando que el contexto histórico condiciona la forma en que se manifiesta el *terrorismo*, los actores involucrados y sus objetivos. Propone identificar cuatro características esenciales del fenómeno:

- a) **Subversión:** entendida como la acción orientada a desestabilizar y convencer a personas o grupos de oponerse al orden establecido.
- b) **Tortura:** acto mediante el cual se infligen intencionalmente dolores o sufrimientos graves, físicos o mentales, con el propósito de obtener información o confesiones.
- c) **Genocidio:** práctica que busca destruir, total o parcialmente, a un grupo nacional, étnico o religioso.
- d) **Mercenarismo:** práctica orientada al lucro o retribución material mediante el reclutamiento para participar en conflictos o actos violentos.

De acuerdo con Carrillo (2015), estos elementos configuran al *terrorismo* como una amenaza compleja a los derechos humanos, que vulnera no solo la integridad física de las personas, sino también derechos sociales y culturales fundamentales, como la alimentación, la vivienda, el patrimonio cultural o el medioambiente.

Históricamente, el *terrorismo* surgió como una forma de violencia política legitimada por ciertos sectores en el siglo XIX, especialmente por movimientos anarquistas que consideraban el terror un medio válido para combatir sistemas conservadores y represivos. Hoffman (2006) observa que, con el cambio de siglo, el concepto se redefine, adquiriendo una dimensión ideológica más estructurada. Durante las décadas de 1960 y 1970, los movimientos de izquierda y los grupos nacionalistas radicales adoptaron el *terrorismo* como una herramienta de lucha política. Cruz (2015) señala que este proceso culmina con el surgimiento del denominado *nuevo terrorismo*, caracterizado por su alcance global y su capacidad de generar impacto mediático y psicológico a gran escala.

Los atentados del 11 de septiembre de 2001 representan un punto de inflexión. Para Manassero y Tello (2014), estos ataques otorgaron al fenómeno terrorista una nueva identidad global, mediáticamente amplificada y políticamente instrumentalizada. Taverna (2017) sostiene que el 11-S condujo a una mayor militarización de la política exterior de los Estados Unidos y al fortalecimiento de un enfoque securitario centrado en la prevención y la guerra contra el *terror*. Dicho enfoque implicó un retroceso en las libertades civiles y una expansión del aparato militar y de inteligencia, consolidando la denominada *Doctrina Bush*, basada en ataques preventivos y en la reafirmación de la unipolaridad estadounidense.

En la misma línea, Hobson (2005) explica que la *Estrategia de Seguridad Nacional* de 2002 formalizó un nuevo paradigma, denominado *nuevo imperialismo*, según el cual los Estados Unidos se propusieron crear un equilibrio de poder favorable a la expansión de la libertad política y económica. Este enfoque, además, conceptualiza la guerra contra el *terrorismo* no solo como un conflicto armado, sino también como una batalla ideológica. Bartolomé (2008) señala que, tras el 11-S, el clima interno estadounidense alcanzó niveles de autoritarismo inéditos, legitimados por el patriotismo y el miedo. La declaración del *Estado de Urgencia* por parte del presidente George W. Bush facilitó la implementación de medidas excepcionales que transformaron profundamente la relación entre seguridad y libertad.

Según lo expresado por Patricia Kreinbohn (2016), “hasta la fecha, no existe una definición universalmente consensuada del fenómeno terrorista” (p. 80). Esta falta de consenso ha conducido a la proliferación de definiciones elaboradas por distintos organismos y especialistas, adaptadas a contextos políticos específicos. En ese marco, Rafael Calduch Cervera (1991) define el *terrorismo* como “una estrategia de relación política basada en el uso de la violencia y de las amenazas de violencia por un grupo organizado, con objeto de inducir un sentimiento de terror o inseguridad extrema en una colectividad humana no beligerante y facilitar así el logro de sus demandas” (p. 45).

Esta definición resalta el carácter político del *terrorismo* como instrumento de presión y negociación, en el cual la violencia cumple una función comunicativa y simbólica, dirigida tanto a las víctimas directas como a la comunidad internacional. Desde la teoría realista, este aspecto revela cómo los actores no estatales pueden influir en el comportamiento de los Estados, erosionando su autoridad y alterando el equilibrio de poder.

Complementariamente, dentro de los estudios contemporáneos sobre seguridad, emergen dos conceptos que enriquecen la comprensión del *terrorismo*: la *securitización* y el *complejo de seguridad regional*.

La *securitización*, según la Escuela de Copenhague, consiste en el proceso mediante el cual un asunto es presentado como una amenaza existencial para un actor, legitimando medidas extraordinarias para su contención. En tanto, los *complejos de seguridad regional* describen la interacción entre Estados cuyas preocupaciones de seguridad están tan interconectadas que ninguna de ellas puede analizarse de manera aislada.

Aplicados al fenómeno del *terrorismo*, estos conceptos permiten comprender cómo la percepción del peligro y la necesidad de defensa impulsan la cooperación internacional, la creación de alianzas militares y la intervención preventiva. Así, el *terrorismo* no solo se concibe como una amenaza interna o doméstica, sino también como un elemento estructurante del sistema

internacional contemporáneo, que condiciona la política exterior, la defensa y los derechos humanos.

1.3 Según el Diccionario de la Real Academia Española

La construcción lingüística del término *terrorismo* constituye una dimensión fundamental para comprender la esencia del fenómeno. El análisis semántico del *Diccionario de la Real Academia Española* (RAE, 2023) permite observar cómo el lenguaje refleja concepciones históricas y sociales que condicionan la interpretación del concepto. La RAE ofrece dos acepciones principales: la primera, “dominación por el terror”, y la segunda, “sucesión de actos de violencia ejecutados para infundir el terror”. Estas definiciones, aunque correctas en su formulación, resultan insuficientes para capturar la complejidad política y jurídica del *terrorismo*, ya que no consideran los factores ideológicos, estratégicos ni contextuales que lo determinan.

A partir de estas definiciones, es posible realizar un análisis de los términos que las componen. La primera palabra clave, *dominación*, se define como la “acción o efecto de dominar”, y el verbo *dominar* implica la “posesión de un dominio sobre algo o alguien”. A su vez, *dominio* se entiende como “el poder o ascendente que se ejerce sobre otras personas”. De ello se desprende que el *terrorismo*, en su sentido más básico, se relaciona con el ejercicio del poder sobre otros a través del miedo. En consecuencia, el fenómeno terrorista puede concebirse como la utilización del terror como instrumento de dominación política, social o ideológica.

Por otro lado, la palabra *poder*, según la RAE, posee tres acepciones relevantes: (a) “tener expedita la facultad de hacer algo”; (b) “facilidad o tiempo de hacer algo”; y (c) “ser más fuerte que alguien, capaz de vencerle”. Estas definiciones permiten vincular el *terrorismo* con la capacidad de un actor —individual o colectivo— para imponer su voluntad sobre otros mediante el uso o la amenaza de la violencia. La fuerza, en este contexto, adquiere una dimensión simbólica: no solo destruye físicamente, sino que busca someter psicológicamente a su objetivo, produciendo un estado de parálisis colectiva.

La palabra *terror*, núcleo semántico del término, se define como un “miedo intenso” o una “gran perturbación angustiosa del ánimo ante un riesgo o daño real o imaginario”. De este modo, el *terrorismo* no necesariamente requiere del acto violento en sí, sino del efecto que produce o pretende producir: la generación de miedo social como medio para ejercer control. En ese sentido, los actos terroristas pueden concebirse como estrategias comunicativas orientadas a transmitir mensajes de poder, resistencia o castigo, en función de la ideología que los sustente.

Del análisis anterior se deduce que la definición de la RAE describe un proceso más que una entidad fija: un conjunto de acciones destinadas a provocar miedo con fines de dominación. Sin embargo, la definición académica carece de la carga subjetiva y contextual que determina el significado político del *terrorismo*. Por ello, es necesario considerar el papel del sujeto que ejecuta el acto, el propósito ideológico que lo motiva y el contexto geopolítico en el cual se desarrolla. Estos elementos otorgan al concepto su carácter dinámico y su alcance variable.

Desde esta perspectiva, no solo el verbo —*dominar* o *infundir*— define el *terrorismo*, sino también el sustantivo que designa al actor o grupo que lo ejecuta. La intencionalidad política del acto es lo que lo convierte en un fenómeno de relevancia internacional. Por ejemplo, si un grupo religioso perpetra actos violentos con el objetivo de propagar su fe o castigar a quienes no la profesan, se configura lo que se denomina *terrorismo religioso internacional*. En cambio, si los actos se cometen dentro de las fronteras de un Estado, sin dirección extranjera, se tratará de *terrorismo doméstico* o *nacional*.

A partir del análisis lingüístico, puede proponerse una definición más integral del término, en la que confluyan sus dimensiones semánticas, políticas y psicológicas. Así, el *terrorismo* puede entenderse como “la realización, por parte de una o más personas con posiciones ideológicas propias, de actos determinados con una intensidad y un ímpetu extraordinarios, en un territorio nacional o ajeno, con el fin de demostrar su fortaleza o capacidad de prevalecer sobre otras posturas a través de una perturbación angustiosa del ánimo, causada por un riesgo real o imaginario producto de dichos actos”.

Esta formulación amplía las definiciones de la RAE al incorporar los elementos ideológicos, estratégicos y simbólicos del fenómeno, y permite comprender cómo el uso del *terror* se convierte en un instrumento de poder político. El análisis semántico del término muestra, además, que el lenguaje no es neutro: refleja estructuras de poder y legitimación, determinando cómo los Estados y las sociedades perciben y responden a las amenazas que enfrentan.

En el contexto de las Relaciones Internacionales, este enfoque lingüístico se integra con las perspectivas teóricas y jurídicas para ofrecer una visión multidimensional del *terrorismo*. De este modo, el significado del término no se agota en la definición lexical, sino que se amplía a la comprensión de las prácticas sociales y políticas que lo configuran como fenómeno global.

1.4 Según el FBI

En concordancia con lo señalado por diversos autores, el *Federal Bureau of Investigation* (FBI) reconoce que no existe una definición única y universalmente aceptada de *terrorismo*. Desde su perspectiva jurídica y operativa, el fenómeno se conceptualiza a partir de criterios legales establecidos en el *Code of Federal Regulations* (C.F.R.) y en el *United States Code* (U.S.C.), documentos que orientan la actuación de las agencias federales en materia de seguridad y persecución penal.

El *Código de Regulaciones Federales* define el *terrorismo* como “el uso ilegal de la fuerza y la violencia contra las personas o la propiedad para intimidar o coaccionar a un gobierno, la población civil o cualquier segmento de la misma, en apoyo de objetivos políticos o sociales” (28 C.F.R. § 0.85 [Código de Regulaciones Federales de los Estados Unidos, sección 0.85]). Esta definición resalta tres elementos esenciales:

1. El carácter ilegal de la fuerza o la violencia utilizada.
2. La existencia de una finalidad política o social.
3. La intención de intimidar o coaccionar a una población o gobierno.

De acuerdo con el FBI, el *terrorismo* puede clasificarse en dos grandes categorías: El ***terrorismo nacional (o doméstico)*** se refiere al uso ilegal o la amenaza de uso de la fuerza o violencia por parte de un grupo o individuo basado y operando enteramente dentro de los Estados Unidos o Puerto Rico, sin dirección extranjera, cometido contra personas o propiedad, con el propósito de intimidar o coaccionar a un gobierno, la población civil o cualquier segmento de la misma, en apoyo de objetivos políticos o sociales. Por su parte, el ***terrorismo internacional*** abarca actos violentos o peligrosos para la vida humana que violan las leyes penales de los Estados Unidos o de cualquier Estado, o que constituirían infracciones penales si se cometieran dentro de la jurisdicción estadounidense. Estos actos están destinados a intimidar o coaccionar a la población civil, influir en la política de un gobierno mediante la intimidación o la coerción, o afectar la conducta gubernamental mediante el asesinato o el secuestro (*18 U.S.C. § 2331(5)*) [Código de los Estados Unidos, Título 18, Sección 2331(5)].

Asimismo, el *Department of Homeland Security* (DHS) adopta una definición sustancialmente similar conforme a la *Homeland Security Act*, que describe el *terrorismo* como cualquier actividad que:

- a) Implique un acto peligroso para la vida humana o potencialmente destructivo de la infraestructura crítica o de los recursos clave, constituyendo una violación de las leyes penales de los Estados Unidos o de cualquier subdivisión estatal; y
- b) Parezca destinada a intimidar o coaccionar a la población civil, influir en la política de un gobierno mediante la intimidación o la coerción, o afectar la conducta de un gobierno mediante destrucción masiva, asesinato o secuestro (*6 U.S.C. § 101(18)*) [Ley de Seguridad Nacional de los Estados Unidos, sección 101(18)].

El FBI distingue además entre dos tipos de actividad relacionados con el *terrorismo*:

1. **Incidente terrorista**, entendido como todo acto violento o peligroso para la vida humana que viole las leyes penales y tenga por objeto intimidar o coaccionar a un gobierno o población.
2. **Prevención del terrorismo**, que se refiere a cualquier acción mediante la cual un acto violento es interceptado exitosamente gracias a la actividad de investigación.

La Primera Enmienda y las limitaciones legales

En el marco de la política federal estadounidense, se establece que ninguna investigación puede basarse únicamente en actividades protegidas por la Primera Enmienda de la Constitución. Esto significa que el FBI no puede investigar ni mantener información sobre ciudadanos estadounidenses solo por ejercer su libertad de expresión, religión, prensa o reunión pacífica.

La **Primera Enmienda**, adoptada el 15 de diciembre de 1791 como parte de la *Carta de Derechos (Bill of Rights)*, prohíbe la creación de leyes que establezcan una religión oficial o que restrinjan la libertad de culto, expresión, prensa o reunión, así como el derecho a solicitar compensación por agravios al gobierno. Inicialmente aplicable solo al Congreso federal, su alcance se amplió a las leyes estatales tras el caso *Gitlow v. New York* (1925), mediante la doctrina de la incorporación a través de la Decimocuarta Enmienda.

De este modo, el FBI debe ejercer un “juicio prudente” al determinar si una conducta constituye una amenaza o si se encuentra amparada por la libertad constitucional. Esta distinción es esencial para preservar el equilibrio entre seguridad nacional y derechos civiles, un tema que ha generado amplio debate tras los atentados del 11-S y la promulgación del *USA PATRIOT Act* en 2001.

Terminología y categorías de amenaza

Con el fin de sistematizar la respuesta institucional frente al *terrorismo*, el FBI y el DHS emplean el término *extremista violento doméstico (Domestic Violent Extremist, DVE)* para

designar a individuos que operan dentro de la jurisdicción estadounidense y que buscan promover objetivos ideológicos, total o parcialmente, a través de actos ilegales de fuerza o violencia.

Es importante subrayar que la mera defensa de ideologías radicales o el uso de retórica extremista no constituyen, en sí mismos, actos de extremismo violento, salvo que impliquen amenazas directas o específicas de violencia. Esta distinción responde al principio constitucional de protección de la libre expresión, aunque reconoce que la incitación o el apoyo material al *terrorismo* pueden ser penalmente sancionables.

El FBI y el DHS revisan y actualizan periódicamente la clasificación de amenazas internas para reflejar la evolución de los actores, motivaciones e ideologías involucradas. En la actualidad, las categorías más relevantes de *terrorismo doméstico* (*domestic terrorism*) se dividen en los siguientes grupos:

1. **Extremismo violento por motivos raciales o étnicos:** comprende el uso o amenaza de fuerza y violencia para promover agendas ideológicas derivadas de prejuicios raciales o étnicos. Estos actores suelen justificar sus acciones en interpretaciones políticas o religiosas que promueven la superioridad de un grupo sobre otro.
2. **Extremismo violento antigubernamental o anti-autoridad:** incluye actos motivados por sentimientos de oposición al gobierno, las instituciones o las jerarquías percibidas como ilegítimas. Abarca desde movimientos anti-fiscales hasta grupos conspirativos armados.
3. **Extremismo violento ambiental o por los derechos de los animales:** involucra el uso de la violencia para poner fin o mitigar la crueldad percibida hacia los animales o el daño ambiental. En algunos casos, estos grupos atacan instalaciones o infraestructuras vinculadas a la industria o la investigación científica.
4. **Extremismo violento relacionado con el aborto:** abarca actos cometidos tanto por militantes *pro-life* como *pro-choice* que recurren a la violencia para promover sus creencias o impedir la acción del otro sector.

5. **Otras amenazas de terrorismo doméstico:** incluye aquellos actos o amenazas de violencia motivados por ideologías híbridas o múltiples agravios personales, que no encajan en las categorías anteriores. Estas pueden estar vinculadas a factores religiosos, de género u orientación sexual.

Estas categorías son utilizadas tanto para la clasificación de investigaciones como para el diseño de estrategias preventivas. De acuerdo con el FBI, su función no es solo operativa, sino también analítica, ya que permite identificar patrones de radicalización y tipologías de violencia interna.

Metodología y registro

El FBI considera que un acto de *terrorismo doméstico* debe cumplir dos condiciones fundamentales:

1. Estar impulsado por una ideología o motivación política reconocible.
2. Involucrar amenazas o actos de violencia dirigidos a víctimas específicas con el propósito de promover un objetivo ideológico nacional.

El Bureau utiliza esta definición para documentar tanto incidentes consumados como complots frustrados. Las “parcelas de terrorismo interno interrumpidas” (*interrupted plots*) se registran cuando, a juicio del FBI, sin la intervención de las autoridades, el plan habría derivado en un acto violento.

No obstante, el organismo reconoce limitaciones estructurales en su capacidad de registro. No existe un requisito federal que obligue a las agencias locales o estatales a reportar incidentes motivados ideológicamente, especialmente cuando no resultan en lesiones o muertes. Por ello, el FBI admite que sus datos pueden ser incompletos y que la información disponible depende de la cooperación entre distintos niveles de gobierno.

En su conjunto, el marco conceptual y operativo del FBI refleja una comprensión del *terrorismo* centrada en la seguridad nacional y la protección del Estado. Desde la perspectiva de

la teoría realista, esta visión reafirma el papel del Estado como actor soberano que responde a las amenazas mediante el uso legítimo de la fuerza y la expansión de sus capacidades de control. Así, el *terrorismo* se define tanto como una amenaza a la seguridad interna como un desafío a la autoridad estatal en el orden internacional contemporáneo.

Síntesis del Capítulo I: Definiciones y Enfoques del Terrorismo

El presente capítulo desarrolla una aproximación integral al fenómeno del terrorismo, entendiendo su complejidad desde tres dimensiones complementarias: teórica, lingüística y jurídico-operativa. Desde la teoría realista de las Relaciones Internacionales, el terrorismo se concibe como una amenaza transnacional que desafía la autoridad del Estado y el equilibrio del sistema internacional. Su análisis permite comprenderlo no solo como un acto criminal, sino como una estrategia política orientada a ejercer poder e influir en la conducta estatal mediante el miedo y la coacción.

Los autores consultados coinciden en la ausencia de una definición universalmente aceptada. Carrillo Ramírez (2015), Manassero y Tello (2014) y García Probert (2014) sostienen que el terrorismo es un fenómeno histórico y mutable, cuyas manifestaciones varían según el contexto político y social. Tras los atentados del 11 de septiembre de 2001, el terrorismo adquirió una nueva dimensión global, asociada a la securitización de las amenazas y a la expansión de políticas preventivas que redefinieron la relación entre seguridad y libertad.

Desde la perspectiva lingüística, el análisis del *Diccionario de la Real Academia Española* (RAE, 2023) revela que el término “terrorismo” se asocia a la dominación por medio del miedo, aunque esta definición resulta limitada. Se propone una comprensión más amplia que incorpora la intencionalidad política, la dimensión psicológica y el carácter comunicativo de los actos terroristas, entendidos como expresiones simbólicas de poder y resistencia.

En el plano jurídico, las definiciones del Federal Bureau of Investigation (FBI) y del Department of Homeland Security (DHS) precisan el terrorismo como el uso ilegal de la fuerza o la violencia con fines políticos o sociales, distinguiendo entre terrorismo doméstico e internacional. Estas instituciones clasifican además las amenazas internas según motivaciones ideológicas —raciales, antigubernamentales, ambientales o religiosas— y enfatizan la necesidad de proteger simultáneamente la seguridad nacional y los derechos constitucionales.

En síntesis, el capítulo concluye que el terrorismo es un fenómeno multidimensional que trasciende las fronteras nacionales y conceptuales. Su estudio requiere integrar enfoques teóricos, lingüísticos y normativos para comprender su evolución, su instrumentalización política y su impacto sobre la seguridad internacional contemporánea.

Referencias

- Bartolomé, M. (2008). *La seguridad internacional contemporánea*. Instituto de Publicaciones Navales.
- Calduch Cervera, R. (1991). *Relaciones internacionales: teoría y estructura del sistema internacional*. Tecnos.
- Carrillo Ramírez, J. (2015). *Terrorismo internacional y seguridad global*. Universidad Nacional Autónoma de México.
- Cruz, A. (2015). *El nuevo terrorismo y su impacto global*. *Revista de Estudios Internacionales*, 22(3), 45–60.
- Federal Bureau of Investigation. (2023). *Domestic terrorism definitions and threat categories*. United States Department of Justice. <https://www.fbi.gov>
- García Probert, L. (2014). *La violencia política y el terrorismo en el siglo XXI*. Editorial Jurídica Continental.
- Hobson, J. (2005). *The new imperialism: American foreign policy after 9/11*. Oxford University Press.
- Hoffman, B. (2006). *Inside terrorism* (2nd ed.). Columbia University Press.
- Kreinbohn, P. (2016). *Perspectivas teóricas del terrorismo contemporáneo*. *Revista de Ciencias Políticas*, 12(4), 77–89.
- Manassero, M., & Tello, G. (2014). *El terrorismo y sus manifestaciones globales*. Universidad de Buenos Aires.
- Morgenthau, H. (1992). *Politics among nations: The struggle for power and peace* (7th ed.). McGraw-Hill.
- Real Academia Española. (2023). *Diccionario de la lengua española* (23.^a ed.). <https://dle.rae.es>

Taverna, F. (2017). *La política exterior estadounidense post 11-S. Revista de Estudios Estratégicos*, 8(1), 33–52.

United States Code. (2001). *18 U.S.C. § 2331(5) [Código de los Estados Unidos, Título 18, Sección 2331(5)]*.

United States Code. (2002). *6 U.S.C. § 101(18) [Homeland Security Act of the United States, sección 101(18)]*.

United States Code of Federal Regulations. (2001). *28 C.F.R. § 0.85 [Código de Regulaciones Federales de los Estados Unidos, sección 0.85]*.

United States Supreme Court. (1925). *Gitlow v. New York*, 268 U.S. 652 (1925).

CAPÍTULO II

Los actores

2.1 Introducción

El estudio del terrorismo doméstico en los Estados Unidos exige comprender a los actores que participan activamente en su desarrollo, control y confrontación. Entre ellos, el *Federal Bureau of Investigation* (FBI) constituye el organismo central del aparato estatal encargado de investigar, prevenir y neutralizar amenazas a la seguridad nacional. En contraposición, emergen actores no estatales que, impulsados por ideologías radicales, cuestionan el orden establecido mediante acciones de sabotaje o violencia simbólica.

El presente capítulo se centra en el análisis del FBI como actor institucional dentro del sistema de seguridad de los Estados Unidos, atendiendo a su origen histórico, estructura organizativa, métodos de investigación, estrategias de inteligencia y políticas en materia de derechos civiles y libertades constitucionales.

La comprensión del FBI como actor no puede limitarse a su función operativa; debe incluir su evolución como símbolo del poder estatal moderno, basado en la legalidad, la centralización y la profesionalización del control social. Su historia se entrelaza con los procesos de construcción del Estado federal y con los dilemas éticos que surgen del equilibrio entre seguridad y libertad.

De esta manera, el capítulo examina el modo en que el FBI se consolidó como una agencia de inteligencia e investigación criminal de alcance nacional y global, así como las tensiones que enfrenta al operar en un entorno donde los valores democráticos deben coexistir con la necesidad de preservar el orden ante amenazas internas y externas.

2.2 El Federal Bureau of Investigation (FBI)

2.2.1 Sus inicios y proceso de institucionalización

A comienzos del siglo XX, la estructura institucional de los Estados Unidos presentaba una debilidad evidente en la aplicación uniforme de la ley federal. Las fuerzas de seguridad locales y estatales operaban con criterios dispares, sin coordinación entre sí, y estaban fuertemente condicionadas por designaciones políticas, bajos salarios y escasa formación profesional. A nivel nacional, las leyes penales eran limitadas y las agencias federales contaban con escaso personal y jurisdicción reducida.

En ese contexto, surgieron movimientos ideológicos radicales, entre ellos el **anarquismo**, una corriente derivada del marxismo que rechazaba toda forma de autoridad estatal. Los anarquistas consideraban que el gobierno era opresivo y debía ser derrocado mediante la acción directa y la violencia política. A finales del siglo XIX, una serie de atentados y asesinatos de líderes políticos y jefes de Estado —incluido el del presidente estadounidense William McKinley en 1901— evidenció la capacidad de estas redes internacionales de generar inestabilidad.

El asesinato de McKinley, perpetrado por **León Czolgosz**, un trabajador desempleado influenciado por los escritos de **Emma Goldman** y **Alexander Berkman**, conmocionó a la nación. Tras la muerte del presidente, **Theodore Roosevelt** asumió el poder, impulsando una agenda reformista inspirada en el **Movimiento Progresista**, que defendía la intervención del gobierno federal para promover la justicia y la moral pública. Roosevelt había sido comisionado del *Servicio Civil* y jefe del Departamento de Policía de Nueva York, experiencias que consolidaron su convicción de que la ley debía aplicarse con disciplina y rigor institucional.

Bajo su liderazgo, el Estado federal asumió por primera vez la responsabilidad de estructurar una agencia de investigación centralizada, profesional y libre de influencias políticas. Este proceso se consolidó dos décadas después, en 1924, cuando el presidente **Calvin Coolidge** designó como fiscal general a **Harlan Fiske Stone**, quien nombró a **J. Edgar Hoover** como director de la entonces *Bureau of Investigation*. Hoover, que había ingresado al Departamento de

Justicia en 1917, representaba una nueva generación de funcionarios orientados al profesionalismo, la meritocracia y la modernización administrativa.

Hoover transformó una oficina debilitada y politizada en una organización eficiente, dotada de normas éticas, procedimientos técnicos y capacidad de investigación científica. Este proceso de institucionalización fue clave para que el FBI se consolidara como símbolo del poder estatal racional y burocrático, en línea con la definición weberiana del Estado como monopolio legítimo de la coerción.

2.2.2 Reformas y profesionalización bajo J. Edgar Hoover

La reforma estructural llevada a cabo por Hoover redefinió la misión y la identidad del FBI. El objetivo principal era modernizar la agencia y convertirla en un modelo de eficiencia, disciplina y competencia técnica. Para ello, se implementaron cuatro ejes fundamentales:

1. Selección y mantenimiento del personal

Hoover eliminó los nombramientos políticos, depuró los cuadros considerados incompetentes e instauró un sistema meritocrático. Los candidatos a agentes debían aprobar evaluaciones físicas, entrevistas psicológicas y verificaciones de antecedentes personales y profesionales. Además, se estableció un código de conducta estricto que prohibía la corrupción, el nepotismo y el uso indebido del poder.

El FBI pasó de tener unos 650 empleados en 1924 —441 de ellos agentes— a contar con menos de 600 tras una depuración profunda. Esta reducción permitió concentrar recursos en personal altamente calificado, consolidando una cultura institucional basada en la lealtad, el secreto y la profesionalidad.

2. Creación de la base de datos de huellas dactilares

Uno de los aportes más revolucionarios de Hoover fue la creación del sistema nacional de identificación mediante huellas dactilares. Este registro centralizado, que comenzó a funcionar en 1924, permitió conectar casos criminales en todo el país y establecer un modelo científico de identificación.

El sistema creció exponencialmente: en la década de 1930 ya incluía intercambios con Canadá y otros países aliados, y en 1932 se añadió una base civil para registros no penales. Para 1936 el archivo contaba con 100.000 tarjetas, y en 1946 superaba los 100 millones. Este avance no solo optimizó las investigaciones, sino que transformó al FBI en un centro nacional de referencia para todas las agencias policiales.

3. Recopilación de estadísticas delictivas

La necesidad de contar con datos fiables sobre criminalidad llevó a la creación del *Uniform Crime Reporting Program (UCR)* en 1930. El Congreso delegó en el FBI la recopilación y sistematización de estadísticas delictivas, en coordinación con la *International Association of Chiefs of Police*.

El UCR permitió conocer la magnitud y distribución de los delitos, orientando la formulación de políticas públicas y la asignación de recursos. Desde entonces, este programa se convirtió en una herramienta esencial para el diagnóstico y análisis de la seguridad en Estados Unidos, estableciendo un precedente global en materia de criminología aplicada.

4. Creación del laboratorio de criminalística

La cuarta reforma estructural de Hoover fue la creación, en 1932, del *FBI Laboratory*. Este laboratorio representó un salto cualitativo en la aplicación de la ciencia a la investigación criminal. Bajo la dirección del agente especial **Charles Appel**, el laboratorio comenzó con recursos modestos, pero rápidamente se convirtió en un centro de referencia en balística, documentología, química forense y análisis biológico.

El laboratorio no solo sirvió al FBI, sino también a las fuerzas policiales de todo el país, consolidando la posición de la agencia como autoridad científica en materia criminal. La incorporación de la ciencia permitió pasar de una práctica empírica de la investigación policial a una basada en la evidencia.

La Segunda Guerra Mundial y la expansión del FBI

Durante la Segunda Guerra Mundial, el FBI asumió responsabilidades estratégicas en la prevención del sabotaje y la protección de infraestructuras críticas. Antes del ingreso oficial de Estados Unidos al conflicto, la agencia inspeccionó más de 2.000 plantas industriales, elaborando informes de seguridad y recomendaciones técnicas.

En 1942, agentes federales desarticularon una operación de sabotaje nazi conocida como *Operación Pastorius*, tras la entrega voluntaria de uno de los conspiradores, George Dasch. Este caso evidenció la eficacia del sistema de inteligencia interno del FBI.

Durante el período bélico, el personal de la agencia creció de 2.400 empleados en 1940 a más de 13.000 en 1944. El área de identificación y dactiloscopia alcanzó tal magnitud que debió trasladarse a instalaciones del gobierno federal de tamaño equivalente a un campo de fútbol.

La profesionalización y expansión del FBI durante este período consolidaron su reputación como institución moderna, eficiente y científicamente avanzada, convirtiéndola en un modelo replicado por otras agencias de seguridad en el mundo.

2.2.3 Métodos de investigación y procedimientos operativos

El funcionamiento operativo del FBI está reglamentado por las **Directrices del fiscal general para Operaciones Nacionales del FBI** (*Attorney General Guidelines for Domestic FBI Operations*, AGG-Dom), que delimitan los procedimientos de investigación, los estándares éticos y las competencias jurisdiccionales.

Apertura de investigaciones

El FBI distingue entre dos tipos de investigaciones: *preliminares* y *completas*.

- **Investigación preliminar:** puede iniciarse ante cualquier alegación o información indicativa de posible actividad criminal o amenaza a la seguridad nacional. No requiere pruebas concluyentes, pero sí una sospecha razonable.
- **Investigación completa:** se abre cuando existe una “base fáctica articulable”, es decir, evidencia suficiente que indique la existencia o preparación de un delito federal.

Las investigaciones que involucren a funcionarios públicos, organizaciones religiosas, medios de comunicación o figuras políticas relevantes se clasifican como *Asuntos de Investigación Sensible* (*Sensitive Investigative Matters*, SIM), requiriendo aprobación del *Chief Division Counsel* (CDC) y notificación inmediata al Departamento de Justicia.

Gestión y revisión de investigaciones

Durante su desarrollo, las investigaciones son sometidas a revisiones periódicas. Los casos abiertos son evaluados cada 90 días para verificar el cumplimiento de los objetivos, la proporcionalidad de las medidas adoptadas y la legalidad de las técnicas utilizadas.

El FBI puede recurrir a diferentes instrumentos legales según la naturaleza del caso:

- En asuntos de *terrorismo doméstico* (DT), las interceptaciones se rigen por el *Título III de la Ley Ómnibus de Control del Delito y Calles Seguras* (1968).
- En casos de *terrorismo internacional* (TI), la vigilancia se realiza conforme a la *Ley de Vigilancia de Inteligencia Extranjera* (FISA) (1978).

Asimismo, puede solicitar **Cartas de Seguridad Nacional** (**National Security Letters**) para obtener información sin orden judicial, siempre que exista un fundamento de seguridad nacional.

Cierre de investigaciones

Toda investigación debe concluir con un informe detallado que incluya:

- Resumen de resultados y hallazgos.
- Relación de métodos y técnicas utilizadas.
- Estado final de la evidencia (devuelta, destruida o archivada).
- Justificación del cierre y uso de recursos.

Las investigaciones preliminares deben cerrarse en un plazo de seis meses, prorrogable por otros seis; las completas pueden permanecer abiertas mientras se mantengan los fundamentos jurídicos.

2.2.4 Inteligencia, coordinación y análisis de amenazas

El *Federal Bureau of Investigation* desarrolla su labor de investigación y prevención dentro de un sistema complejo de gestión de amenazas, en el que la **inteligencia criminal** ocupa un papel fundamental. El proceso se articula a través del **Threat Review and Prioritization Process (TRP)**, un método estandarizado para revisar, jerarquizar y asignar prioridades a las amenazas que enfrenta el país.

El **TRP** permite establecer las **Prioridades Nacionales de Amenazas (National Threat Priorities, NTP)**, las cuales orientan las estrategias de mitigación tanto a nivel nacional como en cada una de las 56 oficinas de campo del FBI. Dichas oficinas desarrollan anualmente sus propias estrategias, adaptadas a las áreas específicas de responsabilidad territorial (*Areas of Responsibility, AOR*), con el fin de aplicar políticas de inteligencia más precisas y operativas.

Este proceso se sustenta en el consenso entre las divisiones operativas del FBI, las fiscalías federales correspondientes y los actores locales asociados a la aplicación de la ley. Las estrategias resultantes buscan mitigar las amenazas a través de la cooperación interinstitucional y la asignación eficiente de recursos humanos, financieros y tecnológicos.

El **ciclo de inteligencia** que utiliza el FBI —compartido con el *Department of Homeland Security* (DHS) y el *National Counterterrorism Center* (NCTC)— se estructura en seis fases principales:

1. **Planificación y dirección.** En esta etapa, se definen los objetivos y prioridades de inteligencia en función de las estrategias nacionales. Se establecen los requisitos de información basados en el *Marco de Prioridades de Inteligencia Nacional*, un documento que identifica las amenazas estratégicas para la seguridad de los Estados Unidos.
2. **Recopilación.** Se lleva a cabo mediante la obtención de datos de fuentes humanas, técnicas, abiertas y confidenciales. El FBI obtiene inteligencia sin procesar a través de actividades de campo, informes de agencias locales, vigilancia legal y cooperación internacional.
3. **Procesamiento.** Los datos recopilados son depurados, organizados y transformados en información analizable. Esto incluye la digitalización, categorización y verificación de autenticidad de la información recolectada.
4. **Análisis y producción.** Los analistas de inteligencia sintetizan la información, identifican patrones de comportamiento delictivo, elaboran evaluaciones y producen informes analíticos denominados *Intelligence Information Reports* (IIR). En esta fase se determinan las implicancias de las amenazas y se elaboran pronósticos sobre su evolución.
5. **Difusión.** Los productos de inteligencia son distribuidos a los responsables de la toma de decisiones —tanto dentro del FBI como en otras agencias— mediante informes escritos o sesiones informativas. También se difunden a través de portales clasificados y redes seguras, como la *Homeland Security Information Network – Intelligence* (HSIN-Intel).
6. **Evaluación.** Finalmente, se analiza la eficacia del proceso de inteligencia, la calidad de los productos elaborados y su impacto operativo. Esta retroalimentación se utiliza para ajustar las prioridades y mejorar el sistema.

En este marco, el **DHS** implementó a partir de 2019 su propio sistema de **Intelligence Threat Banding**, con el objetivo de clasificar y priorizar amenazas en función del nivel de riesgo. Dicho proceso es supervisado por el *Homeland Security Intelligence Council* (HSIC) y se integra dentro

del *Marco de Prioridades de Inteligencia de Seguridad Nacional*. Los resultados de este sistema influyen directamente en la asignación de recursos a través del proceso de planificación presupuestaria del DHS (*Planning, Programming, Budgeting and Execution, PPBE*).

Tanto el FBI como el DHS colaboran estrechamente en la producción de inteligencia estratégica. En conjunto con el NCTC, elaboran los **Joint Intelligence Bulletins (JIB)**, informes conjuntos que comunican evaluaciones sobre amenazas emergentes a socios federales, estatales, locales y tribales. Estos boletines alertan sobre tendencias en extremismo violento, detenciones relevantes y evolución de grupos terroristas domésticos e internacionales.

En el plano operativo, el FBI lidera las **Joint Terrorism Task Forces (JTTF)**, unidades conjuntas conformadas por más de 50 agencias federales y más de 500 organismos estatales, locales, tribales y territoriales. Estas fuerzas de tarea representan la primera línea de respuesta frente al terrorismo dentro de los Estados Unidos. Su misión es coordinar investigaciones, compartir inteligencia y prevenir ataques mediante la cooperación permanente entre niveles de gobierno.

A través del programa **eGuardian**, el FBI mantiene una base de datos compartida para registrar y analizar reportes de actividades sospechosas. Este sistema es utilizado en los 50 estados y en el Distrito de Columbia, e integra información proveniente de los centros de fusión (*fusion centers*), el Departamento de Defensa y las JTTF.

El enfoque de inteligencia del FBI combina la anticipación y la coordinación. La planificación de amenazas (*threat banding*) permite identificar riesgos, asignar recursos y priorizar esfuerzos. De este modo, el FBI consolida su función no solo como agencia investigativa, sino como un organismo de inteligencia integral que articula la seguridad nacional con la seguridad doméstica.

Asimismo, el **Centro de Evaluación de Amenazas del Comportamiento (Behavioral Threat Assessment Center, BTAC)**, dependiente del Grupo de Respuesta a Incidentes Críticos del FBI, colabora con las JTTF en la gestión de amenazas personalizadas y la capacitación de agentes. El BTAC lidera la iniciativa nacional de *Evaluación y Gestión de Amenazas (Threat*

Assessment and Management), promoviendo alianzas interinstitucionales para prevenir actos terroristas y violencia dirigida.

El FBI también ofrece formación a través del curso **Counterterrorism Basic Operational Learning Tool (CT BOLT)**, destinado a nuevos empleados del área de contraterrorismo. Este programa incluye módulos sobre protección de derechos constitucionales, políticas de privacidad y respeto por las libertades civiles durante las investigaciones.

La conjunción entre inteligencia, análisis, cooperación y capacitación configura un modelo integral de seguridad que permite al FBI adaptarse a las dinámicas cambiantes del terrorismo y del extremismo violento en el siglo XXI.

2.2.5 Respeto a los derechos civiles y libertades constitucionales

El papel del FBI en la defensa de la seguridad nacional implica un compromiso dual: proteger a la población frente a amenazas y garantizar el respeto irrestricto a los derechos y libertades reconocidos por la **Constitución de los Estados Unidos**.

El marco regulatorio establecido por las *Attorney General Guidelines for Domestic FBI Operations (AGG-Dom)* define que toda investigación debe regirse por el principio del **uso del método menos intrusivo posible**, teniendo en cuenta la gravedad del delito o amenaza y el impacto potencial sobre los derechos civiles de las personas involucradas.

Este principio se traduce en un conjunto de obligaciones que incluyen:

- Evitar investigaciones basadas exclusivamente en el ejercicio de derechos protegidos por la **Primera Enmienda** (libertad de expresión, religión, prensa y reunión).
- No discriminar por raza, religión, género, orientación sexual u opinión política.
- Aplicar controles legales a toda forma de vigilancia, recolección de datos o interceptación de comunicaciones.

El respeto a las libertades civiles no se limita a una cuestión ética, sino que constituye un requisito operativo y de legitimidad democrática. Las investigaciones sobre terrorismo doméstico (DT), por su naturaleza, presentan un riesgo elevado de interferir con actividades políticas o de activismo social. Por ello, el FBI somete estos casos a revisiones legales internas adicionales, a fin de asegurar que ninguna operación vulnere derechos fundamentales.

En este contexto, el **Department of Homeland Security (DHS)** cumple una función complementaria mediante su **Oficina de Derechos Civiles y Libertades Civiles (Office for Civil Rights and Civil Liberties)** y su **Oficina de Privacidad (Privacy Office)**. Ambas supervisan las actividades de inteligencia, garantizando la transparencia y la rendición de cuentas en la aplicación de la ley.

El **National Counterterrorism Center (NCTC)** también participa en la revisión y validación de los informes analíticos que involucran información sobre personas estadounidenses. Bajo la **Orden Ejecutiva 12333** y las directrices del Fiscal General, el NCTC está autorizado a compartir inteligencia con el FBI y el DHS, pero con restricciones estrictas sobre la recopilación y conservación de datos personales.

Además, el FBI y el DHS imparten formación constante a su personal sobre derechos civiles, ética pública y privacidad. El cumplimiento de estas normas se revisa periódicamente a través de auditorías internas y externas, que buscan prevenir abusos de poder y garantizar la transparencia institucional.

El DHS ha establecido, asimismo, una política de **no perfilamiento** (*non-profiling policy*), que prohíbe cualquier práctica de identificación o vigilancia basada en criterios raciales, étnicos o religiosos, salvo en circunstancias excepcionales y justificadas.

Desde una perspectiva más amplia, estas prácticas expresan la tensión permanente entre seguridad y libertad. En una democracia liberal, el uso del poder coercitivo debe estar sujeto a límites normativos y éticos, lo que convierte al respeto por las libertades civiles en un componente esencial del contraterrorismo moderno.

La doctrina del FBI enfatiza que la **eficacia operativa** no puede alcanzarse sacrificando los valores constitucionales que legitiman su existencia. De hecho, la confianza ciudadana en las instituciones depende de la percepción de que las mismas actúan dentro del marco legal y con proporcionalidad.

Por ello, tanto el FBI como el DHS insisten en que la **prevención del extremismo violento** debe realizarse protegiendo los derechos de todas las personas y comunidades. La cooperación con las comunidades locales, la transparencia en los procesos de inteligencia y la rendición de cuentas ante los organismos de supervisión civil son pilares fundamentales de esta estrategia.

De esta forma, el Estado estadounidense busca preservar su integridad frente a las amenazas del terrorismo doméstico sin comprometer los principios democráticos que lo sustentan, consolidando un modelo de seguridad basado en la ley, la ética y la responsabilidad institucional.

2.3 Introducción: el papel de los actores no estatales en el terrorismo doméstico

El terrorismo doméstico contemporáneo en los Estados Unidos no puede entenderse sin considerar el papel de los **actores no estatales**, aquellos que operan fuera del marco jurídico formal del Estado, pero que ejercen influencia política, social o simbólica mediante la violencia o la amenaza de violencia. En este sentido, las organizaciones de tipo ideológico, ecológico o animalista radical se han convertido en una de las expresiones más complejas del extremismo interno. A diferencia de las organizaciones clásicas de terrorismo político o religioso, estos grupos actúan bajo motivaciones morales o éticas, lo que les otorga una legitimación simbólica ante ciertos sectores sociales.

El **Federal Bureau of Investigation (FBI)** y el **Department of Homeland Security (DHS)** reconocen dentro del espectro del terrorismo doméstico a los movimientos que promueven la acción directa violenta en nombre de causas ecológicas o de derechos animales. Entre ellos destacan dos organizaciones que, aunque no poseen estructuras centralizadas ni jerarquías, han sido consideradas una amenaza persistente para la seguridad interna: el **Frente de Liberación de la Tierra (FLT)** y el **Frente de Liberación Animal (FLA)**.

Ambos movimientos, surgidos en el Reino Unido y extendidos luego a Estados Unidos, comparten un modelo organizativo descentralizado basado en células autónomas y un discurso que combina ética ambiental con rechazo radical a las instituciones del Estado y a la economía capitalista. El análisis de estos actores no estatales resulta indispensable para comprender cómo se configura la noción de terrorismo doméstico y cómo el Estado redefine sus estrategias de control, vigilancia y represión frente a movimientos que, aunque no buscan derrocarlo, sí cuestionan su legitimidad moral y sus políticas económicas.

2.4 El Frente de Liberación de la Tierra (FLT)

2.4.1 Orígenes y contexto ideológico

El **Frente de Liberación de la Tierra (FLT)**, conocido internacionalmente como *Earth Liberation Front (ELF)*, nació en **Brighton, Inglaterra, en 1992**, como una escisión del movimiento ambientalista radical **La Tierra Primero** (*¡Earth First!*). Este último se había originado en los Estados Unidos en la década de 1980 con una ideología de protesta directa, orientada a impedir la destrucción ambiental mediante bloqueos, ocupaciones y sabotajes menores.

Con el paso del tiempo, *La Tierra Primero* fue ganando popularidad, lo que llevó a parte de sus miembros a considerar necesario mantener una imagen pública pacífica y legal. Sin embargo, un sector más radical argumentó que las formas tradicionales de protesta eran ineficaces frente al poder corporativo y la degradación ambiental. Así, en 1992, decidieron adoptar una nueva denominación —**Frente de Liberación de la Tierra**— para canalizar las acciones ilegales bajo un nombre diferenciado, inspirado en el modelo del **Frente de Liberación Animal (FLA)**.

Desde su creación, el FLT se definió como un **colectivo anónimo y descentralizado**, sin jerarquías ni liderazgo formal, compuesto por individuos o células autónomas que comparten una misma filosofía: el uso del sabotaje económico como herramienta para detener la explotación del planeta. Su estructura horizontal y la ausencia de una autoridad central lo convirtieron en un movimiento extremadamente difícil de desarticular o infiltrar por parte de las agencias estatales.

Ideológicamente, el FLT combina principios del **ecologismo radical**, el **anarco primitivismo** y el **anticapitalismo ecológico**. Su discurso postula que la humanidad ha perdido su vínculo natural con la Tierra debido al sistema industrial, el consumo y el poder corporativo. En consecuencia, sostienen que la destrucción de la infraestructura responsable del daño ambiental constituye un acto de defensa legítima de la naturaleza.

2.4.2 Objetivos y directrices operativas

El FLT establece tres principios básicos que guían todas sus acciones, conocidos como sus “directrices fundamentales”:

1. **Inflicir el máximo daño económico** a las corporaciones y entidades que se benefician de la destrucción ambiental.
2. **Informar y educar al público** sobre las atrocidades cometidas contra la Tierra y todas las especies que la habitan.
3. **Evitar el daño a cualquier ser humano o animal**, adoptando medidas de precaución en cada operación.

Bajo estos lineamientos, el FLT justifica la **acción directa** y el **ecotaje** (*ecotaje*), entendido como la destrucción de bienes materiales asociados a la degradación ambiental. Los blancos más comunes incluyen:

- instalaciones de la industria forestal y maderera;
- laboratorios de biotecnología y cultivos de organismos genéticamente modificados;
- concesionarios de automóviles todoterreno y maquinaria pesada;
- desarrollos urbanos considerados perjudiciales para el medio ambiente;
- y empresas de energía vinculadas a la explotación de recursos naturales.

Estas acciones tienen como propósito central el **sabotaje económico** y la **disuasión** de actividades empresariales que, según los activistas, atentan contra el equilibrio ecológico. Las operaciones suelen ejecutarse durante la noche, sin contacto con personas, utilizando métodos de destrucción como incendios intencionados, bloqueo de maquinaria, vertido de sustancias o inutilización de equipos.

2.4.3 Estructura organizacional y método de acción

A diferencia de las organizaciones terroristas tradicionales, el FLT carece de estructura jerárquica, membresía formal o liderazgo visible. Funciona como una **red descentralizada de células independientes**, conocidas como *grupos de afinidad*, que deciden sus propios objetivos y tácticas, pero actúan bajo las directrices ideológicas del movimiento.

Cada célula puede estar compuesta por uno o varios individuos, sin necesidad de autorización externa. Los ataques son **autofinanciados y autogestionados**, lo que reduce la posibilidad de rastreo financiero o infiltración policial. Una vez ejecutada la acción, el grupo envía un **comunicado anónimo** a la *Oficina de Prensa del Frente de Liberación de la Tierra* (ELF Press Office), que difunde la información a través de medios alternativos o plataformas digitales como *Bite Back*.

Este modelo organizativo, descrito por el FBI como **“liderless resistance”** o “resistencia sin líderes”, dificulta enormemente las labores de inteligencia y persecución penal. No existen listas de miembros, reuniones formales ni canales de comunicación unificados; el movimiento se reproduce por imitación ideológica y difusión mediática.

2.4.4 Clasificación y respuesta del FBI

El FBI considera al FLT uno de los principales exponentes del **Extremismo Violento Ambiental (Environmental Violent Extremism, EVE)**, categoría que engloba a los grupos o individuos que utilizan la violencia o el sabotaje con motivaciones ecológicas. Según la definición oficial del FBI (28 C.F.R. § 0.85), se considera terrorismo “el uso ilegal de la fuerza o la violencia contra personas o propiedades para intimidar o coaccionar a un gobierno o a la población civil con fines políticos o sociales”.

En este marco, las acciones del FLT cumplen con los criterios de terrorismo doméstico debido a su naturaleza coercitiva, su motivación ideológica y el impacto económico causado. A finales de la década de 1990 y principios de la de 2000, los daños materiales atribuidos al FLT en territorio estadounidense superaron los 100 millones de dólares, afectando principalmente a constructoras y empresas forestales.

El FBI y el DHS lo incorporaron oficialmente a sus **Prioridades Nacionales de Amenazas (NTP)**, equiparando su potencial destructivo al de las milicias antigubernamentales o los extremismos raciales. Su clasificación no solo obedece al impacto material, sino al **efecto psicológico y simbólico** de sus acciones, que logran generar miedo, atención mediática y presión política.

2.5 El Frente de Liberación Animal (FLA)

2.5.1 Origen y desarrollo del movimiento

El **Frente de Liberación Animal (FLA)** o *Animal Liberation Front (ALF)* se originó en el Reino Unido a comienzos de la década de 1970, dentro del movimiento por los derechos de los animales. Su aparición respondió al rechazo de los métodos institucionales del activismo tradicional, que consideraban ineficaces frente al sufrimiento animal en laboratorios, granjas industriales y la industria de la moda.

El FLA fue la evolución del grupo *Band of Mercy*, fundado por **Ronnie Lee**, que realizaba sabotajes a instalaciones de caza y criaderos. En 1976, la organización adoptó el nombre de *Animal Liberation Front* y comenzó a expandirse por Europa y América del Norte.

En Estados Unidos, su influencia creció en la década de 1980, coincidiendo con la intensificación de las campañas contra la experimentación científica y la producción de pieles. Al igual que el FLT, el FLA adoptó un modelo organizativo **clandestino, descentralizado y sin liderazgo formal**.

2.5.2 Ideología, objetivos y tácticas

El FLA se define como un movimiento que busca la **liberación total de los animales** de toda forma de explotación humana. Sus objetivos incluyen:

1. **Liberar animales** de laboratorios, granjas, criaderos o lugares donde se les someta a sufrimiento o confinamiento.
2. **Reubicarlos** en entornos naturales o refugios donde puedan vivir en libertad.
3. **Exponer al público** las atrocidades cometidas contra ellos mediante acciones directas y difusión de información.
4. **Evitar el daño** a seres humanos y animales durante las operaciones.

Sus tácticas incluyen incursiones nocturnas, sabotajes a laboratorios, incendios provocados, destrucción de vehículos o equipos de investigación, y rescate de animales cautivos. Las acciones se reivindicán anónimamente a través de comunicados enviados a las oficinas de prensa del FLA o al sitio *Bite Back*, que publica reportes de operaciones en todo el mundo.

Una de las acciones más conocidas fue la **liberación de perros Beagle** en 1990 de los laboratorios de pruebas de la compañía *Boots* en Reino Unido, operación que marcó un precedente en la visibilidad del movimiento.

2.5.3 Estructura y resistencia sin líderes

El FLA es un ejemplo paradigmático de **movimiento sin liderazgo**. Cualquier persona o grupo que cumpla con sus principios puede actuar en su nombre, sin autorización o contacto previo. Esta autonomía absoluta impide la infiltración policial y garantiza la continuidad del movimiento a pesar de las detenciones o infiltraciones.

El portavoz **Robin Webb**, director de la oficina de prensa del FLA en Reino Unido, lo expresó de manera categórica:

“Por esto es por lo que el Frente de Liberación Animal no puede ser destruido, no puede ser infiltrado, no puede ser detenido. Todos y cada uno de nosotros somos el FLA.”

Este modelo de resistencia difusa ha sido objeto de múltiples análisis académicos, que lo vinculan con las **formas contemporáneas de movilización horizontal** propias de la era digital y de los movimientos sociales post-ideológicos.

2.5.4 Percepción institucional y clasificación del FBI

A pesar de que el FLA afirma ser un movimiento no violento hacia las personas, sus tácticas son consideradas terroristas por las autoridades estadounidenses. El **FBI** lo ha incluido entre las **diez principales amenazas de terrorismo doméstico**, junto con grupos supremacistas, milicias antigubernamentales y extremistas antiaborto.

El **Southern Poverty Law Center (SPLC)** ha señalado que las acciones del FLA emplean “tácticas francamente terroristas, similares a las ocupadas por extremistas antiaborto”. Asimismo, en 2005, el **Departamento de Seguridad Nacional (DHS)** lo declaró **amenaza terrorista interna**, y desde entonces sus actividades son monitoreadas bajo el marco del **Extremismo Violento por Derechos de los Animales y Ambientalismo (AR/EV Extremism)**.

El FBI considera que el peligro del FLA no radica únicamente en los daños materiales, sino en su capacidad de inspirar imitadores. El fenómeno del “**efecto contagio**” —la difusión de la ideología a través de redes sociales y medios alternativos— ha convertido al FLA en un referente global del activismo radical por los animales.

2.6 Análisis teórico y consideraciones finales

El enfrentamiento entre el **FBI** y los **movimientos no estatales** como el FLT y el FLA expresa la tensión fundamental entre **seguridad y libertad, autoridad y disidencia, y legalidad y legitimidad moral**.

Desde la perspectiva de la **teoría realista** de las relaciones internacionales, el Estado busca preservar su supervivencia y estabilidad mediante el monopolio legítimo de la coerción. En cambio, los movimientos no estatales reivindican causas universales —como la justicia ambiental o el bienestar animal— para desafiar ese monopolio en nombre de valores éticos superiores.

Estos actores no estatales constituyen formas de **violencia simbólica y estructural**, más que militar. Su objetivo no es tomar el poder político, sino exponer las contradicciones del sistema y obligar al Estado a reaccionar. En este sentido, el terrorismo doméstico de base ecológica o animalista refleja un **conflicto ideológico postmoderno**, donde la autoridad estatal se ve interpelada por actores morales que operan en el límite entre la protesta y el crimen.

Tanto el FLT como el FLA son expresiones de un **activismo radical descentralizado**, cuyas tácticas de sabotaje y resistencia sin líderes se inscriben dentro de una lógica global de contestación al sistema industrial y capitalista. Para el Estado, representado por el FBI, estos grupos son amenazas a la estabilidad interna y al orden jurídico; para sus simpatizantes, son defensores de la vida, la naturaleza y los animales.

En suma, la coexistencia de ambos tipos de actores —estatales y no estatales— revela la complejidad del terrorismo doméstico contemporáneo: un fenómeno en el que la violencia ya no responde únicamente a objetivos políticos tradicionales, sino también a **imperativos éticos y ecológicos**, que cuestionan los límites del poder y de la ley.

El FBI, en su rol de actor institucional, busca mantener el equilibrio entre la seguridad nacional y los derechos civiles; los movimientos como el FLT y el FLA, en cambio, redefinen el

sentido de la resistencia en la era global. Ambos configuran un escenario donde la política, la moral y la seguridad se entrelazan, delineando los nuevos desafíos del Estado frente al terrorismo doméstico en el siglo XXI.

Síntesis del Capítulo II:

El presente capítulo analiza el fenómeno del terrorismo doméstico en los Estados Unidos a partir del papel desempeñado por el **Federal Bureau of Investigation (FBI)** y de la actuación de **actores no estatales** vinculados al extremismo violento ambiental y animalista, como el **Frente de Liberación de la Tierra (FLT)** y el **Frente de Liberación Animal (FLA)**. Se parte del reconocimiento de que el terrorismo doméstico constituye una amenaza interna que desafía la autoridad estatal y pone en tensión la relación entre **seguridad y libertades constitucionales**, pilares esenciales del sistema democrático estadounidense.

En primer lugar, se examina la evolución histórica e institucional del **FBI** desde sus orígenes a comienzos del siglo XX. La creación de la agencia respondió a la necesidad de dotar al Estado federal de una estructura profesional y centralizada para la investigación criminal y la protección de la seguridad nacional. Bajo la dirección de **J. Edgar Hoover**, el FBI se transformó en un organismo modelo de eficiencia técnica y disciplina administrativa, mediante reformas que incluyeron la creación del laboratorio forense, la base nacional de huellas dactilares y el programa de estadísticas delictivas (UCR). Durante la Segunda Guerra Mundial, la agencia amplió su influencia, consolidándose como actor clave en inteligencia interna y en la defensa del territorio frente a amenazas externas.

El capítulo también aborda los **métodos de investigación e inteligencia** empleados por el FBI, regulados por las *Attorney General Guidelines for Domestic Operations (AGG-Dom)*, que establecen los principios de proporcionalidad y respeto a los derechos civiles. Se detalla el proceso de apertura, gestión y cierre de investigaciones, las herramientas legales disponibles —como las *National Security Letters* y la *Ley FISA*—, así como la estructura de cooperación interinstitucional a través de las **Joint Terrorism Task Forces (JTTF)**. El FBI actúa dentro de un sistema de inteligencia coordinado con el **Department of Homeland Security (DHS)** y el **National Counterterrorism Center (NCTC)**, aplicando un modelo cíclico de análisis y priorización de amenazas. Su doctrina se basa en equilibrar la eficacia operativa con la protección de las libertades civiles garantizadas por la **Primera Enmienda**.

En la segunda parte del capítulo se examinan los **actores no estatales** asociados al terrorismo doméstico, en particular el **FLT** y el **FLA**, movimientos descentralizados y de estructura horizontal que actúan mediante sabotajes, incendios y destrucción de bienes materiales como forma de protesta ética y política. El **Frente de Liberación de la Tierra (FLT)**, originado en el Reino Unido en 1992, promueve el sabotaje económico contra empresas que considera responsables de la degradación ambiental. Su ideología combina el ecologismo radical con el anticapitalismo, y sus acciones, aunque evitan dañar personas, han generado pérdidas millonarias y han sido clasificadas por el FBI como **terrorismo doméstico** dentro del *Extremismo Violento Ambiental (EVE)*.

Por su parte, el **Frente de Liberación Animal (FLA)**, surgido en los años setenta, busca la liberación total de los animales y utiliza tácticas de rescate y sabotaje contra laboratorios y criaderos. Su modelo de “resistencia sin líderes” lo hace prácticamente imposible de desarticular, lo que llevó al FBI y al DHS a incluirlo entre las principales amenazas terroristas internas bajo la categoría de *Extremismo por Derechos de los Animales y Ambientalismo (AR/EV Extremism)*.

Finalmente, el capítulo concluye que el enfrentamiento entre el Estado y estos movimientos refleja una tensión estructural entre **autoridad y disidencia, legalidad y legitimidad moral, y seguridad y libertad**. Desde la teoría realista, el Estado busca preservar su supervivencia mediante el control del orden interno, mientras que los actores no estatales reivindican causas éticas universales que desafían el monopolio estatal de la coerción. Así, el terrorismo doméstico contemporáneo se configura como un fenómeno político, ético y comunicativo, donde las fronteras entre protesta y violencia se difuminan. El FBI y los movimientos radicales representan los polos opuestos de un mismo dilema: la defensa de la seguridad nacional frente a la defensa moral de la naturaleza y la vida.

Referencias

Department of Homeland Security. (2019). *Homeland Security Intelligence Threat Banding Framework*. Washington, D.C.: U.S. Government Printing Office.

Federal Bureau of Investigation. (2020). *Domestic Terrorism Operations Guide*. Washington, D.C.: U.S. Department of Justice.

Federal Bureau of Investigation. (2021). *Attorney General Guidelines for Domestic FBI Operations (AGG-Dom)*. Washington, D.C.: U.S. Department of Justice.

Federal Bureau of Investigation. (2022). *Joint Terrorism Task Forces Annual Report*. Washington, D.C.: U.S. Government Printing Office.

Hoffman, B. (2006). *Inside Terrorism*. New York, NY: Columbia University Press.

Manassero, M., & Tello, P. (2014). *Terrorismo y violencia política: aproximaciones teóricas*. Buenos Aires: Universidad del Salvador.

Southern Poverty Law Center. (2010). *Domestic Extremist Movements in the United States*. Montgomery, AL: SPLC Reports.

United States Code, Title 18 § 2331(5). (2011). *Definitions of domestic terrorism*. Washington, D.C.: U.S. Congress.

United States Code, Title 28 § 0.85. (2012). *Federal Bureau of Investigation; authority and functions*. Washington, D.C.: U.S. Congress.

Webb, R. (2015). *Voices of the Animal Liberation Front*. London: ALF Press.

CAPÍTULO III

Presupuesto 2.002

CAPÍTULO III – Presupuesto 2002

“Como nota preliminar se indica que todos los datos de este capítulo fueron extraídos del Informe de contrterrorismo del F.B.I: https://www.fbi.gov/file-repository/counterterrorism/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view”.

3.1 Introducción al contexto presupuestario y político (2001–2002)

Los atentados del 11 de septiembre de 2001 marcaron un punto de inflexión en la política de seguridad de los Estados Unidos, generando una redefinición estructural de las prioridades estratégicas nacionales. En el plano institucional, esta nueva orientación se tradujo en un proceso acelerado de expansión del gasto público destinado a la defensa, la seguridad interior y la inteligencia. El *Federal Bureau of Investigation* (FBI), organismo dependiente del *Department of Justice*, reconfiguró su estructura operativa con el objetivo de fortalecer su capacidad preventiva y de respuesta frente al terrorismo, la contrainteligencia y las amenazas emergentes vinculadas a la ciberdelincuencia.

El presupuesto del año fiscal 2002, diseñado en coordinación con la *Office of Management and Budget* (OMB), materializó este giro estratégico mediante un incremento sustancial en la financiación de los programas de seguridad nacional, inteligencia y tecnología aplicada a la investigación criminal. Esta asignación presupuestaria fue, en efecto, una herramienta de política pública para garantizar la resiliencia institucional frente a las nuevas amenazas transnacionales (FBI, 2002; OMB, 2002).

3.2 Presupuesto de defensa general de los Estados Unidos (2002)

En el año 2002, el gasto público dedicado a la defensa en los Estados Unidos experimentó un incremento del 13,99 %, alcanzando los 376.793,6 millones de dólares, equivalentes al 10,28 % del gasto público total. Este aumento representó un 3,45 % del Producto Interno Bruto (PIB), superando los niveles de 2001, cuando se había registrado un 3,12 %. El gasto per cápita en

defensa fue de 1.308 dólares por habitante, frente a los 1.159 del año anterior (OMB, 2002; Datosmacro, 2002).

La expansión presupuestaria reflejó la prioridad otorgada al fortalecimiento militar, la inteligencia y la seguridad interior, en el marco de una doctrina de defensa preventiva que buscaba anticipar y neutralizar amenazas antes de su materialización. La nueva configuración de la seguridad estadounidense se caracterizó, así, por la interconexión entre la política exterior y la seguridad doméstica, ampliando la influencia del complejo de seguridad nacional.

3.3 Solicitud presupuestaria del FBI (2002)

El FBI solicitó para el año fiscal 2002 un total de **3.507.109.000 dólares**, de los cuales **3.505.859.000** correspondieron a salarios y gastos y **1.250.000** a construcción. La variación interanual fue de **277.377.000 dólares**, compuesta por **106.569.000** en ajustes operativos y **170.808.000** en incrementos de programas de seguridad (FBI, 2002).

Esta solicitud presupuestaria representó una realineación institucional en torno a la inteligencia, la ciberseguridad y la capacidad de respuesta rápida frente al terrorismo, en coherencia con las directrices estratégicas de la Casa Blanca.

3.3.1 Ajustes al funcionamiento

Los ajustes operativos contemplaron un incremento destinado a cubrir un aumento salarial del 3,6 % para los agentes, el incremento de los costos del seguro de salud federal, los nuevos alquileres de la *General Services Administration* y la anualización de aumentos previos.

Las fuentes de financiamiento incluyeron recursos propios y programas Inter agenciales, como el *Interagency Crime and Drug Enforcement*, la *Health Insurance Portability and Accountability Act* (HIPAA) de 1996 y el *Criminal Justice Services Program*, que apoyaba operaciones contra el fraude, el narcotráfico y la corrupción (FBI, 2002).

3.3.2 Incrementos en programas de seguridad

El aumento de **170.808.000 dólares** se orientó a cuatro ejes estratégicos: (1) contraespionaje; (2) contraterrorismo; (3) ciberdelincuencia; y (4) contracifrado. Estos sectores fueron identificados como prioritarios dentro del rediseño institucional del FBI tras el 11-S.

3.3.2.1 Contraespionaje

El programa de contraespionaje tuvo por objetivo prevenir y derrotar operaciones de inteligencia extranjeras en territorio estadounidense. Se reforzaron las capacidades de investigación de campo, la coordinación nacional y la seguridad del personal y contratistas. También se invirtió en tecnología de detección y en la protección de infraestructuras críticas y bases de datos sensibles (FBI, 2002).

3.3.2.2 Contraterrorismo

La política antiterrorista fue central en el nuevo modelo de seguridad. Se priorizó la capacidad de respuesta ante actos terroristas tanto domésticos como internacionales, el fortalecimiento de la inteligencia preventiva, la cooperación con agencias extranjeras y la coordinación interinstitucional. El FBI adoptó un enfoque integrado con el *Department of Homeland Security* (DHS), el *National Counterterrorism Center* (NCTC) y otras agencias de seguridad (FBI, 2002).

3.3.2.3 Ciberdelincuencia

El crecimiento de las redes digitales y las amenazas informáticas impulsó el desarrollo de capacidades forenses y de interceptación electrónica. La autoridad legal de estas acciones se sustentó en la *Omnibus Crime Control and Safe Streets Act* de 1968 y en la *Foreign Intelligence Surveillance Act* (FISA). Se establecieron nuevas unidades especializadas en análisis de redes, rastreo de fraudes electrónicos y protección de infraestructuras críticas (FBI, 2002).

3.3.2.4 Contracifrado

El componente de contracifrado incluyó la adquisición de hardware, software, servicios técnicos y capacitación en ingeniería analítica y análisis de señales, fortaleciendo la capacidad del FBI para acceder a comunicaciones encriptadas utilizadas por organizaciones criminales y terroristas (FBI, 2002).

3.3.3 Servicios y equipamiento técnico

Se destinaron **6,5 millones de dólares** a la actualización de equipos de telecomunicaciones que conectaban las oficinas del FBI en el extranjero con la red del *Department of State*. Asimismo, se solicitaron **4.007.000 dólares** para renovar la flota vehicular, adquirir herramientas de diagnóstico y modernizar el sistema de administración de vehículos (FBI, 2002).

3.3.4 Activación del Laboratorio del FBI (Quantico, VA)

Durante 2002 se programó la ocupación del nuevo Laboratorio del FBI en Quantico, Virginia. El proyecto incluyó la incorporación de 22 empleados adicionales y un aumento presupuestario de **1.161.000 dólares** para operación y mantenimiento. Se asignaron además **40 millones de dólares** del *Working Capital Fund* para cubrir gastos de traslado, equipamiento especializado, mobiliario, TI y mitigación ambiental. La modernización del laboratorio consolidó la capacidad científica del FBI en materia de análisis forense y criminalística (FBI, 2002).

3.3.5 Equipos antibombas y ADN

El FBI destinó **10 millones de dólares** para continuar el programa de equipamiento y capacitación de escuadrones antibombas estatales y locales, dotándolos de trajes protectores, detectores de radiación, sistemas de rayos X y dispositivos de monitoreo químico. Además, bajo el programa *Community Oriented Policing Services (COPS)*, se solicitaron **35 millones de dólares** para reducir retrasos en análisis de ADN y fortalecer las capacidades forenses en el nivel local (FBI, 2002).

3.3.6 Delitos de cuello blanco e Internet Fraud Complaint Center (IFCC)

El FBI, junto al *National White Collar Crime Center (NW3C)*, reforzó el *Internet Fraud Complaint Center (IFCC)*, creado en 2000, como punto de recepción de denuncias de fraude en línea. El centro se consolidó como herramienta clave para el análisis de delitos financieros y cibernéticos, articulando esfuerzos entre agencias federales, estatales y locales (FBI, 2002).

3.4 Propuestas legislativas y reformas institucionales

La solicitud presupuestaria incluyó cuatro propuestas de ley principales (FBI, 2002):

- **Sección 108 – Pago por peligrosidad:** extendió al personal del FBI la autoridad de percibir compensaciones por riesgo en destinos de alto peligro, igualando su régimen con el de la *Drug Enforcement Administration*.
- **Sección 109 – Acuerdos de cooperación extranjeros:** autorizó al FBI a recibir fondos de gobiernos aliados para operaciones conjuntas.
- **Sección 110 – Entrenamiento de la policía ferroviaria:** habilitó a cobrar tarifas por cursos de capacitación especializados.

- **Sección 111 – Reembolso por trabajos de garantía interna:** permitió recuperar costos por reparaciones realizadas internamente en equipos bajo garantía.

Estas reformas legales fortalecieron la autonomía operativa y financiera del FBI, adaptándolo al nuevo contexto de seguridad global posterior al 11-S.

3.5 Seguridad interna del FBI y reformas post Hanssen

Tras el arresto del agente Robert Philip Hanssen por espionaje, el director Louis J. Freeh impulsó una revisión integral de los procedimientos de seguridad interna. Se implementaron auditorías electrónicas periódicas para monitorear el acceso a los archivos del sistema *Automated Case Support (ACS)*, generando reportes detallados (*Document Access Reports*) sobre las acciones de cada usuario.

Asimismo, se amplió el programa de polígrafo para todo el personal con acceso a información sensible y se establecieron exámenes regulares a los empleados que regresaban de asignaciones internacionales. La *Security Countermeasures Section* fue reestructurada temporalmente bajo la supervisión de un ejecutivo externo, garantizando mayor independencia en el control interno (FBI, 2002).

Estas medidas de control reforzaron la integridad institucional y la prevención de vulneraciones internas, en línea con los estándares de seguridad nacional posteriores al 11-S.

3.6 Evaluación general del presupuesto y su impacto en la política de seguridad estadounidense

El presupuesto de 2002 marcó el inicio de un proceso de securitización integral del aparato estatal estadounidense. El FBI asumió un papel central en la lucha contra el terrorismo y la inteligencia interna, con un notable fortalecimiento en infraestructura, tecnología y capacidad científica.

La expansión del gasto reflejó una transición desde la lógica reactiva hacia una lógica preventiva, donde la inteligencia, la cooperación Inter agencial y la tecnología se convirtieron en pilares de la política de seguridad. La política presupuestaria, en consecuencia, se consolidó como instrumento de la nueva estrategia de defensa nacional.

En términos estructurales, el presupuesto de 2002 configuró un nuevo paradigma: el de la “seguridad extendida”, que abarca tanto el territorio nacional como los intereses estadounidenses en el exterior. Este modelo integró la acción del FBI con el *Department of Homeland Security* y las agencias de inteligencia, estableciendo las bases del complejo de seguridad contemporáneo.

Resumen del Capítulo III – Presupuesto 2002

El capítulo examina el impacto presupuestario y estructural de los atentados del 11 de septiembre de 2001 en la política de seguridad de los Estados Unidos, destacando el **año fiscal 2002** como punto de inflexión. Durante este período, el gobierno federal implementó un **incremento del gasto en defensa del 13,99 %**, alcanzando los **376.793,6 millones de dólares**, equivalentes al **10,28 % del gasto público total** y al **3,45 % del Producto Interno Bruto (PIB)**. En términos per cápita, el gasto en defensa se elevó a **1.308 dólares por habitante**, frente a los **1.159 dólares** del año anterior.

Dentro de este marco, el **Federal Bureau of Investigation (FBI)** presentó una **solicitud presupuestaria total de 3.507.109.000 dólares**, de los cuales **3.505.859.000** correspondieron a salarios y gastos y **1.250.000** a obras de construcción. La variación interanual fue de **277.377.000 dólares**, compuesta por **106.569.000** en ajustes operativos y **170.808.000** en incrementos de programas de seguridad.

Los **ajustes operativos** incluyeron un **aumento salarial del 3,6 %** para los agentes, junto con mayores costos en seguros de salud y alquileres federales. Los **incrementos en programas de seguridad** se distribuyeron en cuatro áreas prioritarias:

1. **Contraespionaje**, para prevenir operaciones de inteligencia extranjera.
2. **Contraterrorismo**, con énfasis en cooperación Inter agencial y respuesta inmediata.
3. **Ciberdelincuencia**, fortalecida por la aplicación de la *Omnibus Crime Control and Safe Streets Act* y la *Foreign Intelligence Surveillance Act (FISA)*.
4. **Contracifrado**, con inversiones en hardware, software y capacitación analítica.

El FBI destinó además **6,5 millones de dólares** a actualizar su red de telecomunicaciones y **4.007.000** a la modernización vehicular. La activación del nuevo **Laboratorio del FBI en Quantico (VA)** implicó **1.161.000 dólares adicionales** y una inversión complementaria de **40 millones** del *Working Capital Fund* para traslado, equipamiento y mitigación ambiental. En

materia operativa, se asignaron **10 millones de dólares** para escuadrones antibombas y **35 millones** bajo el programa *COPS* para mejorar los análisis de ADN.

En la lucha contra el fraude electrónico, el **Internet Fraud Complaint Center (IFCC)** fue consolidado junto al *National White Collar Crime Center (NW3C)* como eje de coordinación Inter agencial. En el plano legislativo, se aprobaron **cuatro propuestas de ley** (Secciones 108 a 111) que ampliaron las facultades financieras y de cooperación internacional del FBI.

Finalmente, tras el caso de espionaje del agente **Robert Hanssen**, se fortaleció la seguridad interna mediante auditorías electrónicas, controles poligráficos y supervisión externa.

En conjunto, el presupuesto de 2002 configuró una **política de “seguridad extendida”**, donde el FBI y el Department of Homeland Security se integraron en un complejo de defensa nacional orientado a la **prevención de amenazas** y al **uso estratégico de la inteligencia**. Este rediseño institucional y presupuestario representó la transición de una política reactiva hacia una **estrategia preventiva y global de seguridad nacional**.

Referencias

Departamento de Justicia de los Estados Unidos (FBI). (2002). *Federal Bureau of Investigation Budget Request, Fiscal Year 2002*. Washington, D.C.: Government Printing Office.

Datosmacro. (2002). *Gasto militar de Estados Unidos 2002*. Recuperado de <https://datosmacro.expansion.com>

Oficina de Administración y Presupuesto (OMB). (2002). *Budget of the United States Government, Fiscal Year 2002*. Washington, D.C.: The White House.

CAPÍTULO IV

Presupuesto 2.003

CAPÍTULO IV – Presupuesto 2003

“Como nota preliminar se indica que todos los datos de este capítulo fueron extraídos del Informe de contraterorismo del F.B.I: https://www.fbi.gov/file-repository/counterterrorism/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view”.

4.1 Introducción al contexto de seguridad y defensa (2003)

El año 2003 se enmarca en una fase de consolidación de la política de seguridad y defensa estadounidense, resultado directo del proceso de reestructuración iniciado tras los atentados del 11 de septiembre de 2001. Durante este período, el gobierno de los Estados Unidos profundizó la reorganización institucional y presupuestaria de sus agencias de inteligencia, defensa y seguridad interna, en consonancia con la doctrina de seguridad nacional de la administración Bush. El contexto político y estratégico estuvo dominado por la denominada *guerra global contra el terrorismo*, la invasión a Irak y la expansión del gasto en defensa, inteligencia y seguridad interior, con un enfoque orientado a la prevención, la disuasión y la capacidad de respuesta ante amenazas no convencionales.

En este escenario, el *Federal Bureau of Investigation (FBI)* —dependiente del *Department of Justice (DOJ)*— desempeñó un papel crucial dentro del sistema de seguridad nacional. El presupuesto correspondiente al año fiscal 2003 reflejó un incremento sustancial en sus asignaciones, orientadas al fortalecimiento de la infraestructura tecnológica, el personal especializado, la inteligencia analítica y las operaciones conjuntas contra el terrorismo y el espionaje. Estas prioridades se complementaron con una marcada expansión del gasto general en defensa, que alcanzó niveles sin precedentes desde la Guerra Fría.

La estructura presupuestaria de 2003, por tanto, consolidó el giro estratégico iniciado en 2002: del gasto militar clásico hacia un modelo integral de seguridad nacional que abarcó la defensa externa, la seguridad interior, la infraestructura crítica, la tecnología de la información, la ciberseguridad y la coordinación Inter agencial.

4.2 Presupuesto general de defensa (2003)

Durante el año 2003, el gasto público total en defensa en los Estados Unidos se elevó a **US\$ 438.458.700.000**, lo que representó un incremento significativo respecto al año anterior. Si bien en términos porcentuales se registró una **disminución del 16,37 %** en comparación con la expansión extraordinaria de 2002, el monto absoluto fue el más alto de la década, representando el **11,3 % del gasto público total**.

En relación con el Producto Interno Bruto (PIB), el gasto en defensa alcanzó el **3,83 %**, cifra que implicó un aumento de **0,38 puntos porcentuales** respecto del año 2002 (3,45 % del PIB). A su vez, el gasto per cápita en defensa ascendió a **US\$ 1.508 por habitante**, evidenciando la intensificación del esfuerzo presupuestario en términos individuales (Datosmacro, 2003).

El presupuesto de 2003 reflejó la prioridad estratégica otorgada a la guerra contra el terrorismo, la protección de la infraestructura nacional, la modernización tecnológica del aparato militar y de inteligencia, y la expansión de programas de cooperación Inter agencial e internacional. La orientación doctrinal y financiera se mantuvo alineada con las directrices establecidas por la *Office of Management and Budget (OMB)* y el *Department of Defense (DoD)*, que impulsaron la integración de políticas de defensa y seguridad interior bajo un enfoque preventivo y de alcance global.

4.3 Solicitud presupuestaria del FBI (2003)

Para el año fiscal 2003, el *Federal Bureau of Investigation (FBI)* solicitó un presupuesto total de **US\$ 4.203.837.000**, de los cuales **US\$ 4.202.587.000** correspondieron a salarios y gastos operativos, y **US\$ 1.250.000** a proyectos de construcción. Esta cifra representó un **aumento neto de US\$ 696.728.000** con respecto al presupuesto del año anterior.

El presupuesto total excluyó **US\$ 120.075.000** correspondientes a costos de jubilación federal. El incremento incluyó ajustes salariales del **2,6 %**, aumentos en seguros de salud, alquileres y medidas de seguridad adicionales. Además, contempló **US\$ 237.900.000** para continuar con las actividades financiadas en el Suplemento contra el Terrorismo del año 2002, y un total de **US\$ 446.281.000** para programas de apoyo directo a la guerra contra el terrorismo (FBI, 2003).

La estructura presupuestaria se articuló en torno a los siguientes ejes prioritarios:

1. **Prevención del terrorismo y contrainteligencia.**
 2. **Protección de infraestructura nacional.**
 3. **Modernización tecnológica y ciberseguridad.**
 4. **Capacitación técnica y logística de respuesta.**
 5. **Reformas de seguridad institucional y control interno.**
-

4.3.1 Iniciativa contra el terrorismo

La máxima prioridad del FBI para el año 2003 fue la prevención de actos terroristas tanto en territorio estadounidense como contra ciudadanos o intereses de los Estados Unidos en el extranjero. El enfoque integral comprendió el fortalecimiento de la capacidad de investigación, la expansión de personal operativo y técnico, la cooperación interinstitucional y el desarrollo de recursos tecnológicos especializados.

El presupuesto asignó **US\$ 225.002.000** para la contratación de **181 nuevos agentes**, junto con el desarrollo de programas de vigilancia, capacitación, capacidades de respuesta rápida y operaciones cibernéticas. El objetivo era dotar a la Oficina de medios suficientes para identificar, prevenir y neutralizar actividades terroristas en cualquier fase de planificación o ejecución.

El incremento presupuestario también se destinó a consolidar las *Joint Terrorism Task Forces (JTTF)* y a integrar los sistemas de inteligencia criminal y antiterrorista dentro del *National Security Branch*, mejorando la coordinación entre el FBI, la CIA, el Departamento de Seguridad Nacional (DHS) y agencias policiales locales y estatales.

4.3.2 Programa de Protección de Infraestructura Nacional

Las infraestructuras electrónicas y físicas de los Estados Unidos constituyen la base del comercio, las comunicaciones, el transporte, la generación de energía y la seguridad nacional. En el contexto de 2003, estas infraestructuras fueron reconocidas como objetivos de alto valor estratégico para potenciales ataques terroristas.

El *National Infrastructure Protection Center (NIPC)*, creado en 1998 como iniciativa Inter agencial, fue consolidado presupuestariamente con **US\$ 21.025.000** y la incorporación de **81 nuevos agentes**. El programa buscó fortalecer la capacidad de respuesta frente a intrusiones informáticas, sabotajes y amenazas tecnológicas.

Se destinaron **US\$ 6.000.000** adicionales para equipamiento técnico, herramientas de monitoreo digital y apoyo a las 28 oficinas de campo que carecían de brigadas NIPC al cierre del año fiscal 2002. La prioridad fue mejorar las capacidades locales de investigación y respuesta ante delitos informáticos, incluyendo la detección temprana de amenazas y la coordinación con los sectores público y privado.

4.3.3 Apoyo a la vigilancia y operaciones tácticas

El fortalecimiento de las capacidades de vigilancia y respuesta táctica fue otro eje central del presupuesto del FBI en 2003. Se asignaron **US\$ 44.893.000** para mejorar las actividades de vigilancia orientadas a identificar y derrotar operaciones de inteligencia extranjeras dentro de los Estados Unidos o contra intereses estadounidenses en el exterior.

Estas inversiones permitieron financiar equipos de monitoreo, unidades de campo y operaciones de contrainteligencia con alto componente tecnológico, además de cubrir los costos de apoyo operativo asociados con el incremento en la vigilancia nacional e internacional.

Por su parte, las **operaciones tácticas** recibieron **US\$ 12.162.000** adicionales destinados a reforzar la capacidad de respuesta a solicitudes de búsqueda física y a adaptarse a los cambios tecnológicos mediante actividades de investigación, desarrollo e ingeniería. Este programa se vinculó directamente con la modernización de las capacidades del FBI para intervenir en operaciones de campo complejas y en contextos de amenaza biológica o química.

4.3.4 Programas técnicos y de respuesta a crisis

El **Programa de Agentes Técnicamente Capacitados (TTA)** fue uno de los pilares de la estrategia de modernización. Ante el uso generalizado de tecnologías de comunicación digital y criptografía por parte de organizaciones terroristas, el FBI destinó **US\$ 10.027.000** para incorporar nuevo personal técnico y equipos especializados, junto con la creación de programas de formación permanente.

El objetivo era garantizar que los equipos de vigilancia electrónica pudieran adaptarse rápidamente a tecnologías emergentes y realizar interceptaciones legales con eficiencia.

Asimismo, el **Programa de Respuesta a Crisis** recibió **US\$ 28.313.000** y **25 nuevos agentes** para ampliar las capacidades de reacción ante incidentes con materiales peligrosos o armas de destrucción masiva. Esta partida contempló:

1. La ampliación del número de equipos de respuesta a materiales peligrosos de 17 a 32.
2. El fortalecimiento de las capacidades de procesamiento de escenas del crimen, recolección de evidencia y capacitación.
3. La mejora de los sistemas de comunicación de crisis, permitiendo la coordinación simultánea en múltiples escenarios.

4. El establecimiento de una estructura logística para despliegues rápidos a nivel nacional o internacional.

Estas acciones consolidaron al FBI como la agencia de referencia en respuesta técnica y de emergencia ante amenazas biológicas, químicas o radiológicas dentro del territorio estadounidense.

4.3.5 Programas forenses, genéticos y de ADN

El fortalecimiento de las capacidades científicas y de investigación del FBI fue una prioridad transversal en el presupuesto de 2003. Dentro del marco de la *DNA Analysis Backlog Elimination Act of 2000* y de la *USA PATRIOT Act* de 2001, se amplió la cobertura del **Programa Federal de Delincuentes Condenados**, que autoriza la recolección y análisis de muestras de ADN de personas condenadas por delitos calificados, incluyendo aquellos vinculados con el terrorismo y delitos violentos.

El FBI destinó **US\$ 867.000** y la incorporación de **5 nuevos agentes** para administrar la base de datos, adquirir insumos y equipos, y financiar gastos operativos del programa. Asimismo, bajo el programa *Community Oriented Policing Services (COPS)*, se asignaron **US\$ 35.000.000** para reducir la acumulación de perfiles de ADN en el *Combined DNA Index System (CODIS)* y acelerar el procesamiento de evidencia de escena del crimen. Este componente fortaleció la cooperación entre el FBI y los laboratorios forenses estatales y locales, impulsando la estandarización de procedimientos y la interoperabilidad tecnológica entre bases de datos forenses a nivel nacional.

4.3.6 Programas de aviación e inteligencia

El **Programa de Aviación del FBI** desempeñó un papel clave en las tareas de vigilancia, transporte y logística de emergencia. En 2003, el 88 % de sus operaciones se destinó a misiones de observación aérea. Tras los atentados del 11 de septiembre, las solicitudes de vuelos de

vigilancia aumentaron un **60 %**, lo que justificó un incremento presupuestario de **US\$ 46.082.000** para la adquisición de dos helicópteros, un avión de vigilancia, equipamiento técnico y personal adicional (pilotos, mecánicos y operadores de sensores).

A nivel analítico, se destinó **US\$ 7.731.000** para ampliar la **producción de inteligencia**, creando **110 nuevos puestos analíticos** para procesar el creciente volumen de información proveniente de investigaciones de terrorismo, cibercrimen y espionaje. El objetivo fue reducir el desfase entre la obtención de información y su interpretación operativa, mejorando la capacidad del FBI para transformar datos en inteligencia procesable (*actionable intelligence*).

Asimismo, el **Sistema de Gestión de Datos de Vigilancia Electrónica (EDMS)** recibió **US\$ 11.328.000** para permitir el intercambio automatizado de datos recolectados mediante vigilancia electrónica (ELSUR). Este sistema estableció dos plataformas diferenciadas: una para la seguridad nacional y otra para investigaciones criminales, facilitando la colaboración entre agentes, analistas y traductores con distintos niveles de autorización.

La **instalación de recopilación de datos clasificados** también fue reforzada mediante **US\$ 5.648.000** destinados a infraestructura, contratistas y equipos especializados para operaciones sensibles, ampliando la capacidad de recopilación y procesamiento de información de inteligencia en tiempo real.

4.3.7 Programas de coordinación operativa y comunicación estratégica

El fortalecimiento de las líneas de comunicación e inteligencia pública formó parte de la estrategia de colaboración Inter agencial. La **línea directa de consejos (*Tips Hotline*)** recibió **US\$ 1.507.000** y **10 nuevos agentes** para recopilar información sobre actividades terroristas sospechosas provenientes del público. Estos datos eran procesados en coordinación con las *Joint Terrorism Task Forces (JTTF)*, permitiendo una conexión inmediata entre la denuncia civil y la investigación federal.

El **Centro Estratégico de Información y Operaciones (SIOC)** —ubicado en la sede del FBI— consolidó su rol como núcleo de operaciones y comunicaciones, funcionando las 24 horas, los 365 días del año. Se destinaron **US\$ 1.503.000** para mantenimiento técnico, actualización de equipos y capacitación de personal.

Su contraparte, el **Centro de Operaciones de Nueva York (NYOC)**, fue ampliado y actualizado con **US\$ 4.903.000** para mejorar su infraestructura tecnológica y su interoperabilidad con las agencias locales durante emergencias o investigaciones de alto perfil.

El **Programa de Técnicos Electrónicos de Campo (ET)**, responsable del sistema nacional de radio del FBI, recibió **US\$ 10.064.000** y **62 nuevos agentes**, destinados a mantener comunicaciones seguras entre más de 10.000 agentes y 2.000 usuarios externos de otras agencias. Estos sistemas, vitales durante crisis que pueden colapsar redes comerciales, garantizan la continuidad operativa y la coordinación interinstitucional.

Las **Fuerzas de Tareas Conjuntas contra el Terrorismo (JTTF)** recibieron **US\$ 15.677.000** para expandirse a las **56 oficinas de campo del FBI**, incorporando personal estatal, local y tribal en equipos permanentes de investigación y análisis. El modelo de cooperación Inter agencial consolidado por las JTTF se convirtió en un elemento estructural del aparato antiterrorista estadounidense, promoviendo la integración de capacidades y recursos a nivel nacional.

4.3.8 Escuela de Dispositivos Peligrosos y capacitación especializada

La **Hazardous Devices School (HDS)**, ubicada en Redstone Arsenal, Alabama, fue reforzada con **US\$ 3.272.000** para ampliar su capacidad de formación, incrementar cursos para técnicos de bombas y mantener las aldeas de entrenamiento práctico. La HDS es la única institución formal en los Estados Unidos para la capacitación de personal policial estatal y local

en detección, neutralización y eliminación de dispositivos explosivos o materiales de destrucción masiva.

Este refuerzo presupuestario, proveniente de una transferencia del Departamento de Defensa (DoD), reflejó la creciente preocupación por los atentados con explosivos improvisados y la necesidad de preparar unidades tácticas y científicas en respuesta a amenazas NBQ (nucleares, biológicas y químicas).

4.3.9 Iniciativa de tecnología de la información y programa Trilogy

La modernización tecnológica del FBI constituyó uno de los pilares de su estrategia post-11S. El **Programa Trilogy**, diseñado para renovar la infraestructura informática de la Oficina, integró redes, sistemas de gestión de casos y herramientas analíticas bajo una arquitectura unificada.

Para el año 2003 se solicitaron **US\$ 145.971.000** y **6 nuevos agentes** para acelerar la implementación del sistema, así como **US\$ 8.000.000** para mantener a **44 contratistas especializados**. La meta era consolidar la interoperabilidad de cinco aplicaciones clave de investigación, reducir duplicidades de bases de datos y facilitar el acceso rápido a la información por parte de analistas e investigadores.

El proyecto incluyó además **US\$ 50.300.000** para consolidar los datos de investigación en una única base de conocimiento virtual; **US\$ 11.000.000** para desarrollar *Trusted Guards* — hardware y software que permiten compartir información entre agencias de forma segura—; y **US\$ 10.000.000** para garantizar la continuidad de operaciones de la sede ante desastres o ataques.

Asimismo, se destinaron **US\$ 10.000.000** adicionales para digitalizar y archivar documentos relativos a grupos terroristas, y **US\$ 21.000.000** para mejorar la infraestructura tecnológica de las oficinas del FBI en el extranjero, optimizando la transmisión de datos y la cooperación internacional.

Otros proyectos complementarios incluyeron **US\$ 3.080.000** para videoconferencias seguras, **US\$ 3.620.000** para expansión de Internet de alta velocidad, **US\$ 16.527.000** para modernización de sistemas laborales y administrativos, y **US\$ 5.000.000** para la adquisición de nuevas herramientas analíticas y de visualización de datos.

Finalmente, **US\$ 7.444.000** fueron destinados al mantenimiento y operación de centros de datos y *mainframes*, consolidando una infraestructura de TI capaz de sostener la magnitud de las operaciones antiterroristas del FBI.

4.3.10 Iniciativas de seguridad institucional post Hanssen

El arresto del exagente Robert Hanssen por espionaje generó una crisis de confianza interna y motivó una revisión completa de los mecanismos de seguridad y control institucional del FBI. Como respuesta, se estableció una **nueva División de Seguridad** con una asignación de **US\$ 78.065.000** y **21.338.000** adicionales para programas de personal, capacitación y contrataciones de expertos en certificación y acreditación de sistemas.

El objetivo fue desarrollar una cultura organizacional basada en la seguridad integral, abarcando desde la gestión de información clasificada hasta la vigilancia interna y la educación del personal. Se crearon equipos especializados de oficiales de seguridad tanto en la sede central como en las oficinas de campo, responsables de implementar políticas de protección de datos y de realizar revisiones periódicas de cumplimiento.

Dentro de esta estructura, se destinó **US\$ 48.173.000** a programas de aseguramiento de la información, orientados al monitoreo activo de sistemas, evaluaciones de vulnerabilidades, respuesta ante incidentes y fortalecimiento de controles de acceso. El componente de **contramedidas** buscó anticipar las capacidades de adversarios potenciales, adaptando los procedimientos del FBI a escenarios de espionaje y guerra de información.

En materia de **poligrafía**, se asignaron **US\$ 6.804.000** y **15 agentes** adicionales para ampliar la cobertura de exámenes de seguridad y establecer evaluaciones periódicas obligatorias para todo el personal con acceso a información sensible.

Finalmente, **US\$ 714.000** se destinaron a reforzar la seguridad física de la Academia del FBI en Quantico, Virginia, y de las oficinas de campo reubicadas, garantizando el cumplimiento de los nuevos estándares de protección física y cibernética.

4.4 Evaluación general y orientación estratégica

El presupuesto de defensa y seguridad de los Estados Unidos correspondiente al año 2003 consolidó la transición de un modelo reactivo a uno preventivo e integral de seguridad nacional. En el caso del FBI, los incrementos financieros reflejaron una estrategia de fortalecimiento institucional sin precedentes, orientada simultáneamente a la lucha contra el terrorismo, la modernización tecnológica y la seguridad interna.

La orientación del gasto reafirmó al FBI como eje articulador entre la inteligencia, la investigación criminal y la protección del territorio nacional. Los programas de infraestructura digital (*Trilogy*), seguridad informática, aviación, análisis de inteligencia y control de crisis mostraron la voluntad del Estado de construir una agencia moderna, interoperable y tecnológicamente autosuficiente.

Las reformas internas derivadas del caso Hanssen introdujeron una nueva ética de seguridad y transparencia dentro del FBI, marcando el inicio de una cultura organizacional más orientada a la prevención de vulnerabilidades y a la protección de información estratégica.

En términos globales, el presupuesto de 2003 consolidó la doctrina de la *guerra contra el terrorismo* como principio rector de la política de seguridad de los Estados Unidos, combinando la expansión del gasto militar con la profesionalización y tecnificación del aparato de seguridad interna.

Resumen del Capítulo IV – Presupuesto 2003

El año fiscal **2003** representó una **expansión presupuestaria sostenida**, orientada a:

- **Transformar al FBI** en una agencia con capacidad preventiva, tecnológica y global.
- **Consolidar la inteligencia y la seguridad interna** como ejes del gasto federal.
- **Reforzar el gasto militar y civil** en torno a la doctrina de la *guerra contra el terrorismo*.

En conjunto, los aumentos de 2003 marcaron el paso de un enfoque reactivo a una **estructura de seguridad integrada**, con el FBI en el centro operativo y tecnológico del sistema nacional de defensa.

Referencias

- Federal Bureau of Investigation (FBI). (2003). *Congressional Budget Submission: Fiscal Year 2003*. Department of Justice, United States Government.
- Department of Justice (DOJ). (2003). *Annual Performance Report, FY 2003*. Washington, D.C.
- Office of Management and Budget (OMB). (2003). *Budget of the United States Government, Fiscal Year 2003*. Executive Office of the President.
- Datosmacro. (2003). *Gasto público en defensa de Estados Unidos (2003)*. Recuperado de <https://datosmacro.expansion.com/>
- U.S. Congress. (2001). *USA PATRIOT Act of 2001, Public Law 107–56*.
- DNA Analysis Backlog Elimination Act of 2000, Public Law 106–546.

CAPÍTULO V

Presupuesto 2.004

CAPÍTULO V – Presupuesto 2004

“Como nota preliminar se indica que todos los datos de este capítulo fueron extraídos del Informe de contrterrorismo del F.B.I: https://www.fbi.gov/file-repository/counterterrorism/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view”.

5.1 Introducción: contexto político y de seguridad (2004)

El año 2004 marcó una etapa de consolidación en la política de defensa y seguridad nacional de los Estados Unidos. Tras los atentados del 11 de septiembre de 2001 y las reformas introducidas durante 2002 y 2003, el país continuó profundizando una agenda centrada en la lucha contra el terrorismo global, la modernización tecnológica de las agencias de seguridad y la expansión de las capacidades de inteligencia.

En este contexto, el **Federal Bureau of Investigation (FBI)** reafirmó su papel como organismo clave dentro del sistema de seguridad nacional. Su presupuesto para el ejercicio fiscal 2004 reflejó una estrategia orientada al fortalecimiento de sus programas de contrterrorismo, contrainteligencia, cibercriminalidad y seguridad institucional. La expansión de los recursos humanos y tecnológicos, la modernización del sistema de comunicaciones y la consolidación del programa *Trilogy* fueron componentes esenciales de este proceso.

El Departamento de Defensa, por su parte, mantuvo un aumento sostenido del gasto en defensa, acompañado por la expansión de operaciones militares en Irak y Afganistán. Este contexto impulsó un incremento del presupuesto total y un reforzamiento de las capacidades logísticas, tecnológicas y estratégicas, tanto a nivel interno como internacional.

5.2 Presupuesto general de defensa (2004)

Durante el año fiscal 2004, el gasto público en defensa en los Estados Unidos ascendió a **US\$ 490.681 millones**, lo que representó un incremento de **US\$ 52.222,3 millones** respecto al año anterior, es decir, un **11,91 %** de aumento. El gasto en defensa equivalió al **11,97 % del gasto**

público total, alcanzando el **4,02 % del Producto Bruto Interno (PIB)**, con un incremento de **0,19 puntos porcentuales** respecto de 2003, cuando representaba el 3,83 %.

El gasto público per cápita en defensa fue de **U\$S 1.672 por habitante**, reflejando el impacto directo del proceso de expansión militar y de seguridad impulsado por la administración federal. Este incremento consolidó la tendencia ascendente iniciada tras los atentados del 11-S, evidenciando una estrategia presupuestaria sostenida en la prioridad de la defensa y la seguridad como ejes de la política nacional.

5.3 Solicitud presupuestaria para el contraterrorismo

La solicitud de presupuesto para el año 2004 incluyó **aproximadamente U\$S 1.000 millones en apoyo directo a la lucha contra el terrorismo**, de los cuales **U\$S 250 millones** (casi el 50 % de los cambios de programa propuestos) fueron específicamente destinados a fortalecer las capacidades del FBI en materia de contraterrorismo.

La propuesta contempló la creación de **430 nuevos puestos**, orientados a reforzar el apoyo operativo en todo el territorio nacional y mejorar la gestión, coordinación y asesoramiento técnico y legal en la sede central. Este incremento de personal permitiría al FBI ampliar su capacidad de respuesta y coordinación con las agencias estatales y locales, así como fortalecer su capacidad de análisis estratégico y su estructura de inteligencia preventiva.

El presupuesto también destinó recursos significativos al fortalecimiento de las **Joint Terrorism Task Forces (JTTF)**, que se expandieron a **66 grupos de trabajo**. Estas fuerzas de tarea multidisciplinarias integran agentes federales, estatales y locales, y constituyen la “primera línea” de defensa contra el terrorismo, facilitando la cooperación interinstitucional y el intercambio de información en tiempo real.

Además, el plan presupuestario contempló la ampliación de la presencia internacional del FBI mediante la creación de nuevas **oficinas de agregados legales (Legats)** en Sarajevo (Bosnia),

Ciudad de Kuwait (Kuwait), Tashkent (Uzbekistán), Kabul (Afganistán) y Belgrado (Serbia). El objetivo era fortalecer las alianzas internacionales y mejorar la capacidad del FBI para actuar frente a amenazas transnacionales, particularmente en regiones consideradas estratégicas para la seguridad de los Estados Unidos.

El incremento de recursos también apuntó a **mejorar las capacidades de respuesta ante crisis**, garantizando la disponibilidad inmediata de equipos, personal especializado y recursos logísticos para intervenir en la escena de un ataque terrorista tanto en territorio estadounidense como en el extranjero.

5.4 Solicitud presupuestaria de contrainteligencia

En el marco del presupuesto de 2004, el FBI solicitó **U\$S 63 millones** y la incorporación de **599 nuevos puestos**, incluyendo **94 agentes especiales**, destinados a impulsar su estrategia de **contrainteligencia**. Esta partida tuvo como propósito fortalecer la capacidad de la Oficina para detectar y neutralizar actividades de espionaje, proteger los activos tecnológicos y científicos del país, y prevenir la infiltración de agentes extranjeros en instituciones nacionales y universidades.

El fortalecimiento de la contrainteligencia respondió al reconocimiento de una creciente amenaza global en materia de espionaje económico y cibernético. Los recursos asignados se destinaron a la modernización de los sistemas de vigilancia fija y móvil, a la adquisición de tecnología avanzada de detección y al aumento del personal especializado en análisis de inteligencia.

De esta manera, la contrainteligencia se consolidó como una línea de acción prioritaria dentro del FBI, complementaria a las estrategias de contrterrorismo y de ciberseguridad, en un entorno internacional marcado por la expansión de amenazas híbridas y asimétricas.

5.5 Delito cibernético y nuevas amenazas

El año 2004 fue testigo de una transformación institucional dentro del FBI con la **creación de la División Cibernética (Cyber Division)**, destinada a gestionar las investigaciones sobre delitos informáticos y a coordinar esfuerzos con el sector público y privado. Esta nueva división se encargó de liderar las acciones contra las intrusiones informáticas, los ataques a infraestructuras críticas, los fraudes electrónicos y la explotación infantil en línea.

Para ese año, **47 oficinas de campo** contaban o estaban en proceso de establecer **escuadrones cibernéticos especializados**, de los cuales **8** tendrían múltiples equipos. Además, el FBI integró **más de 30 grupos de trabajo Inter agenciales** dedicados a la investigación del delito cibernético, con el apoyo de **Equipos de Acción Cibernética (CATs)** con experiencia técnica avanzada.

Los resultados del programa fueron significativos: el **Programa de Intrusión Informática** identificó **2.554 computadoras comprometidas**, con **95 condenas** y **US\$ 186 millones en restituciones**. Asimismo, la **Iniciativa Nacional Innocent Images** registró **692 arrestos**, **648 acusaciones** y **646 condenas** durante 2002, reflejando un aumento sostenido en las investigaciones de explotación infantil en Internet.

Pese a utilizar solo el **5 % de los recursos totales del FBI**, el programa cibernético demostró su efectividad y su impacto transversal en las actividades de investigación de toda la Oficina.

La estrategia cibernética del FBI se orientó a la identificación y neutralización de cuatro tipos de amenazas principales:

1. Personas o grupos dedicados a **intrusiones informáticas y propagación de códigos maliciosos**;
2. **Ladrones de propiedad intelectual** y violadores de derechos de autor;
3. **Estafadores de Internet** vinculados a delitos financieros; y

4. **Depredadores en línea** involucrados en la explotación sexual de menores.

5.6 **Solicitud presupuestaria para protección contra ataques cibernéticos**

Para el ejercicio fiscal 2004, el FBI solicitó **US\$ 234,4 millones** destinados específicamente a **proteger a los Estados Unidos frente a ataques cibernéticos y delitos de alta tecnología**. Este monto incluyó cambios de programa por **US\$ 62 millones** y la incorporación de **194 nuevos puestos**, entre ellos **77 agentes especiales**.

Los fondos tenían como objetivo reforzar los escuadrones de intrusión informática en las oficinas de campo, mejorar las capacidades técnicas para la identificación de intrusos y fortalecer los programas de capacitación y equipamiento del personal.

El presupuesto también se orientó a **ampliar la capacidad forense digital** del FBI, ya que **6 de cada 10 investigaciones requerían soporte informático forense**. El plan buscó asegurar que la Oficina pudiera responder eficazmente al crecimiento exponencial de casos de ciberdelito, con un enfoque integral que combinara prevención, investigación y análisis forense.

Además, se destinaron recursos a la **lucha contra la explotación sexual infantil en Internet**, un fenómeno que había aumentado de **113 casos en 1996 a más de 2.300 en 2003**. El FBI reforzó así su compromiso con la protección de menores y la persecución de redes criminales dedicadas al tráfico y abuso infantil digital.

5.7 **Avances tecnológicos y programa Trilogy**

Entre 2002 y 2004, el **Programa Trilogy** se consolidó como el principal eje de modernización tecnológica del FBI. Este proyecto, iniciado tras los ataques del 11-S, tenía como propósito transformar la infraestructura informática y digital de la institución, reemplazando los sistemas obsoletos y centralizando la información en una plataforma unificada y segura.

Para 2004, el FBI había implementado **21.025 nuevas computadoras de escritorio**, redes de área local de alta velocidad en **622 ubicaciones**, **3.408 impresoras** y **1.463 escáneres**. Asimismo, **524 de las 594 oficinas** de campo operaban bajo la nueva red de área amplia (*wide area network*), lo que representaba el **92 % de los empleados** del FBI en territorio estadounidense.

El *Enterprise Operations Center*, encargado de administrar datos, redes, hardware y seguridad, comenzó a operar ese mismo año. El programa *Trilogy* cambió la cultura organizacional del FBI, sustituyendo los sistemas de búsqueda manual y fragmentada por una arquitectura electrónica integrada que permitía conectar múltiples bases de datos, evidencias y pistas mediante un único portal.

Además, el *Integrated Data Warehouse* permitió la vinculación de **31 bases de datos** bajo un solo entorno de búsqueda, mientras que el programa de **Capacidades Colaborativas** facilitó el intercambio electrónico seguro de información con otras agencias federales.

En conjunto, el *Trilogy* representó un salto cualitativo en la capacidad del FBI para procesar, almacenar y compartir información crítica, convirtiéndose en la base de su modernización tecnológica y en un pilar esencial de la seguridad nacional estadounidense.

5.8 Solicitud de actualización tecnológica

En la etapa de consolidación del programa *Trilogy*, el FBI reconoció la necesidad de garantizar la sostenibilidad de las inversiones realizadas en materia de tecnología de la información. Por ello, la solicitud presupuestaria para el año fiscal 2004 incluyó **cambios en el programa por US\$ 82.000.000**, destinados a financiar la **renovación tecnológica**, el **mantenimiento operativo** y las **actualizaciones de ciclo de vida** de los sistemas implementados.

La estrategia presupuestaria tuvo como objetivo preservar la infraestructura tecnológica recientemente desplegada, asegurando su correcta operatividad y evitando que volviera a producirse el fenómeno de obsolescencia que había afectado gravemente al FBI durante la década de 1990. En esa línea, se buscó establecer un sistema de renovación ordenada y continua del

equipamiento informático, servidores y software esenciales para la gestión de datos de inteligencia.

La sostenibilidad del *Trilogy* se consideró una cuestión crítica no solo para la eficacia operativa, sino también para la seguridad institucional. La capacidad de interconectar información en tiempo real entre distintas oficinas y agencias, junto con el resguardo de datos clasificados bajo altos estándares de seguridad digital, era vista como un factor indispensable para la eficiencia investigativa y la protección de los intereses nacionales.

5.9 Programas complementarios y seguridad institucional

El presupuesto de 2004 también incluyó un conjunto de programas complementarios destinados a **reforzar la seguridad interna del FBI y optimizar la estructura organizativa**. Tras el caso de espionaje protagonizado por el ex agente Robert Hanssen, la Oficina implementó una profunda reestructuración orientada a prevenir vulneraciones a la seguridad de la información y mejorar los protocolos de control.

En este sentido, se **creó la División de Seguridad** como organismo especializado dentro del FBI, con la función de garantizar, supervisar y consolidar un sistema de seguridad integral que protegiera tanto la información clasificada como las instalaciones y el personal. La solicitud presupuestaria correspondiente a esta área incluyó **US\$ 37.000.000** en modificaciones de programa y **126 nuevos puestos**, entre ellos **32 agentes especializados** en seguridad.

Los fondos se destinaron a tres líneas de acción principales:

1. **Fortalecimiento de la seguridad de la información**, incluyendo auditorías, monitoreo de accesos, evaluación de vulnerabilidades y respuestas ante incidentes.
2. **Reforzamiento de la seguridad física**, a través de mejoras en los sistemas de control de acceso, videovigilancia y custodia de instalaciones críticas.

3. **Ampliación del programa de polígrafo y control de confianza**, destinado a personal con acceso a información sensible o a funciones críticas.

El programa de **polígrafo**, considerado una herramienta de prevención y control, recibió **US\$ 6.804.000** y **15 nuevos agentes**, junto con recursos para equipamiento, capacitación y espacios de evaluación.

En el ámbito de **aseguramiento de la información**, la Oficina destinó **US\$ 48.173.000** y **13 agentes** a tareas de ciberseguridad, monitoreo de sistemas, control de accesos digitales y desarrollo de prácticas de seguridad basadas en capas múltiples de protección.

Asimismo, se incorporó el concepto de **contramedidas** como componente central del nuevo modelo de seguridad. Estas contramedidas comprendían la identificación de las capacidades de adversarios potenciales, la adaptación de los procedimientos internos y la reducción de vulnerabilidades en los sistemas de información y en las operaciones de campo.

El fortalecimiento de la seguridad institucional también se reflejó en la destinación de **US\$ 21.338.000** para personal, formación y servicios de certificación de sistemas, junto con **US\$ 714.000** para mejorar la seguridad física de la Academia del FBI en Quantico, Virginia, y de cinco oficinas de campo reubicadas en instalaciones de uso exclusivo.

5.10 Programa criminal del FBI

En paralelo al desarrollo de programas de contraterrorismo, ciberseguridad y contrainteligencia, el FBI mantuvo su compromiso con el cumplimiento de la ley en materia de **delitos financieros y corrupción corporativa**. Durante el año fiscal 2004, la Oficina abrió **más de 85 investigaciones de fraude corporativo**, ocho de las cuales superaban los **US\$ 1.000 millones en pérdidas**.

Cuarenta y cinco oficinas de campo participaron activamente en grupos de trabajo interinstitucionales dedicados al **fraude financiero**, integrando esfuerzos con la **Securities and Exchange Commission (SEC)**, el **Department of Justice (DOJ)** y otras agencias regulatorias.

El presupuesto para esta iniciativa incluyó **U\$S 16.000.000** y **164 nuevos puestos**, entre ellos **54 agentes especiales**, destinados a analistas financieros, expertos en contabilidad forense e investigadores especializados.

El fortalecimiento de las capacidades analíticas permitió al FBI responder de manera más eficiente al auge de delitos económicos complejos, fraudes bursátiles, lavado de dinero y manipulación corporativa, fenómenos que habían ganado visibilidad pública tras los casos de **Enron (2001)** y **WorldCom (2002)**.

Este enfoque integral reflejó el compromiso de la Oficina con la aplicación del principio de legalidad, combinando su función tradicional de investigación criminal con los nuevos desafíos derivados de la globalización económica y tecnológica.

5.11 Evaluación general y orientación estratégica

El presupuesto de defensa y seguridad de 2004 consolidó un **modelo de gestión integral de amenazas**, basado en la interconexión entre inteligencia, tecnología y cooperación Inter agencial. El aumento sostenido del gasto en defensa y la expansión del presupuesto del FBI mostraron una clara continuidad de la política de seguridad post 11-S, orientada a la **prevención proactiva del terrorismo** y la **modernización institucional**.

En términos estratégicos, el ejercicio 2004 destacó por tres avances principales:

1. **Integración tecnológica:** el proyecto *Trilogy* transformó la capacidad operativa del FBI al centralizar la información y digitalizar los procesos de investigación.

2. **Fortalecimiento de la seguridad interna:** la creación de la División de Seguridad y la adopción de protocolos estrictos de aseguramiento de la información aumentaron los niveles de control y transparencia.
3. **Ampliación de la cooperación internacional y regional:** la expansión de las oficinas de agregados legales reforzó la presencia global del FBI, contribuyendo a la coordinación internacional contra el terrorismo y el crimen organizado.

En el plano macroeconómico, el presupuesto de defensa de 2004 representó un **4,02 % del PIB**, consolidando a los Estados Unidos como la potencia con el mayor gasto militar del mundo. El esfuerzo financiero reflejó una política de Estado orientada a garantizar la superioridad tecnológica, la seguridad nacional y la capacidad de respuesta frente a amenazas emergentes, tanto convencionales como no convencionales.

En conjunto, la planificación presupuestaria de 2004 evidencia un viraje estructural del FBI hacia una **agencia de inteligencia de alcance global**, que combina funciones policiales tradicionales con herramientas tecnológicas, capacidades de análisis estratégico y una visión integral de la seguridad. Este proceso de modernización, iniciado tras el 11 de septiembre, marcaría el rumbo de las reformas institucionales de la década siguiente y sentaría las bases para la articulación de la política de seguridad nacional en el siglo XXI.

Conclusión del capítulo V

El análisis del presupuesto de defensa y seguridad de los Estados Unidos correspondiente al año fiscal 2004 permite identificar una etapa de consolidación y madurez en el proceso de reestructuración institucional iniciado tras los atentados del 11 de septiembre de 2001. Este período se caracterizó por la convergencia entre **expansión presupuestaria, modernización tecnológica y fortalecimiento operativo**, configurando un modelo de seguridad nacional integral orientado a la prevención, la inteligencia y la cooperación Inter agencial.

En el plano macroeconómico, el **incremento del gasto en defensa hasta el 4,02 % del PIB** y la inversión de casi **US\$ 491.000 millones** reflejaron la prioridad política del sector defensa dentro de la estrategia global de seguridad de la administración estadounidense. Este esfuerzo financiero no solo respondió a las exigencias militares en Irak y Afganistán, sino también a la necesidad de consolidar un aparato estatal capaz de enfrentar amenazas híbridas —terrorismo, espionaje, ciberdelincuencia y crimen organizado transnacional— de forma coordinada y sostenible.

Desde el punto de vista institucional, el **FBI emergió como un actor central** del sistema de seguridad nacional, ampliando su estructura, capacidades técnicas y presencia internacional. Las inversiones en programas como **Trilogy** y la **División Cibernética** transformaron profundamente la arquitectura operativa de la Oficina, permitiendo la integración digital de la información y la profesionalización de la respuesta ante amenazas tecnológicas. Al mismo tiempo, la creación de la **División de Seguridad** y el fortalecimiento de los mecanismos de control interno consolidaron una cultura organizacional basada en la transparencia, la vigilancia permanente y la protección de la información clasificada.

El capítulo evidencia así que 2004 representó un **punto de inflexión estratégico** en la política de seguridad estadounidense: el tránsito definitivo hacia un modelo de **seguridad nacional tecnológicamente integrada y globalmente proyectada**, en el cual el poder militar, la inteligencia y la infraestructura digital se articularon como pilares complementarios de una misma

lógica de defensa preventiva. Este proceso sentó las bases de la transformación del FBI en una agencia de inteligencia de alcance mundial y reafirmó la supremacía de los Estados Unidos como potencia en materia de seguridad, defensa y tecnología aplicada al control del riesgo en el siglo XXI.

Referencias

Datosmacro. (2004). *Gasto público en defensa de Estados Unidos (2004)*.

Departamento de Justicia de los Estados Unidos [FBI]. (2004). *Budget Request, Fiscal Year 2004*. Washington D.C.

Oficina de Administración y Presupuesto [OMB]. (2004). *Budget of the U.S. Government, Fiscal Year 2004*. Washington D.C.

Departamento de Defensa de los Estados Unidos. (2004). *Defense Budget Overview*. Washington D.C.

Taverna, M. (2017). *Política exterior y seguridad nacional de los Estados Unidos post 11-S*. Buenos Aires: Universidad Católica de Salta.

CAPÍTULO VI

Presupuesto 2.005

CAPÍTULO VI – Presupuesto 2005

“Como nota preliminar se indica que todos los datos de este capítulo fueron extraídos del Informe de contrterrorismo del F.B.I: https://www.fbi.gov/file-repository/counterterrorism/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view”.

6.1 Introducción: contexto general del ejercicio 2005

El año 2005 representó una etapa de consolidación y madurez dentro del proceso de transformación de la política de seguridad nacional estadounidense iniciado tras los atentados del 11 de septiembre de 2001. Luego de la expansión presupuestaria registrada entre 2002 y 2004, el gobierno federal, a través del Departamento de Defensa y del Departamento de Justicia, continuó priorizando la lucha contra el terrorismo, el fortalecimiento de las capacidades de inteligencia, y la modernización de la infraestructura institucional de los organismos de seguridad.

La política presupuestaria de 2005 mantuvo una tendencia ascendente, pero con una distribución más estratégica del gasto, orientada a la eficiencia operativa, la integración Inter agencial y la inversión tecnológica. El **Federal Bureau of Investigation (FBI)** consolidó su papel como eje central de la seguridad interna, con nuevas partidas para operaciones de inteligencia, modernización de instalaciones, y refuerzo del **Centro de Detección de Terroristas (Terrorist Screening Center, TSC)**.

Al mismo tiempo, el contexto internacional, signado por la guerra en Irak y el sostenimiento de la ocupación en Afganistán, incidió directamente en la estructura del gasto en defensa, que alcanzó nuevos máximos históricos. En este escenario, el presupuesto de 2005 no solo fortaleció las capacidades militares y tecnológicas, sino que también buscó reforzar la prevención, la cooperación y la respuesta ante amenazas híbridas y de carácter transnacional.

6.2 Presupuesto general de defensa (2005)

Durante el año fiscal 2005, el gasto público en defensa de los Estados Unidos se incrementó en **U\$S 42.626,8 millones**, equivalente a un **8,69 % de aumento** respecto al año anterior, alcanzando un total de **U\$S 533.307,8 millones**. Este monto representó el **12,05 % del gasto público total**, consolidando la defensa como el mayor componente del presupuesto federal. En términos del **Producto Bruto Interno (PIB)**, el gasto militar llegó al **4,09 %**, lo que supuso un incremento de **0,07 puntos porcentuales** en relación con el 4,02 % registrado en 2004.

En términos per cápita, el gasto en defensa ascendió a **U\$S 1.801 por habitante**, frente a los U\$S 1.672 del año anterior, lo que significó un incremento del **7,57 %** (equivalente a U\$S 129 por persona). Este crecimiento reflejó la continuidad de la estrategia de expansión del gasto en seguridad y defensa, aunque con un ritmo ligeramente más moderado que en los años inmediatos posteriores al 11-S.

El aumento estuvo asociado al mantenimiento de las operaciones militares en Medio Oriente, a la necesidad de reabastecimiento logístico y tecnológico de las fuerzas armadas, y al refuerzo de la estructura de seguridad interna frente a amenazas no convencionales. La política presupuestaria de defensa del año 2005 continuó, por tanto, dentro del marco de la **Doctrina Bush**, consolidando un modelo de seguridad preventiva y global, en el que la defensa del territorio estadounidense dependía de la capacidad de acción anticipada más allá de sus fronteras.

6.3 Solicitud presupuestaria para el FBI

Para el ejercicio fiscal 2005, el **Federal Bureau of Investigation** obtuvo un **suplemento presupuestario de U\$S 74 millones**, orientado principalmente a reforzar sus operaciones en Irak y a fortalecer la lucha contra el terrorismo en el ámbito interno. Esta asignación adicional complementó los incrementos sostenidos de los años previos, permitiendo al FBI ampliar sus capacidades de inteligencia, contraterrorismo, respuesta ante crisis y análisis de información.

El suplemento de 2005 tuvo como finalidad mantener la continuidad operativa de las unidades de investigación desplegadas en zonas de conflicto, al tiempo que financiaba programas de modernización institucional en territorio estadounidense. Las partidas fueron dirigidas a tres áreas estratégicas:

1. **Fortalecimiento de la inteligencia táctica y operativa**, con nuevas contrataciones y desarrollo de capacidades analíticas.
2. **Modernización de infraestructura tecnológica y física**, con inversiones en sistemas de comunicación y nuevas instalaciones.
3. **Ampliación de capacidades Inter agenciales**, reforzando la coordinación con el Departamento de Seguridad Nacional (DHS), el Departamento de Defensa (DoD) y agencias estatales y locales.

De este modo, el FBI consolidó su papel como puente entre la inteligencia interna y la acción judicial, en un contexto de redefinición de su estructura funcional hacia un modelo más flexible y adaptado a la lógica de amenazas globales.

6.4 Centro de Detección de Terroristas (TSC)

Uno de los ejes más relevantes del presupuesto de 2005 fue el fortalecimiento del **Terrorist Screening Center (TSC)**, una iniciativa Inter agencial creada en 2003 para centralizar la detección y el seguimiento de terroristas conocidos o sospechosos. El TSC surgió en cumplimiento de la **Directiva Presidencial de Seguridad Nacional N.º 6 (HSPD-6)**, como parte de los esfuerzos por unificar las bases de datos de inteligencia y aplicar criterios estandarizados de identificación de amenazas.

Durante los primeros meses de 2005, el TSC ya había alcanzado una notable capacidad operativa: recibió **21.650 llamadas** (de las cuales **3.500** provenían de fuerzas de seguridad

estatales y locales), realizó **11.300 identificaciones positivas** y colaboró en **más de 340 arrestos**, incluyendo **seis casos directamente vinculados con terrorismo**.

Para el año fiscal 2005, el FBI solicitó **US\$ 75 millones** adicionales y **61 nuevos puestos**, entre ellos **6 analistas de inteligencia** y **8 agentes especiales**, con el fin de fortalecer la estructura funcional del TSC y responder al crecimiento exponencial de consultas y requerimientos.

El objetivo era dotar al Centro de la capacidad necesaria para atender nuevos desafíos derivados de:

- **Controles fronterizos más estrictos**, en el marco de la Ley Patriota y las reformas del DHS.
- **Requisitos de control de pasajeros** en vuelos nacionales e internacionales, sin afectar el comercio o la movilidad civil.
- **Verificación de organizaciones receptoras de fondos públicos**, garantizando que no mantuvieran vínculos con entidades terroristas.

El TSC se proyectó como el núcleo del sistema nacional de detección, con previsiones de crecimiento de hasta **tres millones de consultas diarias** para el año fiscal 2006. Este proceso implicó una profunda transformación en la arquitectura de intercambio de información de seguridad en los Estados Unidos, con un enfoque cada vez más automatizado, interoperable y basado en inteligencia de datos.

6.5 Mejoras de infraestructura y fortalecimiento institucional

Paralelamente, el presupuesto de 2005 incluyó una serie de **mejoras estructurales y organizativas** destinadas a consolidar las capacidades del FBI en materia de recursos humanos, capacitación y gestión operativa.

Durante 2004 se había realizado un estudio interno para optimizar los **procesos de contratación de personal de apoyo**, cuyos resultados se implementaron en 2005.

Las recomendaciones del informe propusieron **racionalizar los procedimientos administrativos, realinear los recursos humanos y acelerar los tiempos de selección**, con especial énfasis en la incorporación de personal calificado para áreas críticas como la **Dirección de Inteligencia**.

El nuevo sistema de reclutamiento permitió acortar los plazos de entrevistas y procesamiento de postulantes, particularmente en las regiones de **Washington D. C. y Baltimore**, donde se concentraban los programas prioritarios del FBI. Estas mejoras respondieron a la necesidad de asegurar una dotación de personal adecuada para cumplir los objetivos estratégicos definidos en el marco de la lucha contra el terrorismo.

En materia de **capacitación**, se llevaron a cabo reformas sustanciales en la **Academia del FBI en Quantico, Virginia**, que brindaba instrucción diaria a cerca de **1.500 miembros del personal de inteligencia y de aplicación de la ley**. Las instalaciones fueron renovadas y modernizadas para atender la creciente demanda de programas especializados en **análisis de inteligencia, contraterrorismo y ciberdelincuencia**.

Como parte del plan de fortalecimiento de infraestructura, el FBI solicitó **U\$S 10 millones** para **estudios de arquitectura e ingeniería** destinados a la creación de una nueva instalación para el **Grupo de Respuesta a Incidentes Críticos (Critical Incident Response Group, CIRG)**. Esta inversión incluía la **adquisición de terrenos** y la planificación de un **complejo centralizado** que integrara las áreas de comando, control, respuesta táctica y capacitación. El nuevo complejo permitiría una gestión más eficiente de los recursos y una capacidad de respuesta más rápida ante emergencias nacionales o internacionales.

Estas acciones de modernización reflejaron una visión institucional integral, orientada no solo a la ampliación presupuestaria, sino a la construcción de una estructura flexible, tecnológicamente avanzada y preparada para las amenazas del siglo XXI.

6.6 Evaluación general y perspectivas estratégicas

El presupuesto de defensa y seguridad de 2005 consolidó la transición del FBI y del sistema federal hacia una **arquitectura de seguridad integral**, donde la información, la tecnología y la cooperación interinstitucional se convirtieron en los pilares de la prevención. El crecimiento del gasto en defensa hasta el **4,09 % del PIB** mostró la persistencia del paradigma securitario post 11-S, que combinaba la defensa nacional con la intervención internacional y la vigilancia interna.

La creación y expansión del **Terrorist Screening Center** simbolizó el avance hacia una infraestructura de seguridad basada en la **interconexión de datos**, mientras que las mejoras en la **Academia de Quantico** y la **planificación del nuevo complejo del CIRG** representaron el fortalecimiento del capital humano y operativo.

La tendencia del presupuesto de 2005 evidenció, en suma, un equilibrio entre la **continuidad del esfuerzo militar internacional** y la **consolidación de las capacidades domésticas** de inteligencia, control y respuesta ante amenazas. En términos estructurales, el FBI emergió como un organismo más autónomo, tecnológicamente robusto y con un papel central en la gestión de la seguridad nacional estadounidense.

Conclusión Capítulo VI

El ejercicio fiscal 2005 marcó una fase de consolidación estructural en la política de defensa y seguridad de los Estados Unidos, reflejando la madurez de las reformas implementadas tras los atentados del 11 de septiembre de 2001. Lejos de los incrementos abruptos observados en los primeros años del período, el presupuesto de este año evidenció una tendencia de crecimiento sostenido, pero más racionalizado, con un énfasis en la eficiencia operativa, la integración Inter agencial y la modernización tecnológica. El gasto total en defensa alcanzó los **U\$S 533.307,8 millones**, equivalente al **4,09 % del PIB**, reafirmando la centralidad del sector militar dentro de la estructura fiscal y estratégica del Estado.

En este marco, el **Federal Bureau of Investigation (FBI)** se consolidó como el principal pilar de la seguridad interna, extendiendo su capacidad operativa tanto en el ámbito doméstico como en zonas de conflicto. La asignación suplementaria de **U\$S 74 millones** permitió profundizar su reestructuración institucional, ampliar sus unidades de inteligencia y fortalecer los mecanismos de coordinación con el **Departamento de Seguridad Nacional (DHS)** y el **Departamento de Defensa (DoD)**. Este proceso de expansión reafirmó el tránsito del FBI hacia un modelo de agencia híbrida, con funciones preventivas, analíticas y operativas, adaptadas a las dinámicas del terrorismo global y a las exigencias del nuevo orden securitario.

El fortalecimiento del **Terrorist Screening Center (TSC)** representó un hito dentro de la arquitectura de seguridad nacional, al consolidar la centralización de datos sobre sospechosos de terrorismo y permitir una respuesta más ágil ante potenciales amenazas. La asignación de **U\$S 75 millones adicionales** y la creación de nuevos puestos especializados reflejaron la importancia estratégica del TSC como eje del sistema de inteligencia y control interno. Su funcionamiento operativo —que incluyó más de **11.000 identificaciones positivas** y **340 arrestos** en pocos meses— demostró la efectividad del enfoque basado en la información compartida y la interoperabilidad tecnológica.

Por otra parte, las **inversiones en infraestructura y fortalecimiento institucional** del FBI, especialmente en la **Academia de Quantico** y en el plan para el **Critical Incident Response Group (CIRG)**, mostraron una visión de largo plazo orientada al desarrollo de capital humano especializado y a la profesionalización del aparato de seguridad. Estas iniciativas evidenciaron un desplazamiento conceptual desde la simple expansión del gasto hacia la construcción de una **capacidad estatal integral**, capaz de responder a amenazas tanto convencionales como híbridas.

En síntesis, el año 2005 puede interpretarse como un punto de inflexión entre la expansión reactiva de los años posteriores al 11-S y la consolidación de un modelo estructurado de seguridad nacional. El presupuesto de este año combinó el **mantenimiento del esfuerzo militar internacional** con la **consolidación doméstica** de capacidades de inteligencia, gestión y control. Así, el FBI emergió como una institución central dentro del entramado de seguridad estadounidense, simbolizando la transición hacia un paradigma de **seguridad preventiva, interconectada y tecnológicamente sustentada**, que definió las bases operativas de la política de defensa de los Estados Unidos en la segunda mitad de la década de 2000.

Referencias

Departamento de Defensa de los Estados Unidos. (2005). *Defense Budget Overview*.

Washington D.C.

Departamento de Justicia de los Estados Unidos [FBI]. (2005). *Budget Request, Fiscal Year 2005*. Washington D.C.

Oficina de Administración y Presupuesto [OMB]. (2005). *Budget of the U.S. Government, Fiscal Year 2005*. Washington D.C.

Datosmacro. (2005). *Gasto público en defensa de Estados Unidos (2005)*.

Taverna, M. (2017). *Política exterior y seguridad nacional de los Estados Unidos post 11-S*.

Buenos Aires: Universidad Católica de Salta.

CAPÍTULO VII

Proyectos especiales

CAPÍTULO VII – Proyectos Especiales

“Como nota preliminar se indica que todos los datos de este capítulo fueron extraídos del Informe de contraterroismo del F.B.I: https://www.fbi.gov/file-repository/counterterrorism/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view”.

7.1 Introducción

Dentro del proceso de modernización tecnológica y operativa emprendido por el *Federal Bureau of Investigation (FBI)* tras los atentados del 11 de septiembre de 2001, surgieron diversos **proyectos especiales** destinados a fortalecer las capacidades de recopilación, gestión y análisis de información. Estas iniciativas respondieron a la necesidad de dotar a la agencia de herramientas técnicas que permitieran **adaptar la inteligencia y la investigación criminal** al contexto de nuevas amenazas globales, especialmente en los campos del **terrorismo internacional, la ciberdelincuencia y la contrainteligencia**.

El año 2005 marcó una etapa clave en esta evolución institucional, con la consolidación de dos grandes proyectos: **Webhouse** y **Trilogy**, los cuales representaron hitos en la infraestructura tecnológica y de datos del FBI. Ambos se enmarcan en la transición del modelo tradicional de investigación —basado en archivos físicos y comunicaciones fragmentadas— hacia una **estructura digital integrada, segura y colaborativa**.

7.2 Proyecto Webhouse

7.2.1 Objetivo general

El **Proyecto Webhouse** fue concebido como una **base de datos distribuida de nueva generación**, diseñada para ofrecer a los agentes, analistas y traductores del FBI **acceso simultáneo y controlado** a información previamente procesada, grabaciones de audio, datos digitales y reportes generados por sistemas de recopilación electrónica. Para su implementación, el FBI solicitó **US\$ 10.920.000** y la incorporación de **tres nuevos agentes especializados**, con el objetivo de consolidar un sistema unificado que mejorara la eficiencia analítica y la seguridad de los datos.

7.2.2 Arquitectura y funcionamiento

El sistema Webhouse se estructuró sobre **dos bases de datos independientes**, una destinada a la **aplicación de la ley penal** y otra a la **contrainteligencia extranjera**. Esta separación obedeció al estricto cumplimiento de la **Orden Ejecutiva 12.333**, la cual prohíbe la mezcla o intercambio de información entre ámbitos de jurisdicción penal y de inteligencia. A través de **cortafuegos (firewalls)**, **protocolos de seguridad criptográfica** y sistemas de **autenticación multinivel**, se garantizó que solo los usuarios debidamente autorizados pudieran acceder a los datos, eliminando así la posibilidad de accesos externos no controlados.

7.2.3 Funcionalidades y ventajas operativas

El Webhouse ofreció un entorno analítico en el que los datos **minimizados** —es decir, procesados para excluir información sensible o no relevante para la investigación— podían ser **compartidos y analizados entre oficinas** y unidades del FBI. Entre sus principales innovaciones se destacaron:

- **Identificación de palabras clave** mediante algoritmos de procesamiento del lenguaje natural (PLN).

- **Reconocimiento de voz** para búsqueda automatizada en grabaciones de audio.
- **Capacidades de análisis transversal** entre diferentes casos o jurisdicciones.

Estas herramientas transformaron la forma en que los analistas podían **visualizar, escuchar y actuar sobre la información de vigilancia electrónica**. El resultado fue un sistema que permitió **reducir tiempos de investigación**, mejorar la **interoperabilidad entre divisiones**, y aumentar la **capacidad de respuesta** ante amenazas emergentes.

De este modo, Webhouse se convirtió en un pilar estratégico para la integración de inteligencia y evidencia digital dentro del marco jurídico estadounidense, garantizando la legalidad y el respeto a los derechos civiles durante el proceso de análisis y almacenamiento de datos.

7.3 Proyecto Trilogy

7.3.1 Antecedentes y propósito

El **Proyecto Trilogy** representó una de las transformaciones tecnológicas más ambiciosas en la historia del FBI. Concebido como un plan de modernización de tres años, su objetivo fue **actualizar el software, el hardware y las redes de comunicación** en todas las oficinas de la agencia, reemplazando sistemas obsoletos y creando una infraestructura digital segura y escalable.

El proyecto fue financiado parcialmente con **fondos no comprometidos de años anteriores**, y su primera fase contó con una inversión de **US\$ 100.700.000**, destinada a crear las bases de una red informática moderna que garantizara la conectividad entre todas las dependencias del FBI a nivel nacional e internacional.

7.3.2 Fase I: Infraestructura tecnológica

Durante el primer año de implementación, las actividades se concentraron en tres componentes esenciales:

1. **Aplicaciones de usuario:** desarrollo de herramientas de software específicas que mejoraran la organización, el acceso y el análisis de la información por parte de los agentes y analistas.
2. **Presentación de información:** instalación de nuevo hardware de reemplazo y software de automatización de oficina, integrando a los empleados a una red de comunicación interna.
3. **Red de comunicaciones:** adquisición de redes de área local (LAN) y área amplia (WAN) de alta velocidad, con circuitos de telecomunicación seguros que permitieran el flujo rápido y protegido de datos.

El objetivo fue garantizar que los usuarios pudieran acceder, en tiempo real, a la información crítica desde cualquier oficina o puesto operativo, fortaleciendo la coordinación interdepartamental.

7.3.3 Fase II: Consolidación operativa

Para el segundo año del proyecto, los **costos de implementación ascendieron a U\$S 142.390.000**. El FBI destinó **U\$S 38.230.000** del presupuesto vigente y **U\$S 36.500.000** en fondos no comprometidos del año anterior, solicitando además una mejora presupuestaria de **U\$S 67.660.000** para completar la fase.

Las actividades principales incluyeron:

1. La implementación de **herramientas analíticas de casos múltiples**.
2. La actualización de **intranets corporativas y archivos de casos electrónicos multimedia**.
3. La mejora continua de la **automatización de oficinas** en terreno.
4. La expansión de **redes seguras y circuitos de comunicación** entre sedes.

Estas acciones permitieron avanzar hacia la interoperabilidad total de la información criminal y de inteligencia, elemento esencial para el nuevo modelo de gestión basado en datos centralizados y análisis predictivo.

7.3.4 Fase III: Integración total

La tercera etapa de Trilogy completó las actualizaciones de automatización en todas las sedes y oficinas de campo del FBI, consolidando una infraestructura informática que permitió **conectar al personal operativo, analítico y administrativo** bajo un mismo sistema digital. El proyecto no solo mejoró la capacidad técnica de la organización, sino que redefinió su cultura institucional, orientándola hacia la **inteligencia colaborativa** y la **resiliencia cibernética**.

7.4 Evaluación general

Los proyectos **Webhouse** y **Trilogy** constituyen ejemplos paradigmáticos del proceso de transformación tecnológica del FBI en el marco de la política de seguridad posterior al 11-S. Ambas iniciativas respondieron a una visión estratégica orientada a integrar la información, garantizar la legalidad en el tratamiento de datos y maximizar la eficiencia de los procesos investigativos.

Mientras **Webhouse** fortaleció la capacidad analítica y la seguridad en la gestión de inteligencia electrónica, **Trilogy** sentó las bases de una infraestructura informática moderna que permitió la comunicación y colaboración a escala institucional. Ambos proyectos se complementaron en la construcción de una agencia más dinámica, digitalizada y alineada con los estándares de inteligencia global del siglo XXI.

Conclusión

La implementación de los proyectos **Webhouse** y **Trilogy** representó un punto de inflexión en la historia tecnológica del **Federal Bureau of Investigation (FBI)**, al marcar la transición definitiva hacia una infraestructura digital integrada, eficiente y alineada con las demandas del siglo XXI. Estas iniciativas no solo respondieron a la urgencia de modernizar los sistemas informáticos y de gestión de datos tras los atentados del **11 de septiembre de 2001**, sino que también reflejaron un cambio profundo en la **cultura institucional** del organismo, orientado a la cooperación interdepartamental, la inteligencia predictiva y la protección de la información sensible.

El **Proyecto Webhouse** consolidó un sistema de gestión de datos seguro y analítico que permitió optimizar la recopilación, clasificación y uso de la información proveniente de fuentes electrónicas y de inteligencia. Su diseño, basado en la separación jurídica entre los ámbitos penal y de contrainteligencia, garantizó la legalidad y el respeto a los derechos civiles, al tiempo que dotó al FBI de capacidades técnicas avanzadas como el **procesamiento del lenguaje natural**, el **reconocimiento de voz** y el **análisis transversal de casos**.

Por su parte, el **Proyecto Trilogy** impulsó una modernización estructural de las redes, los equipos y las aplicaciones del FBI, asegurando una **interconectividad operativa nacional e internacional**. Su desarrollo permitió unificar la infraestructura tecnológica de la agencia, mejorando la comunicación entre oficinas, reduciendo los tiempos de respuesta y potenciando la eficiencia del trabajo analítico. Esta modernización sentó las bases para el desarrollo posterior de sistemas más avanzados de gestión de inteligencia y para la creación de un entorno operativo centrado en la información digital.

En conjunto, ambos proyectos transformaron al FBI en una organización más **resiliente, interconectada y orientada al conocimiento**, capaz de afrontar con mayor eficacia las amenazas contemporáneas del terrorismo, la ciberdelincuencia y la contrainteligencia extranjera. Así, la modernización tecnológica de 2005 no solo supuso una mejora administrativa, sino una

redefinición estratégica del papel del FBI dentro del sistema de seguridad nacional estadounidense, consolidándolo como una agencia de inteligencia moderna, legalmente responsable y tecnológicamente avanzada.

Referencias

Departamento de Justicia de los Estados Unidos [FBI]. (2002–2005). *Budget Requests and Technological Development Reports*. Washington D.C.

Oficina de Administración y Presupuesto [OMB]. (2003). *Budget of the U.S. Government*. Washington D.C.

Departamento de Defensa de los Estados Unidos. (2004). *Defense Infrastructure Modernization Initiatives*. Washington D.C.

Taverna, M. (2017). *Política exterior y seguridad nacional de los Estados Unidos post 11-S*. Buenos Aires: Universidad Católica de Salta.

CAPÍTULO VIII

Los incidentes terroristas

CAPÍTULO VIII – LOS INCIDENTES TERRORISTAS

8.1 Introducción

Durante el período comprendido entre los años 2002 y 2005, los Estados Unidos experimentaron una intensificación en la amenaza terrorista, tanto en su dimensión internacional como doméstica. La respuesta estatal, liderada por el *Federal Bureau of Investigation* (FBI), reflejó una reorganización institucional y presupuestaria orientada a prevenir actos de violencia política, sabotaje y destrucción de infraestructura, en el marco de la denominada *Guerra contra el Terrorismo* impulsada tras los atentados del 11 de septiembre de 2001.

A lo largo de estos años, el fenómeno del terrorismo interno mostró una evolución significativa: desde actos dispersos de sabotaje ecológico hasta conspiraciones de mayor complejidad, con la participación de grupos ideológicamente diversos. La emergencia del *Earth Liberation Front* (ELF) y el *Animal Liberation Front* (ALF) evidenció una nueva forma de radicalización ambientalista, caracterizada por ataques a la propiedad como forma de resistencia simbólica frente al modelo económico y urbano estadounidense.

En paralelo, el FBI enfrentó la amenaza de individuos vinculados a movimientos supremacistas, religiosos o de extrema derecha, cuyas motivaciones ideológicas respondían a la lógica del “enemigo interno”. Este capítulo presenta un análisis detallado de los principales incidentes y acciones preventivas registrados entre 2002 y 2005, identificando sus patrones, motivaciones y respuestas institucionales.

8.2 Año 2002: Emergencia del terrorismo ecológico y prevención ideológica

8.2.1 Incidentes terroristas

El año 2002 representó el inicio de una nueva etapa del terrorismo doméstico, centrado en ataques de motivación ambientalista. En marzo, la policía estatal de Pennsylvania descubrió en una obra en construcción maquinaria pesada dañada y pintada con mensajes como “ELF, para

la protección de la madre tierra” y “detener la deforestación”. Este hecho fue seguido por el incendio intencional de una grúa hidráulica en el mismo sitio, con pérdidas de aproximadamente 500.000 dólares. Un fax, presuntamente enviado por el ELF, reivindicó la autoría del atentado.

Entre mayo y septiembre, un grupo de desconocidos liberó 250 visones de una granja de pieles en Harborcreek, Pennsylvania, acto que fue reivindicado conjuntamente por ELF y ALF. En noviembre, el mismo establecimiento fue incendiado deliberadamente, evidenciando un patrón de acción sostenido. En agosto, se registraron incendios forestales provocados en un laboratorio científico en Warren, Pennsylvania, y sabotajes en Goochland, Virginia, donde se destruyeron viviendas y maquinaria de construcción mediante la colocación de azúcar en los tanques de combustible.

Durante septiembre y octubre, en el condado de Henrico, Virginia, se produjeron múltiples ataques coordinados. Veinticinco vehículos utilitarios deportivos (SUV) fueron vandalizados en un concesionario Ford, mientras que dos restaurantes de comida rápida fueron dañados con grafitis alusivos a la organización. Los atacantes dejaron notas que decían “Los SUV están matando a todo el mundo” y “Frente de Liberación de la Tierra”, reafirmando el discurso del ELF.

Los incidentes de 2002 mostraron la consolidación del **ecoterrorismo** como forma de acción política, basada en la destrucción de bienes materiales sin causar víctimas humanas, pero con un fuerte impacto económico y psicológico. Su objetivo era visibilizar la oposición radical al progreso industrial y a la expansión urbana, expresando una narrativa de resistencia contra el “modelo civilizatorio depredador”.

8.2.2 Prevenciones terroristas

En paralelo, las agencias federales lograron neutralizar diversas amenazas de carácter ideológico. En agosto, la policía del condado de Pinellas, Florida, detuvo a **Robert J. Goldstein**, quien planeaba atacar instalaciones islámicas. Durante el allanamiento se encontraron explosivos, armas y una “declaración de misión” detallada, que describía sus intenciones de ejecutar una

campaña de violencia religiosa. Junto a él fueron arrestados **Michael Wallace Hardee**, **Samuel V. Shannahan III** y **Kristi Goldstein**. Este hecho representó una de las primeras expresiones de **terrorismo doméstico de extrema derecha** posterior al 11S, evidenciando un desplazamiento del odio religioso hacia comunidades musulmanas dentro del territorio estadounidense.

8.3 Año 2003: Expansión del extremismo ecológico y resurgimiento del terrorismo ideológico

8.3.1 Incidentes terroristas

El año 2003 presentó un aumento tanto en la frecuencia como en la severidad de los ataques. En enero, desconocidos incendiaron vehículos en un concesionario de Girard, Pennsylvania, y el ELF asumió la responsabilidad. En marzo, un grupo de individuos atacó un restaurante McDonald's en Chico, California, utilizando bidones con combustible y pintadas con mensajes del ALF como “La carne es asesinato” y “La igualdad de especies”.

En agosto, el *Frente de Liberación de la Tierra* incendió el complejo residencial “Jardín” en San Diego, California, destruyendo viviendas y lesionando a dos personas. En los meses siguientes, se registraron nuevos ataques en viviendas en construcción, acompañados por grafitis del ELF. Estos hechos evidenciaron una tendencia de **radicalización logística**, con el uso de explosivos improvisados y operaciones nocturnas coordinadas.

Asimismo, el año 2003 fue testigo de ataques contra el sector científico. En agosto y septiembre, el laboratorio *Chiron Corporation* y la *Shaklee Corporation* —ambos vinculados a la experimentación animal— fueron objeto de atentados con artefactos explosivos. Los comunicados reivindicatorios del ALF denunciaban la “complicidad” de las empresas con el sufrimiento animal, en lo que se interpretó como una forma de “sabotaje moral”.

8.3.2 Prevenciones terroristas

El FBI logró desarticular varias conspiraciones de terrorismo interno con motivaciones diversas. En febrero, fue detenido **David Wayne Hull**, líder del *Ku Klux Klan*, acusado de fabricar y detonar artefactos explosivos en eventos del grupo. En abril, **David Roland Hinkson** fue arrestado por conspirar para asesinar a un juez federal, mientras que, en Texas, **William Joseph Krar** fue encontrado con armas, cien mil municiones y 800 gramos de cianuro de sodio. En junio, **Paul Douglas Revak** fue capturado por planear un ataque contra una instalación de la Guardia Costera, y en noviembre, **Stephen John Jordi** fue arrestado por planear atentados contra clínicas de aborto.

Estos casos reflejaron una diversidad de **motivaciones terroristas internas** — ambientales, raciales, religiosas y políticas— y llevaron al FBI a fortalecer su enfoque de inteligencia preventiva. Las *Joint Terrorism Task Forces (JTTF)* se consolidaron como instrumentos clave de cooperación Inter agencial para coordinar información, análisis forense y vigilancia técnica.

8.4 Año 2004: Intensificación del ecoterrorismo y consolidación del extremismo religioso

8.4.1 Incidentes terroristas

En 2004 se registró un incremento notable de ataques con fines simbólicos y religiosos. En enero, en Henrico, Virginia, cuatro cócteles molotov fueron utilizados para incendiar un concesionario Ford, con grafitis “ELF” en los vehículos dañados. En abril, **Sean Michael Gillespie**, vinculado a las Naciones Arias, arrojó un artefacto incendiario contra la sinagoga *B’nai Israel* en Oklahoma City, generando daños estructurales y provocando alarma en la comunidad judía.

Ese mismo mes, en Snohomish, Washington, varios incendios destruyeron casas nuevas en urbanizaciones, acompañados de mensajes de ELF que advertían: “Verde es igual a no quemar;

todos los demás son un juego justo”. Se encontraron trece artefactos incendiarios, lo que reveló una planificación técnica precisa. En julio, un ataque en la Universidad Brigham Young destruyó el laboratorio *Ellsworth de Ciencia Animal*, con grafitis de ALF y frases como “Ustedes son los terroristas”. Finalmente, en diciembre, fueron arrestados **Ryan Lewis, Holland Eva, Holland Lili y Jeremías Colcleasure** por colocar artefactos incendiarios en viviendas en Lincoln, California.

8.4.2 Análisis y respuesta institucional

El patrón delictivo del ELF y el ALF consolidó un tipo de **terrorismo no letal**, basado en el impacto económico y mediático. Su estructura celular y descentralizada dificultaba la infiltración y detección. El FBI respondió mediante la ampliación de su División Antiterrorista, priorizando la vigilancia digital, el análisis de patrones de incendios y la cooperación con agencias locales.

8.5 Año 2005: Persistencia y sofisticación del extremismo

8.5.1 Incidentes terroristas

En 2005, los ataques del ELF continuaron, con una notable expansión geográfica. En enero, cinco dispositivos incendiarios fueron hallados en un sitio de construcción en Auburn, California; semanas después, el ELF envió cartas a la prensa asumiendo la autoría. En febrero, un incendio en Sutter Creek destruyó un complejo de apartamentos, acompañado de grafitis “ELF” y “WeWillWin”.

En abril, en Sammamish, Washington, se incendió una vivienda en construcción, y se halló una sábana con la leyenda “¿Dónde están todos los árboles? Quema violador quema. ELF”. En julio, un vehículo perteneciente a un empleado de los Servicios de Animales de Los Ángeles fue incendiado, mientras que, en septiembre, un intento de atentado en el edificio del director del

mismo organismo fue reivindicado por el ALF. En noviembre, cinco casas en Hagerstown, Maryland, fueron destruidas por incendios provocados con queroseno, también atribuidos al ELF.

8.5.2 Prevenciones terroristas

Durante el mismo año, el FBI frustró varios complots de alto riesgo. En mayo, fue arrestado **Ronald Allen Grecula**, quien ofreció vender una bomba a miembros de Al Qaeda. En julio, **Levar Washington** y **Gregory Patterson** fueron detenidos tras un robo armado que pretendía financiar ataques contra sinagogas y bases militares. En diciembre, **Michael Curtis Reynolds** fue capturado en Idaho por ofrecer apoyo técnico a grupos terroristas.

Estos casos mostraron la **evolución del terrorismo doméstico hacia formas híbridas**, donde confluyen ideologías extremas con motivaciones personales o financieras. El FBI, en respuesta, fortaleció la cooperación internacional mediante agregados legales en Europa y Asia, y consolidó la estructura de su *Terrorist Screening Center (TSC)*.

8.6 Conclusiones generales

Entre 2002 y 2005, el terrorismo doméstico en Estados Unidos presentó una multiplicidad de formas y motivaciones. Desde el ecoterrorismo del ELF y ALF hasta el supremacismo racial, el extremismo religioso y los complots individuales, la amenaza se diversificó y exigió al Estado una respuesta integral.

El FBI implementó una **estrategia de inteligencia preventiva**, apoyada en tecnología, cooperación Inter agencial y legislación reforzada (como el *USA PATRIOT Act*). Las *Joint Terrorism Task Forces* se convirtieron en el núcleo operativo de coordinación, mientras que el *Terrorist Screening Center* permitió centralizar la información de vigilancia y control.

Estos años constituyen una etapa de consolidación del modelo **proactivo y preventivo de seguridad nacional**, que combina el uso de inteligencia estratégica con el monitoreo

tecnológico, y que marcó el rumbo de la política antiterrorista estadounidense durante las décadas siguientes.

8.7 Conclusión

El período comprendido entre 2002 y 2005 marcó una fase de transición y complejizarían del terrorismo doméstico en los Estados Unidos. Los incidentes registrados durante estos años evidencian un fenómeno multifacético, en el que convergieron motivaciones ambientales, religiosas, raciales y políticas, reflejando la diversidad de amenazas que enfrentó la seguridad interna posterior al 11 de septiembre de 2001.

El surgimiento y consolidación de grupos como el *Earth Liberation Front* (ELF) y el *Animal Liberation Front* (ALF) configuraron una nueva modalidad de terrorismo no letal, caracterizado por la destrucción de propiedad como forma de protesta ideológica. Este tipo de violencia simbólica, orientada a generar impacto económico y mediático, introdujo el concepto de “ecoterrorismo” como una categoría diferenciada dentro de las amenazas domésticas. Paralelamente, el resurgimiento de expresiones de odio racial y extremismo religioso — representadas por células supremacistas y actores individuales radicalizados— mostró que el terrorismo interno seguía enraizado en tensiones históricas del tejido social estadounidense.

Ante esta diversificación de las amenazas, el *Federal Bureau of Investigation* (FBI) implementó un modelo de seguridad proactivo basado en la inteligencia preventiva, la cooperación Inter agencial y la modernización tecnológica. Las *Joint Terrorism Task Forces* (JTTF) se consolidaron como herramientas esenciales para la detección y neutralización temprana de amenazas, mientras que la creación del *Terrorist Screening Center* (TSC) permitió centralizar la información sobre individuos sospechosos, fortaleciendo los mecanismos de control y respuesta rápida.

En términos estructurales, el período analizado consolidó un cambio de paradigma en la política antiterrorista estadounidense: la transición de una estrategia reactiva, centrada en la represión posterior al hecho, hacia un enfoque preventivo y analítico apoyado en la inteligencia estratégica. Esta transformación no solo redefinió las capacidades operativas del FBI, sino que también sentó las bases del modelo contemporáneo de seguridad nacional, en el que la

cooperación tecnológica, la vigilancia digital y la coordinación institucional constituyen pilares fundamentales para enfrentar las amenazas híbridas del siglo XXI.

Referencias

- Federal Bureau of Investigation (2002–2005). *Domestic Terrorism Incident Reports*. U.S. Department of Justice.
- Department of Justice (2003–2005). *Counterterrorism and National Security Reports*. Government Printing Office.
- Office of Management and Budget (2002–2005). *Federal Budget Outlays for Defense and Law Enforcement*. Washington, D.C.
- Carrillo Ramírez, J. (2015). *Terrorismo y seguridad internacional*. Bogotá: Universidad del Rosario.
- García Probert, M. (2014). *El fenómeno del terrorismo contemporáneo*. Madrid: Síntesis.
- Torres Rodríguez, P. (2017). *La política exterior de Estados Unidos y el nuevo terrorismo*. Buenos Aires: Ediciones Universitarias.

CONCLUSIONES GENERALES

La investigación se centró en responder a la pregunta sobre la inversión económica realizada por el Gobierno de los Estados Unidos a través del Federal Bureau of Investigation (FBI) para prevenir y enfrentar los ataques del terrorismo religioso, y cómo se compara con el costo económico de dichos ataques frente a la inversión destinada a la prevención del terrorismo ambiental entre los años 2002 y 2005. A lo largo de los capítulos, se ha logrado responder a esta interrogante de manera exhaustiva.

Entre 2001 y 2005, se observó una expansión sostenida del presupuesto federal destinada a la seguridad nacional, la inteligencia y la modernización del FBI. Tras los atentados del 11 de septiembre de 2001, el gasto en defensa, seguridad interior y contraterrorismo aumentó considerablemente. Bajo el marco de la USA PATRIOT Act, aprobada en 2001, y la reorganización del Departamento de Justicia (DOJ), el FBI recibió incrementos presupuestarios anuales superiores al 10%, destinados a fortalecer la División Antiterrorista y las Joint Terrorism Task Forces (JTTF), desarrollar proyectos tecnológicos de inteligencia y datos como Trilogy y Webhouse, e incrementar los recursos humanos para el análisis y la vigilancia preventiva. Entre 2002 y 2005, el presupuesto del FBI aumentó de aproximadamente 4,3 mil millones de dólares a 5,6 mil millones, con un 40% de las partidas anuales destinadas a operaciones de contraterrorismo según el US DOJ Budget Summary de 2005. Esto consolidó al FBI como el eje central de la política antiterrorista de Estados Unidos, concentrando gran parte de los recursos nacionales para prevenir los ataques terroristas.

El terrorismo religioso, es considerado una de las mayores amenazas para la seguridad interior lo cual motivó una fuerte inversión preventiva por parte del FBI. Entre 2002 y 2005, se destinó entre el 60% y el 65% del gasto en contraterrorismo a la prevención de ataques de motivación religiosa o ideológica, lo que representó entre 1,4 y

1,8 millones de dólares anuales, considerando la porción efectiva del presupuesto según el FBI Counterterrorism Program Report de 2005.

Los ataques religiosos domésticos, aunque de menor impacto material que los internacionales, tuvieron un alto impacto simbólico y político. Ejemplos como el ataque incendiario a la sinagoga B'nai Israel en Oklahoma en 2004 mostraron pérdidas materiales limitadas (2 a 5 millones de dólares en pérdidas totales estimadas), pero justificaron la alta inversión preventiva debido a su impacto social y político. Las células vinculadas a movimientos supremacistas blancos, neonazis o extremistas religiosos cristianos protagonizaron diversos incidentes domésticos, aunque de alcance limitado si se los compara con los ataques internacionales. El FBI reforzó la vigilancia sobre individuos radicalizados, comunidades vulnerables y centros religiosos

En contraposición, el terrorismo ambiental o ecoterrorismo, perpetrado principalmente por grupos como el Earth Liberation Front (ELF) y el Animal Liberation Front (ALF), provocó daños económicos significativos entre 2002 y 2005. Estos grupos llevaron a cabo ataques no letales pero costosos contra infraestructuras civiles, laboratorios, concesionarias de automóviles, proyectos inmobiliarios y universidades. Durante este período, los incidentes de ecoterrorismo generaron pérdidas materiales estimadas en más de 110 millones de dólares, acumuladas entre 2002 y 2005, concentrándose la mayoría de los ataques en los años 2002–2004 según los informes del FBI de 2005. En respuesta, el FBI destinó entre el 20% y el 25% de su presupuesto en contraterrorismo doméstico para combatir estas amenazas, lo que representó entre 400 y 500 millones de dólares anuales en personal especializado, operaciones encubiertas y análisis forense de incendios y sabotajes. Aunque los costos directos de los ataques ambientales superaron la inversión preventiva, estos no implicaron pérdida de vidas humanas, lo que los clasificó como de bajo riesgo.

El FBI destinó una proporción mayor de recursos a prevenir ataques religiosos e ideológicos, a pesar de que los costos materiales del terrorismo ambiental fueron significativamente más altos. Esto se debe a la mayor ponderación política y simbólica del terrorismo religioso, visto como una amenaza directa a la cohesión nacional ya la seguridad del Estado, mientras que el ecoterrorismo se percibió como una forma de "radicalismo interno" sin vinculación con redes globales de terror.

El gasto en defensa por habitante aumentó considerablemente entre 2001 y 2005: en 2001 (referencia previa) fue de 1.159 dólares por habitante; en 2002, 1.308 dólares (aumento inicial tras el 11-S y la implementación de la Doctrina Bush); en 2003, 1.508 dólares (inicio de la invasión a Irak y Afganistán); en 2004, 1.672 dólares (consolidación de la ocupación en Irak y Afganistán); y en 2005, 1.801 dólares (incremento del 7,57% respecto al año anterior, un aumento de 129 dólares por persona). Entre 2001 y 2005, el costo de la defensa por ciudadano aumentó en 642 dólares, lo que representa un incremento total del 55% en solo cuatro años, evidenciando el esfuerzo económico exigido a la sociedad estadounidense fue significativo: cada ciudadano estadounidense pasó a pagar \$642 dólares más al año para sostener el aparato de defensa, y el gasto per cápita creció un 55,39% entre 2001 y 2005, indicando una militarización acelerada de la economía.

Este crecimiento es muy superior a la inflación o al crecimiento poblacional normal, lo que indica una militarización acelerada de la economía. El aumento per cápita financió una transformación estructural: sistemas como Trilogy y Webhouse del FBI, bases de datos de ADN y centros de fusión de inteligencia (como el TSC); operaciones en el extranjero (Irak/Afganistán) simultáneamente con la protección doméstica (seguridad en aeropuertos, fronteras y prevención de bioterrorismo); y la creación y expansión de organismos como el DHS (Departamento de Seguridad Nacional) y la

reestructuración masiva del FBI (nuevos agentes, analistas y oficinas en el extranjero). El aumento de \$1.159 a \$1.801 por persona demuestra que la seguridad nacional se convirtió en la prioridad absoluta del Estado, absorbiendo recursos crecientes de la riqueza nacional (llegando al 4,09% del PIB en 2005) para sostener la doctrina.

Para la realización del análisis anterior se recurrió a un cuerpo de fuentes que incluyen: Datosmacro (2002, 2003, 2004, 2005) para calcular los montos por habitante y el porcentaje del PIB; la Oficina de Gestión y Presupuesto (OMB) (2002-2005) para las cifras oficiales del presupuesto federal total y las asignaciones de defensa; el Departamento de Justicia (DOJ) / Oficina Federal de Investigaciones (FBI) a través de sus Congressional Budget Submission / Budget Request para los años fiscales 2002, 2003, 2004 y 2005, informes sobre incidentes de terrorismo interno (2002-2005) e informes sobre contraterrorismo y seguridad nacional; y la Oficina Federal de Investigaciones (2005) para los informes sobre incidentes de terrorismo doméstico donde se detallan las pérdidas materiales causadas por el ELF y el ALF (los 110 millones de dólares mencionados), así como referencias del Departamento de Seguridad Nacional (DHS) a la clasificación de amenazas y asignación de recursos. Todas estas fuentes se encuentran listadas en las secciones de "Referencias" al final de cada capítulo y en la Bibliografía General.

La creación de estructuras como el Terrorist Screening Center (TSC), la expansión de las Joint Terrorism Task Forces y la implementación de sistemas informáticos integrados (Trilogy y Webhouse) fortalecieron la capacidad del FBI para detectar, analizar y neutralizar amenazas tanto religiosas como ambientales. El modelo de inteligencia preventiva adoptado en esos años permitió reducir significativamente los incidentes de gran escala y mejorar la cooperación interagencial. En términos comparativos, puede afirmarse que la inversión económica realizada por el Gobierno

estadounidense a través del FBI fue eficaz en reducir la frecuencia y letalidad del terrorismo religioso, aunque el costo-beneficio en relación con el ecoterrorismo evidencia un menor rendimiento financiero, dado que los daños materiales superaron en varios casos la inversión.

Entre 2002 y 2005, el Gobierno de los Estados Unidos destinó al FBI entre 1,8 y 2,3 mil millones de dólares anuales en promedio para la prevención del terrorismo doméstico, de los cuales aproximadamente dos tercios se orientaron a amenazas de tipo religioso o ideológico, y un cuarto a las de tipo ambiental. El terrorismo religioso generó un gasto preventivo alto y daños materiales bajos, mientras que el terrorismo ambiental representó un costo económico considerable en relación con su inversión preventiva.

En consecuencia, la comparación revela que el criterio político-estratégico, más que el estrictamente económico, guió la asignación presupuestaria del FBI durante este período. La amenaza percibida como más peligrosa para la seguridad nacional —el terrorismo religioso— recibió la mayor inversión, aunque los daños materiales causados por el ecoterrorismo resultaron más cuantiosos. Esta diferencia demuestra cómo, en el marco de la Guerra contra el Terrorismo, la política de seguridad estadounidense priorizó la prevención de amenazas simbólicas y doctrinales por encima de aquellas de impacto económico, reafirmando el papel del FBI como garantía de la estabilidad ide.

En resumen, la investigación logró alcanzar su objetivo general de determinar la inversión económica general y la transformación institucional del FBI para la defensa de la seguridad nacional frente a las amenazas terroristas. Esto se logró a través del análisis del contexto presupuestario general, evaluando la expansión del gasto federal tras el 11-S, el impacto de la USA PATRIOT Act y la reorganización del Departamento de Justicia, y examinando los aumentos presupuestarios anuales y su destino. Se demuestra que el presupuesto total del FBI creció de 4,3 mil millones de dólares en 2002 a 5,6 mil millones

en 2005, priorizando la seguridad nacional y destinando un promedio del 40% de las partidas anuales directamente a operaciones de contraterrorismo. Esto consolidó al FBI como el eje central de la política antiterrorista, focalizando recursos en fortalecer la División Antiterrorista, las Joint Terrorism Task Forces (JTTF) y el desarrollo tecnológico (proyectos Trilogy y Webhouse).

Asimismo, se logró el primer objetivo específico de cuantificar la inversión destinada a prevenir el terrorismo religioso/ideológico y contrastarla con el costo económico real de sus ataques. Esto se alcanzó mediante el análisis de la amenaza, calculando la porción del presupuesto preventivo asignada a la vigilancia de supremacistas y extremistas religiosos, y comparándola con los daños materiales reportados en los incidentes. Se estima que, al ser considerada una amenaza directa a la seguridad del Estado, el terrorismo religioso recibió la mayor inversión: entre el 60% y el 65% del gasto en contraterrorismo (aproximadamente 1,4 a 1,8 mil millones de dólares anuales). A pesar de la alta inversión, el costo económico de los ataques fue marginal (entre 2 y 5 millones de dólares). La inversión se justificó por el alto impacto simbólico y político de estos grupos, logrando una eficacia institucional alta al reducir su letalidad.

Finalmente, se logró el segundo objetivo específico de cuantificar la inversión destinada a prevenir el terrorismo ambiental y contrastarla con el costo económico real de sus ataques. Esto se alcanzó a través del estudio de los incidentes del ELF y ALF, sumando las pérdidas materiales acumuladas y estimando el porcentaje del presupuesto del FBI dirigido a esta amenaza específica. Se identificó que el ecoterrorismo recibió una inversión significativamente menor, representando aproximadamente el 20% al 25% del presupuesto de contraterrorismo doméstico (aproximadamente 400 a 500 millones de dólares anuales). Los ataques ambientales generaron el mayor daño económico, superando los 110 millones de dólares en pérdidas materiales. Existe un desequilibrio

financiero; los daños superaron la inversión preventiva debido a que estos ataques no implicaban pérdida de vidas humanas, clasificándose como amenazas de bajo riesgo para la seguridad.

Hasta aquí se pudo dar respuesta a todas las preguntas de la investigación, pero a través del desarrollo de la misma surgieron nuevas inquietudes que irán siendo trabajadas con el correr de mi carrera profesional.

BIBLIOGRAFÍA

- Hernández Sampieri, Roberto, Metodología de la Investigación, Ed. Mc Graw Hill, México, 2.014.
- Encendiendo la Llama del Ecologismo Revolucionario, Recopilación, 2009, <http://www.archive.org/details/ecologismo-revolucionario>
- Patricia Kreinbohn, http://www.iri.edu.ar/revistas/revista_dvd/revistas/cd%20revista%2035/menu.html.
- Informe sobre terrorismo 2002-2005. <https://www.fbi.gov/stats-services/publications/terrorism-2002-2005>.
- “Acciones de las Naciones Unidas contra el Terrorismo”. En www.un.org/es
- ARENAL, C. Del (1988) Teoría de la Política Internacional. Bs. As. GEL.
- ARON, Raymond (1976) *Penser la guerre, Clausewitz. II L'ageplanétaire*. By Editions Gallimard. Edición utilizada, *Pensar la guerra, Clausewitz. II. La era planetaria*. Instituto de Publicaciones Navales, 1987.
- ASÚA BATARRITA, Adela (2009) “Concepto jurídico de terrorismo y elementos subjetivos de finalidad. Fines políticos últimos y fines de terror instrumental”. En: *Estudios Jurídicos en Memoria de José María Lidón*. Área de Derecho Penal, Universidad de Deusto, Bilbao.
- AVILÉS, Juan (2004) “Balance del terrorismo en el mundo en el año 2003”, Grupo de Estudios Estratégicos (GEES), España.
- BAKUNIN, Mijail (1979) *Tácticas revolucionarias*. Editorial Logal.

- BANDURA, Albert (1992) “Mecanismos de desconexión moral” en REICH, WALTER, *Orígenes del Terrorismo: Psicología, ideología, teología, estados mentales*. Ediciones Pomares, Corredores, S.A., Barcelona.
- BARTOLOMÉ, Mariano (2008) *La seguridad internacional post 11S: contenidos, debates y tendencias*. 1ª. ed. Buenos Aires: Instituto de Publicaciones Navales.
- BECK, Ulrich (2003) “Las instituciones de gobernanza global en la sociedad mundial del riesgo” en *Guerra y paz en el siglo XXI: una perspectiva europea*. Compiladores SERRA-CASTELLS. Editorial: Tusquets.
- BRIEGER, Pedro (2005) “Al Qaeda un movimiento no tradicional”. Revista de Relaciones Internacionales N°28. Instituto de Relaciones Internacionales. Universidad Nacional de La Plata. Buenos Aires.
- BRIEGER, Pedro (2005) “Al Qaeda como nuevo fenómeno político” en www.mindef.gov.ar.
- BRIEGER, Pedro (2005) “Al Qaeda como nuevo fenómeno político” en www.mindef.gov.ar. Texto publicado originalmente en *Terrorismo Siglo XXI*. Universidad de Mar del Plata, 2005.
- CALLE, Fabián; MERKE, Federico, “La Estrategia de Seguridad Nacional de EE.UU. en la Era Bipolar”. *Agenda Internacional* Año 1, N° 3, Diciembre 2004. Enero/Febrero 2005.
- CHOMSKY, Noam (2006) “La Nueva Guerra contra el Terror”, en *LA GUERRA CONTRA EL TERROR: Estados Unidos, Afganistán y la lucha contra el terrorismo*. Coordinadores: Zeraoui, Zidane; Montiel, Fernando. México: Instituto Tecnológico de Monterrey-Ariete, primera edición.

- MANASSERO-TISERA (2009) “Una salida esperada: la retirada de las tropas norteamericanas de Irak”, Anuario de Relaciones Internacionales. Instituto de Relaciones Internacionales, Universidad Nacional de La Plata
- Cvitanic, F. (2014). El realismo político y su presencia y eficacia en la acción internacional. Revista Jurídica Piélagus, 13(1), 39-52. doi: <https://journalusco.edu.co/index.php/pielagus/article/view/663/1265>
- Morgenthau, H. (1992). Política entre las Naciones: la lucha por el poder y la paz. Buenos Aires: Grupo Editor Latinoamericano.
- Torres Rodríguez, J. (2017). La Securitización en Colombia posterior al 11 de septiembre de 2001. Quito: FLACSO.
- Wardlaw, G. (1986). Terrorismo Político: teoría, táctica y contramedidas. Madrid: Ed. del Ejército.
- Barrientos, F. (2008). La política antiterrorista de Estados Unidos. Academia Nacional de Estudios Políticos y Estratégicos, 1-42.
- Carrillo Ramírez, L. (2015). Actualidad del terrorismo: sus orígenes, el caos y la geoestrategia. Cuba: CLASCO.
- Cruz, M. (2015). Re-pensando el concepto de terrorismo: una discusión político-histórica. ICONOS 52, 179-192.
- García Probert, M. (2014). Dar al-islam y dar al-harb, conceptos fundamentales para entender la noción de seguridad en las sociedades musulmanas. Paz, seguridad y desarrollo, México, pág. 14.
- Hobson, D. (2005). Estrategia de liberación en el Medio Oriente: la promoción de la democracia americana y la guerra del terror. Australian Journal of International Affairs, 33.

- Hoffman, B. (2006). Dentro del Terrorismo. New York: Columbia University Press.
- Manassero, S., & Tello, P. (2014). Terrorismo Internacional. Buenos Aires: Universidad Nacional de La Plata.
- Pachter, D. (2014). Las consecuencias de la guerra contra el terrorismo post 11S. PalermoEdu, 5-45.
- Taverna, E. (2017). Las políticas de seguridad de Estados Unidos y su impacto
- ANEPE. (2010). El fracaso de la Comunidad de Inteligencia de Estados Unidos el 11 de Septiembre de 2001. Estados Unidos: Revista Política y Estrategia.
- Chavarro, F. (2009). Análisis del gasto militar desde la perspectiva de la economía de la defensa. Ecos de Economía, 199-237.
doi:<https://www.redalyc.org/pdf/3290/329027278006.pdf>
- Desch, M. (2005). Culture versus Structure in Post 9/11. Security Studies: Strategic Insight, Vol. IV.
- Fonfría Mesa, A. (2007). El gasto en defensa en los países desarrollados: evolución y factores explicativos. España: GRINEI.
doi:https://www.ief.es/docs/destacados/publicaciones/papeles_trabajo/2007_14.pdf
- ANEPE. (2010). El fracaso de la Comunidad de Inteligencia de Estados Unidos el 11 de Septiembre de 2001. Estados Unidos: Revista Política y Estrategia.

ÍNDICE

Hoja de califica	2
Introducción	6
CAPÍTULO I – Definiciones de terrorismo	12
1.1 Introducción	13
1.2 Según algunos autores consultados	14
1.3 Según el Diccionario de la Real Academia Española	18
1.4 Según el FBI	20
Síntesis del Capítulo I	26
Referencias	28
CAPÍTULO II – Los actores	30
2.1 Introducción	31
2.2 El Federal Bureau of Investigation (FBI)	32
2.2.1 Sus inicios y proceso de institucionalización	32
2.2.2 Reformas y profesionalización bajo J. Edgar Hoover	33
2.2.3 Métodos de investigación y procedimientos operativos	35
2.2.4 Inteligencia, coordinación y análisis de amenazas	37
2.2.5 Respeto a los derechos civiles y libertades constitucionales	40
2.3 El papel de los actores no estatales en el terrorismo doméstico	42
2.4 El Frente de Liberación de la Tierra (FLT)	44
2.4.1 Orígenes y contexto ideológico	44
2.4.2 Objetivos y directrices operativas	45
2.4.3 Estructura organizacional y método de acción	46
2.4.4 Clasificación y respuesta del FBI	46
2.5 El Frente de Liberación Animal (FLA)	47
2.5.1 Origen y desarrollo del movimiento	47
2.5.2 Ideología, objetivos y tácticas	48
2.5.3 Estructura y resistencia sin líderes	48
2.5.4 Percepción institucional y clasificación del FBI	49
2.6 Análisis teórico y consideraciones finales	50
Síntesis del Capítulo II	52
Referencias	54
CAPÍTULO III – Presupuesto 2002	56
3.1 Introducción al contexto presupuestario y político	57
3.2 Presupuesto general de defensa de los Estados Unidos	57
3.3 Solicitud presupuestaria del FBI	58
3.3.1 Ajustes al funcionamiento	58
3.3.2 Incrementos en programas de seguridad	59
3.3.2.1 Contraespionaje.....	59

3.3.2.2 Contraterrorismo.....	59
3.3.2.3 Ciberdelincuencia	59
3.3.2.4 Contracifrado.....	60
3.3.3 Servicios y equipamiento técnico	60
3.3.4 Activación del Laboratorio del F.B.I	60
3.3.5 Equipos antibombas y ADN.....	61
3.3.6 Delitos de cuello blanco e Internet.....	61
3.4 Propuestas Legislativas.....	61
3.5 Seguridad interna del FBI y reformas post Hanssen.....	62
3.6 Evaluación general del presupuesto y su impacto en la política de seguridad estadounidense.....	62
Conclusión del Capítulo III	64
Referencias Capítulo III.....	66
CAPÍTULO IV – Presupuesto 2003	67
4.1 Introducción al contexto de seguridad y defensa.....	68
4.2 Presupuesto general de defensa.....	69
4.3 Solicitud presupuestaria del FBI.....	69
4.3.1 Iniciativa contra el terrorismo.....	70
4.3.2 Programa de Protección de Infraestructura Nacional.....	71
4.3.3 Apoyo a la vigilancia y operaciones tácticas.....	71
4.3.4 Programas técnicos y de respuesta a crisis.....	72
4.3.5 Programas forenses, genéticos y de ADN.....	73
4.3.6 Programas de aviación e inteligencia.....	73
4.3.7 Programas de coordinación operativa y comunicación estratégica.....	74
4.3.8 Escuela de Dispositivos Peligrosos y capacitación especializada.....	75
4.3.9 Iniciativa de tecnología de la información y programa Trilogy.....	76
4.3.10 Iniciativas de seguridad institucional post Hanssen.....	77
4.4 Incrementos y prioridades estratégicas	78
Resumen del Capítulo IV	79
Referencias Capítulo IV.....	80

CAPÍTULO V – Presupuesto 2004	81
5.1 Introducción: contexto político y de seguridad	82
5.2 Programas de modernización tecnológica	82
5.3 Presupuesto operativo del FBI	83
5.4 Inversiones en inteligencia y contraterrorismo	84
5.5 Delito cibernético y nuevas amenazas.....	85
5.6 Solicitud presupuestaria para protección contra ataques cibernéticos.....	86
5.7 Avances tecnológicos y programa Trilogy.....	86
5.8 Solicitud de actualización tecnológica.....	87
5.9 Programas complementarios y seguridad institucional.....	88
5.10 Programa criminal del FBI.....	89
5.11 Evaluación general y orientación estratégica.....	90
Conclusión del Capítulo V	92
Referencias Capítulo V.....	94
CAPÍTULO VI – Presupuesto 2005	95
6.1 Introducción: contexto general del ejercicio	96
6.2 Consolidación presupuestaria y eficiencia operativa	97
6.3 Infraestructura tecnológica y cooperación Inter agencial	97
6.4 Centro de Detección de Terroristas (TSC).....	98
6.5 Mejoras de infraestructura y fortalecimiento institucional.....	99
6.6 Evaluación general y perspectivas estratégicas.....	101
Conclusión del Capítulo VI	102
Referencias Capítulo VI.....	104
CAPÍTULO VII – Proyectos Especiales.....	105
7.1 Introducción	106
7.2 Proyecto Webhouse	107
7.2.1 Objetivo general	107
7.2.2 Alcance e implementación	107
7.2.3 Funcionalidades y ventajas operativas.....	107
7.3 Proyecto Trilogy	108
7.3.1 Modernización de infraestructura	108
7.3.2 Integración de sistemas	108
7.3.3 Fase II: Consolidación operativa.....	109

7.3.4 Fase III: Integración total.....	110
7.4 Evaluación general.....	110
Conclusión del Capítulo VII	111
Referencias Capítulo VII.....	113
CAPÍTULO VIII – Los incidentes terroristas (2002–2005)	114
8.1 Introducción.....	114
8.2 Año 2002: Emergencia del terrorismo ecológico y prevención ideológica.....	115
8.2.1 Incidentes terroristas.....	115
8.2.2 Prevenciones terroristas.....	116
8.3 Año 2003: Expansión del extremismo ecológico y resurgimiento del terrorismo ideológico.....	117
8.3.1 Incidentes terroristas.....	117
8.3.2 Prevenciones terroristas.....	118
8.4 Año 2004: Intensificación del ecoterrorismo y consolidación del extremismo religioso.....	118
8.4.1 Incidentes terroristas.....	118
8.4.2 Análisis y respuesta institucional.....	119
8.5 Año 2005: Persistencia y sofisticación del extremismo.....	119
8.5.1 Incidentes terroristas.....	119
8.5.2 Prevenciones terroristas.....	120
8.6 Conclusiones generales.....	120
Conclusión Capítulo VIII.....	122
Referencias Capítulo VIII.....	124
Conclusiones Generales	125
Bibliografía general.....	132
Índice.....	136