



Doctrina de la Actividad de Inteligencia

BRASILIA
Noviembre 2023



**PRESIDENCIA DE LA REPÚBLICA
CASA CIVIL
AGENCIA BRASILEÑA DE INTELIGENCIA**

Doctrina de la Actividad de Inteligencia

REPÚBLICA FEDERATIVA DE BRASIL
Presidente Luiz Inacio Lula da Silva

CASA CIVIL
Ministro Rui Costa

AGENCIA BRASILEÑA DE INTELIGENCIA (ABIN)
Director general Luiz Fernando Correa

SECRETARÍA DE PLANEAMIENTO Y GESTIÓN
Secretario Rodrigo de Aquino

ESCUELA DE INTELIGENCIA
Director Marco Cepik

COORDINACIÓN
Coordinación de Doctrina e Inteligencia / Escuela de Inteligencia

CATALOGACIÓN BIBLIOGRÁFICA INTERNACIONAL Y NORMALIZACIÓN
División de Conocimiento y Memoria / Escuela de Inteligencia

EDICIÓN GRÁFICA
Coordinación de Comunicación Social / ABIN

IMPRESIÓN
División de Servicios Gráficos / ABIN

PORTADA
Luciano Daniel da Silva / Coordinación de Comunicación Social / ABIN

AGENCIA BRASILEÑA DE INTELIGENCIA
SPO Área 5, quadra 1
CEP: 70610-905 – Brasília/DF

1a edição em espanhol: noviembre de 2024

Dados Internacionais de Catalogação na Publicação (CIP)

D726 Doctrina de la Actividad de Inteligencia. - Brasília:
Abin, 2023.

177 p.

Aprovada pela Portaria GAB/DG/ABIN/CC/PR
nº 1.205, de 27 de novembro de 2023.

1. Atividade de Inteligência - doutrina – Brasil.
2. Atividade de Inteligência - ensino. I. Agência
Brasileira de Inteligência. II. Título.

CDU 355.40(81)



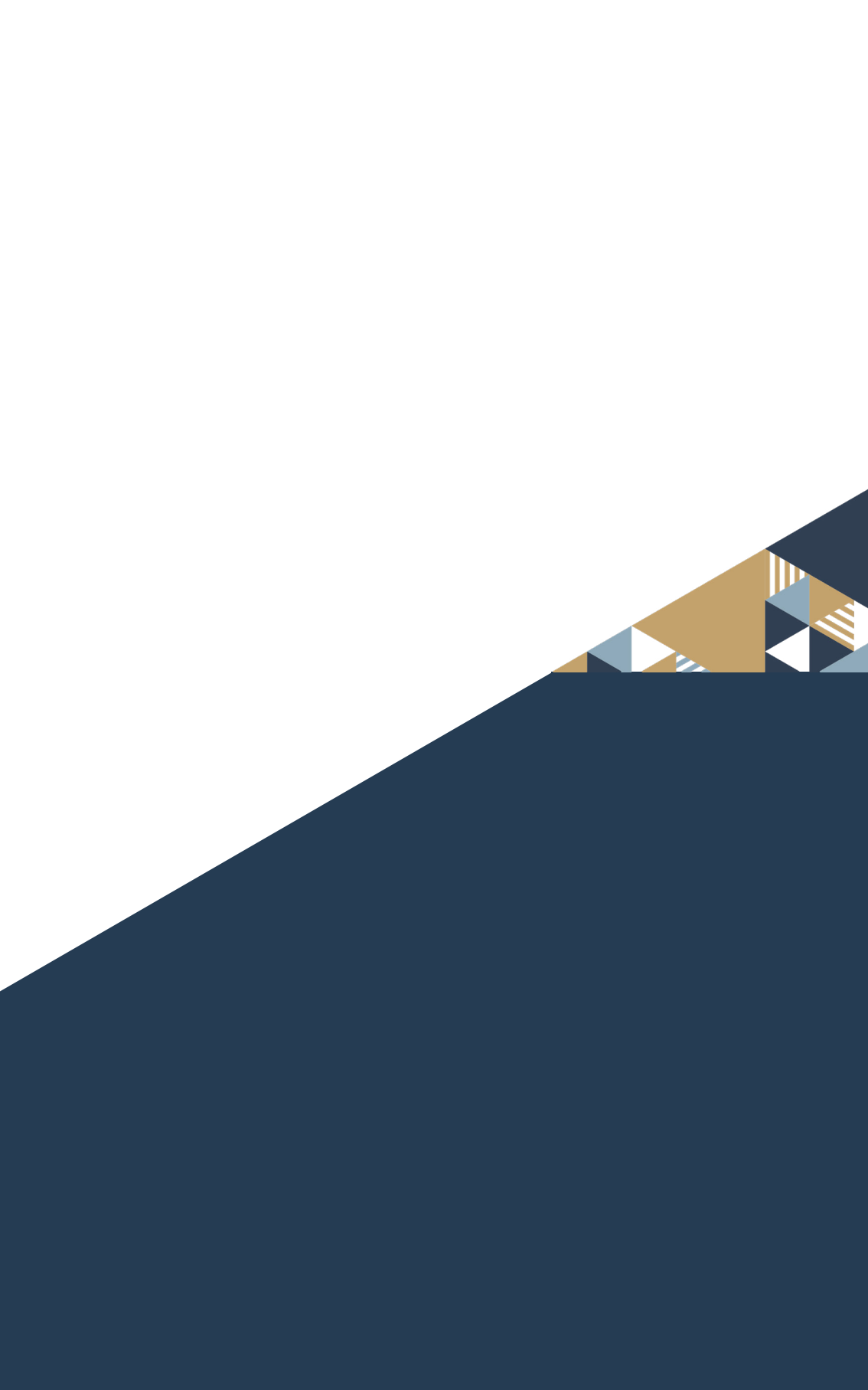
**Doctrina de la
Actividad de
Inteligencia**



Tabla de contenido

Presentación	7
2. Fundamentos de la Actividad de Inteligencia	11
2.1. Especialización	13
2.2. Democracia	20
2.3. Organización	23
2.4. Ética	27
2.5. Principios	31
2.6. Valores	36
3. Rama de Inteligencia	41
3.1. Clasificaciones	42
3.2. Ámbitos de actividad	51
3.3. Amenazas y oportunidades	54
3.4. Ciclo de inteligência	56
4. Rama de Contrainteligencia	63
4.1. Contrainteligencia preventiva	64
4.2. Contrainteligencia activa	71
4.3. Contrainteligencia y seguridad	76
4.4. Ciclo de contrainteligência	78
5. Elemento de Análisis	89
5.1. Aspectos teóricos	91
5.2. Insumos para el análisis	99
5.3. Conocimiento de inteligencia	103
5.4. El ciclo de análisis	105
5.5. Técnicas de apoyo al análisis	116
5.6. Lenguaje de la Inteligencia	123

6. Elemento Operativo	125
6.1. Aspectos teóricos	127
6.2. Tipos de acción	131
6.3. Ciclo de las operaciones	132
6.4. Técnicas operativas	137
7. Consideraciones Finales	139
8. Glosario	143
Fuentes y Lecturas Adicionales	173





1

Presentación

1. Presentación

Este documento es la versión actual de la Doctrina sobre Actividades de Inteligencia adoptada por Agencia Brasileira de Inteligencia (ABIN). Es importante aclarar qué se entiende por doctrina y cuáles son los objetivos de esta publicación.

El término doctrina se refiere a un conjunto de principios que sirven de base para el funcionamiento de cualquier sistema de acción y reflexión. Se trata, por tanto, de un conocimiento declarativo, siempre sujeto a crítica, flexible y provisional. Este conjunto de principios contribuye a educar y orientar las prácticas individuales y colectivas de una organización. Para cumplir adecuadamente esta función, una doctrina debe ser clara, parsimoniosa, autocrítica y revisable. Este es el caso que nos ocupa, ya que se espera que esta versión de la doctrina se revise y mejore de vez en cuando.

La fuerza prescriptiva de una doctrina es necesariamente menor que la de una ley. Además, las doctrinas son insuficientes como fuente de conocimiento y base para la acción, ya que los modelos descriptivos, los métodos y las teorías explicativas también siguen siendo necesarios para resolver los desacuerdos sobre cuestiones de hecho y de valor. Las doctrinas tampoco son capaces de predecir el futuro, ni siquiera de guiar todas las acciones en todos los contextos imaginables. Sin embargo, las doctrinas son importantes precisamente porque registran entendimientos conceptuales que proporcionan una base prescriptiva común para actuar en el tiempo y en el espacio. El objetivo de este documento es definir y explicitar al público la comprensión actual de ABIN sobre la actividad de inteligencia y cómo debe ser practicada por la Agencia en Brasil, con base en la Constitución Federal y en la legislación.

ABIN es un órgano de la Presidencia de la República dedicado a producir conocimiento para subsidiar las decisiones del Presidente de la República y de sus ministros. Sus funciones y actividades están previstas en la Ley 9.883/1999, que instituyó ABIN y creó también el Sistema Brasileño de Inteligencia (Sisbin). La organización y el funcionamiento del Sisbin están regulados por el Decreto 11.693/2023. De acuerdo con este decreto y con la Ordenanza GAB/DG/ABIN/CC/

PR número 926, en noviembre de 2023 el Sisbin contaba, además de ABIN como órgano coordinador, con once (11) órganos permanentes, nueve (09) órganos y fracciones de inteligencia dedicados y veintisiete (27) asociados. El nuevo reglamento también prevé la posibilidad de integración de órganos federales al Sisbin, siempre que se cumplan los criterios legales y de procedimiento.

El artículo 10, inciso XIV del reglamento también establece que una de las atribuciones de ABIN es fomentar y apoyar el desarrollo de la doctrina para las actividades de inteligencia en el país. Este documento no pretende sustituir o subordinar las doctrinas de inteligencia del sistema, subsistemas y demás organizaciones de inteligencia en Brasil. Disponer de doctrina propia es una obligación para ABIN. Su publicación pretende, en los términos del Decreto 11.693/2023, facilitar el diálogo y la sinergia entre los diversos componentes del Sisbin.

Los conocimientos de ABIN sobre las actividades de inteligencia son el resultado de sus propias experiencias desde la creación de la organización en 1999. También son el resultado de la incorporación de elementos considerados relevantes de otros documentos oficiales brasileños sobre diversas doctrinas, debates públicos en el Congreso Nacional y en el seno de la sociedad civil, producción científica y técnica sobre la actividad de inteligencia en Brasil y en el exterior, e incluso del conocimiento tácito disponible sobre el tema. Por tratarse de un documento de orientación destinado a facilitar la comunicación entre los miembros de la agencia y entre ésta y la sociedad, incluyendo las demás organizaciones responsables del desarrollo de la actividad de inteligencia del país, se decidió no indicar las diversas fuentes examinadas en cada página del documento. El lector interesado encontrará al final una lista preliminar de textos y documentos que inspiraron algunos de los juicios adoptados. Esas referencias sirven también como lectura complementaria para el avance del debate sobre la doctrina de inteligencia en Brasil. Muchas otras nociones y conceptos son fruto de la producción colectiva de personas que trabajan en el propio ABIN.

En este sentido, la Agencia es plenamente responsable de los conceptos, métodos, procesos, normas, principios y valores sistematizados en este cuerpo doctrinal.

La adopción de la Doctrina también permite aplicar dos principios adicionales: el control público y la impersonalidad en el comportamiento de los empleados de la Agencia. Por tratarse de una actividad que tiene el sigilo (forma de regulación pública y legalmente delimitada de determinados flujos de información) como instrumento y, en cierta medida, como condición de su eficacia, debe ser controlada tanto internamente, por la correcta dirección de sus actuaciones, como externamente, por los órganos previstos en la ley. Esta Doctrina expresa el compromiso de ABIN de reforzar estos controles y la impersonalidad en la aplicación de los procedimientos derivados de la comprensión común del significado de las acciones en el marco de un Estado Democrático de Derecho, razón y finalidad de la existencia de la propia ABIN y del Sisbin.

El texto se divide en ocho partes, además de esta Introducción. La Sección 2 presenta los fundamentos de la actividad de inteligencia tal como es entendida por ABIN. Esta sección explica el entendimiento de que la actividad de inteligencia se divide en dos ramas (inteligencia y contrainteligencia) y dos elementos (análisis y operaciones). Cada rama y cada elemento se analizan, respectivamente, en las secciones 3 a 6 del texto. En la sección 7 se ofrece una breve conclusión. El texto se completa con un glosario de términos utilizados (sección 8) y una lista (sección 9), incompleta y ejemplificativa, de obras consideradas relevantes para la redacción de esta doctrina y para el debate sobre el tema.

Feliz lectura.



2

Fundamentos de la Actividad de Inteligencia

2. Fundamentos de la Actividad de Inteligencia

La actividad de inteligencia produce conocimiento y realiza acciones destinadas a reducir vulnerabilidades y neutralizar amenazas a la seguridad de las personas y de las instituciones brasileñas. También tiene como objetivo proteger informaciones, personas, áreas, instalaciones y medios sensibles, previniendo, detectando, identificando, obstruyendo y neutralizando acciones adversas de inteligencia. En los términos de la ley, la actividad de inteligencia también identifica oportunidades para la realización de objetivos de política pública críticos para la seguridad y el bienestar de la sociedad.

En un mundo marcado por rápidas y radicales transformaciones globales en el clima, la demografía, la matriz energética y las tecnologías de la Era Digital, la coexistencia política entre distintas sociedades sigue estando definida en gran medida por la existencia de Estados soberanos, tal y como reconocen la Convención de Montevideo sobre los Derechos y las Obligaciones de los Estados (1933) y la Carta de las Naciones Unidas (1945). En el mundo hay casi doscientos Estados, muy desiguales entre sí. También existe una densa red formada por miles de organizaciones internacionales, así como una enorme diversidad de empresas, grupos, redes y miles de millones de individuos que persiguen distintos objetivos en todo el mundo. Cuando hay conflictos de intereses y de valores, no siempre los resuelven las instituciones internacionales formales e informales. Por lo tanto, la preservación de la soberanía popular y nacional, entendida aquí como la capacidad colectiva de los brasileños para tomar decisiones y actuar en los términos de su Constitución, es un imperativo que justifica y explica la necesidad de los servicios de inteligencia. También explica por qué, al igual que las fuerzas armadas y la diplomacia, los servicios de inteligencia existen en tantos países con sistemas constitucionales muy diferentes en el mundo contemporáneo.

En los términos del artículo 1º de la Constitución de 1988, la República Federativa de Brasil está formada por la unión indisoluble de los estados y municipios y del Distrito Federal. Esta unión se constituye como un Estado democrático de derecho y tiene como fundamentos la soberanía, la ciudadanía, la dignidad de la persona humana,

los valores sociales del trabajo y de la libre empresa, así como el pluralismo político. El artículo 3 de la Constitución define como objetivos fundamentales de esta República la construcción de una sociedad libre, justa y solidaria, la garantía del desarrollo nacional, la erradicación de la pobreza y de la marginación, la reducción de las desigualdades sociales y regionales, así como la promoción del bien de todos, sin perjuicio de origen, raza, sexo, color, edad o cualquier otra forma de discriminación. El artículo 4 define los principios que rigen las relaciones internacionales de Brasil, a saber, la independencia nacional, la prevalencia de los derechos humanos, la autodeterminación de los pueblos, la no intervención, la igualdad entre los Estados, la defensa de la paz, la resolución pacífica de los conflictos, el repudio del terrorismo y del racismo, la cooperación entre los pueblos para el progreso de la humanidad, la concesión de asilo político y la integración de los pueblos de América Latina.

Junto con los derechos y garantías fundamentales (Título II de la Constitución Federal), las normas y leyes constitucionales definen un conjunto de objetivos a ser alcanzados, así como los medios a ser empleados, por todos los brasileños, individual y colectivamente. Por lo tanto, toda actividad de inteligencia realizada en Brasil debe seguir los mismos principios, que constituyen las premisas básicas de la actual Doctrina ABIN. En los términos de la Ley n° 9.883/1999, de la Política Nacional de Inteligencia establecida por el Decreto n° 8.793/2016, y del Decreto n° 11.693/2023, complementados por otras disposiciones legales y administrativas legítimamente establecidas, la actividad de inteligencia en el Estado brasileño es realizada por organismos públicos, de forma constante y metódica, por profesionales especializados, asignados a estructuras propias de trabajo continuo, denominados órganos de inteligencia.

2.1. Especialización

Estas organizaciones pueden ser clasificadas como servicios de inteligencia, cuando su finalidad principal es la realización de actividades de inteligencia, o como unidades de inteligencia, cuando forman parte de órganos con otras finalidades. Los centros de inteli-

gencia de las fuerzas armadas, así como los departamentos de inteligencia de los organismos policiales y las oficinas de coordinación de inteligencia de otras instituciones federales, por ejemplo, pertenecen a organismos que tienen sus propios fines dentro del Estado. El Sisbin está formado por diversos órganos de inteligencia que apoyan el proceso de toma de decisiones del gobierno federal en áreas de política pública relacionadas con la provisión de seguridad pública, relaciones exteriores, defensa nacional y otras cuestiones críticas para el desarrollo nacional y el bien común.

Para llevar a cabo el trabajo definido por la legislación y las prioridades gubernamentales, los profesionales de inteligencia de ABIN vigilan diversos objetos definidos por la Dirección General de la agencia. Estos objetos se sitúan en entornos nacionales, internacionales, transnacionales o cibernéticos. Esta dimensión informativa de la labor de inteligencia (producción de conocimientos en apoyo de decisiones) es similar a la que realizan otros organismos de investigación, estadística y asesoramiento, pero centrada en cuestiones específicas de seguridad y conflictos. Además de la función informativa, la actividad de inteligencia también debe actuar en circunstancias determinadas por la ley. Dichas circunstancias incluyen la obtención de datos no disponibles, la protección de conocimientos, información y datos sensibles, así como de las personas, zonas, instalaciones y medios que los poseen o transmiten, y la prevención, detección, identificación, evaluación, obstrucción y neutralización de acciones de inteligencia adversas.

Para cumplir su doble misión, la actividad de inteligencia se organiza en dos ramas: inteligencia y contrainteligencia. Las ramas son áreas de especialización, que indican la aplicación de conocimientos específicos a la práctica de la actividad. En este sentido, no denotan una estructura organizativa específica, que es contingente y se define por decreto federal. Lo importante es garantizar que los profesionales que ejercerán cada tipo de actividad estén capacitados para ello y actúen de acuerdo con una base jurídica, institucional y doctrinal común.

Inteligencia es la rama de actividad centrada en la producción y diseminación de conocimiento relativo a hechos, eventos, situaciones

o fenómenos ocurridos dentro y fuera del territorio nacional, que tengan influencia inmediata o potencial en el proceso de toma de decisiones y en la acción gubernamental, y que constituyan o indiquen oportunidades o amenazas a los objetivos fundamentales del Estado.

Los hechos son objetos verificables que pueden describirse o predecirse. Así, un hecho es una representación lo más objetiva posible de la realidad externa al observador que trata de conocerla, y puede ser calibrado por cualquiera que utilice referencias conceptuales y métodos que puedan ser calibrados y validados.

Los acontecimientos son sucesos situados en el tiempo y el espacio. Un acontecimiento es un suceso que puede delimitarse geográfica y cronológicamente mediante hitos concretos. Los acontecimientos son producidos por mecanismos que vinculan contextos, estructuras y actores.

Las situaciones son acontecimientos contextualizados basados en la experiencia humana. Es a partir de las experiencias compartidas por una sociedad como se establecen las condiciones de interpretación de estos acontecimientos y, por tanto, se determinan las situaciones en las que se insertan. Para la inteligencia, las situaciones son una parte constitutiva de la realidad de los acontecimientos, ya que designan el contexto en el que deben evaluarse uno o varios acontecimientos en curso.

Los fenómenos son procesos constituidos por la evolución de hechos, acontecimientos y situaciones, la dinámica entre ellos y los efectos que producen a lo largo del tiempo sobre la experiencia humana y el mundo exterior.

Por ejemplo, la alta productividad del sector agroindustrial brasileño es un hecho. Las medidas adoptadas por países con organizaciones multilaterales de regulación de la competencia para bloquear las importaciones de productos agrícolas brasileños son hechos. La permanente competencia internacional por los mercados de exportación de productos agrícolas es una situación. La dinámica de formación de bloques comerciales internacionales a medida que se desarrolla el capitalismo global es un fenómeno que necesita ser monitoreado e interpretado.

A modo de ejemplo, la existencia de grupos criminales organizados es un hecho. Las rebeliones secuenciales en unidades penitenciarias, con represalias entre grupos criminales antagónicos, son hechos. Una dinámica de conflicto por el dinero y los territorios de influencia entre organizaciones delictivas, con impacto en la situación de seguridad de la sociedad, es un ejemplo de situación. A su vez, los flujos de oferta y demanda y las interacciones de la delincuencia organizada transnacional, que generan este entorno de tensión, constituyen un fenómeno que hay que seguir e interpretar.

Una oportunidad se entiende como una condición o factor favorable a la consecución de los intereses nacionales establecidos por la Constitución y la legislación; una amenaza se entiende como una oposición antagónica a la consecución de dichos intereses y a la salvaguarda de conocimientos y datos sensibles. Las amenazas pueden distinguirse según el grado de intencionalidad. Los antagonismos son amenazas que se oponen intencionadamente a la consecución de los intereses nacionales. Los óbices, por su parte, se interponen en el camino de los intereses nacionales, pero no expresan necesariamente la intencionalidad de un actor de causar daños, privaciones, violencia y sufrimiento a personas e instituciones.

Contrainteligencia es la rama de actividad que produce conocimiento y desarrolla acciones especializadas destinadas a prevenir, detectar, identificar, evaluar, obstruir y neutralizar actividades adversas de inteligencia, incluyendo acciones que constituyan una amenaza a los intereses de la sociedad y del Estado, al proceso de toma de decisiones, a la salvaguarda de conocimientos, informaciones y datos sensibles, a los medios que los poseen o transitan por ellos, a sus poseedores y a sus áreas e instalaciones.

La acción adversa se define como una acción intencional de uno o más actores, patrocinada o no, que se opone al logro de los intereses nacionales buscando ilegítimamente el acceso a conocimientos, informaciones y datos sensibles, amenazando la seguridad de las personas e instituciones de la República Federativa de Brasil. En el ámbito de la contrainteligencia, se monitorean y analizan las acciones adversas perpetradas por organizaciones e individuos que utilizan técnicas especializadas (inteligencia adversa), como el reclutamiento,

la entrada, la ocultación, la desinformación y la propaganda, entre otras. Otras acciones adversas, perpetradas por actores sin el uso de técnicas de inteligencia especializadas, son supervisadas y analizadas por la rama de inteligencia. Por lo tanto, las amenazas de las que se ocupa la contrainteligencia son siempre antagonismos y no meros óbices.

Prevenir es anticiparse a las amenazas en abstracto, con el fin de evitar que se materialicen o mitigar sus efectos. Detectar es descubrir una acción adversa planificada o realizada, ya sea finalizada o en curso, y comprender sus características. Identificar es atribuir a un agente (persona o entidad) la autoría o coautoría de la acción adversa, incluso como mentor o patrocinador intelectual. Evaluar es analizar, integrar y contextualizar la amenaza y sus perjuicios reales y potenciales para Brasil. Obstruir es impedir el inicio de una acción adversa cuya planificación ha sido detectada o interrumpir su desarrollo una vez iniciada. La obstrucción se produce mientras la acción no se haya completado. Neutralizar es anular o mitigar los efectos de una acción adversa que se ha completado o está en curso. La neutralización pretende eliminar o reducir el daño causado por la acción adversa emprendida.

Así, la función primordial de la contrainteligencia es contrarrestar la amenaza que supone la existencia de acciones adversas de inteligencia, ya sean patrocinadas por un Estado-nación extranjero o por una entidad no estatal. Se entiende que contrarrestar las actividades adversas de inteligencia, que utilizan técnicas especializadas, es más eficaz si lo hacen quienes conocen estas técnicas, es decir, otros profesionales de la inteligencia. Esta es la razón por la que la contrainteligencia es una función primordial de las agencias y ramas de inteligencia en casi todos los países.

Además de distinguir entre las ramas de inteligencia y contrainteligencia, es importante distinguir la actividad de inteligencia en dos elementos constitutivos: análisis y operaciones. En este caso, los profesionales de la inteligencia pueden estar más o menos especializados en cada uno de los dos elementos, pero la sinergia entre el análisis y las operaciones, con sus técnicas y métodos de trabajo propios, es una condición para la eficacia y efectividad de las unidades

y organismos de inteligencia, y también es fundamental para la legitimidad y eficiencia de sus funciones. En distintos países y organizaciones, los elementos de análisis y operaciones pueden asignarse a equipos especializados o incluso a organizaciones diferentes. Lo importante aquí es reconocer y destacar los requisitos de cada elemento.

El elemento de análisis se encarga de producir el conocimiento de inteligencia. Su principal función es informar. Para ello, los profesionales que actúan en este elemento recolectan y reúnen insumos, los procesan, los analizan y producen el conocimiento bajo la forma de reportes u otros productos, que son difundidos para las autoridades competentes por la dirección de los organismos de inteligencia. Los insumos para análisis son compuestos por datos, informaciones y conocimientos pertinentes para la comprensión del objeto que se analiza. La mayoría de los insumos procesados por la actividad de inteligencia está disponible y se los pueden acceder sin el empleo de técnicas sigilosas especializadas. No obstante, en muchas ocasiones puede ser necesaria la obtención de un insumo indisponible, lo que corresponde a la función del elemento de operaciones, obedeciendo a la demanda del elemento de análisis.

El elemento de operaciones se encarga de llevar a cabo acciones encubiertas especializadas para cumplir objetivos preestablecidos. Su función principal es ejecutar. Estas acciones tienen por objeto obtener insumos no disponibles, contrarrestar acciones adversas y crear situaciones favorables a los intereses nacionales. Es a través de las acciones operativas que la actividad de inteligencia actúa en el mundo. Son una forma de sortear obstáculos para alcanzar el objetivo fijado por los Estados en contextos conflictivos y adversos.

Es importante reiterar que la caracterización de la actividad de inteligencia como constituida por dos ramas (inteligencia y contrainteligencia) y dos elementos (analítico y operativo) no significa que todas las agencias de inteligencia del mundo necesiten o sean capaces de desarrollar esta actividad en su totalidad. Pero es, de hecho, una función estatal legítima y, en el caso de Brasil, por mandato legal, que forma parte de la evolución moderna del sistema internacional y de los Estados contemporáneos.

La obtención de datos e información para ayudar a un responsable de la toma de decisiones a determinar el mejor curso de acción es una actividad muy antigua. Sin embargo, durante mucho tiempo se utilizó esporádicamente, en situaciones de conflicto abierto, es decir, cuando existía una clara relación de adversidad. Así, los mandos militares trataban de conocer de antemano las capacidades de sus adversarios para prepararse mejor para la batalla. Del mismo modo, los jefes de unidades políticas en competencia económica trataban de estimar la situación de sus oponentes para posicionarse mejor en la disputa, adquiriendo ventajas competitivas sobre sus competidores.

Sin embargo, no existían estructuras permanentes y/o centradas exclusivamente en la obtención de datos e información, especializadas en proporcionar información para las decisiones gubernamentales. Esta situación cambió a partir del siglo XIX, cuando el desarrollo de la actividad de inteligencia se hizo más patente en las fuerzas armadas, las cancillerías y los organismos policiales y de seguridad de los distintos países. A partir de mediados del siglo XX, el contexto de la Guerra Fría y la descolonización afroasiática aumentaron el número de Estados en el sistema internacional y las condiciones tecnológicas, económicas, políticas y culturales en las que se desarrollaron estos servicios de inteligencia. Desde la década de 1990, con la globalización del sistema económico y jurídico internacional, impulsada por la transformación digital, los sistemas nacionales de inteligencia se han vuelto más complejos.

Hoy en día, los países suelen contar con una comunidad de inteligencia, que puede estar total o parcialmente articulada en un sistema. Esta comunidad está formada por los servicios de inteligencia, por fracciones características de sus tres raíces (militar, diplomática y policial), pero también por otras unidades especializadas en temas tan diversos como el medio ambiente o las finanzas, cuyo papel en la actividad se ha caracterizado posteriormente.

En Brasil, el Servicio Nacional de Inteligencia (SNI), creado en 1964 en el contexto de la dictadura militar (1964-1985), fue abolido en 1990. A principios de la década de 1990, la actividad de inteligencia en apoyo directo a la Presidencia de la República era llevada a cabo por secciones de inteligencia de la Secretaría de Asuntos Estratégicos.

cos (SAE). En 1994, se creó el Secretaría de Inteligencia de la Presidencia de la República, cuando se convocó el primer concurso público para contratar funcionarios para el organismo, de conformidad con la Constitución Federal de 1988.

En diciembre de 1999, tras deliberación del Congreso Nacional, la Ley 9883/1999 fue sancionada por el Presidente de la República, creando ABIN y Sisbin. La misma ley determinó la creación de una Comisión de Control de la Actividad de Inteligencia (CCAI) permanente por el Congreso Nacional, formada por diputados y senadores federales. Desde entonces, el Sisbin se ha desarrollado institucionalmente en un marco democrático y constitucional, aunque sujeto a crisis y necesitado de mejoras permanentes.

2.2. Democracia

El Estado en Brasil se compone de tres poderes separados y mutuamente necesarios: el Ejecutivo, el Legislativo y el Judicial. Las organizaciones de inteligencia brasileñas suelen ubicarse en el Poder Ejecutivo, como es el caso de ABIN, vinculada a la Casa Civil de la Presidencia de la República, y de los demás órganos y unidades que componen el Sisbin.

El cargo de Director General de ABIN es de carácter especial, para el cual la persona designada por el Presidente de la República debe tener su nombre aprobado por la CCAI del Congreso Nacional y por el plenario del Senado Federal.

La Constitución Federal de 1988 definió Brasil como un Estado Democrático de Derecho, constituido por tres poderes independientes y armónicos. Como tal, el pueblo tiene el poder de definir el rumbo del país mediante el voto y otras formas de participación popular. Se garantizan las libertades fundamentales de los ciudadanos, la impersonalidad de las decisiones y el ejercicio de las funciones públicas por los agentes públicos elegidos, los funcionarios y empleados públicos, así como los militares. Todos están igualmente obligados a cumplir la Constitución y las leyes. En 2021, la Ley n° 14.197/2021 añadió el Título XII al Código Penal brasileño, derogando la Ley de Seguridad

Nacional (1983) y definiendo los crímenes contra el Estado Democrático de Derecho. La preservación de la democracia es una cláusula fundamental de la Constitución Federal.

En Brasil, el Presidente de la República cumple las funciones de jefe de Estado y jefe de gobierno. Corresponde a la actividad de inteligencia asesorar a los sucesivos gobernantes, sin confundirse con ellos, actuando siempre de acuerdo con los designios legales y buscando el cumplimiento de los objetivos definidos por la Constitución. En otras palabras, corresponde a la inteligencia apoyar el proceso de toma de decisiones en el ámbito del Poder Ejecutivo, a fin de preservar la soberanía nacional, defender el Estado democrático de derecho y garantizar la dignidad de la persona humana, tal como lo establece el Decreto 11.693/2023.

Los gobiernos elegidos democráticamente ejercen el poder que emana de la voluntad soberana de la población, a través de elecciones periódicas, libres y seguras. La inteligencia, al asesorar a los sucesivos gobiernos, se ocupa de cuestiones relacionadas con la defensa nacional, las relaciones exteriores y la seguridad pública, pero siempre orientada a promover el desarrollo de toda la población nacional. Esta totalidad de personas afectadas por la ley en el territorio nacional debe ser alcanzada a través de la implementación de obligaciones de políticas públicas que reflejen y preserven su dignidad. Las políticas públicas se definen sobre la base de objetivos estipulados para la acción pública, seleccionados por los votantes mediante el voto, y se traducen en prioridades gubernamentales. Una de las principales expresiones de este proceso decisorio se consolida en el Plan Plurianual (PPA), que, en consonancia con lo dispuesto en el §1 del art. 165 de la Constitución Federal, debe contener directrices, objetivos y metas definidos con el fin de "posibilitar la implementación y gestión de las políticas públicas, orientar la definición de prioridades y contribuir a promover el desarrollo sostenible". Una vez elaborado, el Plan Plurianual debe presentarse al Congreso Nacional para su examen y aprobación.

En conjunto, los objetivos establecidos en la Constitución, las directrices gubernamentales y el PPA proporcionan una base sólida para la actualización periódica de la Política Nacional de Inteligencia

(PNI), la Estrategia Nacional de Inteligencia (ENINT) y el Plan Nacional de Inteligencia (PLANINT), los principales instrumentos sectoriales para orientar las acciones de ABIN y Sisbin.

En los regímenes democráticos, sin embargo, el control de la administración pública es fundamental para la realización de los derechos de los ciudadanos y el buen funcionamiento de la maquinaria estatal. Como función estatal, la actividad de los servicios de inteligencia debe ser controlada para garantizar que sigue siendo legal, analíticamente sólida y al servicio de la sociedad y del Estado democrático de derecho. Debido a su naturaleza parcialmente secreta, es necesario adoptar mecanismos de control específicos, además de los métodos ordinarios, tanto internos como externos al poder ejecutivo.

En el caso de ABIN, existen controles internos al poder ejecutivo de supervisión, ombudsman, asuntos internos y auditoría. El control interno ordinario es ejercido por la Contraloría General de la Unión (CGU). En el caso específico de ABIN, este control también es ejercido por la Secretaría de Control Interno de la Presidencia de la República (CISSET/PR). El Sistema de Integridad Pública del Poder Ejecutivo Federal (SIPEF), incluyendo la Comisión de Ética de la Presidencia y Vicepresidencia de la República (CEPR), también forma parte de ese control interno del Poder Ejecutivo. Leyes específicas, como la Ley General de Protección de Datos (LGPD) y la Ley de Acceso a la Información (LAI), refuerzan los mecanismos de transparencia y legitimidad de la actividad de inteligencia.

El control externo es ejercido por el Tribunal de Cuentas de la Unión (TCU), el Poder Judicial, especialmente el Supremo Tribunal Federal (STF) y la CCAI del Congreso Nacional. La CCAI tiene amplios poderes definidos por la Resolución 2 de 2013, que añadió las normas de la Comisión al Reglamento Común del Congreso Nacional. De acuerdo con la resolución, la CCAI es responsable de la supervisión y control externo de las ramas de inteligencia y contrainteligencia, así como de los elementos de análisis y operaciones, desarrollados en Brasil o en el extranjero, por cualesquiera órganos y entidades de la Administración Pública Federal, directos o indirectos, especialmente por los componentes del Sisbin. Esta Comisión podrá requerir a cada órgano o entidad del Sisbin la presentación de informes parciales,

generales y extraordinarios. Además, la CCAI está facultada para realizar inspecciones en áreas e instalaciones de los organismos que integran el Sisbin, con derecho de acceso a documentos y archivos.

La supervisión de la Política Nacional de Inteligencia (PNI) y de las acciones de ABIN es realizada por el Presidente de la República, el Ministro de la Casa Civil y la Cámara de Relaciones Exteriores y Defensa Nacional (CREDEN) del Consejo de Gobierno. Dentro del Sisbin, ABIN es responsable de coordinar y facilitar las actividades realizadas de acuerdo con el PLANINT.

La supervisión y el control de la actividad de inteligencia de ABIN son facilitados por la existencia de reglamentos como el Código de Ética, la Doctrina de Inteligencia, los Manuales de Procedimiento y las Instrucciones Normativas. Estos documentos ayudan a coordinar las acciones de las facciones que producen conocimiento de inteligencia y comunicación externa, por un lado, y, por otro, orientan la formación de los profesionales de inteligencia, tanto de los que analizan como de los que ejecutan las operaciones.

Antes de exponer los fundamentos éticos y morales de la actividad de inteligencia, es importante hacer una distinción adicional entre la comunidad de inteligencia y el sistema de inteligencia, para tener claro el ámbito específico en el que se desarrollan las actividades de ABIN.

2.3. Organización

La actividad de inteligencia, tal y como se entiende en esta doctrina, es llevada a cabo por organizaciones de inteligencia. Conviene reiterar que estas organizaciones pueden clasificarse como servicios de inteligencia, cuando su finalidad es la realización de actividades de inteligencia, o como unidades de inteligencia, cuando forman parte de organismos con otras finalidades.

Las organizaciones de inteligencia de un país constituyen su comunidad de inteligencia. El uso del término comunidad denota aquí el carácter informal y factual de las interacciones que puedan existir. Cuando la comunidad de inteligencia de un Estado, de un subconjunto

funcional o de un país está sujeta, en todo o en parte, a normas formales e institucionalizadas que rigen su interacción, se constituye un sistema de inteligencia. Cabe destacar que una comunidad puede ser más amplia e informal que un sistema. Muchos países ni siquiera establecen un sistema de inteligencia, dejando que la interacción entre sus miembros se produzca según las costumbres locales.

En Brasil, las agencias federales de inteligencia están organizadas en su propio sistema legalmente definido, el Sisbin. También existen subsistemas sectoriales, como el Sistema de Inteligencia de Defensa (SINDE), regulado por una Ordenanza del Ministerio de Defensa, o el Subsistema de Inteligencia de Seguridad Pública (SISP), regulado por un Decreto Federal. Lo importante es destacar que la comunidad de inteligencia del país es más amplia que el Sisbin, e incluye también instituciones estaduais y municipales, otros poderes del Estado y organizaciones privadas de interés para la actividad. En este sentido, el Decreto 11.693/2023, que reglamenta el Sisbin, constituyó un cambio significativo al establecer categorías, criterios y metas colectivas para la institucionalización del Sistema.

Además, ABIN y los demás órganos del Sisbin forman parte de una realidad fáctica que puede denominarse comunidad internacional de inteligencia. Los niveles de cooperación bilateral o multilateral alcanzan diferentes grados de institucionalización, en función de los lazos de confianza y acuerdos internacionales establecidos. Esta cooperación se da en temas de interés mutuo e involucra el intercambio de datos, informaciones y conocimientos, reuniones y eventos de formación de profesionales de inteligencia. Brasil forma parte de esta comunidad a través de sus agregados de inteligencia, establecidos con el objetivo de apoyar el trabajo de la diplomacia brasileña y fomentar los intercambios con los países en los que están acreditados, y a través de su participación en diversos grupos y foros multilaterales.

En 2023, con la publicación del decreto 11.693/2023, hubo una reorganización estructural del Sisbin. Esta reorganización tuvo cuatro pilares. En primer lugar, el refuerzo del papel de ABIN como facilitador y coordinador, definido como órgano central del sistema. En segundo lugar, el reposicionamiento del Consejo Consultivo, convirtiéndolo en una estructura consultiva de alto nivel formada por

Ministros de Estado. En tercer lugar, la clasificación de los organismos en categorías (permanentes, dedicados, asociados y federados). Por último, el cuarto pilar fue la definición de criterios y procedimientos para la inclusión efectiva de las unidades de la Federación en el Sisbin. En virtud del decreto, la creación de subsistemas también pasó a ser responsabilidad del órgano central, con el fin de organizar iniciativas sectoriales de integración de la inteligencia, por ejemplo, en el caso de la fiscalidad, las finanzas y el Tesoro.

El papel facilitador de ABIN como órgano central de Sisbin se expresa en las competencias previstas en el art. 10 del decreto 11.693, tales como "promover la cooperación entre los órganos y entidades miembros de Sisbin y la integración de sus actividades de inteligencia", o "coordinar las acciones integradas temporales o permanentes de los órganos y entidades miembros de Sisbin", o, sobre todo, "consolidar las necesidades específicas de conocimiento comunicadas por los órganos en los planes de trabajo".

El Consejo Consultivo fue reformulado por el Decreto 11.693 para clarificar su papel y el alto nivel de los miembros y temas tratados. Por ejemplo, el Consejo Consultivo se encargará de proponer actualizaciones del PNI y analizar los informes de gestión de los órganos del sistema. El Consejo está compuesto por el Ministro de la Casa Civil de la Presidencia de la República (que lo presidirá), el Gabinete de Seguridad Institucional de la Presidencia de la República, el Ministerio de Justicia y Seguridad Pública (MJSP), el Ministerio de Relaciones Exteriores (MRE) y el Ministerio de Defensa, además del Director General de ABIN.

La clasificación de los órganos en categorías promueve una mayor organicidad en el sistema, ajustando las expectativas en la participación de los miembros de acuerdo con las características de su categoría. El Decreto 11.693, en su 7º párrafo, nombró los órganos permanentes del Sisbin, que representan las principales expresiones del Estado brasileño, a saber: relaciones exteriores, defensa externa y seguridad interna. Estos componentes ya estaban previstos en el art. 2º de la Ley 9.883/1999, pero se añadió también la expresión gobernabilidad, representada por la Casa Civil de la Presidencia de la República y por la GSI. Los órganos permanentes expresan, por lo tanto,

funciones esenciales del poder del Estado (defensa externa, seguridad interna y relaciones exteriores), además de la gobernabilidad, que se aborda desde la perspectiva de la reducción de vulnerabilidades y de la seguridad de las personas y de las instituciones.

Los órganos denominados dedicados en el Decreto 11.693 son aquellos que cuentan con unidades (fracciones) dedicadas a la inteligencia, es decir, órganos con una cultura de inteligencia consolidada y mejores estándares de seguridad. Además, como parte de sus atribuciones, deben actuar en cuestiones estratégicas relacionadas con la Política Nacional de Inteligencia.

Las agencias que no tienen unidades dedicadas a actividades de inteligencia, pero que trabajan en cuestiones relacionadas con la Política Nacional de Inteligencia (PNI), pueden incorporarse a Sisbin como asociadas. El ingreso en las categorías dedicadas o asociadas depende del procedimiento de ingreso establecido en la Orden n° 925 del Director General de ABIN, de 6 de septiembre de 2023.

El procedimiento consiste en evaluar a los candidatos en relación con los siguientes criterios: función, sensibilidad de los datos, nivel de seguridad y recursos disponibles. El nivel más alto de servicio corresponderá a la categoría dedicada y el nivel intermedio a la categoría asociada. De este modo se fomentará la profesionalización y la seguridad en el Sisbin. El Decreto n° 11.693 y la Ordenanza n° 925 permiten que los órganos estadales y municipales se constituyan como entidades federadas en Sisbin, creando mayor seguridad jurídica para la cooperación que ABIN y los demás órganos de Sisbin desarrollarán con estos órganos y fracciones federadas.

En la nueva configuración establecida, ABIN tiene ahora mayor capacidad para colaborar con los trabajos de inteligencia desarrollados de acuerdo con los socios, a efectos de prestar un asesoramiento superior y rendir cuentas a la CCAI. Consisbin también contribuye como órgano oído en la valoración del informe de gestión de Sisbin. A su vez, ahora es obligación del órgano central, según lo establecido en el art. 10, XI del Decreto 11.693, "proporcionar herramientas para la comunicación segura y plataformas digitales para apoyar el intercambio de datos, información y conocimiento del SISBIN". Esta medida proporcionará mayor seguridad en el tráfico de documentos, mejo-

rando la trazabilidad de lo que se produce e intercambia en el Sistema. En definitiva, esta obligación refuerza el compromiso de ABIN con la mejora de los instrumentos de gestión y control.

Las instituciones democráticas, la soberanía y los intereses nacionales necesitan de un sistema de inteligencia ágil, coordinado, competente y legitimado, capaz de neutralizar amenazas e identificar oportunidades. En este sentido, el nuevo modelo operativo de Sisbin refuerza la necesidad de principios éticos y valores rectores comunes para todos los profesionales de inteligencia de ABIN y Sisbin.

2.4. Ética

El comportamiento ético es un componente esencial del trabajo de inteligencia. Es a través del comportamiento ético que se realiza el control social interno específico, es decir, el control ejercido por el propio profesional de inteligencia, por razones de conciencia, sobre sus acciones. Los profesionales de inteligencia son, ante todo, personas, ciudadanos brasileños y miembros del pueblo al que sirven. Su ética es profesional, como miembros de la administración pública, pero también es personal.

La distinción entre lo que es cierto y lo que es equivocado está en el centro de la definición del comportamiento ético. En su vida personal, cada ciudadano puede atribuir un valor relativo a ambos conceptos, en función de su entorno familiar y cultural. En su vida profesional, los funcionarios encuentran ya definidos estos valores de forma más constante, dentro del marco jurídico que delimita sus actuaciones. Lo cierto se refiere a respetar las normas vigentes y lo equivocado a violarlas. Así, en el ámbito profesional, el comportamiento ético es una forma de respetar el orden jurídico, constitucional e infraconstitucional, y la jurisprudencia; evitar costos personales, para sí mismo, para los demás y para el pueblo; y prevenir daños políticos, para el gobierno y para el Estado.

Además, los funcionarios públicos tienen una responsabilidad con el bienestar de la sociedad. Esta orientación sirve para matizar aún más la preocupación no sólo por el respeto a las normas, sino también

por su alcance y su posible impacto en el buen funcionamiento de la organización social vigente. Es en la instancia ética donde el pueblo deja de ser una pieza retórica, un icono para invocar la legitimidad, y se convierte en la referencia que garantiza la constitucionalidad de una decisión. La acción de gobierno queda así legitimada por la sostenibilidad ética de su finalidad. La constante preocupación por el bien público añade una capa adicional de atención a cuestiones éticas que no están necesariamente presentes en la vida cotidiana de los ciudadanos de a pie

De forma aún más contundente, los profesionales de los servicios de inteligencia están implicados en una tercera capa de preocupación ética. Debido a su trabajo especializado, a la necesidad de sigilo que rodea la producción de conocimiento y a la posibilidad permanente de acceder a datos sensibles, el profesional tiene que ser capaz de tomar decisiones éticas que van más allá de la simple distinción entre lo correcto y lo incorrecto y van más allá de la preocupación por el bien público y el bienestar de la sociedad.

El procedimiento ético representa también la defensa de la propia dignidad del profesional de inteligencia, ya que promueve el correcto desempeño de esta actividad. La discreción y la moderación que favorecen la actividad son rasgos de conducta que deben ser considerados para lograr la confidencialidad que la caracteriza. Dado que la labor de inteligencia es una profesión, debe considerarse que la profesionalidad en esta categoría implica un sentido de responsabilidad colectiva asociado a altos estándares de competencia técnica y un compromiso de servicio a los intereses sociales. Por lo tanto, debe ser de suma importancia que la actividad no sea objeto o medio de explotación política y económica.

El tratamiento responsable de la cuestión ética en la actividad de inteligencia implica reconocer que su producto se dirige al Estado y sólo con fines democráticamente legitimados. Estos fines están orientados a apoyar a las instituciones estatales en la formulación y ejecución de políticas, programas y operaciones tendientes al logro de objetivos nacionales, teniendo en cuenta los beneficios generados para la población. De este modo, la actividad de inteligencia se compromete a satisfacerse a sí misma y a los demás con sus acciones y a

actuar de la forma más competente posible. Dado que implica opciones y deliberaciones morales, su ejercicio es necesariamente susceptible de escrutinio ético.

Para tratar de la ética de la actividad de inteligencia, se señalan tres fuentes que pueden orientar a sus empleados como miembros de una categoría profesional específica: el código de ética profesional, los principios de la actividad de inteligencia contenidos en esta Doctrina y la literatura académica sobre el tema.

Específicamente en lo que se refiere al elemento de análisis, el principal aspecto de la ética que debe observarse es el deber de representar la verdad, incluso cuando esta representación sea inconveniente para el usuario del producto de inteligencia. Para lograr la veracidad, este profesional también debe respetar la metodología de producción del conocimiento de inteligencia, procurando evitar precipitaciones y suposiciones que conduzcan a la distorsión de la realidad. También se espera de los analistas de inteligencia que sean profesionales y adopten las medidas de seguridad adecuadas al tratar los insumos y conocimientos producidos, respetando el sigilo y la discreción inherentes a su trabajo. Aunque la actividad de inteligencia recurra al sigilo, en los términos de la ley, para garantizar la preservación de la seguridad de la sociedad y del Estado, sus acciones y las de sus profesionales están sujetas al escrutinio de órganos de control externo e interno.

En cuanto al elemento de operaciones de inteligencia, las acciones secretas se llevan a cabo en la búsqueda de datos, informaciones o conocimientos no disponibles o para contrarrestar amenazas adversas de inteligencia. Estas características imprimen a las acciones operativas un potencial que exige a los funcionarios implicados un mayor cuidado para actuar ética y legalmente. Todo funcionario es responsable de sus acciones, que deben respetar la legislación vigente y sus límites: cualquier orden manifestamente ilegal debe ser rechazada y no puede servir de justificación para un comportamiento inadecuado.

La legislación brasileña prevé el uso de operaciones de inteligencia para obtener datos y detectar, identificar, obstruir y neutralizar acciones adversas. Esta disposición, sin embargo, no permite la acción indiscriminada. Además de los principios éticos establecidos

en el Código de Ética Profesional de los Servidores Públicos, establecido por el Decreto 1171/1994, están los siguientes: impersonalidad en el trato con los blancos; respeto al estado democrático de derecho; y promoción de los intereses de la sociedad y del Estado.

Aunque secretas, las actividades de inteligencia deben estar sujetas a control interno y externo y ser lo más transparentes posible. La conducta ética protege el elemento operativo, promoviendo la actuación correcta y digna de sus profesionales. En este sentido, la planificación y ejecución operativa deben cumplir tres reglas:

- ◆ **Idoneidad:** los medios y técnicas elegidos conducirán al cumplimiento del objetivo de la acción encubierta.
- ◆ **Indispensabilidad:** los medios y técnicas operativas elegidos son alternativas necesarias para el cumplimiento del objetivo de la acción encubierta.
- ◆ **Proporcionalidad:** los medios y técnicas elegidos se llevarán a cabo en la medida estrictamente necesaria para el cumplimiento del objetivo de la acción encubierta.

Además, la conducta ética en las operaciones de inteligencia debe tener en cuenta ciertas reglas para el trabajo de los profesionales en este campo. La primera se refiere al hecho de que no se puede, bajo ninguna circunstancia o justificación, acceder a las herramientas y sistemas de que dispone el elemento de operaciones para uso personal o para satisfacer demandas ajenas a las misiones institucionales de la organización de inteligencia. El segundo se refiere a que los datos e informaciones de carácter personal obtenidos en el contexto del trabajo operativo que no sean relevantes para la finalidad de la acción encubierta no serán registrados ni almacenados por el elemento de operaciones y deberán ser eliminados de forma segura respetando la intimidad de sus poseedores. Por último, todo trabajo operativo deberá adoptar instrumentos de verificación e información sobre sus distintas etapas, con el fin de gestionar y controlar mejor el desarrollo de sus acciones.

En resumen, los deberes éticos de los profesionales de inteligencia son: representar la verdad; aplicar métodos en la elaboración

del conocimiento, rechazar las ilusiones y cualquier interferencia impenitente en el proceso de producción de conocimiento; promover el país a través de su trabajo; tratar a los sujetos de su trabajo con discreción; considerar la dignidad individual y el interés colectivo como referencia para la adquisición y producción de conocimiento; considerar, en el trato con extranjeros, el principio de reciprocidad y los derechos humanos; y reflexionar críticamente sobre la necesidad y las implicaciones morales de sus acciones y decisiones.

Estos deberes éticos impiden a los profesionales de la inteligencia transformar el conocimiento en poder, que es prerrogativa del usuario y sólo suya. Desde una perspectiva ética, la actividad de inteligencia no actúa en consideración de la sociedad y del Estado - dos entidades relativamente abstractas e impersonales - sino en consideración de las personas, de la población, del pueblo, como destinatarios de obligaciones constitucionales y democráticas. Esta atención es el principal recurso decisorio y técnico para que la actividad de inteligencia evite el sesgo político y participe en la construcción de un país mejor.

2.5. Principios

La actividad de inteligencia se rige por unas normas básicas de conducta, cuyo cumplimiento es imprescindible para su correcto y eficaz desarrollo. Estas reglas se dividen en principios generales, que abarcan la actividad en su conjunto, y principios sectoriales, que afectan específicamente a alguno de sus elementos constitutivos.

Se consideran principios generales de la actividad de inteligencia los siguientes: Control, Cooperación, Objetividad, Oportunidad, Trazabilidad, Seguridad, Simplicidad y Utilidad.

El principio de control determina que toda actividad de inteligencia debe estar sujeta a una supervisión que garantice la conformidad de sus medios y la correcta finalidad de su aplicación. Cuando se aplica al elemento de análisis, el principio de control asegura el estándar de calidad de los conocimientos de inteligencia estableciendo instancias de validación paritaria y de gestión tanto de los resultados

de las etapas metodológicas como del producto. Cuando se aplica al elemento de operaciones, el principio de control determina que las acciones trazadas estén coordinadas para evitar comprometer y dispersar esfuerzos. Las acciones paralelas y descoordinadas pueden dar lugar a reprocesos o dificultar la consecución de los objetivos. En este sentido, es necesario contar con un órgano de control de las acciones emprendidas, capaz de centralizar sus esfuerzos y resultados, garantizando así la eficacia de la actuación de este elemento.

El principio de cooperación prescribe que el trabajo de inteligencia se realice de forma colaborativa. Cuando se aplica al elemento de análisis, el principio de cooperación fomenta el trabajo de análisis en equipo y la optimización de los esfuerzos, de forma colaborativa, compartiendo insumos siempre que sea necesario, con vistas a los objetivos de producción y a la mitigación de sesgos. Aplicado al elemento de operaciones, el principio de cooperación establece y refuerza los intercambios que permiten optimizar los esfuerzos para alcanzar los objetivos trazados para cada acción a realizar.

El principio de objetividad exige que los profesionales de la inteligencia trabajen en pos de objetivos claros y definidos, evitando esfuerzos innecesarios y el despilfarro de recursos. Cuando se aplica al elemento de análisis, el principio de objetividad exige que los objetos del seguimiento analítico estén previamente definidos y delineados. Cuando se aplica al elemento de operaciones, el principio de objetividad significa que el objetivo de las acciones operativas debe ser claro y estar bien definido, para facilitar la planificación y la correcta aplicación de los recursos disponibles, reduciendo costes y esfuerzos.

El principio de oportunidad significa que el trabajo realizado por los profesionales de inteligencia debe producir resultados dentro de un plazo adecuado para ser utilizado eficazmente. Cuando se aplica al elemento de análisis, el principio de oportunidad indica que los esfuerzos de análisis y producción deben adecuarse al tiempo necesario para ser útiles al usuario de los conocimientos de inteligencia. Cuando se aplica al elemento de operaciones, significa que los resultados de las acciones operativas deben difundirse con tiempo suficiente para su utilización.

El principio de trazabilidad establece que las acciones realizadas en el marco de la actividad de inteligencia deben ser registradas de forma que se garantice que puedan ser auditadas de acuerdo con mecanismos e instrumentos previa y formalmente definidos. Cuando se aplica al elemento de análisis, el principio de trazabilidad determina que se mantenga el control sobre los procedimientos e insumos de producción, desde la obtención de datos, información o conocimiento hasta el producto, con el fin de garantizar que el proceso de desarrollo del conocimiento de inteligencia sea verificable, validable y auditable. Aplicado al elemento operaciones, el principio de trazabilidad exige que la planificación y ejecución de las acciones operativas estén debidamente registradas y controladas, con el fin de garantizar que el proceso llevado a cabo pueda ser verificado.

El principio de seguridad exige la adopción de medidas de salvaguardia adecuadas a cada situación, con el fin de garantizar que los conocimientos producidos y las acciones realizadas estén debidamente protegidos. Cuando se aplica al elemento de análisis, el principio de seguridad preconiza que estas medidas sean implementadas de forma a garantizar la correcta clasificación de los datos, informaciones, conocimientos e inteligencia obtenidos, procesados y difundidos por la actividad de inteligencia, así como protegerlos de exposiciones perjudiciales a la sociedad y al Estado. Aplicado al elemento de las operaciones, el principio de seguridad determina que el planeamiento y la ejecución de las acciones secretas deben garantizar la seguridad de la agencia de inteligencia, del equipo involucrado en su realización y de la propia acción.

El principio de simplicidad establece que las acciones llevadas a cabo por la actividad de inteligencia deben planificarse y ejecutarse de forma que se eviten la complejidad, los costes y los riesgos innecesarios. Aplicado al elemento de análisis, el principio de simplicidad indica que el proceso de producción de conocimiento debe privilegiar medidas simples de reunión, procesamiento y diseminación, resultando en conocimiento de inteligencia claro y accesible. Cuando se aplica al elemento de operaciones, el principio de simplicidad significa optimizar los recursos y reducir los esfuerzos operativos que no añaden valor al resultado deseado, reduciendo el tiempo, los costes y los riesgos. Esto implica que los esfuerzos deben dirigirse de forma

combinada, de lo más sencillo a lo más complejo, de lo más económico a lo más caro y de lo más seguro a lo más arriesgado, teniendo en cuenta la complejidad del entorno operativo y la importancia concedida a los resultados esperados.

El principio de utilidad significa que la actividad de inteligencia debe orientar sus resultados hacia las necesidades de quienes la utilizarán, proporcionando así un producto potencialmente útil. Cuando se aplica al elemento de análisis, el principio de utilidad indica que los temas, secciones y enfoques adoptados durante el proceso de producción de conocimientos tienen en cuenta el uso previsto de los conocimientos de inteligencia. Cuando se aplica al elemento de operaciones, la acción esbozada, su objetivo y su ejecución tienen en cuenta la utilidad que el resultado tendrá para quienes lo reciban, lo procesen y actúen en consecuencia.

Además de estos principios generales, cada elemento constitutivo de la actividad de inteligencia tiene principios que guían sus prácticas.

El elemento de análisis debe realizar sus acciones guiado por los principios generales de la actividad de inteligencia, así como por el conjunto de principios específicos de la profesión analítica: amplitud, imparcialidad y reflexión crítica.

El principio de amplitud establece que los objetos de análisis deben abordarse con el alcance necesario para dilucidar el tema propuesto de la forma más completa posible. Debe hacerse todo lo posible por agotar las posibilidades de reunir información sobre los objetos y sus posibles repercusiones en la conducta del país, a fin de garantizar una base coherente para la toma de decisiones.

El principio de imparcialidad determina que los objetos de análisis deben abordarse con imparcialidad, para evitar que juicios de valor derivados de intereses, convicciones personales o ideas preconcebidas distorsionen los resultados de la producción.

El principio de reflexión crítica exige que el analista sea muy crítico con su propia comprensión de la realidad. Para mitigar la incidencia de sesgos y heurísticas en el proceso de generación de conocimiento de inteligencia, las organizaciones deben invertir en inicia-

tivas para comprender estos fenómenos y en las herramientas para controlar sus efectos.

El elemento operativo debe desarrollar sus acciones guiado por los principios generales de la actividad de inteligencia, así como por el conjunto de principios específicos del oficio operativo: adaptabilidad, disponibilidad, finalidad, integración y resiliencia.

El principio de adaptabilidad estipula que la planificación y la ejecución de las acciones operativas permitan la aplicación rápida y eficaz de los ajustes y reorientaciones que sean necesarios. Las operaciones de inteligencia se llevan a cabo en entornos potencialmente inestables, complejos y hostiles, cuyas características pueden sorprender a los equipos sobre el terreno. Además, el contexto en el que se desarrolla la operación puede sufrir cambios imprevisibles. El elemento de operaciones debe ser flexible y capaz de adaptar sus acciones, absorbiendo las sorpresas y los posibles cambios y adaptándose a los nuevos contextos.

El principio de disponibilidad significa que el elemento de operaciones debe estar estructurado de forma que pueda activarse inmediatamente siempre que sea necesario, con el máximo alcance posible, teniendo en cuenta las amenazas enumeradas en los instrumentos que rigen la actividad de inteligencia.

El principio de finalidad estipula que las acciones secretas deben realizarse en apoyo de los intereses de la sociedad y del Estado, teniendo como lema el bien común. Estas acciones deben cumplir una finalidad colectiva, respetando lo establecido en el ordenamiento jurídico general, en la Política Nacional de Inteligencia y demás normas específicas de la actividad de inteligencia.

El principio de integración exige que el elemento operativo actúe de forma integrada, ordenada, sistemática y continua. La naturaleza híbrida y compleja de las amenazas y oportunidades, puntos de interés de las actividades de inteligencia, exige que los profesionales de inteligencia actúen con total sinergia metodológica y esfuerzo conjunto. Para que las acciones se desarrollen con fluidez, es necesario que trabajen de forma colaborativa, complementaria, integrada y armoniosa. Además, las operaciones de inteligencia suelen implicar

una variedad de recursos y el uso de diferentes técnicas en diferentes momentos. Por ello, es habitual que en las acciones operativas participen equipos formados por personas con múltiples competencias y diversos recursos técnicos. La integración de los medios y el carácter multidisciplinar del equipo operativo permiten asimilar y poner a disposición del equipo sobre el terreno todos los recursos necesarios para el buen desarrollo de la operación.

A su vez, el principio de resiliencia exige que los profesionales de operaciones sean resistentes a las dificultades y frustraciones, para poder percibir, evaluar y reaccionar rápidamente ante situaciones adversas y controlar sus acciones para no poner en peligro las acciones operativas que se están llevando a cabo. Los profesionales de la inteligencia suelen enfrentarse a contextos complejos y cambiantes. En el terreno, esta situación exige respuestas equilibradas y acciones de control.

2.6. Valores

Las acciones llevadas a cabo por la actividad de inteligencia se basan en un conjunto de características, cuya promoción se considera esencial para una acción segura, permanente y eficaz. Estas características son:

Formación continua de los profesionales de inteligencia

La naturaleza de la actividad de inteligencia exige que los profesionales que la llevarán a cabo estén debidamente preparados a través de procesos continuos de enseñanza, investigación y extensión. La utilización de técnicas especializadas, ya sean analíticas u operativas, exige la formación continua de los profesionales que actúan en ABIN. Para ello, es importante que estos profesionales asistan periódicamente a eventos de capacitación para mantenerse preparados para su trabajo. También es deseable que, siempre que sea posible, se compartan continuamente entre ellos experiencias, buenas prácticas, errores y lecciones aprendidas.

Los profesionales del elemento de análisis deben estar al día de los temas que supervisan y de las herramientas utilizadas en esta supervisión. La necesidad de mitigar los sesgos también exige invertir en el estudio de distintas disciplinas del ámbito de la psicología cognitiva -como la percepción, la emoción, el pensamiento y la conciencia- y la lingüística -como el lenguaje, el análisis del discurso y la semántica-. Además, es esencial animar continuamente a estos profesionales a desarrollar la creatividad, la criticidad reflexiva y la capacidad de mantener una actitud abierta hacia nuevas perspectivas sobre viejos temas.

Los profesionales del elemento de operaciones deben estar preparados para aplicar técnicas especializadas en un entorno hostil, una situación que plantea riesgos para la agencia de inteligencia y las personas encargadas de llevar a cabo sus acciones. Por lo tanto, la cualificación técnica del elemento de operaciones es esencial para su buen desempeño. Por ello, el elemento de operaciones debe favorecer el desarrollo sistemático de sus profesionales y el intercambio de experiencias entre equipos.

Fiabilidad de la seguridad

El sistema de gestión de la seguridad adoptado por la organización debe ser eficaz y fiable. La fiabilidad de la seguridad es un factor indispensable para construir la reputación de una institución, favorecer la interacción con otras agencias de inteligencia y disuadir posibles acciones adversas.

La disuasión es la capacidad de la institución para disuadir a su adversario de intentar llevar a cabo una acción adversa. Es importante que la institución pueda persuadir a su adversario de que los riesgos o costes de llevar a cabo la acción serían superiores a los beneficios. Es importante que los adversarios de la institución se den cuenta de que se han aumentado los niveles de seguridad y de que las acciones intentadas podrían suponer riesgos para sus agentes, así como para la imagen del patrocinador.

Además de ser un elemento disuasorio para el adversario, tener una alta fiabilidad de seguridad favorece la cooperación y la interac-

ción entre las agencias de inteligencia, lo que a su vez aumenta los datos disponibles para el seguimiento de sus objetos, generando contramedidas más eficaces y la evaluación de oportunidades.

Pensamiento crítico

Los profesionales de inteligencia están interesados en tomar conciencia del modelo mental que compromete la imparcialidad de su juicio. El pensamiento crítico es la forma de pensar en la que el sujeto pensante cuestiona constantemente el propio acto de pensar mientras piensa. Al hacerlo, mejora su modelo mental y profundiza en su capacidad reflexiva, lo que le permite aumentar la calidad de la respuesta resultante de su esfuerzo racional. Por lo tanto, pensar críticamente corresponde al proceso cognitivo del pensamiento impulsado por el trabajo consciente de pensar sobre el pensamiento.

El pensamiento crítico puede aprenderse y reforzarse mediante la repetición. Además de tomar conciencia de las propias presunciones y motivaciones, otro recurso para reforzar la criticidad es el entrenamiento en técnicas de precisión intelectual. Con cada juicio emitido, los profesionales de la inteligencia deben preguntarse sobre su claridad y precisión. También deben comprobar si la amplitud con la que se ha considerado y la profundidad con la que se ha tratado lo hacen pertinente. El resultado del trabajo mental también debe ser lógico para el interlocutor, significativo para la actividad y útil para el usuario. Este circuito evaluativo no se recorre de forma aislada, sino que se somete a otros profesionales entrenados para detectar fallos de razonamiento e incoherencias lógicas.

Junto a las medidas institucionales, los profesionales de la inteligencia dedicados al análisis también deben esforzarse por lograr una mejora constante que favorezca la mitigación de los efectos de los sesgos en los resultados de su trabajo. Esto incluye el desarrollo de un autoconocimiento continuo y la adopción de una actitud inquisitiva, colaborativa y sin pretensiones orientada al aprendizaje constante. Por lo tanto, es importante que el analista comprenda su propio modelo de pensamiento y cuestione su propio grado de imparcialidad. Esto significa tomar conciencia de cómo su trabajo está influido por

su historia personal, sus peculiaridades y sus tendencias políticas e ideológicas; y de cómo su condición social, su formación académica y su desarrollo profesional influyen en la construcción de su visión del mundo y su percepción de la realidad.

Orientación a resultados

Las acciones llevadas a cabo por la actividad de inteligencia se orientan hacia objetivos claros predeterminados por una autoridad competente. En sus dos funciones, informar y ejecutar, sus profesionales actúan para asesorar el proceso nacional de toma de decisiones y ayudar al país a alcanzar sus intereses nacionales. Así pues, esta actividad se lleva a cabo con vistas a la obtención de resultados.

La ejecución de las acciones analíticas debe estar siempre guiada por los objetivos del Estado, buscando adecuar el objeto analizado, su alcance y su enfoque a los intereses nacionales. Lo que define una acción analítica es su utilidad potencial para alcanzar los objetivos del Estado. Los esfuerzos analíticos deben tener en cuenta la relevancia del tema y la oportunidad de difundir el conocimiento, con el fin de garantizar la utilidad de su producto.

La ejecución de las acciones operativas debe guiarse por la adecuación de las demandas recibidas, los objetivos, los recursos disponibles, los riesgos implicados, las características de los blancos, el entorno operativo y las consideraciones éticas y jurídicas. Lo que orienta una acción operativa son los principios de eficacia, efectividad, eficiencia y legitimidad de los actos de la administración pública.

Transparencia activa

Brasil es un Estado democrático de derecho y, como tal, se rige por el respeto a la ley, a las libertades y derechos individuales y a la voluntad popular. Uno de los derechos a ser observados es el derecho a la información, del cual deriva la Ley de Acceso a la Información, Ley nº 12.527, de 18 de noviembre de 2011, y que constituye un elemento fundamental para la transparencia gubernamental. La transparencia en la gestión pública es un factor importante en la conducción del

Estado, ya que permite que la sociedad conozca lo que se está haciendo, facilita la evaluación de la administración por parte de la población y asegura que sus actividades sean fiscalizadas por los órganos competentes. No obstante, existen excepciones al derecho a la información. Los datos personales en poder del Estado, por ejemplo, no pueden ser consultados por terceros. Determinados procedimientos judiciales, por la naturaleza de su objeto, se desarrollan en sigilo, etc.

La actividad de inteligencia se ocupa de cuestiones relacionadas con la defensa y la seguridad. Actúa en entornos de competencia abierta o velada entre Brasil y otros actores de la escena internacional. Por eso, es importante que el planeamiento y la ejecución de sus acciones sean sigilosos. Se utiliza precisamente en aquellas ocasiones en las que es necesario buscar información de difícil acceso que garantice al Estado y a la sociedad ventajas competitivas en la persecución de sus intereses. Si estas acciones son previamente publicitadas, o si están abiertas a la consulta de cualquiera, incluidos los adversarios, la ventaja competitiva deja de existir.

El carácter sigiloso de la actividad de inteligencia, sin embargo, no la exime de establecer un diálogo franco, abierto y constante con la sociedad a la que sirve. Siempre que sea posible, debe aclarar sus acciones a la sociedad de forma segura. En este sentido, es esencial que sus agencias pongan a disposición de forma proactiva informaciones de interés público, cuya publicación perjudique poco el desarrollo de sus actividades.

Una vez definidos los fundamentos de la actividad de inteligencia tal como debe ser practicada por ABIN, es importante especificar los entendimientos doctrinarios de las ramas de inteligencia y contrainteligencia, así como los elementos del análisis de operaciones.



3

**Rama de
Inteligencia**

3. Rama de Inteligencia

Inteligencia es la rama de la actividad de inteligencia centrada en la función de información. Sus profesionales se encargan de obtener, procesar y difundir datos, informaciones y conocimientos relativos a hechos, acontecimientos, situaciones o fenómenos que constituyan o indiquen oportunidades o amenazas para los objetivos fundamentales del Estado. Su ámbito de producción abarca acontecimientos que ocurren tanto dentro como fuera del territorio nacional, con influencia inmediata o potencial en el proceso de toma de decisiones y en la acción gubernamental. La finalidad primordial de esta rama es asesorar al Estado en la consecución y protección de los objetivos nacionales y proporcionar elementos que ofrezcan ventajas decisorias al gobernante, observando los principios que rigen el Estado Democrático de Derecho y las relaciones internacionales de Brasil.

3.1. Clasificaciones

La producción de conocimiento en el campo de la inteligencia puede ser agrupada por su finalidad, su marco temporal o la naturaleza de los datos recogidos. Estas clasificaciones sirven para comprender mejor la naturaleza del trabajo a realizar y así optimizar las actividades de inteligencia, ayudando a crear nichos especializados entre sus profesionales.

Clasificación por finalidad

La clasificación por finalidad diferencia los productos de inteligencia en función de su alcance y del uso que se pretende dar a cada uno de ellos. En este sentido, el conocimiento puede apoyar la toma de decisiones sobre el diseño de una política pública (Inteligencia Estratégica), sobre las acciones propuestas para alcanzarla (Inteligencia Táctica), sobre la operacionalización de estas acciones (Inteligencia Operativa) o puede constituir la base para comprender el marco que da lugar a la adopción de dicha política (Inteligencia Básica). Cada

una de estas instancias requiere su propio enfoque para ayudar a producir un conocimiento que sea útil para el usuario y favorezca el asesoramiento en el proceso de toma de decisiones.

La finalidad de la Inteligencia de Base es construir un conjunto de fundamentos y referencias para comprender y contextualizar las cuestiones objeto de seguimiento, sirviendo de base para otros análisis con un enfoque más definido. Es el resultado del seguimiento temático ordinario realizado por los profesionales de inteligencia. El usuario de este producto es generalmente interno a la actividad de inteligencia y lo utilizará para producir conocimiento posterior.

El conocimiento producido en la Inteligencia Básica tiene por objeto comprender los hechos, acontecimientos, situaciones, actores, relaciones y datos estadísticos que caracterizan el objeto de estudio. Para producir conocimiento de fondo, el profesional considera el desarrollo histórico del tema analizado y de los actores relacionados con él, y recoge datos e información relevantes para la comprensión del tema y para apoyar inferencias y análisis posteriores.

El producto resultante de la Inteligencia de Base es el conocimiento narrativo-descriptivo o interpretativo, que relaciona acontecimientos y situaciones de interés para el usuario, permitiéndole conocer el contexto de un tema determinado. Eventualmente, este producto puede difundirse a usuarios ajenos a la agencia, con el fin de contextualizarlos sobre el tema u objeto.

Ejemplos de Inteligencia Básica son las explicaciones sobre la política interna de los países y sus instituciones, las estadísticas económicas y los estudios sobre la evolución histórica de actores de interés para la sociedad y el Estado.

El objetivo de la Inteligencia Estratégica es analizar e interpretar fenómenos que tengan potencial para impactar en los objetivos e intereses fundamentales del Estado. Esta inteligencia busca identificar tendencias y escenarios que puedan señalar amenazas y oportunidades para la sociedad brasileña y el Estado, asesorando la toma de decisiones sobre políticas públicas en los temas analizados.

La Inteligencia Estratégica monitorea las dinámicas y variables relacionadas con los fenómenos de interés, realizando investigacio-

nes dirigidas a su comprensión. Sus profesionales necesitan tener una comprensión consolidada de los temas monitoreados y ser capaces de analizar datos, informaciones y conocimientos, validarlos, interpretarlos y contextualizarlos.

El producto de la Inteligencia Estratégica es el conocimiento interpretativo o prospectivo sobre fenómenos de interés para la sociedad y el Estado. Ejemplos de Inteligencia Estratégica son las proyecciones a corto plazo sobre la situación política y económica de otros países y su impacto en Brasil; el seguimiento de fenómenos transnacionales, como las actividades de organizaciones criminales, grupos extremistas y ciberactores en forma de Amenazas Persistentes Avanzadas (APTs); y el análisis de demandas sociales recurrentes.

El objetivo de la Inteligencia Táctica es recopilar datos, información y conocimientos para apoyar el desarrollo de políticas gubernamentales previamente definidas. El conocimiento resultante de esta inteligencia tiene como objetivo asesorar en las decisiones relativas a la implementación de políticas públicas, buscando ayudar a la intervención del Estado. Es el resultado del seguimiento de situaciones y actores concretos.

A través de la Inteligencia Táctica, se observan los actores y variables relacionados con la situación del objeto de estudio, realizando investigaciones dirigidas a su comprensión. Al igual que en la Inteligencia Estratégica, sus profesionales necesitan tener un conocimiento consolidado del tema objeto de seguimiento, ser capaces de integrar e interpretar las fracciones significativas recientes y contextualizarlas para comprender y explicar la situación estudiada.

El producto de la Inteligencia Táctica es el conocimiento narrativo-descriptivo, interpretativo o prospectivo sobre una situación de interés para la sociedad y el Estado. Este producto debe ser útil para asesorar en la toma de decisiones sobre un caso concreto o en el marco de una política previamente determinada.

Ejemplos de Inteligencia Táctica son el análisis de la viabilidad de la implementación de una determinada política pública y sus probables desafíos; el sondeo de la posición de determinados países sobre la adopción o el apoyo a una determinada política internacional

de interés para Brasil; la caracterización del grupo responsable de un ciberataque; y el análisis de acciones que puedan promover el desarrollo nacional, en Brasil y en el exterior.

La Inteligencia Operativa tiene como objetivo contextualizar la acción concreta del Estado, en apoyo a la ejecución de acciones ya definidas en el ámbito de una determinada política pública. En este sentido, asesora sobre la operacionalización de esta acción. Resulta del monitoreo de hechos y eventos en curso, con énfasis en la obtención de datos para apoyar acciones estatales previamente establecidas. Para ello, la Inteligencia Operativa necesita conocer los planes de acción a apoyar y comprender el contexto en el que actuará el Estado.

El producto resultante de la Inteligencia Operativa es de carácter narrativo-descriptivo o interpretativo, buscando facilitar la toma de decisiones que implican la utilización de recursos humanos y logísticos en una acción determinada. Este producto no se desarrolla para la alta dirección del Gobierno, sino para los responsables de llevar a cabo las acciones planteadas.

Ejemplos de Inteligencia Operativa incluyen viajes preliminares para tratar la seguridad del jefe de Estado y otras autoridades en visitas oficiales; acciones para apoyar el despeje de tierras indígenas y la policía dirigida por inteligencia; e indicadores técnicos de ciberataques en curso.

Clasificación por marco temporal

La clasificación por marco temporal diferencia los productos de inteligencia según la distancia cronológica entre el producto y su objeto. Se refiere a la oportunidad del conocimiento que debe producirse, prestando atención al plazo adecuado para su utilización y al grado de anticipación que se espera de él. En este sentido, el conocimiento puede estar destinado a desarrollar escenarios para un futuro lejano, ayudando a determinar políticas a largo plazo; puede referirse a la evolución a corto plazo de situaciones actuales; puede acompañar acontecimientos en curso y anticipar situaciones que requerirán la intervención del Estado. Cada una de estas categorías requiere su propio enfoque para ayudar a producir conocimientos que sean útiles

para el usuario y favorezcan el asesoramiento en el proceso de toma de decisiones.

La Inteligencia de Alerta tiene como objetivo anticipar acontecimientos que puedan tener impacto en el cumplimiento de los objetivos constitucionales, el orden nacional o la seguridad de la sociedad y del Estado. Se basa en el diagnóstico y la predicción y resulta del seguimiento de amenazas, adversarios, actores hostiles, antagonismos u óbices a los objetivos fundamentales del Estado, con el fin de asesorar sobre la dirección de la acción estatal. El objetivo de esta inteligencia es dar tiempo a los responsables de la toma de decisiones para evitar las amenazas o mitigar sus efectos. Para ello se tienen en cuenta los actores antagonistas, sus antecedentes, intenciones, motivaciones y medios, que deben ser cartografiados y permanentemente monitorizados.

El producto de la Inteligencia de Alerta es la emisión de un aviso que contiene los indicios, con las representaciones adecuadas, que han dado lugar a la alerta, así como una descripción de la amenaza prevista y de la tendencia a que se produzca.

Ejemplos de Inteligencia de Alerta incluyen alarmas sobre situaciones sanitarias, económicas o políticas, y conflictos inminentes que puedan tener un impacto en la sociedad y el Estado, tanto en Brasil como en el extranjero. La Inteligencia de Alerta también puede utilizarse para anticipar situaciones adversas en el contexto del despliegue de fuerzas brasileñas en operaciones de mantenimiento de la paz.

La Inteligencia Actual se destina a mantener a las autoridades decisorias continuamente actualizadas sobre los acontecimientos y situaciones en curso y su evolución. Es de naturaleza objetiva, con enfoque descriptivo e interpretativo, y se mantiene atenta a los hechos y actores relevantes en el proceso monitoreado y en su desenvolvimiento. Para ello, la Inteligencia Actual considera toda la producción previa sobre la situación objeto de seguimiento, tratando de comprender qué actores y variables intervienen y cómo interactúan.

El producto resultante de esta inteligencia es el conocimiento descriptivo, breve, directo y periódico, en el que se informa de la evo-

lución de la situación o evento y, si es posible, el conocimiento interpretativo, con la tendencia de evolución a corto plazo. Ejemplos de Inteligencia Actual son el seguimiento de manifestaciones y paros con potencial de alterar el orden nacional; información sobre accesos ilegales a redes informáticas de infraestructuras estratégicas; seguimiento de emergencias y crisis económicas y medioambientales, tanto si ocurren en Brasil como en el extranjero.

El objetivo de la Inteligencia Explicativa es asesorar continuamente al proceso nacional de toma de decisiones sobre hechos, acontecimientos, situaciones y fenómenos que puedan representar amenazas u oportunidades para la consecución de los objetivos fundamentales del Estado. Es el resultado del seguimiento constante de cuestiones y objetos de interés para la sociedad y el Estado. Para ello, la Inteligencia Explicativa recopila datos, información y conocimientos sobre estas cuestiones y objetos, los contrasta con otros conocimientos y realiza breves proyecciones sobre su evolución.

El producto de esta inteligencia es un conocimiento descriptivo o interpretativo conciso, en el que se explica su objeto y se ofrecen claves para predecir su evolución. Ejemplos de Inteligencia Explicativa son las explicaciones de fenómenos de interés para la sociedad y el Estado, como las dinámicas sociales, las acciones de grupos extremistas, los ciberataques contra infraestructuras críticas, la interacción de actores en el ámbito internacional y las previsiones para el futuro próximo.

La Inteligencia Prospectiva pretende ofrecer escenarios sobre el futuro para asesorar sobre la dirección de la acción del Estado. Para ello, tiene un carácter diagnóstico y pronóstico y debe señalar las variables y actores que influyen en el fenómeno analizado e inferir su evolución en el periodo estipulado, así como la forma en que interactúan dichas variables y actores. Idealmente, indicará las evoluciones más probables del fenómeno en cuestión.

El producto resultante de la Inteligencia Prospectiva es el conocimiento interpretativo-prospectivo, utilizado para asesorar el proceso de toma de decisiones sobre acontecimientos futuros, resultante del estudio sistematizado de los elementos que han actuado en la trayectoria del objeto, con sus peculiaridades y valores, con el obje-

tivo de reducir incertidumbres y orientar mejores decisiones sobre el futuro. Ejemplos de Inteligencia Prospectiva son los estudios que anticipan la evolución de situaciones transnacionales, la posibilidad de beneficios o pérdidas en inversiones en países extranjeros, la pertinencia de firmar acuerdos internacionales y los resultados a largo plazo de grupos nacionales.

Clasificación por el origen de los datos

La clasificación por el origen de los datos diferencia la producción de conocimiento por las características de las fuentes de las que proceden los datos. Existen tres categorías en esta clasificación: Inteligencia procedente de fuentes humanas, Inteligencia procedente de fuentes técnicas e Inteligencia procedente de fuentes abiertas. Estas categorías y sus subcategorías se designan mediante siglas derivadas de sus nombres en inglés. Idealmente, estos diferentes tipos se complementan y validan mutuamente.

La principal característica de cada una de las siguientes categorías está relacionada con la naturaleza o el modo en que se generan u obtienen los propios datos, lo que impone diferentes medidas, necesidades y competencias para su tratamiento y procesamiento. Ello repercute en la planificación, utilización, análisis y alcance de los resultados presentados, lo que exige una especialización en la formación de los funcionarios. También permite establecer unidades específicas dentro de la agencia de inteligencia, con estructuras diferentes para la recolección y el análisis en cada categoría.

La Inteligencia Humana (*Human Intelligence* – Humint) es la inteligencia basada en datos obtenidos de las personas. Recoge datos, información, conocimientos y percepciones procedentes de informes elaborados por personas ajenas a la agencia de inteligencia o aportados por ellas. Su reto consiste en hacer frente a las lagunas de percepción y a las simplificaciones heurísticas naturales resultantes de las observaciones, interpretaciones, generalizaciones e intereses presentes en los relatos de las personas.

A la hora de analizar las aportaciones recibidas, hay que distinguir entre el origen de los datos (fuente) y el emisor a través del cual

llegan a conocimiento de la agencia de inteligencia (canal). Cuanto más lejana sea la fuente, mayor será la posibilidad de que los datos se distorsionen por el camino. Su correcta interpretación requiere la aplicación de técnicas de análisis del discurso y la percepción del lugar desde el que se emite, así como de los filtros por los que pasa hasta llegar al receptor.

La Inteligencia Técnica (*Technical Intelligence* - Techint) es la inteligencia basada en datos obtenidos por medios técnicos. Recopila información y datos a partir del uso de equipos que requieren experiencia en su manejo. Se basa en técnicas específicas para analizar cada tipo de información obtenida.

Las limitaciones generales de esta categoría de inteligencia son que requiere habilidades específicas para manejar el equipo y que necesita información adicional para obtener los datos para la contextualización. Se compone de varios tipos, cada uno con sus propias metodologías y técnicas de recolección y tratamiento de datos. Una lista no exhaustiva de tipos incluye: Sigint (Inteligencia de Señales); Imint (Inteligencia de Imágenes); Geoint (Inteligencia Geoespacial); y Masint (Inteligencia de Medidas).

La Inteligencia de Señales (*Signals Intelligence*) se basaba originalmente en datos obtenidos mediante la interpretación y descodificación de comunicaciones y señales electromagnéticas. Inteligencia de Señales era el nombre utilizado tradicionalmente para cualquier recopilación que no procediera de fuentes humanas, sino de equipos, y que por tanto no estuviera sujeta a la falibilidad humana a la hora de describir o comunicar datos, sino a las restricciones técnicas del dispositivo. Incluye, por ejemplo, grabaciones de audio, vídeo y fotografía realizadas con cualquier equipo. Con la evolución de los equipos electroelectrónicos, ha ido ganando subdivisiones relevantes. En las últimas décadas, el término Sigint también ha pasado a englobar la inteligencia producida a partir de datos obtenidos en el ciberespacio, entendido como el conjunto de infraestructuras informáticas y telemáticas interconectadas que comprenden hardware y software, datos y usuarios, y cualquier relación lógica entre ellos.

La Inteligencia de Imágenes (*Imagery Intelligence* - Imint) se realiza a partir de datos obtenidos mediante la producción de imáge-

nes fotográficas y multiespectrales. Puede ir desde la especialización en imágenes geoespaciales obtenidas por satélite hasta la evaluación de fotografías digitales o analógicas. Geoint (*Geospatial Intelligence*) se basa en imágenes y datos de geolocalización obtenidos para describir, evaluar y representar visualmente características físicas o actividades referenciadas geográficamente.

La Inteligencia de Medición (*Measurement Intelligence*) se basa en datos obtenidos midiendo ciertos tipos de emanaciones, como las sísmicas y térmicas, generalmente resultantes de firmas de eventos como explosiones atómicas. Se centra en elementos, rastros y patrones o firmas de mediciones, como patrones observados en radares, sonares o mediciones de elementos radiológicos, biológicos o químicos. Sus datos son generalmente descriptivos y no permiten por sí mismos la prescripción o el diagnóstico.

Entre los subtipos de Masint se encuentra la Acint (*Acoustical Intelligence*), Inteligencia Acústica, que es la inteligencia realizada mediante la recolección de datos de firmas acústicas obtenidas por buques, submarinos y, eventualmente, aeronaves que vuelan cerca de la superficie, como los helicópteros.

La Inteligencia de Fuentes Abiertas (*Open Source Intelligence* - Osint) es la inteligencia basada en datos de libre acceso. El término Osint adquirió relevancia con la llegada de Internet, pero también incluye otras formas públicas de obtener datos.

La Osint se lleva a cabo mediante técnicas especializadas de recolección metódica de los datos disponibles y se basa en medios propios de análisis de cada tipo de insumo obtenido. Utiliza datos, información y conocimientos procedentes de insumos disponibles para cualquiera, aunque el acceso sea de pago. Permite recolectar grandes volúmenes de datos, lo que hace posible identificar patrones de comportamiento. Las limitaciones de este tipo de inteligencia son que requiere mucho tiempo de investigación, así como una actualización constante y el dominio de las herramientas de recolección.

Una subcategoría de Osint es la Socmint (*Social Media Intelligence*) o Inteligencia de los Medios Sociales, que se centra en la información y los datos publicados en los medios sociales y los metada-

tos asociados a ellos. Este subtipo permite, por ejemplo, recolectar grandes volúmenes de información para analizar el sentimiento, los patrones de publicación y evaluar la relevancia de los temas de masas.

Interacción entre categorías

Los distintos tipos de clasificación presentados no se excluyen mutuamente. Existen muchas combinaciones posibles. Así, un tipo de conocimiento puede ser táctico, prospectivo y basado en datos e información recogidos por medios técnicos. Otro conocimiento puede ser estratégico, de alerta y proceder de fuentes humanas e imágenes. Y así sucesivamente.

En general, el conocimiento tendrá una única finalidad y un único marco temporal (que pueden combinarse de varias maneras), pero puede contener datos de distintas fuentes. Una vez obtenidos y procesados, estos datos se confrontarán, analizarán e interpretarán conjuntamente, siguiendo el proceso descrito en el apartado sobre el elemento de análisis.

El tipo de documento que se elabore dependerá del uso que se le vaya a dar. A veces, el solicitante pide un documento de una categoría determinada, para un uso específico a su discreción. Otras veces, el profesional de inteligencia responsable de la producción de un documento elige su categoría en función del uso que se prevé hacer de él, teniendo en cuenta la función de asesoramiento al proceso nacional de toma de decisiones.

3.2. Ámbitos de actividad

La rama de inteligencia sigue diversos temas y produce conocimientos sobre ellos. Algunos temas se circunscriben al ámbito interno, en el que los usuarios del conocimiento pueden ejercer un mayor grado de intervención, definiendo políticas y acciones gubernamentales. Otros tratan de fenómenos y situaciones que ocurren en la esfera internacional, donde las acciones del Estado dependen de su interacción con otros actores. Algunas cuestiones tienen implica-

ciones tanto internas como externas, lo que requiere un enfoque que abarque ambos aspectos del fenómeno. Por último, otras cuestiones están relacionadas con el ciberespacio, lo que requiere que el Estado actúe frente a las amenazas en este entorno.

Cada uno de estos tipos de producción implica escopo y enfoque propios, que tienen en cuenta el entorno en el que se tomará una decisión, los límites del poder del usuario en la materia y las alternativas para alcanzar los objetivos nacionales. El conocimiento de inteligencia producido en las distintas áreas de actividad debe ser capaz de contextualizar e informar al usuario sobre los hechos, acontecimientos, situaciones o fenómenos analizados, los actores y variables relacionados con ellos, así como las consecuencias de su ocurrencia para la sociedad y el Estado.

La Inteligencia Externa se ocupa de asuntos en los que el Estado tiene poco o ningún poder de decisión o intervención unilateral y que requieren estrategias de posicionamiento internacional para negociar y lograr los intereses nacionales. El foco de esta inteligencia es reunir datos, informaciones y conocimientos para comprender y contextualizar hechos, eventos, situaciones y fenómenos que ocurren en el contexto global, así como su impacto en la actuación de Brasil en el escenario internacional.

El conocimiento producido por la inteligencia externa permite a Brasil aprovechar oportunidades, contrarrestar amenazas y definir estrategias para alcanzar los intereses de la sociedad y del Estado en el exterior, respetando los principios que rigen las relaciones internacionales del país. Ejemplos de inteligencia externa son el seguimiento político y económico de otros países, los foros multilaterales de interacción entre países, la cuestión armamentística, la situación económica mundial y el asesoramiento en políticas culturales con el objetivo de promover la imagen internacional de Brasil.

La inteligencia interna, por su parte, se ocupa de cuestiones que son de competencia exclusiva de la intervención del Estado, respetando la situación política y jurídica del país. Su foco es reunir datos, informaciones y conocimientos para apoyar las acciones del Estado en el territorio nacional, asesorando en el diseño de políticas públicas de largo, medio y corto plazo.

El conocimiento producido por la Inteligencia Interna permite a Brasil definir estrategias para la realización de los intereses de la sociedad y del Estado en el ámbito interno, en cumplimiento de los objetivos y restricciones expresados en la Constitución Federal y en otras normas. Ejemplos de inteligencia interna son la observación de demandas sociales persistentes, el seguimiento de la implementación de políticas públicas y el monitoreo de la situación ambiental del país.

La inteligencia transnacional se ocupa de cuestiones transfronterizas, en parte dentro de la capacidad de intervención del Estado, pero que requieren negociaciones y asociaciones internacionales para adoptar políticas eficaces que permitan alcanzar los objetivos del Estado. Su objetivo es recopilar datos, información y conocimientos que apoyen las acciones de Brasil en cuestiones que trascienden el ámbito nacional al internacional y viceversa, ayudando al país a posicionarse de manera informada.

El conocimiento producido por la inteligencia transnacional permite a Brasil contrarrestar amenazas y definir estrategias para alcanzar los intereses de la sociedad y del Estado en cuestiones que exigen tanto el cumplimiento de los objetivos y restricciones expresados en la Constitución Federal y demás normas nacionales, como la aplicación de la política exterior del país. Ejemplos de inteligencia transnacional son el seguimiento del extremismo internacional que tiene vínculos o fracciones en Brasil, los fenómenos migratorios y el seguimiento de las organizaciones criminales brasileñas que operan en otros países.

La inteligencia cibernética se ocupa de cuestiones relacionadas con el ciberespacio, cuya naturaleza ubicua, distribuida y descentralizada implica una capacidad limitada de intervención estatal. Su foco es reunir datos, informaciones y conocimientos para apoyar las acciones de Brasil frente a las vulnerabilidades y amenazas cibernéticas, informando políticas públicas y planes estatales en esta área, así como monitorear y evaluar las capacidades, intenciones y actividades de actores externos en el ciberespacio.

El conocimiento producido por la inteligencia cibernética permite a Brasil identificar, caracterizar y enfrentar amenazas de origen estatal y no estatal en el ciberespacio, en cumplimiento de los

objetivos y límites expresados en la Constitución Federal. Ejemplos de Inteligencia Cibernética son el análisis de incidentes cibernéticos contra infraestructuras críticas, la atribución técnica de ciberataques y el asesoramiento en estrategias nacionales de seguridad y defensa cibernéticas.

3.3. Amenazas y oportunidades

La rama de inteligencia está orientada al reconocimiento de amenazas y oportunidades para la consecución de los objetivos e intereses fundamentales de la sociedad brasileña y del Estado. Estos objetivos e intereses se materializan en las diversas políticas públicas y en la planificación y ejecución de acciones que hacen posible que Brasil obtenga ventajas competitivas. En definitiva, se trata de comprender la realidad para promover una acción política capaz de generar el bien común. Así, se trabaja desde una doble perspectiva: aprovechar y explotar las oportunidades para alcanzar esos objetivos e intereses, e identificar y contrarrestar las amenazas para su consecución.

Las oportunidades son circunstancias favorables, acontecimientos que pueden aprovecharse para potenciar estos intereses y garantizar ventajas competitivas para el país. La búsqueda de oportunidades incluye la identificación e interpretación de hechos, acontecimientos o situaciones que pueden ayudar al país a alcanzar un estado mejor mediante la realización de sus objetivos fundamentales.

Las amenazas son circunstancias que dificultan la realización de esos mismos intereses, hechos que retrasan o impiden su consecución. En el contexto de la actividad de inteligencia, existen amenazas derivadas de acciones de inteligencia adversas que, por ser resultado del uso de técnicas especializadas, son objeto de seguimiento por parte de la rama de contrainteligencia. Todas las demás amenazas, sin embargo, pertenecen a la rama de inteligencia y deben ser vigiladas por ella.

En este sentido, las acciones extremistas pueden ser seguidas por la inteligencia, que contextualizará su ocurrencia, identificará y comprenderá a sus actores, y analizará e interpretará el fenómeno del

que forman parte. Sin embargo, cuando se perciba el uso de una técnica especializada en su ejecución, serán necesarias medidas de contrainteligencia para contrarrestar esta amenaza. Lo que delimita si una amenaza pertenece o no a la rama de inteligencia no es el asunto o tema al que está vinculada, sino si los agentes responsables de su ejecución son susceptibles o no de utilizar acciones especializadas de inteligencia.

En el ámbito de la inteligencia, las amenazas pueden ser intencionadas (antagónicas), es decir, dirigidas deliberadamente a impedir o dificultar la consecución de los intereses nacionales. Pero también pueden ser fortuitas (óbices), es decir, no destinadas a causar daño y, por lo tanto, no resultado de acciones específicamente dirigidas contra la realización de esos intereses. Diferenciar entre antagonismos y óbices es necesario para estimar la probabilidad de que estas amenazas persistan y esbozar la mejor manera de contrarrestarlas.

Así, los hechos, eventos, situaciones y fenómenos descritos, interpretados y explicados por la rama de inteligencia se definen en función de la realización de los objetivos fundamentales y de los intereses nacionales de la sociedad y del Estado brasileños. El desarrollo del conocimiento de inteligencia se orienta por estos objetivos e intereses y busca contextualizar a los usuarios en términos de factores favorables y desfavorables.

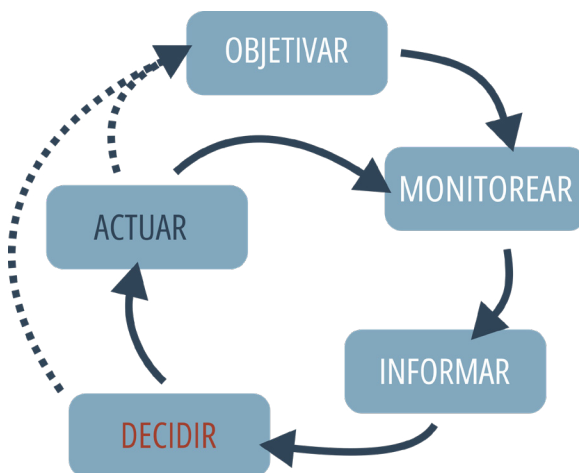


Figura 1: Ciclo de inteligencia

3.4. Ciclo de inteligência

El funcionamiento de la rama de inteligencia puede ser esquematizado en un ciclo compuesto por cinco fases, caracterizadas por acciones: objetivar, monitorear, informar, decidir y actuar. Las tres primeras fases son llevadas a cabo por las organizaciones de inteligencia, pero las dos últimas suelen tener lugar en otros ámbitos. La decisión corresponde siempre al usuario, y la acción a los organismos que éste determine.

Aunque las fases están dispuestas de forma ordenada con fines didácticos, debe tenerse en cuenta que las acciones de una fase pueden solaparse o fusionarse con las de la siguiente, dependiendo de la dinámica del asunto tratado.

El ciclo comienza con lo que aquí se denomina fase de objetivar, en la que se determinan los temas, apartados y enfoques de las áreas sobre las que trabajará la rama de inteligencia. Durante esta fase se definen los objetos de seguimiento continuo por parte de los profesionales de inteligencia. Es cuando la agencia de inteligencia evalúa los intereses y objetivos, expresos o implícitos, de la sociedad brasileña y del Estado.

El propósito de esta fase es concretizar las demandas que surgen de las políticas públicas, directrices y diagnósticos elaborados por las autoridades gubernamentales en objetos de monitoreo. Al especificar los temas clave para el procesamiento, se pretende que el trabajo de la organización de inteligencia sea más focalizado y eficaz.

La fase objetivar suele correr a cargo de la alta dirección de las organizaciones de inteligencia, basándose en los estímulos recibidos en su interacción con los usuarios. ¿Qué les interesa? ¿Cuáles son sus prioridades? ¿Qué metas quieren alcanzar en la búsqueda de los objetivos fundamentales del Estado? Son definiciones de alcance y finalidad que se revisan constantemente a la luz de las políticas adoptadas por el Estado brasileño.

Así como es importante comprender los intereses nacionales, es esencial que la agencia de inteligencia comprenda los contextos en los que estos intereses serán perseguidos o contradichos. ¿Qué intere-

ses pueden entrar en conflicto con los de Brasil? ¿Cuáles son los obstáculos y amenazas para su realización? Por otro lado, ¿qué oportunidades se vislumbran para su realización? ¿Cómo o de qué manera podrían aprovecharse estos contextos en favor de los objetivos fundamentales del Estado brasileño? Estas aportaciones ayudan a la agencia de inteligencia en su función de asesorar a los responsables de la toma de decisiones. La fase objetiva incluye la definición de las áreas que abarcará la rama de Inteligencia, su enfoque, los recursos que se asignarán y la organización del trabajo.

Al final de la fase objetivar, se espera que la agencia tenga una agenda de acción definida, dirigida a la consecución de los intereses de la sociedad brasileña y del Estado. Tradicionalmente, esta agenda se formaliza en el documento Plan de Inteligencia, que contiene las directrices de la actividad, los objetivos de inteligencia y los conocimientos necesarios para vigilar eficazmente las áreas de interés.

La segunda fase, seguir suele tener lugar de forma permanente a lo largo del ciclo. Implica el proceso constante de planificación, reunión y procesamiento de datos, información y conocimientos sobre las áreas objeto de seguimiento. Es la fase en la que el profesional de inteligencia examina el tema bajo su responsabilidad, definido en la fase anterior, buscando determinar el alcance, la función y la finalidad de la producción. Para ello, necesita comprender los intereses nacionales y los objetivos fundamentales del Estado en relación con su objeto.

El propósito de la acción de seguir, por lo tanto, es permitir que las unidades de producción de inteligencia perciban las amenazas y oportunidades para el logro de los intereses y objetivos mencionados, así como mantenerse actualizadas sobre los fenómenos que requieren la toma de decisiones por parte del poder ejecutivo federal. Este seguimiento es una parte vital de la base del asesoramiento que se proporcionará al proceso nacional de toma de decisiones.

En la fase seguir se realizan estudios para comprender los contextos en los que se inscriben los intereses nacionales y los objetivos fundamentales del Estado en cada zona. ¿Qué variables influyen en su realización? ¿Qué aspectos son favorables y cuáles desfavorables para su consecución? ¿Existen intereses contrapuestos? ¿Qué actores

se oponen a ellos? ¿Cuál es la capacidad de actuación de estos actores? ¿Cómo suelen actuar? El objetivo es capacitar a los profesionales de inteligencia para interpretar y contextualizar los hechos, acontecimientos y situaciones que se producen en estas áreas y que son de interés para la sociedad brasileña y el Estado.

Al final de la fase seguir, se espera que la organización de inteligencia esté al día sobre los objetivos fundamentales del Estado y los contextos en los que se inscriben. Esta fase se formaliza mediante mecanismos y herramientas de construcción de la Inteligencia Básica. Es deseable que los conocimientos resultantes sean accesibles a los profesionales de inteligencia que posean las credenciales de seguridad adecuadas y necesiten conocerlos.

Cuando el procesamiento indica que es necesario producir conocimientos pertinentes para la toma de decisiones, se pasa a la fase de información. Es entonces cuando el conocimiento producido se formatea y difunde a los distintos órganos de gobierno. Es la fase en la que la inteligencia describe, narra, contextualiza y explica a las autoridades competentes hechos, acontecimientos, situaciones o fenómenos que pueden indicar la necesidad de tomar decisiones sobre uno o varios ámbitos de interés de la inteligencia. Incluye las fases de formalización y difusión del conocimiento y es el resultado del seguimiento realizado en la fase anterior.

La fase de informar tiene lugar siempre que el equipo responsable de la vigilancia de un área determinada se percata de que se ha producido un hecho, suceso o situación que debe ser comunicado a las autoridades competentes, bien porque contribuye al diagnóstico de la situación, bien porque requiere la toma de posición del Estado. También puede ser el resultado de una petición explícita de un usuario para producir conocimiento sobre un determinado fenómeno y sus repercusiones.

Los medios de formalización y difusión de los conocimientos producidos deben tener en cuenta la oportunidad de su transmisión, es decir, los conocimientos deben estar disponibles a tiempo para su utilización. También deben tenerse en cuenta los requisitos de seguridad pertinentes para su tratamiento. Por lo tanto, hay que dar prioridad a la agilización del acceso a los conocimientos, pero sin descuidar

las capas de protección necesarias para garantizar la eficacia de los procesos de producción y utilización de los conocimientos. La difusión del conocimiento puede realizarse a través de documentos textuales, archivos de audio, imagen o vídeo, gráficos con datos consolidados o mediante la exposición en reuniones sincrónicas presenciales o a distancia, entre otros medios disponibles.

Al final de la fase de informar, se espera que se haya producido y difundido un conocimiento de inteligencia capaz de situar al decisor sobre el asunto objeto de seguimiento, su contexto, naturaleza, estado de desarrollo, impacto en la consecución de los intereses del Estado y consecuencias potenciales. Con este conocimiento, el órgano competente decidirá, en las dos fases siguientes, cómo actuar, teniendo en cuenta los recursos de que dispone el Estado. La fase de actuar será llevada a cabo por otros órganos gubernamentales encargados de ejecutar las políticas públicas relacionadas con el objeto del conocimiento.

Decidir es la fase en la que el decisor, en la instancia correspondiente, define cómo proceder en la búsqueda de la realización de un interés nacional. Uno de los elementos básicos de esta decisión debe ser el conocimiento de la inteligencia que considera el interés y su contexto y da lugar a la definición de una acción que el Estado debe poner en práctica. La complejidad de esta acción, las circunstancias de su puesta en práctica y sus implicaciones para el país determinarán qué órgano decidirá sobre esta acción.

Así pues, en esta fase se produce la deliberación, por parte de quienes están facultados para ello, sobre las medidas que deben aplicarse para alcanzar un objetivo, así como el orden derivado de dicha deliberación. La inacción y el acto de no decidir también son posibilidades para el decisor. El papel que debe desempeñar el profesional de inteligencia en esta fase es el de asesorar en el proceso de toma de decisiones, tomando como punto de partida los conocimientos de inteligencia difundidos en la fase anterior. Al final, se espera que la inteligencia haya ayudado al proceso de toma de decisiones sobre el asunto objeto de seguimiento, facilitando la toma de decisiones.

Actuar es la fase en la que el Estado adopta medidas y procedimientos para realizar lo decidido en la fase anterior. Después de

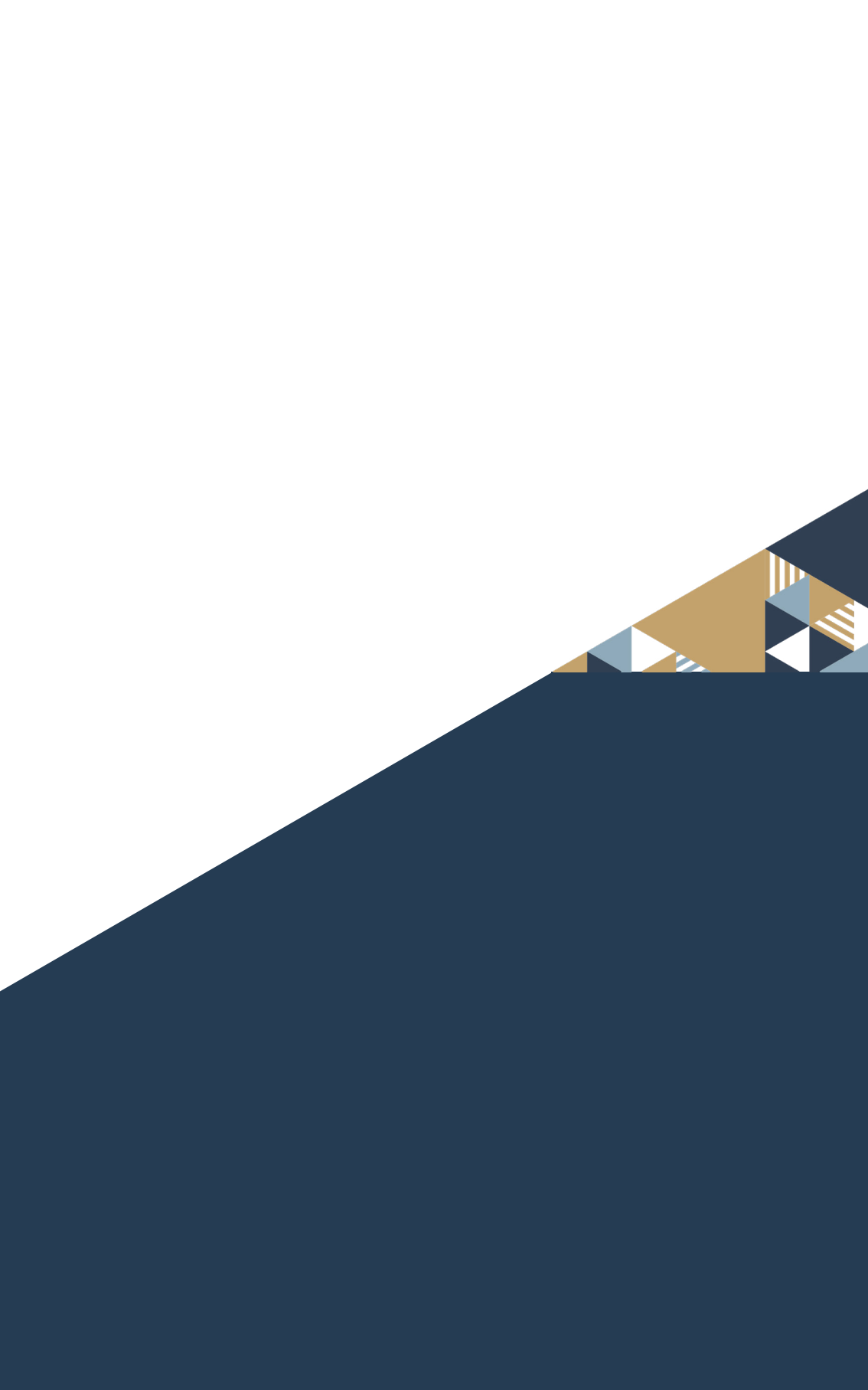
actuar, dependiendo del contexto, se puede adoptar más de un curso de acción al mismo tiempo. Se trata de acciones estatales que suelen implicar la actuación de otras instancias u organismos públicos. La finalización de la fase actuar no es responsabilidad de la agencia de inteligencia. Por el contrario, la ejecución de la acción definida en la fase de decidir es responsabilidad de otras instancias directamente involucradas en la ejecución de la política exterior y de las políticas públicas del país. Estos órganos pueden eventualmente solicitar la asistencia de la inteligencia, en los términos de la ley, generando nuevos conocimientos. Al final de la fase actuar, se espera que la inteligencia haya contribuido a crear condiciones favorables para la consecución de los objetivos nacionales.

Al final de la quinta fase del ciclo de inteligencia, se lleva a cabo una autoevaluación del proceso de asesoramiento, en la que se enumeran las mejores prácticas y las deficiencias observadas, con vistas a mejorar la actuación del servicio de inteligencia. A veces, será necesario redefinir el objeto mismo del seguimiento una vez aplicada la decisión. Las acciones emprendidas por los poderes públicos pueden dar lugar a modificaciones que, a su vez, provoquen cambios en el alcance y el enfoque de este objeto, añadan nuevos temas para el monitoreo o, por el contrario, indiquen que el alcance de esta área puede reducirse. En este caso, volvemos a la fase de objetivación. Sin embargo, si nada de esto es necesario, el objeto seguirá siendo objeto de seguimiento de acuerdo con las mismas premisas y directrices expuestas anteriormente.

La finalidad de la rama de inteligencia es, en primer lugar, asesorar con conocimiento de causa al proceso nacional de toma de decisiones sobre la consecución de los objetivos del Estado y, en ocasiones, actuar como instrumento facilitador de dicha consecución. Por lo tanto, es necesario que sus profesionales traten de comprender los intereses nacionales y la forma en que la inteligencia puede actuar para hacerlos realidad. Por lo tanto, además de conocer estos objetivos, uno de los aspectos fundamentales de esta rama es comprender la naturaleza, la dinámica y el papel de la inteligencia y cómo puede ser empleada por el Estado.

En definitiva, el ciclo de inteligencia ofrece un marco metodológico útil para el trabajo de los profesionales de la inteligencia, sistematizando los procedimientos en fases que se retroalimentan entre sí. Las acciones de la fase seguir se llevan a cabo de forma permanente, a partir de la definición de las áreas de actividad de la rama, consolidadas en la fase objetivar. La tercera fase, informar, se lleva a cabo idealmente cada vez que se produce un hecho, acontecimiento o situación que repercute en la conducción de las políticas públicas internas o en el posicionamiento externo del país, y debe ser comunicada a la autoridad competente. La fase de decidir tiene lugar necesariamente fuera de la agencia de inteligencia, por quien tenga el mandato o la prerrogativa de ejecutar la política gubernamental del país. Del mismo modo, la fase de actuar suele correr a cargo de los organismos responsables de dicha aplicación. La fase de seguir continúa una vez ejecutada la acción decidida, e incluye la supervisión de sus efectos y resultados. En ocasiones, tras la autoevaluación del proceso por parte de los profesionales implicados, se decide adoptar un nuevo enfoque o incluir un nuevo tema de seguimiento derivado de las fases de decidir y actuar. En esos momentos, el ciclo vuelve a la primera fase, objetivar.

Una vez comprendida la rama de inteligencia, es el momento de hablar de su homóloga, la rama de contrainteligencia, destacando las características que las diferencian.





4

**Rama de
Constrainteligencia**

4. Rama de Contrainteligencia

La contrainteligencia es la rama de la actividad de inteligencia que desarrolla acciones especializadas destinadas a prevenir, detectar, identificar, evaluar, obstruir y neutralizar acciones adversas de inteligencia que representen una amenaza para: los intereses del Estado y de la sociedad; el proceso de toma de decisiones; y la salvaguardia de conocimientos, informaciones y datos sensibles, los medios que los poseen o transitan por ellos, sus poseedores y las áreas e instalaciones. En este sentido, la contrainteligencia se orienta a la protección de los intereses del Estado, buscando dificultar la obtención de ventajas por parte de los adversarios y neutralizar las ventajas obtenidas mediante las acciones de inteligencia adversa.

Las medidas recomendadas por la CI se agrupan en dos segmentos: la contrainteligencia preventiva, relacionada con la anticipación y la protección frente a las amenazas, y la contrainteligencia activa, relacionada con la lucha contra las amenazas.

Esta división ayuda a hacer operativa la contrainteligencia, generando una su especialización en el trabajo de sus profesionales. No implica, sin embargo, que ambas áreas estén disociadas. Al contrario, son interdependientes. Las acciones llevadas a cabo por la contrainteligencia preventiva sirven de base a la contrainteligencia activa. Al mismo tiempo, las contramedidas llevadas a cabo por la contrainteligencia activa aumentan la percepción de seguridad y actúan como elemento disuasorio de otros intentos de acción adversa, lo que se refleja en la práctica de la contrainteligencia preventiva.

4.1. Contrainteligencia preventiva

Es el segmento de la contrainteligencia que propugna la adopción de medidas y procedimientos preventivos destinados a salvaguardar conocimientos, informaciones y datos sensibles y a sus poseedores, así como materiales, áreas, instalaciones, medios de producción y almacenamiento y canales de comunicación que interesan proteger a la sociedad y al Estado. También es el segmento que busca prevenir

acciones adversas de inteligencia destinadas a influir en el proceso nacional de toma de decisiones, como la interferencia externa, el terrorismo y el sabotaje.

Así, la contrainteligencia preventiva debe trabajar en colaboración con los objetos de interés adverso, es decir, los potenciales blancos de la inteligencia adversa, que pueden incluir personas, instituciones, instalaciones o información. Para ello, los profesionales de este campo deben evaluar los intereses de inteligencia de los competidores en el país e identificar los potenciales blancos de la acción adversa.

Asimismo, es importante que estos profesionales sepan determinar y priorizar los objetos que la sociedad y el Estado están interesados en proteger. Este segmento se basa en la evaluación de los riesgos percibidos por los objetos de interés adverso y las medidas de prevención y seguridad adoptadas por ellos, que deben ser adecuadas a su perfil y al contexto en el que operan.

La contrainteligencia preventiva se subdivide en las siguientes áreas: protección de conocimientos sensibles, protección de infraestructuras físicas y prevención de acciones que interfieran en la toma de decisiones.

Protección de los conocimientos

Es el aspecto de la contrainteligencia preventiva que propugna la adopción de medidas y procedimientos destinados a prevenir, detectar y obstruir antagonismos dirigidos contra los poseedores de conocimientos y datos sensibles, confidenciales o clasificados, el soporte físico que los contiene, el medio que los transmite y los lugares donde se encuentran sus poseedores, ya sean personas, documentos, materiales, medios informáticos y áreas e instalaciones. Los antagonismos, en el contexto de la contrainteligencia, son acciones planificadas con el objetivo de acceder a la información, sustraerla, difundirla o dañarla, poniendo en peligro su utilización. Pueden llevarse a cabo a petición de las instituciones interesadas o a sugerencia de la contrainteligencia, una vez identificado un objeto de interés adverso.

Los conocimientos y datos sensibles son aquellos que, por su importancia para el desarrollo y la seguridad del Estado y de la sociedad, requieren medidas especiales de protección. Conocimientos y datos sensibles son aquellos que, por ser indispensables para la seguridad personal de los ciudadanos, de la sociedad o del Estado, tienen difusión controlada y acceso restringido a personas autorizadas. Los conocimientos y datos clasificados son aquellos que, por su importancia para la seguridad del Estado o de la sociedad, tienen acceso restringido con cierto grado de sigilo. Estos conocimientos y datos serán desclasificados tras un periodo determinado por la legislación vigente, pudiendo entonces ser consultados y publicados.

Las acciones preventivas para proteger el conocimiento incluyen la concienciación, orientación y formación de las instituciones estratégicas nacionales para salvaguardar los activos de interés para el Estado y la sociedad, promoviendo la adopción de comportamientos y medidas de seguridad. La Contrainteligencia también puede identificar y evaluar vulnerabilidades en los sistemas de protección de la institución y hacer recomendaciones para reducir el riesgo de incidentes.

El trabajo de protección del conocimiento lo lleva a cabo un equipo e incluye la promoción de una cultura de protección del conocimiento en las instituciones asociadas; la identificación de amenazas; la detección de vulnerabilidades en los sistemas de protección de estas instituciones; la evaluación de riesgos; y el seguimiento de la aplicación de medidas para proteger sus conocimientos sensibles. La protección de los conocimientos es el resultado de la combinación de la comprensión de la forma de actuar de los agentes y las técnicas que utilizan para acceder indebidamente a datos restringidos y de las mejores prácticas reconocidas internacionalmente en materia de seguridad y gestión de la información. El trabajo de protección se lleva a cabo por capas, considerando cinco áreas didácticamente diferenciadas: gobernanza; personas; documentos y materiales; tecnología de la información y las comunicaciones; y áreas e instalaciones físicas. En la práctica, estas áreas se entremezclan.

La protección del conocimiento pretende permitir y garantizar las siguientes características para cada pieza de conocimiento, información y datos sensibles:

- ◆ Disponibilidad: la condición de estar disponible y ser utilizable a petición de una persona, organización, sistema o entidad determinada.
- ◆ Integridad: la condición de no haber sido alterada o destruida de forma no autorizada.
- ◆ Sigilo: condición de ser revelado únicamente a la persona, organización, sistema o entidad autorizada y acreditada para ello.
- ◆ Autenticidad: condición de identificar a quien lo ha producido, expedido, modificado o destruido.

Protección de infraestructuras críticas

Es el aspecto de la contrainteligencia preventiva que propugna la adopción de medidas y procedimientos destinados a prevenir, detectar y obstruir las amenazas de cualquier tipo dirigidas contra las infraestructuras críticas nacionales. Se consideran infraestructuras críticas (IC), según el art. 1, párrafo único del Decreto N° 9.573/2018 (Política Nacional de Seguridad de Infraestructuras Críticas), a las "instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, total o parcial, tendría un grave impacto social, ambiental, económico, político, internacional o de seguridad para el Estado y la sociedad".

La seguridad de las infraestructuras críticas, a su vez, pretende articular, en diversos ámbitos de los sectores público y privado, el desarrollo de procedimientos preventivos de seguridad de los recursos humanos, equipos, instalaciones, servicios, sistemas, información y otros recursos que garanticen el mantenimiento y funcionamiento de servicios y actividades indispensables para el Estado y la sociedad.

Cada Estado utiliza sus propios criterios para definir sus infraestructuras críticas. Así, lo que se considera infraestructura crítica para un Estado puede no serlo para otro. En cualquier caso, lo que hay

que proteger son las operaciones de infraestructura que se consideran vitales para el funcionamiento del Estado y el desarrollo de la sociedad. Por lo tanto, se hace hincapié en garantizar la continuidad de su pleno funcionamiento. Además, se trata de comprender el funcionamiento de las infraestructuras críticas y su importancia en los distintos sectores, de modo que se puedan cartografiar las repercusiones de una eventual paralización o destrucción de las infraestructuras.

Las infraestructuras críticas de Tecnologías de la Información y la Comunicación (TIC) tienen la peculiar característica de poder formar parte de varias infraestructuras críticas con relaciones de interdependencia horizontal, es decir, la información generada por una determinada área prioritaria de una infraestructura crítica de TIC puede ser un insumo para otra infraestructura crítica, demostrando así su alto grado de acoplamiento e interdependencia. Esto plantea la necesidad de identificar los activos de información esenciales, así como de abordar los riesgos a los que están expuestos, ya que el impacto causado por la pérdida o indisponibilidad de estos activos podría poner en peligro toda la cadena de infraestructuras críticas existentes.

Cuando no existe una lista exhaustiva de infraestructuras críticas en el ordenamiento jurídico, la criticidad de la infraestructura se evalúa a partir de indicadores relacionados con el impacto de su interrupción o destrucción. Para ello, se pueden adoptar criterios como la relación de dependencia entre ellas; los impactos intrasectoriales, económicos y poblacionales; el tiempo de reconstrucción en caso de destrucción; y el daño causado a la imagen del Estado. Son variables a tener en cuenta:

- ◆ Interdependencia, definida como la relación de dependencia entre infraestructuras críticas o la interferencia de una infraestructura crítica con otra, o de un área prioritaria de infraestructuras críticas con otra. Evalúa los impactos de una interrupción en el funcionamiento de la infraestructura (causada por cambios operativos o paralización) en otros sectores estratégicos para el Estado brasileño. Ejemplos: una central termoeléctrica que suministra energía a los aeropuertos (relacionada con el sector de los transportes); un bloqueo de carretera que impide el flujo de cereales, con impacto en el sector agrícola.

- ◆ El impacto poblacional inmediato, que se refiere al contingente de población que se verá directamente afectado por la paralización de la prestación de servicios resultante de la inactivación de la infraestructura. Ejemplos: número de personas que utilizan una autopista bloqueada; personas directamente afectadas por la paralización de un puerto. Las personas afectadas por el efecto cascada no se tienen en cuenta en esta evaluación.
- ◆ El impacto económico de la reconstrucción de infraestructuras críticas, que se refiere al coste de reconstrucción de infraestructuras en caso de destrucción de las mismas.
- ◆ El impacto intrasectorial, definido como el impacto de la paralización de la infraestructura dentro de su sector. Por ejemplo, una refinería paralizada afecta a la distribución de combustible; la paralización del aeropuerto de Brasilia repercute en el aeropuerto de Goiânia. El análisis de la contingencia permite evaluar opciones dentro del sector capaces de suplir la ausencia de la infraestructura evaluada.
- ◆ El tiempo necesario para reconstruir la infraestructura. En el caso de las autopistas, debe considerarse el tiempo necesario para reconstruir los puntos críticos para su funcionamiento.
- ◆ El daño a la imagen del Estado derivado de las repercusiones de la paralización o destrucción de la infraestructura, que conlleva una pérdida de confianza de la población en la capacidad del Gobierno para garantizar su bienestar y resolver el problema. Este criterio se refiere exclusivamente al impacto en la imagen del Estado y no tiene en cuenta otras repercusiones de la acción, como el impacto medioambiental de una catástrofe.

Prevenir las acciones de interferencia en la toma de decisiones

Este es el aspecto de la contrainteligencia preventiva que propugna la adopción de medidas y procedimientos destinados a impedir acciones adversas de inteligencia que pretendan interferir en el proceso nacional de toma de decisiones, en la conducción de políti-

cas públicas o en la consecución de los objetivos fundamentales del Estado.

Las acciones de injerencia en la toma de decisiones son las destinadas a intervenir ilegítimamente, incluso de forma velada o con el uso de la violencia, en el proceso nacional de toma de decisiones, en la conducción de las políticas públicas o en la consecución de los objetivos fundamentales del Estado. Tales acciones pueden ser directas, cuando tratan de persuadir directamente al responsable de la toma de decisiones, por ejemplo, mediante la influencia directa en un área determinada o el reclutamiento de personas con capacidad de decisión dentro del Estado. Pero también pueden ser indirectas, cuando utilizan diversos medios, como campañas destinadas a manipular la opinión pública. Las acciones indirectas también incluyen el uso de la violencia para crear conmoción popular o manipular la percepción que la comunidad tiene de un determinado acontecimiento o situación, provocando presiones sociales que interfieren en el proceso nacional de toma de decisiones.

Las acciones de interferencia sobre la decisión difieren de las acciones de influencia, que son formas legítimas y manifiestas de persuadir al proceso de toma de decisiones para que mantenga o modifique su comportamiento. Los elementos constitutivos de la influencia legítima son que el patrocinador de la acción es ostensible y conocido; el objetivo del patrocinador es transparente; y las tácticas empleadas en la acción son consideradas legítimas por el Estado.

Cada país tiene su propia interpretación de qué tipo de influencia extranjera es aceptable o inaceptable, si está determinada legalmente o es implícita políticamente. Esta definición tiene en cuenta los riesgos o amenazas reales que la influencia extranjera supone para los intereses nacionales, los valores sociales y la soberanía del Estado. La forma en que los Estados se posicionan varía con el tiempo y en diferentes contextos políticos y jurídicos. En otras palabras, lo que puede considerarse una acción de influencia inaceptable en un momento determinado y a los ojos de un determinado actor, puede tratarse como influencia legítima en otro momento.

La prevención de las acciones de injerencia es el resultado de identificar y analizar a los actores que las llevan a cabo, sus objetivos

y su capacidad de actuación, y de comprender cómo actúan y las técnicas operativas que utilizan para llevarlas a cabo. Es más eficaz si se lleva a cabo en colaboración con los posibles blancos de la inteligencia adversa. Así, también es necesario cartografiarlos y orientarlos para que ellos mismos puedan establecer medidas que traten de impedir o dificultar la realización de acciones adversas.

En el caso de acciones de interferencia violenta, como atentados terroristas o extremistas, también se trata de orientar a los posibles blancos de estas acciones para que puedan adaptar sus niveles de seguridad a la amenaza percibida. Los individuos y grupos identificados como adversarios potenciales también son objeto de seguimiento con el fin de promover políticas de desvinculación y desradicalización.

A la hora de evaluar posibles acciones adversas, deben tenerse en cuenta los siguientes criterios:

- ◆ Alcance: este factor se define por el área a la que se dirige la acción, es decir, si pretende influir en decisiones o comportamientos del Estado brasileño en el ámbito interno, externo o transnacional.
- ◆ Grado de influencia: factor medido por el impacto que la realización de esta acción tendría en el proceso de toma de decisiones y en el comportamiento del Estado brasileño y de la sociedad en relación con un determinado asunto.
- ◆ Grado de violencia: factor determinado por su potencial estimado de causar daño.
- ◆ Potencial de coacción: factor establecido por la probabilidad de que la realización de esta acción presione o induzca un cambio en el proceso de toma de decisiones o en el comportamiento del Estado y de la sociedad brasileños en relación con una cuestión determinada.

4.2. Contrainteligencia activa

Es el segmento de la contrainteligencia que propugna la adopción de medidas y procedimientos destinados a detectar la acción

adversa e identificar al agente, así como evaluar, obstruir y neutralizar las acciones de inteligencia adversa. La contrainteligencia activa incluye el contraespionaje, la contra interferencia, la contrainsurgencia y el contraterrorismo.

Contraespionaje

Es la rama de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones de espionaje llevadas a cabo por agentes adversos.

El espionaje es toda actividad destinada a obtener sin autorización datos, informaciones o conocimientos sensibles, confidenciales o clasificados en beneficio de Estados, grupos de países, organizaciones, facciones, grupos de interés, empresas o particulares. Así pues, el espionaje se caracteriza por el acceso y la adquisición de datos, información o conocimientos que no serían accesibles al agente adversario sin la utilización de técnicas especializadas.

El contraespionaje (CE) es un esfuerzo continuo para contrarrestar las acciones de búsqueda llevadas a cabo por agentes adversos. Para ello, los profesionales de la contrainteligencia deben conocer los objetivos, intereses y capacidad de utilización de técnicas especializadas de los adversarios. Cuando se detecta una acción específica de espionaje por parte de la inteligencia adversaria, hay que analizar su fase de desarrollo y determinar sus efectos reales o potenciales. Se evaluará la acción y los probables intereses que la sustentan y se elaborarán estrategias de obstrucción o neutralización.

Contra interferencia

Es la vertiente de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones de interferencia perpetradas por agentes adversos que amenacen los intereses nacionales y la seguridad del Estado y de la sociedad.

La interferencia externa es una forma encubierta de proyectar poder y es un instrumento para influir en otros a fin de que modifiquen su comportamiento de acuerdo con los intereses del patrocinador de la acción. Su naturaleza encubierta sirve para moldear los acontecimientos a favor del patrocinador, que necesita permanecer oculto como requisito previo para lograr los resultados deseados.

Las acciones de interferencia externa tienen objetivos estratégicos definidos, que generalmente se centran en los ámbitos político-social o económico. En el ámbito político-social, entre los diversos objetivos posibles, la acción puede buscar influir directamente en el proceso de toma de decisiones; buscar distraer o manipular a un público específico; socavar el capital político y social del adversario; apoyar a grupos internos para cambios en las políticas públicas; o, en el extremo, cambiar el régimen político de otro Estado. En el ámbito económico, algunos de los objetivos frecuentes son perjudicar a los competidores; frenar el desarrollo tecnológico, económico o comercial; estimular los boicots; y desestabilizar los mercados.

Para lograr sus objetivos, los actores suelen articular múltiples acciones operativas y diversas herramientas que pueden no ser exclusivas de la injerencia exterior, combinando elementos manifiestos y encubiertos. Cuanto más compleja es una operación de injerencia exterior, más capaz es de articular tácticas e instrumentos para engañar y confundir a sus destinatarios.

Las acciones de injerencia exterior pueden clasificarse en función de su objetivo, los medios utilizados y el nivel de ofensividad. A continuación, se presentan algunos ejemplos de acciones de injerencia exterior.

La propaganda adversa es el conjunto de acciones llevadas a cabo utilizando técnicas y métodos mediáticos para persuadir de alguna manera a los destinatarios e influir en su actitud, opinión, emoción y comportamiento. Estas acciones se llevan a cabo mediante la difusión de información recortada, manipulada o distorsionada contextualmente a través de canales directos y medios de comunicación, con el objetivo de promover los intereses ideológicos, políticos o económicos del patrocinador.

La desinformación es el conjunto de acciones que difunden deliberadamente información falsa, con la intención de engañar o confundir a un público específico para causar daño, inducir a error o manipular una situación o acontecimiento a favor de los intereses del patrocinador. En las redes sociales, la difusión de desinformación suele hacerse de forma inauténtica y coordinada. Para ser más eficaz, la desinformación debe contener elementos de veracidad o verosimilitud en su contenido.

El reclutamiento de agentes de influencia es la acción dirigida a la seducción y el control por entidades extranjeras de personas a las que se utiliza como instrumentos para enviar mensajes e interferir en la política, el mercado y la sociedad de forma que se favorezcan los intereses del patrocinador. Se puede reclutar a funcionarios públicos, políticos, académicos y personas influyentes, entre otros.

La promoción encubierta de grupos y organizaciones es un tipo de acción cuyo objetivo es crear, estructurar, financiar, cooptar o mantener de forma encubierta grupos u organizaciones que promuevan los intereses del patrocinador. Puede llevarse a cabo estimulando a un grupo preexistente o articulando un grupo originado en el contexto de la disidencia política que ya existe, aunque de forma latente, en la sociedad que se desea afectar.

El apoyo a la manipulación legal (*Lawfare*) es el uso de maniobras legales para intentar impedir o dificultar la consecución de los intereses de un adversario que entran en conflicto con los del patrocinador. Para apoyar y facilitar esta práctica manipuladora se utilizan habitualmente recursos típicos de la interferencia externa, como la desinformación, el reclutamiento, la propaganda adversa y la promoción de grupos y entidades que puedan actuar como partes en procesos judiciales.

El sabotaje es un tipo de acción dirigida a destruir, dañar, comprometer o inutilizar, total o parcialmente, los conocimientos, datos, materiales, equipos, instalaciones, sistemas logísticos, cadenas de producción e infraestructuras críticas del país, afectando así a la capacidad de satisfacer las necesidades esenciales de la población y los intereses del Estado. Las acciones de sabotaje pueden ser materiales, cuando se realizan sobre maquinaria, equipos o instalaciones;

químicas y biológicas, mediante la manipulación de explosivos, virus o bacterias; nucleares, con el uso de fuentes y elementos radiactivos; y cibernéticas, mediante invasiones y daños a sistemas y redes informáticas.

Contrainsurgencia

La contrainsurgencia es la rama de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones adversas de individuos y grupos insurgentes. Una insurgencia es una rebelión armada contra un poder establecido llevada a cabo o planeada por un grupo formado o apoyado por una parte de la población. Las insurgencias varían según el contexto en el que se producen, y pueden tener diversos aspectos sociales, culturales y económicos. Pueden llevarse a cabo mediante movimientos paramilitares, intentos de golpe de Estado, revoluciones, guerrillas, guerras civiles o guerras de liberación.

Contraterrorismo

El contraterrorismo es la rama de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones adversas de individuos y grupos extremistas violentos. El extremismo violento se refiere a la planificación, preparación, promoción, financiación y ejecución de actos violentos motivados por ideologías extremistas que desprecian preceptos constitucionales fundamentales. Según las ideologías extremistas, la violencia colectiva contra personas, grupos e instituciones que representan enemigos existenciales, o así los perciben, es una condición esencial para garantizar su supervivencia o poner en práctica su visión del mundo.

El extremismo violento es un concepto amplio. Permite incluir, por ejemplo, a personas y grupos que propugnan el uso de la violencia contra la sociedad o parte de ella, pero que aún no han cometido acciones que puedan calificarse de actos terroristas. El término extremismo

violento es una alternativa para describir ciertos comportamientos violentos en contextos en los que el término terrorismo carece de un significado uniforme e inequívoco, como cuando no existe consenso entre los Estados sobre la designación oficial de los grupos terroristas o cuando falta una legislación que tipifique el terrorismo o los actos terroristas.

Aunque no existe consenso sobre la definición de terrorismo, suelen asociarse al fenómeno las siguientes características utilización de la violencia y de la amenaza de violencia como táctica o estrategia de coerción y propaganda; utilización del terror como herramienta de guerra psicológica, generando miedo generalizado, ansiedad y sensación de inseguridad en la población; ataque a víctimas indiscriminadas, en el que los principales objetivos suelen ser civiles, no combatientes o personas indefensas o inocentes, sin responsabilidad directa en el conflicto que dio origen a los actos de terrorismo; carácter ilegal de los actos; y naturaleza predominantemente política de la violencia terrorista, observable en su motivación y en sus repercusiones en la sociedad.

En Brasil, la Ley 13.260/2016 define el terrorismo como la comisión por uno o más individuos de los actos previstos en el § 1 del artículo 2, por motivos de xenofobia, discriminación o prejuicio de raza, color, etnia y religión, cuando cometidos con el propósito de provocar terror social o generalizado, exponiendo a peligro a las personas, los bienes, la paz pública o la seguridad pública, con el propósito de causar terror.

4.3. Contrainteligencia y seguridad

Seguridad y contrainteligencia son conceptos relacionados, pero que no deben confundirse. La seguridad se refiere al mantenimiento de un estado de equilibrio que garantice la estabilidad para llevar a cabo acciones cotidianas o extraordinarias. La contrainteligencia se refiere a prevenir y contrarrestar acciones adversas de inteligencia, llevadas a cabo mediante técnicas especializadas.

La seguridad es un área multidisciplinar. No se limita al trabajo de los profesionales de inteligencia. De hecho, debe incorporar todo tipo de conocimientos que puedan elevar los niveles de protección y aumentar la percepción de seguridad y confianza de las partes implicadas. Esto incluye evaluaciones de protección civil, análisis de expertos técnicos en las áreas relacionadas con los riesgos percibidos y evaluaciones de amenazas por parte de otro tipo de profesionales, como científicos sociales, antropólogos, psicólogos, etc.

La seguridad es una parte esencial de toda actividad de inteligencia, que incluye la rama de contrainteligencia, pero no se limita a ella. La seguridad consiste en la protección contra todo tipo de amenazas, lo que doctrinalmente incluye antagonismos y óbices, es decir, acciones intencionadas y no intencionadas. La seguridad consiste en prevenir y gestionar los riesgos percibidos.

Toda organización de inteligencia debe prestar atención a los aspectos de la seguridad de sus zonas e instalaciones y de su personal, lo que incluye las rutinas de investigación social y el seguimiento del personal. Las organizaciones de inteligencia también deben ocuparse de la seguridad de sus prácticas. Son estas prácticas las que definirán la cultura de seguridad de la organización. Cuanto más sólida sea esta cultura, menos permeable será la organización.

La cultura de seguridad deseable en una agencia de inteligencia incluye observar el principio de compartimentación y no revelar asuntos de trabajo ni involucrarse en situaciones comprometidas que puedan dar lugar a presiones o chantajes. La seguridad debe ser observada por todo su personal, tanto interno como externo.

En cambio, la contrainteligencia tiene como objetivo oponerse a la inteligencia adversa, lo que incluye contramedidas activas. Todo su trabajo está dirigido a frustrar los esfuerzos de los adversarios para obtener una ventaja competitiva mediante el uso de técnicas especializadas.

La Seguridad Institucional es una actividad dentro de las organizaciones que se encarga de aplicar medidas de seguridad, medidas de prevención y, en su caso, contramedidas. En este sentido, puede decirse que combina acciones de seguridad y contrainteligencia.

Esta actividad adopta medidas y procedimientos destinados a salvaguardar a las personas, materiales, áreas, instalaciones y medios de producción, almacenamiento y comunicación de conocimientos y datos dentro del propio organismo o institución. La Seguridad Institucional también es responsable de fomentar y fortalecer la cultura de seguridad institucional. A través de los recursos de comunicación social corporativa se pueden llevar a cabo campañas de sensibilización y orientación con el objetivo de fomentar el cumplimiento de las normas y procedimientos de seguridad.

La Seguridad Institucional es responsable de la aplicación interna de las dos vertientes de la contrainteligencia, la contrainteligencia preventiva y la contrainteligencia activa. Como tal, abarca todos los segmentos de la contrainteligencia y puede recurrir a cualquiera de sus medidas, siempre que sean adecuadas al contexto en el que se utilizan.

En una institución, corresponde a la división responsable de la Seguridad Institucional diseñar, o al menos coordinar, su sistema de gestión de la seguridad. También es responsable de desarrollar acciones para contrarrestar la inteligencia adversa que tenga como blanco la organización, su personal, conocimientos, áreas, instalaciones o tecnología de la información y las comunicaciones.

En el caso de una organización de inteligencia, estas funciones son responsabilidad de más de una unidad. Por lo tanto, para detectar e identificar acciones adversas y contrarrestarlas, es necesario que la fracción Institucional de Seguridad se relacione con otras unidades responsables de acciones de seguimiento de contrainteligencia, generando datos que subsidien continuamente el estudio de amenazas y actores adversos.

4.4. Ciclo de contrainteligência

La contrainteligencia puede modelarse a partir de un ciclo compuesto por seis fases caracterizadas por acciones: seguir, orientar, detectar, evaluar, decidir y actuar. En principio, este ciclo comienza y termina con la misma acción: vigilar. Sin embargo, es posible que

comience en otras fases, en función de los estímulos recibidos por la agencia o el profesional de inteligencia.

Las acciones de cada fase no terminan cuando comienza la siguiente. Al contrario, las dos primeras fases, seguir y orientar, suelen tener lugar de forma permanente y paralela a lo largo del ciclo. Son acciones que continúan, aunque no se perciba ninguna acción adversa. Las otras cuatro fases, representadas en el centro del diagrama, se producen siempre que se percibe una acción adversa.

Seguir es la fase en la que la contrainteligencia examina a los adversarios, estatales o no, que compiten abierta o veladamente con el Estado o las instituciones privadas nacionales. Los objetivos de la acción de seguir son conocer los intereses, capacidades y modus operandi de estos adversarios, e identificar instituciones, grupos o personas que puedan interesarles. Con ello, la organización de inteligencia pretende anticiparse a posibles acciones adversas de los adversarios sobre blancos nacionales.

En la fase de seguir, se realizan estudios para comprender el contexto en el que opera la actividad de inteligencia adversa. ¿Quiénes son los actores? ¿Cuáles son sus objetivos? ¿Quién los patrocina? ¿Qué técnicas y recursos se utilizan para alcanzar estos objetivos? ¿Y cómo se utilizan? Se trata de un seguimiento continuo cuyo objetivo es permitir a los profesionales de la contrainteligencia desarrollar análisis sobre la identidad, la capacidad y el modo de funcionamiento de la inteligencia adversaria.

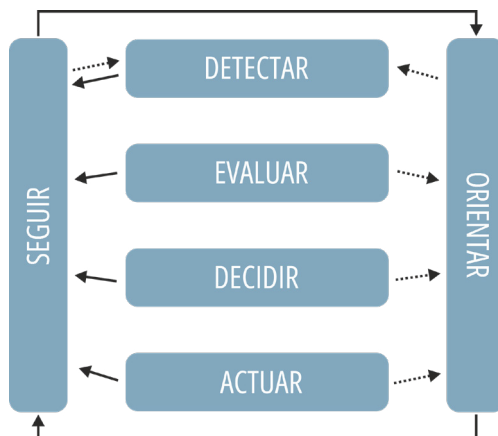


Figura 2: Ciclo de contrainteligencia

Así como es importante comprender a los adversarios, es esencial que los profesionales de contrainteligencia intenten comprender la posición brasileña. ¿Hasta qué punto nuestros intereses entran en conflicto con los de otros países? ¿Cuáles son nuestras vulnerabilidades y cómo pueden ser explotadas? ¿Qué estamos desarrollando que pueda convertirse en blanco de interés para la inteligencia adversa? ¿Cómo o de qué manera? Estos conocimientos permiten a los profesionales de la contrainteligencia idear formas más eficaces de prevenir las amenazas.

Esta fase incluye las prácticas rutinarias de las unidades de contrainteligencia, como el seguimiento de las organizaciones de inteligencia extranjeras y de los grupos insurgentes, terroristas y extremistas, la identificación de posibles blancos para los agentes adversos y la evaluación de la evolución de las acciones adversas a lo largo del tiempo. Al final de la fase seguir se espera que la contrainteligencia conozca qué actores tienen más probabilidades de representar una amenaza para los intereses del Estado y la sociedad brasileños, así como sus modos de acción y blancos probables.

Orientar es la fase en la que la contrainteligencia ofrece instrucciones a los responsables de los blancos potenciales de interés adverso, buscando concienciarlos de la necesidad de protección para evitar o minimizar los daños al Estado y a la sociedad. La orientación establece un canal de comunicación entre la organización de inteligencia y las instituciones percibidas como probables blancos, con el fin de asesorarlas en la aplicación de las medidas de seguridad necesarias.

Una vez identificados los posibles objetos de interés para los actores adversos, se trata de aumentar el nivel de protección de los conocimientos y datos relativos a estos blancos, tratando de evitar o minimizar los daños al Estado y a la sociedad. Del mismo modo, si estos objetos se consideran infraestructuras nacionales críticas, la IC también es responsable de asesorar a los organismos responsables sobre las medidas para aumentar el nivel de protección física de estas instalaciones. El profesional de CI es responsable de asesorar a los organismos y organizaciones nacionales sobre la aplicación de las medidas de seguridad necesarias. Este asesoramiento incluye

una evaluación del riesgo del blanco potencial, sugerencias de mejora, actos de sensibilización para la adopción de medidas de seguridad y una explicación de estas medidas y sus efectos.

La fase de orientación también sirve para sensibilizar a los blancos potenciales sobre las amenazas a las que pueden enfrentarse, ayudarles a obstruirlas y crear un canal de comunicación entre los blancos y la agencia de inteligencia. Esta fase incluye los contactos que las unidades de CI establecen con los blancos potenciales, la elaboración de evaluaciones de riesgos y las directrices para aplicar medidas de prevención y obstrucción de las acciones adversas. Al final de la fase de orientación, se espera que el blanco potencial haya mejorado su nivel de seguridad y establecido sensores capaces de detectar posibles acciones adversas, así como canales para activar la CI en caso de que se produzcan acciones adversas o indicios de que puedan producirse.

Detectar es la fase en la que la contrainteligencia detecta una posible acción adversa, ya sea consumada o en curso. Dicha acción puede consistir en el acceso indebido, sustracción o daño a conocimientos, datos, materiales, equipos, áreas, instalaciones, sistemas o procesos producidos, utilizados o en poder de potenciales blancos, o puede consistir en un intento de interferir en el proceso nacional de toma de decisiones.

La detección puede resultar de la vigilancia, cuando se estiman los intereses prioritarios de un adversario determinado. Una vez comprendidos los posibles intereses adversarios y la capacidad de actuación de determinados actores, la organización o el profesional de inteligencia buscaría indicios de que la inteligencia adversaria está actuando para alcanzar los presuntos intereses.

Otra forma de detección está mediada por la percepción de la acción adversa por parte de la persona que la sufre. Para ello, es importante que, durante la fase de orientación, se hayan establecido canales de comunicación entre la contrainteligencia y el posible objeto de la acción adversa, de forma que las situaciones sospechosas puedan ser comunicadas por éste a aquélla. Lo mismo puede ocurrir internamente en la organización, mediante el enlace de la contrainteligencia con la unidad responsable de la seguridad institucional. La

contrainteligencia se activa mediante sensores instalados a tal efecto y la acción sospechosa se analiza preliminarmente.

También se pueden vislumbrar acciones adversas cuando aún se están planificando, si la contrainteligencia ha conseguido llevar a cabo una intrusión. Esto ocurre cuando un agente está posicionado dentro de la organización de inteligencia adversaria. Dependiendo de su posición, el agente puede tener conocimiento previo de los planes de la organización, lo que permite la detección incluso antes de que se inicie la acción adversa. En ocasiones, la detección procede de información facilitada voluntariamente por terceros, incluso vinculados a la propia inteligencia adversaria, que buscan contrainteligencia por diversos motivos, como financieros, ideológicos y políticos.

Es posible que la identificación de un agente adversario preceda a la detección de su acción. Esto ocurre cuando se constata la presencia de personas cuyos vínculos con la inteligencia adversa han sido identificados durante la fase de seguimiento. Cuando esto ocurre, corresponde al profesional de la contrainteligencia vigilar las actividades de estas personas para tratar de descubrir sus objetivos y blancos potenciales en el país. Esta fase incluye contactos realizados con potenciales blancos de inteligencia adversa, para estimar la ocurrencia de acciones hostiles, y el seguimiento de personas vinculadas, o supuestamente vinculadas, a organizaciones de inteligencia adversa. Al final de la fase de detección, si hay pruebas suficientes de que se ha producido una acción adversa, se espera que la contrainteligencia tenga un caso concreto que evaluar.

La fase de detección va seguida de la fase de evaluación. Para ello, es necesario considerar el objetivo de la acción adversa, cómo se llevó a cabo, sus probables patrocinadores y las consecuencias de su posible realización para el país blanco. No todos estos elementos están siempre disponibles o pueden estimarse. Los únicos elementos esenciales para la evaluación son las hipótesis sobre el objetivo de la acción adversa y su fase de desarrollo.

Así, tras la detección, el profesional de la contrainteligencia tratará de determinar la intención probable de la inteligencia adversa e intentará identificar la autoría, el patrocinio y la fase de desarrollo de la acción (si se ha completado o no). La autoría de la acción se

atribuye al agente adverso, es decir, a la persona encargada de llevar a cabo la acción de inteligencia adversa. El patrocinio de la acción se atribuye al Estado, organización, institución, grupo o persona que concibió, solicitó, fomentó, financió la acción adversa o que hará uso de sus resultados o beneficios.

Las circunstancias de la acción adversa deben determinarse analizando los insumos recolectados y los conocimientos de inteligencia producidos en la fase de seguimiento, así como los insumos proporcionados por personas vinculadas a los blancos potenciales de la inteligencia adversa. El profesional de contrainteligencia intentará reunir más datos, informaciones y conocimientos sobre la amenaza, tratando de estimar el objetivo de la acción, hasta qué punto se ha llevado a cabo y cuál sería el daño si se completara. En el caso de una acción ya finalizada, se intentará estimar las ventajas obtenidas por su promotor.

Tras reunir y analizar estos datos, se elabora un conocimiento que se difunde a la instancia decisoria, que definirá el rumbo a seguir. Esta instancia puede ser interna o externa a la organización, en función de la naturaleza de la amenaza y del lugar y el momento en que tendrá lugar la intervención. Es en esta fase cuando la contrainteligencia elabora un documento en el que se informa al órgano decisorio del riesgo que plantea la acción adversa. Este documento debe contener los elementos necesarios para que el órgano decisorio evalúe las vías de acción existentes y decida qué hacer o no hacer ante la amenaza. La inacción también puede ser un curso de acción a adoptar por el responsable de la toma de decisiones.

Deben esbozarse cursos de acción para contrarrestar la amenaza, que pueden solicitarse para asesorar al responsable de la toma de decisiones. Al final de la fase de evaluación, se espera que la contrainteligencia disponga de conocimientos capaces de informar al responsable de la toma de decisiones sobre el contexto de la amenaza de inteligencia adversa, su naturaleza, fase de desarrollo y daños potenciales causados.

Basándose en la evaluación, el organismo competente decidirá cómo actuar, según el mejor curso de acción. Esta acción se llevará a cabo utilizando las herramientas existentes, tras una cuidadosa pla-

nificación. Decidir es la fase en la que el responsable de la toma de decisiones, en el nivel adecuado, define cómo proceder para prevenir, obstruir o neutralizar la acción adversa, ya haya concluido o esté en curso. Esta decisión se basa en un conocimiento que tiene en cuenta la naturaleza, la autoría, las circunstancias y el daño potencial de la acción adversa. La complejidad del caso, la fase de desarrollo de la acción adversa y sus implicaciones para el país determinarán quién debe decidir sobre las contraacciones.

Así, en esta fase se produce la deliberación, por parte de los legitimados para ello, sobre las medidas a aplicar frente a la acción adversa, finalizada o en curso, así como el orden derivado de dicha deliberación. La inacción y el acto de no decidir también son posibilidades para el decisor.

El papel que debe desempeñar el profesional de inteligencia en esta fase es asesorar en el proceso de toma de decisiones. El punto de partida es la evaluación realizada en la fase anterior, consolidada en el conocimiento producido. A partir de este conocimiento, se debe decidir entre, por un lado, interrumpir la acción adversa o, por otro, no interferir directamente en su desarrollo, procurando observar y desinformar al agente adverso. Si se opta por detener la acción, también habrá que decidir si se expondrá, avergonzando a sus agentes o patrocinadores, o si la contraacción se hará discretamente.

Los factores importantes a estimar son el grado de sensibilidad y el alcance de la acción de inteligencia adversa detectada. Por sensibilidad se entiende la propiedad de un determinado tema o acción de generar tensiones o daños si se revela y explota indebidamente. En este sentido, el daño causado por la amplitud de la acción y su revelación debe evaluarse cuidadosamente.

La decisión es una acción del Estado y no se limita a la agencia de inteligencia. Esta decisión define si se utilizará o no la función de inteligencia, es decir, si la organización de inteligencia actuará para contrarrestar activamente una amenaza. El ejercicio de esta función podría repercutir en las relaciones exteriores del país o en intereses nacionales de diversa índole. Por lo tanto, la decisión corresponde a quienes tienen la capacidad de evaluar mejor el contexto más amplio.

En algunos casos, la decisión puede ser tomada internamente por la organización de inteligencia. En otros, la tomará necesariamente un órgano diferente, normalmente superior. Dependiendo de la situación, uno de los cursos de acción a considerar puede ser no tomar ninguna medida, es decir, asumir cualquier pérdida, si se entiende que sería menor que el daño resultante de cualquier acción para contrarrestar la acción adversa.

Cuando el responsable de la toma de decisiones opta por actuar y decide que la organización de inteligencia actúe, se produce un segundo momento de decisión dentro de la organización. El elemento de análisis podrá activar el elemento de operaciones y, basándose en las capacidades de la agencia, elegir el mejor curso de acción para llevar a cabo la contramedida. Al final de la fase de decisión, se espera que la contrainteligencia disponga de una orientación clara e inequívoca sobre el curso de acción a seguir para hacer frente a la acción adversa detectada y a la amenaza que representa.

Actuar es la fase en la que el Estado adopta medidas y procedimientos para hacer realidad lo decidido en la fase anterior. En la fase de actuación, dependiendo del contexto, se puede adoptar más de un curso de acción. Al igual que en la fase anterior, se trata de una acción del Estado que puede limitarse o no a la labor del profesional de inteligencia. Esta fase incluye acciones para obstruir y neutralizar las acciones de inteligencia adversa; orientación a otras agencias para implementar acciones de esta naturaleza; acciones dirigidas a desinformar y desradicalizar a potenciales agentes adversos; y monitoreo de estas actividades.

La contrainteligencia obstruirá una acción adversa en curso cuando trate de impedir que se desarrolle. Para ello, puede trabajar en colaboración con el blanco de la acción adversa, aumentando su nivel de seguridad. También se puede intervenir sobre el agente adverso, tratando de disuadirle de continuar con la acción o dificultándole el acceso al objeto de interés.

Hay que neutralizar las acciones ya realizadas. El objetivo es reducir las ventajas obtenidas por los adversarios. La naturaleza de los procedimientos de neutralización depende del tipo de acción y del contexto en el que opera la inteligencia adversaria.

En algunos casos, será necesario obstruir la acción adversa y neutralizar las ventajas ya obtenidas. Una acción de inteligencia adversa puede ser simple y puntual, pero también puede ser compleja y prolongada, compuesta de varias etapas. Por lo tanto, la estrategia para contrarrestar esta acción será igualmente compleja y probablemente comprenderá más de una etapa.

También hay que tener en cuenta la capacidad de actuación de la contrainteligencia, sus recursos, habilidades y límites. Es posible que las acciones de obstrucción o neutralización requieran el apoyo de otros órganos de la administración pública, si se decide declarar persona non grata a un agente, expulsarlo del país o abrir una investigación por delito, por ejemplo. Así pues, la finalización de la fase de actuación no depende necesariamente de la agencia de inteligencia. La ejecución de la acción puede incluso ser responsabilidad plena de otros organismos. Sin embargo, la contrainteligencia es responsable de supervisar la ejecución de la acción, observar sus efectos y reevaluarla para garantizar la exhaustividad de la contraacción.

La fase de actuar es el momento en que las áreas de análisis y operaciones colaboran más estrechamente, tanto para evaluar los mejores cursos de acción para la contraacción como para definir las etapas de control que permitan evaluar el curso de la acción y su eficacia. Durante la fase de contraacción activa, se evalúan las medidas de eficacia para su posterior desarrollo o para la adopción de medidas correctoras. Al final de la fase de acción, se espera que la contrainteligencia haya llevado a cabo las acciones pertinentes, basándose en uno o varios planes para contrarrestar la inteligencia adversa.

Al final de la sexta fase del Ciclo de Contrainteligencia, se realiza un *debriefing* de la situación, en el que se enumeran las mejores prácticas y los fallos observados en el proceso, con vistas a subvencionar el estudio sobre Inteligencia Adversa en la fase de seguimiento y mejorar la práctica de la contrainteligencia.

Aplicación del Ciclo de Contrainteligencia

El objetivo de la contrainteligencia es impedir el éxito de las acciones de inteligencia adversa. Por lo tanto, es necesario que sus

profesionales traten de comprender estas acciones, sus objetivos y propósitos y sus configuraciones. Se entiende por objetivo de la acción lo que se pretende conseguir en su totalidad. Su finalidad es el fin al que sirve la acción, es decir, la ventaja que pretende el promotor y que le llevó a planificar la acción. Así pues, comprender la naturaleza, la dinámica y las repercusiones de la amenaza que representa la inteligencia adversa es uno de los aspectos fundamentales de la contrainteligencia.

El Ciclo de Contrainteligencia ofrece un marco metodológico útil para el trabajo de los profesionales sobre el terreno, sistematizando los procedimientos en fases que se intercambian y retroalimentan entre sí. Las acciones de seguir y orientar son permanentes, independientes de la percepción de la ocurrencia de una acción adversa. Las otras cuatro fases (detectar, evaluar, decidir y actuar) se activan idealmente siempre que se percibe una acción adversa. La detección de esta acción establece un caso concreto sobre el que trabajar.

La fase de detectar es la intersección entre la contrainteligencia preventiva y la contrainteligencia activa. En las fases de seguir y orientar, el objetivo es señalar la acción adversa planificada o realizada. Por lo tanto, la preocupación por la detección está presente desde el principio del ciclo y debe tenerse en cuenta en las directrices y las medidas preventivas. La detección es el punto de partida de las fases de evaluación, decisión y acción. Las contramedidas se adoptan ante un caso concreto de acción adversa y comienzan con esta detección.

Una vez detectada una acción adversa, la contrainteligencia debe tratar de comprender su objetivo y la mejor manera de contrarrestarla, para luego pasar a la acción. Una vez finalizada esta etapa, se vuelve a la fase de seguimiento para evaluar la eficacia de la medida adoptada. En cualquier momento del ciclo, puede reanudarse la fase de orientación, según sea necesario. Todas las fases del ciclo dan lugar a nuevos componentes para la acción de seguir.

Las medidas de obstrucción pueden adoptarse en dos momentos del ciclo. En la contrainteligencia preventiva, estas medidas se adoptan para evitar que la amenaza adversa se materialice en abstracto. En la contrainteligencia activa, se llevan a cabo cuando la

acción adversa aún está en curso. Estas medidas se personalizan para interrumpir el desarrollo de dicha acción adversa.

El trabajo de contrainteligencia requiere la integración entre las áreas de análisis y operaciones, cuyas acciones se complementan. El desarrollo del trabajo a lo largo del ciclo de contrainteligencia implica un continuo intercambio de información entre ambas áreas. Al final de cada fase, es conveniente examinar el contexto de la acción adversa y la pertinencia y eficacia de las contramedidas adoptadas hasta ese momento. En estos exámenes deben participar tanto los profesionales de análisis como los de operaciones que trabajen en el caso.

Así, la contracción está dirigida por la interacción entre análisis y operaciones en la fase de decisión y, posteriormente, en las acciones llevadas a cabo en la fase de actuación. Durante esta fase, para evaluar la eficacia de las medidas, es necesario que la información tanto sobre la ejecución de la acción en sí como sobre los efectos percibidos se debata entre el elemento operativo y el sector de análisis. Al término de este debate, se podrán considerar nuevas líneas de actuación.

La aplicación del ciclo de contrainteligencia es el punto de partida para la formulación de políticas de prevención de amenazas adversas, así como de políticas de salvaguarda del conocimiento, la información, los datos y los medios de almacenamiento o transmisión de los mismos, sus poseedores, áreas e instalaciones de interés para el Estado y la sociedad. Estas políticas deben ser elaboradas con el objetivo de orientar a los potenciales blancos de inteligencia adversa para prevenir y obstruir las amenazas, así como para abrir canales de comunicación que permitan a estos blancos activar la contrainteligencia en caso de sospecha de actividad adversa de inteligencia.

Una vez presentadas las ramas de inteligencia y contrainteligencia, debemos pasar a los elementos de análisis y operaciones que conforman el ejercicio práctico de la actividad de inteligencia.



5

**Elemento
de Análisis**

5. Elemento de Análisis

La actividad de inteligencia se caracteriza por el ejercicio permanente de acciones especializadas para cumplir dos funciones: informar y ejecutar. El elemento de análisis es, por excelencia, el principal responsable de cumplir la función de informar.

El análisis transforma sus insumos, datos, informaciones y conocimientos, en productos potencialmente útiles para el proceso nacional de toma de decisiones. Durante la producción analítica, los profesionales de inteligencia procesan estos insumos con el objetivo de hacerlos aptos para el consumo de un decisor, a través de procedimientos que generarán conocimiento de inteligencia. Por lo tanto, el análisis es la esencia del proceso de generación de contenidos de inteligencia.

Los procedimientos de análisis incluyen la identificación, obtención y selección de insumos de interés, que serán desglosados para su evaluación y posteriormente reagrupados en un todo coherente y útil. También forma parte de este proceso la exteriorización de los resultados del tratamiento y la interpretación resultante. Para generar el producto final, los profesionales de la inteligencia utilizan una amplia gama de procedimientos, que se seleccionarán y combinarán en función de los insumos disponibles, la naturaleza de la cuestión a resolver y las especificidades de las condiciones de producción. El esfuerzo analítico emprendido para generar el producto de inteligencia se expresará en el formato propio de la actividad, el lenguaje de inteligencia.

Este esfuerzo se realiza sobre la base de principios racionales o lógicos, apoyados en evidencias y su finalidad es la búsqueda de la verdad. Este último aspecto es condición necesaria para la producción de inteligencia, cuyo objetivo es ayudar a la toma de decisiones en contextos de inseguridad e incertidumbre. Sólo puede lograrse superando supuestos y preconceptos, por un lado, y corroborando afirmaciones demostrables, por otro. Por lo tanto, es importante comprender básicamente el proceso de construcción del conocimiento para favorecer la producción consciente del conocimiento de la inteligencia, según criterios de racionalidad, verdad y demostrabilidad.

5.1. Aspectos teóricos

El conocimiento deriva de la combinación de tres elementos: la realidad, objeto mismo del conocimiento; la perspectiva del sujeto, que construye el conocimiento observando y pensando; y la intersubjetividad, originada en el intercambio de afirmaciones o impresiones entre el sujeto y sus semejantes. Este tercer elemento constituye la prueba del conocimiento. Un analista puede estar convencido de que su conclusión sobre un determinado problema o tema es cierta, de acuerdo con las pruebas y la lógica. Pero sólo la validación de sus conclusiones por sus pares ofrece una especie de garantía, aunque precaria, sobre la representación de la realidad como verdadera, y esta garantía es muy común en la vida cotidiana y en la producción metódica del conocimiento.

Se supone que hay una realidad fuera de la conciencia, pero sólo se puede llegar a ella en parte, dependiendo de la perspectiva del sujeto. La perspectiva es un recorte del objeto impuesto por los límites humanos de aprehensión de la realidad. En otras palabras, somos incapaces de captar todas las dimensiones infinitas de la realidad tal como son. Tenemos límites de comprensión que nos llevan necesariamente a percibirla de forma fragmentada e incompleta. En este sentido, nuestra comprensión de cualquier objeto es el resultado de los aspectos que percibimos. Es importante ser consciente de que siempre habrá aspectos que no se perciban.

Cualquier objeto (concreto, social, psicológico, conceptual) puede abordarse de diferentes maneras. La posición desde la que se acceda a ese objeto cambiará la forma de captarlo. En contacto con la realidad exterior, sólo se puede obtener una parte de su composición, y ésta viene impuesta por la perspectiva, expresada por el "punto de vista" o la "forma de ver". En consecuencia, el conocimiento seguro no sólo se refiere a la evidencia, sino también al intercambio de perspectivas manifiestas. Este intercambio es una especie de prueba para ver si lo que ve un observador se corresponde con lo que ven los demás, es decir, si hay consenso. De lo contrario, el observador quedaría atrapado en su propia perspectiva y nunca podría estar seguro de la pertinencia de su representación del objeto.

La perspectiva depende de tres grupos de factores: ambientales (distancia, ángulo, tiempo, duración, visibilidad, acústica, escala, necesidades fisiológicas como el hambre, el sueño, la temperatura y la excreción), psicológicos (agudeza de los órganos de los sentidos y funcionamiento del sistema nervioso, que incluye aquí las formas peculiares en que el cerebro procesa los estímulos, lo que conduce a inevitables sesgos cognitivos, y condiciones idiosincrásicas como la aptitud y la edad, entre otras) y sociológicos (educación informal y formal, cultura, clase, relaciones interpersonales o sociales, ideales, profesión). Es importante alejarse de cualquier noción de que la "perspectiva" es "la propia verdad". La perspectiva no es más que el punto de vista, es decir, el punto desde el que se observa algo y que condiciona la representación del objeto. Que sea verdad o no dependerá de pruebas basadas en ciertos criterios como la evidencia, la lógica y el debate. La perspectiva no hace la verdad, sólo limita el contacto intelectual o cognitivo con algo.

En el desarrollo del conocimiento de la inteligencia, es importante considerar el aspecto profesional de la perspectiva. Los objetos interesan (o no interesan) a las personas de diferentes maneras o interesan a determinados grupos de personas (observadores, expertos, diletantes, curiosos) por diferentes motivos. El profesional de la inteligencia debe abordar la realidad desde una perspectiva específica, orientada socialmente. Idealmente, se espera que este factor de perspectiva compita con -y en algunos casos anule- los demás factores. La perspectiva de inteligencia se compone de dos elementos: el campo cognitivo y la búsqueda de la verdad. El campo cognitivo es el conjunto imaginado de objetos que la actividad de inteligencia está interesada en conocer. Son los temas, ámbitos y materias que deben ser objeto de la producción de conocimiento de inteligencia. La búsqueda de la verdad es la idea de valor que orienta la aproximación a esos objetos, es decir, la pretensión de saber lo que son a partir de una aproximación desapasionada, imparcial e impersonal.

La construcción del conocimiento de inteligencia favorece la aprehensión abstracta de los objetos analizados. Los profesionales de la inteligencia se aproximan a los objetos racionalmente representados a partir de preguntas previamente formuladas, tratando de establecer hipótesis metódicamente construidas para su interpretación.

Estas hipótesis deben ser validadas por sus pares. En este sentido, puede decirse que el conocimiento de inteligencia deriva necesariamente de formas racionales de conocer.

Formas racionales de conocer

Las formas racionales que actúan en el plano del conocimiento y del saber de la inteligencia son la idea, el juicio y el razonamiento. Estas formas destacan por ser decisivas para la producción del conocimiento de la inteligencia, ya que constituyen el contenido que trata de la realidad y que puede articularse a través del lenguaje.

La idea es la generalización de un objeto dado, reflejando sólo sus aspectos esenciales (por ejemplo, silla, terremoto, persona). Se concibe como una representación conceptual, que refleja aspectos esenciales del objeto como forma de generalización. Al construir este tipo de representación, se abstraen las características inteligibles, comunes y universales de una clase de objetos, lo que hace que el concepto sea válido para todos ellos. Las ideas son la materia prima para formular juicios y razonamientos.

Un juicio es una relación entre ideas, que constituye una proposición o afirmación sobre un objeto (por ejemplo, silla de madera, terremoto de 4,5 grados en la escala de Richter, persona alta). Se formula como una relación entre ideas, que componen un enunciado sobre algún objeto real o ideal, que trata de sus relaciones o acciones. Un juicio asocia dos ideas mediante verbos. Así pues, un juicio es necesariamente una forma de expresar un pensamiento, atribuyendo ideas universales a objetos particulares para describirlos. Lógicamente, el objeto es el sujeto de la oración, y la idea vinculada a él es el atributo o predicado.

El razonamiento es la elaboración mental a partir de la cual juicios anteriores permiten generar lógicamente un nuevo juicio. Suele implicar una conclusión (por ejemplo, la silla es de madera muy densa, por lo que debe ser ignífuga). El razonamiento es un proceso de pensamiento sofisticado que revela propiedades o hechos sobre el objeto que no están disponibles para la aprehensión inmediata. Los

juicios de los que parte el razonamiento sustentan la conclusión, es decir, son las razones en las que se basa.

Verdad

El conocimiento es una representación individual que puede justificarse como verdadera. Para ello, es necesario determinar si esta cualidad de verdadero puede atribuirse a su contenido. Hay tres concepciones de la verdad que hacen posible esta evaluación: correspondencia, coherencia y consenso.

La primera concepción ve la verdad como una cualidad de la realidad externa a la mente. Corresponde a la mente alcanzarla. Lo verdadero es lo que existe como tal, y la verdad depende de que la realidad se manifieste. Esta concepción supone que existe, de hecho, una realidad exterior a la mente, aprehensible mediante la observación y el razonamiento. El verdadero conocimiento está constituido por la percepción intelectual racional de la verdad del objeto. El criterio de verdad es la adecuación del intelecto a este objeto. Este es el concepto de verdad por correspondencia. La referencia temporal de esta concepción, dado que exige la evidencia del objeto, es el presente.

La segunda concepción ve la verdad como una cualidad del lenguaje elaborada por la mente humana. Para esta concepción, el conocimiento verdadero es la composición rigurosa y precisa del discurso que, en sus enunciados y argumentaciones, es capaz de generar la impresión de fidelidad a los hechos. El criterio de verdad es la coherencia interna y externa, que depende de las reglas de los enunciados correctos. Este es el concepto de verdad por coherencia. Es importante señalar que la voluntad, en esta forma de concebir la verdad, es un elemento constitutivo del conocimiento, ya que el enunciado es un artefacto humano, elaborado por decisión y acto. Interfiere en la relación entre la representación y el objeto. El sujeto necesita querer producir un enunciado coherente. La verdad depende, por una parte, de la capacidad de observar y recordar y, por otra, de la capacidad de formular enunciados que parezcan corresponder a los hechos ocurridos. Por tanto, la referencia temporal en este caso es el pasado.

La tercera concepción ve la verdad como una cualidad de la similitud de percepciones entre intérpretes del objeto. Esta concepción se basa en la confianza en la sinceridad de las personas interesadas en el conocimiento verdadero, según acuerdos y pactos. Su sello distintivo es el respeto a las convenciones universales que se derivan del hecho de ser seres dotados de lenguaje, razón y moral. Todos estos elementos desempeñan un papel eficaz en una comunidad de personas capaces de discutir y evaluar representaciones sobre los objetos que desean conocer. El valor de la verdad será atribuido, o no, por los miembros de la comunidad. Este es el concepto de verdad por consenso. El paradigma del consenso indica lo que debe ocurrir con la pluralidad de perspectivas: debate, comparación, crítica, argumentación y, finalmente, decisión sobre la verdad. La referencia temporal de esta concepción es el futuro, que es el momento en que se declarará la verdad.

No se puede alcanzar la verdad por solo una de las vías concebidas. La búsqueda de la verdad necesita hacer uso de la evidencia, la coherencia y el consenso, aunque estos elementos tengan distinto peso según la situación. En función de la dinámica de las concepciones de la verdad, la representación de un objeto puede tomarse como más o menos coherente, generando diferentes estados de ánimo en relación con esta representación de la verdad: certeza, probabilidad, posibilidad e ignorancia.

Estados de la mente ante la representación de la verdad

El elemento de análisis tiene por objeto la búsqueda de la verdad y su representación mediante la elaboración de conocimientos inteligentes. La verdad se entiende aquí como la concordancia entre un hecho, acontecimiento, situación o fenómeno y su respectiva elaboración mental. Sin embargo, la realidad es más compleja de lo que el ser humano puede captar. El mundo percibido por la mente es una simplificación resultante de sus límites sensoriales y de su capacidad de interpretación. Del mismo modo, las circunstancias materiales para percibir y comprender la verdad, como la escasez de recursos, fuentes y plazos, también contribuyen a reducir la calidad de la certeza.

Además de las incertidumbres derivadas de los límites cognitivos, la forma en que se presenta la realidad puede verse oscurecida por la desinformación o la ocultación. El potencial dañino de las *fake news* va de la mano del crecimiento exponencial de la masificación de la información a través de las redes sociales y de la sofisticación tecnológica de los recursos digitales, cada vez más baratos y accesibles. Por ello, la comprensión de la verdad no suele producirse de forma plena o suficiente para la total convicción.

Hay ocasiones en las que la mente está totalmente de acuerdo en que la imagen que forma corresponde al objeto. En otras ocasiones, este acuerdo es sólo parcial. También hay ocasiones en las que la mente es incapaz de optar por una imagen determinada ante opciones alternativas. Por último, la mente puede encontrarse en un estado nulo en relación con el objeto, es decir, sin capacidad para crear una imagen mental.

Los estados o gradaciones en los que puede encontrarse la mente en relación con lo que percibe como verdadero son la certeza; la probabilidad u opinión; la posibilidad o duda; y la ignorancia.



Figura 3: Estados de ánimo en relación con la representación de la verdad

La gradación de los estados de ánimo en relación con la verdad expresa los límites entre la certeza y la incertidumbre, con implicaciones para la producción de conocimiento, que pretende dar lugar a un conocimiento verdadero. Ante el reto de dotar de credibilidad a los consejos que ofrecen, las organizaciones de inteligencia adoptan modelos metodológicos de análisis que tratan de reducir los errores, mitigar los sesgos y conjurar las influencias ideológicas. Aunque este procedimiento no es capaz de eliminar por completo la imprecisión, permite al analista producir conocimiento dentro de un patrón regular, uniforme y controlable.

Una de las soluciones que ofrecen los métodos de análisis es la atribución de diversos grados de certeza al resultado del proceso. Así,

al tratar problemas de interés para el Estado, el elemento de análisis puede ofrecer respuestas con valoraciones probabilísticas de la verdad. Para ser útil, este juicio debe aproximarse a un grado de certeza utilizable, que permita al usuario tener una comprensión de la realidad suficiente para tomar decisiones.

La certeza es el estado mental en el que el individuo considera que su interpretación mental de la realidad se corresponde plenamente con el objeto real considerado, es decir, el individuo entiende que ha alcanzado plenamente la verdad. Este acuerdo es integral debido a la existencia de pruebas suficientes para alcanzar la convicción de plena conformidad. En este estado, la mente cree que no existen lagunas significativas entre la imagen mental y la realidad

Si el conocimiento del objeto se basa en la evidencia, la coherencia lingüística y el consenso, la mente tiende a aceptar esta representación como verdadera. Esta posición permite al sujeto dar por sentado el conocimiento, alcanzando un estado de certeza. Como estado subjetivo, la certeza no es garantía de haber alcanzado la verdad definitiva sobre el objeto. Nuevos datos y conocimientos pueden demostrar que ya no es posible mantener este estado de ánimo.

Ocasionalmente, incluso en ausencia de criterios de verdad, se puede asumir un estado de certeza sobre la verdad de una representación. Según los casos, esto se debe a la convicción del sujeto que conoce el objeto. Por ejemplo, cuando no parece haber ninguna probabilidad de que ese criterio sea refutado por otro, esto puede llevar al sujeto a aceptar plenamente su representación del objeto como verdadera.

Un estado de certeza puede conducir a un exceso de confianza por parte del profesional de la inteligencia, porque la certeza puede ser ilusoria. El peligro de la certeza es que tiende a ser absoluta. Cuando hay certeza, pero la evidencia de la realidad no apoya la imagen mental alcanzada y denota una relación inadecuada, incompatible o insuficiente, hay error, es decir, ilusión de verdad.

La probabilidad es el estado mental en el que el individuo cree que su interpretación de la realidad se corresponde con el objeto real, pero reconoce que existe cierta posibilidad de engaño. En este estado,

los elementos de convicción -pruebas inmediatas; coherencia de las afirmaciones; o consenso entre dos o más sujetos, que evalúan la representación y la asumen como verdadera- son limitados e insuficientes para alcanzar el pleno estado de certeza. La correspondencia es, por tanto, sólo parcial. Por tanto, se dice que la correspondencia es probable.

El estado de probabilidad se expresa, pues, mediante términos que indican la probabilidad o el nivel de confianza. Un ejemplo de descripción textual en estado de probabilidad sería: "es probable que se produzcan nuevos conatos de incendio debido al alto nivel de vertido ilegal de material combustible en condiciones de alta temperatura y baja humedad".

La posibilidad, o duda, es el estado mental en el que no hay pruebas suficientes para apoyar una imagen mental definitiva. Los criterios de verdad son contradictorios en sí mismos. Las pruebas pueden no ser del todo inequívocas, el lenguaje que retrata o informa del objeto puede no ser coherente interna o externamente, el debate entre iguales establece controversia en lugar de consenso. Puede ocurrir que un criterio lleve a refutar otro, sin la condición de señalar cuál es el correcto.

La mente es así incapaz de afirmar o negar la verdad de la representación que ha elaborado. Uno de los objetivos de la MPC es buscar pruebas para aumentar el grado de credibilidad del contenido de la inteligencia, pasando del estado de posibilidad al estado de certeza o probabilidad.

En este estado, la verdad sólo es posible. La actividad de inteligencia no utiliza este estado en el conocimiento de inteligencia. Aunque el estado de posibilidad no constituye conocimiento de inteligencia, en situaciones de producción es normal que se registre este estado para generar indicios de hipótesis para futuras exploraciones, tanto por parte del elemento de análisis como del elemento de operaciones.

La ignorancia es el estado mental caracterizado por la ausencia total de cualquier imagen de la realidad. En esta situación, el profesional de la inteligencia desconoce cualquier característica o no tiene ninguna evidencia sobre el objeto. En el estado mental de ignorancia,

el sujeto o bien es incapaz de formarse ninguna representación del objeto, que es inaccesible a su entendimiento, o bien sólo dispone de datos que no le permiten generar un significado utilizable.

Aunque el principal objetivo de los profesionales de la inteligencia es obtener la verdad, entre la realidad y la mejor representación posible se interpone un amplio abanico de obstáculos. Por ello, la producción de conocimiento de inteligencia totalmente en estado de certeza es la excepción y no la regla, ya que, en el empeño por reducir la incertidumbre mediante el asesoramiento de inteligencia, lo más habitual es que se ofrezcan soluciones dentro de un espectro de probabilidad. En consecuencia, en cada producto entregado al usuario, la misión institucional se cumple en la expresión de un grado de credibilidad suficientemente fiable y útil.

5.2. Insumos para el análisis

El desarrollo del conocimiento de inteligencia consiste en reunir, evaluar, integrar, interpretar, formalizar, validar y difundir distintos insumos de producción. Estos insumos son de cuatro tipos: datos, información, conocimiento y conocimiento de inteligencia. Entre ellos existe una relación de progresión y regresión, siendo este último una categorización particular de la actividad de inteligencia, que, además de ser un insumo, es también el producto mismo del trabajo analítico.

Estos insumos deben gestionarse de forma que se garantice su trazabilidad y auditabilidad, función para la que es esencial el tratamiento de metadatos. Los metadatos permiten almacenar y recuperar insumos en bases de datos para utilizarlos en la producción, así como cumplir requisitos legales y de rendición de cuentas. Los metadatos son elementos de contextualización vinculados a unos insumos, importantes para juzgar los que aún no han sido evaluados por el profesional de la inteligencia. Ejemplos de metadatos con fines de producción de conocimientos son: autor, fuente, equipo de captura, fecha de creación, ubicación, descripción, historial de modificaciones, tipo y precisión del sensor y formato.

Datos

Los datos son una representación registrada o no registrada de un aspecto de la realidad con un significado descontextualizado. Los datos se consideran aquí en su expresión más atomizada, como la unidad más pequeña de representación cualitativa o cuantitativa de un aspecto de la realidad, sin atribución de significado más allá del proceso directo de registro. Los datos pueden ser generados por una persona o por medios técnicos. Los datos suelen clasificarse en estructurados (como los organizados en hojas de cálculo y bases de datos) y no estructurados (no organizados de forma predefinida, como los contenidos en textos, imágenes, vídeos y audios).

Los datos están descontextualizados porque no tienen una estructura amplia de descripción -definición, aspecto, composición, función o rendimiento- ni de narración -qué, quién, cuándo, dónde, por qué, cómo-. Su análisis requiere, en primer lugar, un esfuerzo por identificar los elementos que pueden atribuirse a la composición de la descripción o la narración, según el caso. En este caso, no es posible evaluarlo inmediatamente.

En informática y ciencia de datos, es habitual referirse a los datos en el sentido de registro, término entendido como cualquier registro unitario conservado en un sistema informático. Así, los datos, la información, el conocimiento o la inteligencia, cuando simplemente se almacenan en una base de datos, se denominan datos a efectos de gestión. Un nombre, el código de matrícula de un vehículo, el valor de una compra o un índice pluviométrico, tomados aisladamente, son ejemplos de datos.

Información

La información es una representación registrada o no de un aspecto de la realidad con un significado contextualizado según un tratamiento metódico, racional y objetivo.

La información es el primer paso hacia la comprensión de un hecho, acontecimiento, situación o fenómeno. Es el resultado de procesar (limpiar, corregir, seleccionar, cruzar, organizar, traducir,

formatear, resumir y ordenar) e interpretar datos, idealmente con la ayuda de metadatos. La información es un registro identificado por el contexto con una estructura descriptiva o narrativa, pero que no contiene corroboración o demostración que justifique su capacidad de ser cierta. Analizarla requiere examinar los enunciados, buscar coherencia interna y externa y otras fuentes. En este caso, puede evaluarse inmediatamente.

Como resultado del procesamiento y la interpretación de los datos, la información tiene un contenido y un significado comprensibles. Ayuda a responder a preguntas como "qué", "quién", "cuándo" y "dónde" y puede ser generada tanto por personas como por medios informáticos sin intervención humana.

Un gráfico que represente los vínculos entre una persona (identificada por su nombre), una dirección y un vehículo concreto (identificado por su matrícula), elaborado con ayuda de un programa informático, es un ejemplo de información. Del mismo modo, un extracto anual de la superficie deforestada en una región determinada de Brasil, con registros de evolución mensual, así como una tabla basada en una secuencia de índices pluviométricos para un lugar determinado durante un periodo concreto, también son ejemplos de información.

Conocimiento

El conocimiento consiste en una representación registrada o no de un aspecto de la realidad con un significado contextualizado que se supone verdadero y validado.

El conocimiento contiene el significado del objeto observado y su propiedad decisiva es la creencia de que esta representación es justificadamente plausible, es decir, creíble según criterios que permiten la demostración, la verificación y la réplica. Típicamente, el conocimiento es una producción de especialistas (estudiosos, expertos, científicos, analistas, oficiales de inteligencia, ciertos burócratas), dedicados al estudio metódico y sistemático de objetos en un campo significativo determinado, y se demuestra mediante la experiencia, la experimentación o la aplicación de procesos de análisis y validación, como el proceso científico. Promueve la comprensión o extrapolación

de hechos, acontecimientos, situaciones o fenómenos, utilizando el razonamiento y la verificación de resultados.

El conocimiento justifica su capacidad de ser verdadero por diversos medios racionales y metodológicos. Analizarlo requiere comprender esta justificación o basarse en otros recursos como la fiabilidad, la trayectoria, la reputación y las evaluaciones de otras personas. En este caso, es posible evaluarla inmediatamente.

Como expresión de la verdad, es decir, suficientemente coherente con la realidad, el conocimiento puede utilizarse para tomar decisiones, lo que lo aproxima al concepto de conocimiento de la inteligencia. La proximidad proviene del hecho de que ambos son el resultado de un proceso mental de análisis y síntesis, que implica la identificación de relaciones de causa y consecuencia mediante procesos de convicción personal y convencimiento de los pares, replicables por la relación lógica de las pruebas.

El conocimiento nos ayuda a comprender cuestiones como el "por qué" y el "cómo", y hasta ahora ha sido dominio exclusivo de los procesos cognitivos humanos. Los documentos técnicos y científicos, como un estudio que muestre los cambios en el régimen de lluvias de una determinada región en los últimos 15 años, son ejemplos de conocimiento.

El conocimiento de inteligencia consiste en una representación, registrada o no, de un aspecto de la realidad, contextualizado y asumido como verdadero según los procedimientos metódicos de la actividad de inteligencia, útil para el proceso de toma de decisiones. El conocimiento de inteligencia se caracteriza, en comparación con el concepto de conocimiento, por su finalidad, que es servir al Estado brasileño, y por su producción, que utiliza procedimientos propios. El conocimiento de inteligencia se produce mediante la aplicación de la Metodología de Producción de Conocimiento (MPC), aunque puede involucrar otras técnicas y metodologías complementarias.

5.3. Conocimiento de inteligencia

La función informativa de la actividad de inteligencia se materializa en la producción de conocimiento de inteligencia, un tipo de representación caracterizada por dirigirse a objetos para asesorar el proceso nacional de toma de decisiones, considerando las razones del Estado Democrático de Derecho con foco en los intereses del pueblo. Este conocimiento resulta de la aplicación de procedimientos metódicos propios de la actividad de inteligencia que, a su vez, permiten asumir su contenido como verdadero.

Como producto, el conocimiento de inteligencia debe ser veraz, oportuno y útil, es decir, una representación real o probable de la realidad, entregada de manera oportuna y útil a un usuario con poder de decisión. Puede ser narrativo-descriptivo, interpretativo e interpretativo-prospectivo, de acuerdo con los siguientes atributos: forma racional de conocer, mediante la presencia de juicios o juicios y razonamientos; y temporalidad, mediante la consideración del pasado, presente, futuro inmediato y futuro lejano.



Figura 4: Tipo de conocimiento, temporalidad y forma de conocer

La inteligencia narrativo-descriptiva, tradicionalmente llamada informativa, es el resultado de juicios sobre hechos, acontecimientos, situaciones o fenómenos pasados o presentes. Se limita a narrar o describir los objetos de análisis, ya sea porque la demanda recibida así orienta la producción, ya sea porque las pruebas reunidas no permitían elaborar razonamientos. Un reporte sobre un atentado terrorista sobre el que aún no existen elementos de interpretación en estado de probabilidad o certeza es un ejemplo de conocimiento narrativo-descriptivo. Del mismo modo, un informe elaborado por el elemento de operaciones, que se limita a describir la dinámica de una manifestación pasada o en curso en respuesta a una demanda del elemento de análisis, es también un ejemplo de conocimiento narrativo-descriptivo.

El conocimiento interpretativo de inteligencia, tradicionalmente conocido como apreciación, es el resultado de juicios y razonamientos sobre hechos, acontecimientos, situaciones o fenómenos pasados o presentes. Este tipo de conocimiento permite proyectar los objetos de análisis hacia el futuro inmediato, expresando tendencias o evoluciones. Sin embargo, esta proyección no es prospectiva. Un informe de inteligencia sobre el marco político-electoral de un país sudamericano, que proyecta las probables repercusiones inmediatas en Brasil de los próximos resultados de unas elecciones presidenciales, es un ejemplo de conocimiento interpretativo. Del mismo modo, un informe que narra y describe un acto de sabotaje y, a través de la evaluación e interpretación de las pruebas, indica un grado de probabilidad en cuanto a su autoría o patrocinio, es también un ejemplo de conocimiento interpretativo.

El conocimiento de inteligencia interpretativo-prospectivo, tradicionalmente denominado estimativa, es el resultado de juicios y razonamientos sobre la evolución futura de hechos, acontecimientos, situaciones o fenómenos, con un enfoque en el futuro lejano. Debido a su naturaleza, requiere la utilización de técnicas auxiliares a la MPC (véase el punto 7.2). Un informe de inteligencia que presente diferentes escenarios sobre los impactos de la crisis climática en el sector agroindustrial brasileño en los próximos 15 años es un ejemplo de conocimiento interpretativo-prospectivo. Del mismo modo, un informe que muestra qué factores -y cómo- influyen en la consecución

futura de un escenario deseado en la lucha contra el crimen organizado en Brasil, en un horizonte de cinco años, es también un ejemplo de conocimiento interpretativo-prospectivo.

La inteligencia trabaja con cuatro situaciones temporales: pasado, presente, futuro inmediato y futuro lejano. El presente considera un objeto en su estado temporal actual, en un proceso probable de evolución. En el conocimiento de inteligencia, el tiempo presente se considera el pasado inmediato, es decir, el momento inmediatamente anterior a su difusión. El pasado considera un objeto cuya evolución se juzga completa.

El tiempo futuro, en cambio, considera un objeto cuya aparición o evolución es probable que se produzca en un momento posterior, que puede ser en un futuro inmediato o en un futuro lejano. El futuro inmediato trata de la aparición o evolución de este objeto en un futuro próximo. Normalmente se consideran periodos de tiempo cortos. El futuro lejano considera un objeto cuya aparición o evolución es probable que se produzca en plazos proyectados aún más lejanos o en amplios intervalos de tiempo en el futuro. Debido a la complejidad de la construcción de escenarios de futuro, cuanto más lejos se proyecten en el tiempo, más complejas serán las técnicas de estimación para abordar el futuro.

5.4. El ciclo de análisis

La producción de conocimientos de inteligencia es un proceso cíclico, compuesto por una secuencia de etapas procedimentales interrelacionadas. Este proceso, el ciclo de análisis, se distingue por generar productos que responden a una formulación de interés para el Estado o la sociedad, transformando datos, información y conocimiento en conocimiento de inteligencia. Las diversas técnicas utilizadas para cumplir el proceso tienen en común tareas que consisten en identificar y reunir insumos, examinarlos e interpretarlos, para componer el producto que se entregará a un usuario específico, de acuerdo con parámetros previamente establecidos en la planificación.

El ciclo de análisis describe el desarrollo lógico de los conocimientos de inteligencia, que comienza en una situación concreta de producción y termina con la evaluación del producto por parte del usuario. Las cuestiones de interés nacional se transforman, mediante un proceso lógico-argumentativo, en aspectos a los que hay que dar respuesta. Las respuestas se someten a procedimientos para confirmar su veracidad y, por último, se integran en un conjunto que pretende colmar una determinada laguna de conocimientos para el responsable de la toma de decisiones.

Aunque guiado y realizado por analistas, el ciclo analítico integra los esfuerzos de profesionales de inteligencia de diferentes áreas distintas de las especializadas en análisis, como unidades de búsqueda operativa, gestión de fuentes humanas, administración y tecnología de la información, y apoyo logístico, administrativo y financiero.

La situación de producción que inicia el proceso de producción de conocimiento consiste en una llamada externa (de una autoridad u organismo similar), una previsión en un plan de inteligencia o una iniciativa de la propia unidad. Las diferentes situaciones de producción imponen diferentes necesidades de producción, que se detallan en la planificación.

El ciclo de análisis se retroalimenta con la generación histórica de contenidos. Cada respuesta que se contesta tiende a generar nuevas situaciones de producción, ya sea debido a una demanda externa, a la necesidad de modificar los planes de trabajo o a un aumento de las necesidades de seguimiento del analista. Independientemente del nivel de exhaustividad de la respuesta anterior, se crean nuevos planes, las fuentes activadas siguen produciendo contenidos y los frentes de procesamiento abiertos continúan operando. Asimismo, la recepción de la evaluación del usuario suele iniciar nuevos ciclos de análisis.

Este ciclo es realizado por la Metodología de Producción de Conocimiento de Inteligencia (MPC), utilizada por diferentes agencias de inteligencia brasileñas. Esta metodología permite el uso de técnicas y recursos adicionales de forma complementaria, de acuerdo con las premisas y necesidades de cada situación de producción.

Todo proceso de producción de conocimiento de inteligencia comienza por la identificación de una demanda de asesoramiento, que puede provenir de tres fuentes. Demanda externa, que es cuando la solicitud es hecha por un usuario, autoridad o institución que busca dilucidar un asunto. Demanda interna, que es cuando se produce por exigencia de un superior jerárquico, una autoridad de la institución o un plan de producción interno. Y por iniciativa propia, cuando la demanda procede del propio profesional de inteligencia, que identifica una amenaza u oportunidad para los intereses nacionales.

Una vez identificada la oportunidad de producción, el profesional procede a aplicar el MPC, comenzando por la fase de planificación. En esta fase, la propuesta de producción debe ser aprobada por el superior inmediato. El plan aprobado formaliza la producción y orienta la movilización de recursos y el control de procesos y resultados.

A continuación, el profesional de inteligencia procede a ejecutar lo planificado, empezando por la reunión de insumos. Durante la producción, los principales procedimientos de cada fase, así como sus resultados, se registran para su futura recuperación.

Al final, una vez obtenidos y difundidos los conocimientos de inteligencia, se registran las buenas prácticas, los errores y las lecciones aprendidas para incorporarlos a los próximos ciclos de producción, y se desmoviliza al equipo de producción.

Metodología para la Producción de Conocimientos de Inteligencia (MPC)

La MPC consta de seis fases: planificación; reunión; evaluación; integración e interpretación; formalización y validación; difusión y resultados.

Aunque las fases de la MPC se presentan en secuencia cronológica, en la práctica no implican procedimientos estrictamente ordenados, ni tienen límites precisos. Son fases interpenetradas, interrelacionadas e interdependientes. Aun así, todas ellas deben completarse para realizar plenamente el conocimiento de la inteligencia, y la mayoría de sus procedimientos son necesarios.



Figura 5: Metodología para la producción de conocimientos de inteligencia (MPC)

Estos procedimientos pueden desarrollarse de forma secuencial, paralela o solapada, en función de factores como la composición y organización del equipo, los plazos y las circunstancias de la producción. Aun considerando la existencia de realidades específicas, es importante caracterizar cada fase de la MPC.

Fase de planificación

Es la fase en la que se planifica el trabajo a realizar, a partir de una demanda de producción de conocimiento. Se trata de una fase fundamental para todo el proceso, ya que en ella el profesional de inteligencia define el alcance del trabajo, las limitaciones de producción, las actividades a realizar y las necesidades del equipo.

La fase de planificación incluye la propuesta y aprobación de las siguientes definiciones: Asunto; Usuario; Finalidad; Plazos de estudio; Plazo de entrega; Aspectos esenciales; Indicación preliminar de sigilo; Formatos de divulgación; Acciones previstas a ser realizadas; y Propuesta del equipo.

Cuando la demanda proviene de un usuario externo, superior jerárquico o está prevista en los planes estratégicos de la institución, varias de estas definiciones pueden estar parcialmente determinadas, como en el caso de tema, usuario, propósito y plazo, y corresponde al profesional de inteligencia evaluar la adecuación de estas condiciones y hacer los ajustes necesarios.

Cuando la demanda surge por iniciativa propia del profesional de inteligencia, le corresponde proponer todas las definiciones mencionadas, teniendo siempre en cuenta la pertinencia, la oportunidad y la utilidad para el usuario.

Entre los pasos necesarios para elaborar el plan se encuentran la definición del tema y de los aspectos esenciales. Definir el tema implica formular una pregunta en un área temática a la que hay que dar respuesta. Este tema inicial suele ser una determinación provisional, ya que su percepción por parte del profesional de inteligencia puede cambiar durante el proceso de producción.

Definir los aspectos esenciales consiste en determinar preguntas subsidiarias para dilucidar la cuestión formulada a partir del tema. Los aspectos esenciales son preguntas sobre elementos que componen el objeto de conocimiento, cuyas respuestas aclaran el tema definido. Se dividen en dos tipos:

- ◆ Aspectos esenciales conocidos: preguntas sobre el tema cuyas respuestas ya obran en poder del profesional de inteligencia como resultado de las pruebas que ya posee sobre el tema; y
- ◆ Aspectos esenciales por conocer: preguntas sobre el tema para las que aún no se han obtenido respuestas o que todavía requieren más investigación. Los aspectos esenciales por conocer son los principales motivadores de la recolección y búsqueda de pruebas en la fase de reunión.

Incluso después de la aprobación por las autoridades superiores, la planificación puede y debe revisarse a lo largo del proceso de elaboración, tanto por cambios en las condiciones y circunstancias como por la aparición de pruebas que alteren la percepción inicial del tema.

Fase de reunión

Es la fase en la que se realizan las acciones para obtener y preparar los insumos para responder a los aspectos esenciales a conocer, es decir, las preguntas enumeradas en la planificación que pretenden dilucidar el problema formulado a partir del tema.

Estas aportaciones pueden ser datos, información, conocimientos o incluso otro tipo de inteligencia, reunidos de acuerdo con un plan de reunión. La fase de reunión se divide en dos etapas: formulación del plan de reunión y ejecución del plan de reunión, con medidas para obtener y procesar las aportaciones para la fase de evaluación.

El objetivo del plan de reunión es orientar los esfuerzos de recolección y búsqueda de insumos, sin ser restrictivo ni impositivo, sirviendo de guía para las actividades de los recolectores.

Las acciones de reunión son procedimientos realizados por los profesionales de inteligencia para obtener los insumos necesarios para producir conocimiento de inteligencia. Se dividen en acciones de recolección y de búsqueda. La recolección consiste en acciones especializadas para obtener insumos, realizadas o desencadenadas por el profesional de inteligencia asignado como recolector. Ejemplos de acciones de recolección son: consulta de bases de datos, contrapartes nacionales y extranjeras, individuos, unidades de la agencia; investigación, etc. La búsqueda consiste en acciones especializadas llevadas a cabo por el elemento de operaciones de inteligencia, utilizando técnicas operativas para obtener datos, información y conocimientos no disponibles, una vez agotados los medios de recolección. Las operaciones de búsqueda suelen implicar situaciones muy delicadas, arriesgadas y complejas.

Todos los insumos reunidos en la fase de reunión, basados en el plan de reunión, deben pasar por dos etapas de verificación, realizadas por el propio recolector. La comprobación de pertinencia consiste en confirmar que al menos una parte de las aportaciones reunidas es relevante para resolver el problema. A su vez, la comprobación de significación consiste en confirmar que al menos una fracción de las aportaciones responde al menos a un aspecto esencial.

Si una fracción del insumo responde tanto a la cuestión como a un aspecto esencial, esta fracción se considera significativa y debe separarse para su evaluación en una fase posterior. Tanto el insumo original como sus fracciones extraídas o delimitadas y sus metadatos deben registrarse como entradas para la fase de evaluación, idealmente en una base de datos.

Fase de evaluación

Es la fase en la que se evalúan los insumos reunidos en la fase de reunión, lo que da lugar a una calificación de credibilidad para cada entrada evaluada. La lleva a cabo un profesional de la inteligencia en calidad de evaluador.

La fase de evaluación consta de cuatro etapas:

- a. Validación de la pertinencia y significación: el evaluador comprueba si las fracciones son pertinentes para el tema y significativas para uno o varios aspectos esenciales, es decir, si las fracciones señaladas en los inputs son fracciones significativas.
- b. Verificación de la credibilidad existente: el evaluador comprueba, si la entrada que se está procesando es conocimiento de inteligencia (o una fracción de este conocimiento) producido previamente, qué grado de credibilidad se ha establecido. Si la evaluación anterior sigue siendo válida, no es necesario volver a aplicar la Técnica de Evaluación de Datos, Información y Conocimientos (TAD) a estas fracciones. Ocasionalmente, sin embargo, el evaluador puede identificar la necesidad de volver a evaluar fracciones de conocimiento de inteligencia a la luz de nuevos hechos o pruebas que no se conocían en ese momento, por ejemplo. En tales casos, el evaluador debe llevar a cabo una nueva evaluación, aplicando de nuevo el TAD a las aportaciones de conocimiento en cuestión para volver a determinar la credibilidad.
- c. Validación de los metadatos: el evaluador comprueba y valida los metadatos relativos a los insumos.

- d. Aplicación de la Técnica de Evaluación de Datos, Información y Conocimiento (TAD): el evaluador aplica la TAD a los insumos seleccionados para establecer un grado de credibilidad de las fracciones significativas.

El objetivo de la TAD es asignar un grado de credibilidad a los inputs para la producción de conocimiento de inteligencia mediante la evaluación de todo tipo de insumos por parte de un profesional de inteligencia, ya sean datos, información u otros conocimientos.

Hay dos pasos de evaluación para completar la TAD:

- a. Evaluación de la fuente: comprobación de los aspectos relacionados con la fuente del insumo para establecer una calificación de idoneidad, que sólo es válida en relación con el insumo específico obtenido. Esta evaluación se revisa para cada nueva aportación realizada por la fuente. Los aspectos considerados son: autenticidad, fiabilidad y competencia.
- b. Evaluación del contenido: comprobación de aspectos del contenido del insumo para establecer una calificación de veracidad de dicho contenido. Los aspectos considerados son: coherencia interna, compatibilidad y similitud externa.

Una vez evaluadas la fuente y el contenido mediante la aplicación del TAD, el evaluador puede determinar la credibilidad de las fracciones significativas y establecer si se encuentran en un estado de posibilidad, probabilidad o certeza. En los casos en que se alcanza el grado de probabilidad o certeza, estas fracciones significativas se consideran fracciones de conocimiento de inteligencia, susceptibles de ser integradas en nuevos conocimientos de inteligencia.

Fase de integración e interpretación

Es la fase en la que se aclara el tema, es decir, se da respuesta a la pregunta definida en la planificación. Para ello, se analizan, integran e interpretan las fracciones en estado de certeza o probabilidad, generando una elaboración textual coherente que permita aclarar el

tema. En este sentido, esta fase se caracteriza por los esfuerzos de análisis y síntesis.

El análisis es la operación mental que consiste en descomponer un todo en sus elementos constitutivos para comprender la función de cada elemento en el todo. La síntesis es la operación mental en la que se concibe la composición o recomposición de un todo a partir de los elementos constitutivos ya analizados, proporcionando un conjunto coherente y comprensible.

La clarificación del tema en la fase de integración e interpretación puede hacerse de dos maneras. Por integración simple, que se produce cuando la integración de las fracciones significativas en un texto narrativo-descriptivo es suficiente para dilucidar el problema o la cuestión. Y por interpretación, cuando, además de la integración de las fracciones significativas, es necesario responder a hipótesis formuladas, lo que implica la construcción de argumentos y conclusiones, a partir de las evidencias presentadas.

La integración simple ocurre cuando la pregunta definida en el tema requiere sólo una respuesta descriptivo-narrativa, sin la construcción de argumentos y conclusiones. En este caso, el producto se limita al uso de juicios, sin razonamiento explícito.

La interpretación se produce cuando, además del proceso de integración de fracciones significativas que describen el objeto, se utilizan las evidencias encontradas para construir argumentos que apoyen (o refuten) hipótesis, dando lugar a conclusiones. En este sentido, la interpretación va más allá de los límites del objeto analizado, más allá de la mera descripción o narración, y ofrece como producto un contenido interpretativo (valoración) o interpretativo-prospectivo (estimación). En este proceso, a partir de los juicios que destacan aspectos del objeto, el profesional de la inteligencia infiere juicios derivados - razonamientos. Esta extrapolación del objeto permite al profesional de la inteligencia inferir identidades, causas, responsabilidades, consecuencias y evolución futura de hechos, acontecimientos, situaciones o fenómenos.

La conclusión ofrece una solución total o parcial al problema expresado en el objeto. Su construcción implica el desarrollo de un

razonamiento por inferencia (deducción o inducción), necesariamente vinculado a las pruebas presentes en el texto.

Fase de formalización y validación

Es la fase en la que, teniendo en cuenta los formatos de difusión propuestos en la planificación, se lleva a cabo la formalización final de los conocimientos de inteligencia y su validación analítica y técnica. La fase de formalización y validación comprende tres etapas: revisión, formalización y validación.

La revisión es la comprobación de la composición textual en su conjunto: corrección gramatical, lógica interna, adecuación al lenguaje de inteligencia, presencia de sesgos, adecuación al usuario, etc. Se trata de un proceso menos formal y suele ser realizado tanto por el analista responsable como por otros profesionales de inteligencia disponibles. Tiene lugar antes de la formalización y la validación.

La formalización es el formateado final del documento, con la inserción de elementos formales de identificación, control y seguridad. Es un proceso técnico que implica la aplicación de un formato específico a los conocimientos de inteligencia. Es la etapa en la que los conocimientos de inteligencia se consolidan en un documento oficial, de conformidad con el reglamento interno y la legislación pertinente, incluida la indicación de sigilo.

La validación es la verificación rigurosa del producto final en sus aspectos analíticos y técnicos, con el fin de garantizar que los conocimientos de inteligencia se han elaborado con rigor metodológico y cumplen las normas de calidad exigidas para su difusión al usuario. Se trata de un proceso formal, realizado necesariamente por un profesional de la inteligencia ajeno al equipo de producción con competencia suficiente para comprender el tema y juzgar la metodología y los procedimientos utilizados en su producción. El papel de validador implica una parte de responsabilidad sobre el producto, por lo que la validación debe registrarse formalmente antes de los procesos burocráticos posteriores.

Fase de difusión y resultados

Es la fase en la que se llevan a cabo los procedimientos de difusión de los conocimientos de inteligencia, así como la evaluación de los resultados para mejorar los ciclos de producción posteriores.

La fase de diseminación y resultados se divide en dos etapas: Diseminación, cuando el conocimiento de inteligencia se pone a disposición del usuario y de las unidades internas de la agencia, y Evaluación de resultados, que incluye la evaluación de los procesos de producción y la evaluación del producto.

El proceso de difusión tiene lugar tras la validación por parte del validador y la aprobación para la difusión por parte del jefe de producción y sus superiores. La difusión al usuario se realiza por medios seguros, físicos o digitales, respetando los principios de oportunidad y seguridad. La difusión puede realizarse en forma de documentos textuales, archivos de audio, imagen o vídeo, gráficos con datos consolidados o exposición en reuniones sincrónicas presenciales o a distancia, entre otros medios disponibles. Cuando se realiza en plataformas digitales, la difusión a usuarios externos se produce en paralelo a su puesta a disposición de unidades de producción potencialmente interesadas dentro de la organización y a la puesta a disposición del conocimiento para su investigación y archivo en sistemas internos.

En la fase de evaluación de resultados se realiza una valoración general de la producción realizada, con el objetivo de promover la mejora continua en futuros ciclos de producción y proporcionar métricas para mejorar los procesos de gestión. Hay tres procesos que deben llevarse a cabo de forma secuencial:

- a. Evaluación del proceso: se realiza con la ayuda de todo el equipo de producción y teniendo en cuenta los comentarios proporcionados por el validador. La evaluación del proceso consiste en que cada miembro del equipo (jefe de producción, analista responsable, recolectores de datos, preparadores de datos, evaluadores, analistas de apoyo, revisores) dé su opinión sobre el proceso de producción, con el fin de identificar los problemas encontrados y las oportunidades de mejora.

- b. Evaluación del producto: se basa en la evaluación de los conocimientos de inteligencia por parte del usuario. Se basa en la interpretación que hace el analista responsable de los resultados de la evaluación del usuario sobre los aspectos de calidad y puntualidad y los resultados prácticos de los conocimientos de inteligencia una vez consumidos.
- c. Informe de evaluación final: realizado por el analista responsable sobre la base de las evaluaciones del proceso y del producto. El ciclo de los MPC sólo finaliza una vez completado el informe de evaluación final. Este informe contiene la interpretación de los resultados de las evaluaciones de procesos y productos, así como un registro de métricas e impresiones para uso institucional. Una vez finalizado, el informe se pone a disposición de la unidad responsable de la producción y de los demás miembros del equipo, para que las lecciones aprendidas, los problemas detectados y las mejores prácticas puedan utilizarse en futuros ciclos de producción.

5.5. Técnicas de apoyo al análisis

La Metodología de Producción de Conocimiento (MPC) puede utilizarse junto con técnicas auxiliares y otros recursos adicionales siempre que el equipo de producción lo considere necesario. El uso de estas técnicas debe ser complementario, respetando los procedimientos recomendados por MPC. Ejemplos de técnicas de apoyo al análisis son las técnicas analíticas estructuradas, los métodos de consulta a expertos, los recursos de análisis visual y las técnicas de recopilación.

Técnicas Analíticas Estructuradas (TAE)

Las técnicas analíticas estructuradas son herramientas adicionales a los métodos tradicionales de producción de inteligencia, que históricamente se han desarrollado mediante análisis intuitivos basados en el pensamiento lógico y en las pruebas disponibles. Estas técnicas no pretenden sustituir a las metodologías de producción de conocimiento como la MPC, sino que se utilizan en armonía con ellas.

y como complemento de las mismas. Así, los resultados de su aplicación se someten a la propia MPC antes de integrarse como conocimiento de inteligencia en los productos finales.

El uso de TAE proporciona medios sistemáticos para externalizar los procesos mentales individuales, lo que permite someter el trabajo analítico al control y escrutinio de compañeros, revisores, superiores y validadores, haciendo que el proceso sea más transparente y esté menos expuesto a sesgos cognitivos y otros defectos del pensamiento intuitivo.

Hay una serie de TAE presentadas en manuales específicos, a disposición del público en general, que son útiles para el trabajo de análisis de inteligencia. La elección de una determinada técnica estructurada por parte de un analista o equipo de producción debe tener en cuenta, entre otras cuestiones, el tipo de problema que el profesional o grupo quiere abordar o el tipo de sesgo cognitivo que quiere mitigar. Para ello, existen técnicas de generación de ideas, de descomposición y visualización de elementos, de desafío a las líneas analíticas hegemónicas, de creación de escenarios e indicadores, de generación y comprobación de hipótesis, entre otros ejemplos. Algunos ejemplos de TAE son:

Lluvia de ideas

Se trata de una técnica diseñada para su uso en grupos con el fin de generar nuevas ideas y estimular el pensamiento creativo, de acuerdo con unas reglas y pasos específicos que guían el proceso. Es adecuada para identificar múltiples variables, factores, actores, hipótesis, posibles soluciones a problemas, crear escenarios, etc. La presencia de personas relativamente ajenas al tema es útil para evitar el predominio del sesgo del "pensamiento de grupo". Los resultados de la lluvia de ideas aún deben someterse a otros métodos y evaluaciones específicas, y no constituyen soluciones inmediatas para los analistas.

Matriz de impacto cruzado

Se trata de una técnica de generación de ideas, adecuada para las primeras fases de un proyecto de análisis, cuando el analista o el equipo de análisis aún están intentando comprender una situación compleja. Consiste en enumerar en una matriz sencilla varias variables identificadas en relación con el problema que se está analizando, con el fin de discutir cómo interactúa cada variable con las demás. El impacto de esta interacción puede ser positivo, neutro o negativo, y de mayor o menor intensidad. Registrar en forma de texto la discusión del grupo en torno a la matriz facilita que todos los miembros del equipo comprendan cómo se han ido construyendo las premisas, los argumentos y las conclusiones a lo largo del proceso.

Cronología e línea del tiempo

Son técnicas de descomposición y visualización, especialmente indicadas para analizar cuestiones que se siguen sistemáticamente a lo largo del tiempo. Consiste en colocar los hechos y acontecimientos en orden cronológico para identificar posibles patrones o correlaciones, la existencia o no de causas y efectos, tendencias, anomalías, acontecimientos clave y lagunas de conocimiento.

Análisis de redes

Se trata de una técnica de visualización utilizada principalmente para supervisar las actividades de los individuos, cartografiando redes, interacciones y conexiones entre personas, grupos y otras entidades de interés. El gran volumen de datos e información en determinados contextos suele requerir el apoyo de programas informáticos específicos, así como la formación del personal para interpretar los vínculos, ya que corresponde al analista asignar significado a los gráficos y diagramas generados mediante la aplicación de la técnica. Comprende al menos dos técnicas específicas: el grafismo de redes y el análisis de redes sociales (*Social Network Analysis* - SNA). El SNA implica la medición matemática de variables y el mapeo de relaciones entre personas, grupos, organizaciones, ordenadores, URLs,

IPs y otras entidades de información conectadas. En este contexto, las entidades suelen denominarse nodos y la relación entre ellas, enlace.

Indicadores

Se trata de una técnica destinada a alertar sobre acontecimientos futuros, a identificar tendencias emergentes o cambios no deseados en los escenarios seguidos. Su uso está indicado para el monitoreo de situaciones o fenómenos de interés, siempre que sea necesario evaluar o anticipar cambios en el cuadro a lo largo del tiempo, para prever escenarios no deseados, por ejemplo. Consiste en elaborar una lista de indicadores, es decir, factores observables o potencialmente observables cuya aparición simultánea indica la probabilidad de que se materialice un determinado hecho, acontecimiento, situación o fenómeno. Esta lista de indicadores sirve de guía para las acciones de reunión y su constante monitoreo ayuda a generar alertas a nivel estratégico, táctico u operativo.

Abogado del diablo

Se trata de una técnica diseñada para desafiar las líneas de análisis establecidas, los modelos mentales o el consenso analítico. Consiste en designar a una persona o equipo para que desarrolle argumentos consistentes en contra de una determinada proposición o conclusión. Sus objetivos son fomentar la consideración de otras posibles explicaciones de los hechos o acontecimientos, comprobar la plausibilidad de los argumentos y evaluar las hipótesis y las pruebas contrarias.

Sombrero rojo

Se trata de una técnica diseñada para ayudar a comprender cómo tienden a actuar o comportarse otros actores o agentes adversos en determinadas situaciones. Resulta útil para vigilar a grupos extremistas, delincuentes o dirigentes extranjeros. Se recomienda su uso cuando se quiere evitar el cultural mirroring, es decir, la tenden-

cia natural de los seres humanos a imaginar que los demás piensan y perciben el mundo según ellos mismos o su propio grupo. Consiste en simular el contexto en el que se inserta el oponente o competidor, en una situación determinada, poniéndose en el lugar de la otra persona. Esta técnica requiere un conocimiento profundo de la lengua, la cultura y el entorno personal del blanco analizado.

Análisis de hipótesis competidoras (AHC)

Es una de las técnicas más conocidas para desarrollar y cuestionar hipótesis. Es adecuada para analizar situaciones complejas en las que existen múltiples factores y pruebas que pueden apoyar argumentos diferentes, explicaciones alternativas y conclusiones contradictorias. Consiste en relacionar las pruebas con las proposiciones en una matriz, para compararlas y comprobar su coherencia. El objetivo es refutar -no ratificar- cada hipótesis enumerada, lo que ayuda a evitar el sesgo de confirmación. El proceso de elaboración de diferentes hipótesis plausibles para una misma situación objeto de análisis contribuye también a explicitar la propia incertidumbre presente en la mayoría de los temas trabajados por la actividad de inteligencia. La aplicación del AHC intenta hacer el analista consciente de ello, al tiempo que contribuye a reducir estas incertidumbres en el trabajo analítico.

Además de las técnicas de análisis estructurado mencionadas anteriormente, también es importante destacar diferentes formas de incorporar la consulta con expertos y el uso de técnicas de análisis.

Consulta a expertos

Existen cuestiones específicas que, por su complejidad o particularidad, desbordan los conocimientos o la capacidad de un determinado profesional de inteligencia o equipo de producción para dar respuestas adecuadas. También hay casos en los que los analistas de la agencia no cuentan con los datos empíricos necesarios para analizar un problema, pero otras entidades, investigadores o profesionales pueden colaborar en la generación de estos insumos o llenar estos

vacíos de conocimiento. En estos casos, la agencia de inteligencia puede recurrir a la ayuda de expertos ajenos a sus propias filas.

Esto suele hacerse mediante cuestionarios que se envían a distintos expertos, en los que se pide al experto que evalúe variables o temas clave y, según los casos, emita juicios subjetivos sobre la probabilidad de que se produzcan determinados acontecimientos, por ejemplo. Se adoptan procedimientos específicos tanto para la formulación de los cuestionarios como para el tratamiento de las respuestas obtenidas. En estas situaciones pueden emplearse distintos métodos, incluidos algunos utilizados en los medios académicos y científicos.

Las aportaciones generadas a partir de la consulta a expertos aún deben evaluarse, según el MPC, mediante la TAD, antes de integrarse en el conocimiento de inteligencia en producción. Algunos ejemplos de técnicas o métodos de consulta a expertos son el método Delphi y la inferencia bayesiana.

El método Delphi permite la comunicación colectiva y, eventualmente, la construcción gradual de un consenso entre expertos separados geográficamente. Consiste en elaborar una serie de cuestionarios que los participantes responden secuencial e individualmente. En cada nueva ronda de consultas, los encuestados tienen acceso a un resumen de las respuestas del grupo a los cuestionarios anteriores, lo que crea la posibilidad de un diálogo indirecto entre expertos y la formulación de una respuesta colectiva a un problema determinado, ya que cada participante tiene la oportunidad de refinar, cambiar o defender sus propias ideas ante los investigadores. Puede utilizarse para recabar opiniones sobre tendencias o anticipaciones de la ocurrencia de acontecimientos futuros, en la producción de conocimiento interpretativo-prospectivo, por ejemplo.

La inferencia bayesiana se utiliza en el campo de la estadística para apoyar la toma de decisiones basadas en datos ante la incertidumbre. El objetivo es estimar la probabilidad de que ocurra un suceso a partir de un suceso inicial. Esta técnica permite procesar y actualizar las respuestas subjetivas de un experto tras haber sido expuesto a nuevas pruebas, lo que ayuda a obtener resultados más precisos. Requiere que los analistas tengan profundos conocimientos de matemáticas y estadística, así como experiencia con el método. Dependiendo de la

complejidad del problema, requiere la ayuda de recursos informáticos específicos.

Análisis visual

El uso cada vez más común de recursos visuales y computacionales para procesar datos, información y conocimientos abre un nuevo campo para la actividad analítica, además de ofrecer nuevas formas de presentar y difundir los conocimientos de inteligencia producidos. Así, es posible interpretar grandes volúmenes de datos recolectados y estructurados para mejorar los análisis predictivos. La utilización de algunos de estos recursos requiere una formación específica de los analistas y, en ocasiones, también algunos conocimientos previos por parte de los usuarios. El uso de herramientas que ayuden a los analistas a organizar los insumos y a generar presentaciones visuales sucintas y atractivas de los conocimientos de inteligencia para los usuarios se recomienda en determinadas situaciones, como el seguimiento permanente de acontecimientos dinámicos, en los que los nuevos insumos obtenidos o generados alimentan una base de datos y modifican la situación continuamente.

Técnicas de recolección

Como acción especializada, la recogida debe ser metódica y llevarse a cabo utilizando diversas técnicas destinadas a obtener los insumos que se analizarán. La inteligencia de fuente abierta, por ejemplo, utiliza técnicas que buscan descubrir nuevos insumos relevantes para una pregunta de investigación, basándose en palabras clave y operadores, y puede depender de Interfaces de Programación de Aplicaciones (del inglés *Application Programming Interface*). Entre estas técnicas se encuentra el Raspado de Datos, que consiste en la extracción sistemática para recopilar patrones o datos específicos, normalmente centrándose en páginas web. Para ello, se utilizan herramientas que acceden a la codificación de estas páginas, identifican los datos deseados, como textos, imágenes y enlaces, y organizan la recopilación en un formato estructurado.

5.6. Lenguaje de la Inteligencia

El conocimiento de la inteligencia se expresa a través del lenguaje oral o escrito, que da forma discursiva al pensamiento. A pesar de depender del contexto específico en el que se genera el producto, el lenguaje de inteligencia tiene características propias, como la simplicidad, la objetividad, la concisión y la neutralidad. Estas peculiaridades permiten distinguir un informe de inteligencia de otros tipos de producción escrita, como la académica, la periodística, la retórica, la jurídica o la literaria.

Esto significa que el éxito del trabajo del analista, al exteriorizar el conocimiento como proceso en conocimiento como producto, depende de su capacidad para movilizar los recursos lingüísticos en beneficio de una representación lógica y objetiva de la realidad. La intención es que el texto transmita el mensaje con el menor número de palabras posible y sea lo suficientemente claro como para que el usuario capte su objeto en una sola lectura. Para lograr este objetivo, los profesionales de la inteligencia deben dominar el lenguaje en el que se expresan. Las imprecisiones semánticas, los errores sintácticos y las insuficiencias estilísticas comprometen la credibilidad del producto y la imagen de la organización.

Sin embargo, no basta con que el texto sea gramaticalmente correcto. Los aspectos metodológicos, como las pruebas construidas sobre hechos y las conclusiones basadas en procesos lógicos, dan precisión, coherencia, objetividad e imparcialidad al proceso y su resultado. Esto contribuye a garantizar la impersonalidad y neutralidad que caracterizan el contenido de la inteligencia. La capacidad del analista para elegir la mejor técnica analítica y aplicarla adecuadamente en la producción de conocimiento está, por tanto, en la base de la calidad que caracteriza el lenguaje de la inteligencia.

En el tratamiento de los insumos recogidos, el lenguaje de inteligencia es el recurso que expresa el grado de credibilidad atribuido a las pruebas integradas en el conocimiento. El cruce de estas pruebas da lugar a conclusiones, que también se expresan lingüísticamente en grados de certeza o probabilidad, según la convicción del analista. Así, para transmitir al usuario las respuestas al problema formulado en el

tema, el profesional de la inteligencia hace uso de los tiempos verbales correspondientes a los resultados hallados a lo largo del proceso. La representación fiel y fidedigna de la realidad depende, por tanto, de la calidad del lenguaje utilizado.

El uso de recursos lingüísticos para expresar el grado de credibilidad de una determinada representación debería derivarse de forma natural de la aplicación rigurosa del MPC. Expresiones como "es probable que", así como los verbos en tiempo futuro, sirven para dar fe de la probabilidad en relación con las pruebas y conclusiones a las que se aplican, integrándolas en el contenido de la inteligencia. Por otra parte, los juicios y razonamientos que no superan el grado cualitativo de posibilidad no se consideran satisfactorios para conformar el producto que se pretende difundir y se devuelven al inicio de la fase de tratamiento para mejorar su nivel de confirmación. Este conjunto de procedimientos metodológicos aporta la precisión y la objetividad que caracterizan el lenguaje de la inteligencia.

Así, el estudio de los fenómenos relacionados con el lenguaje de la inteligencia pretende no sólo hacer más claro y útil el conocimiento, sino sobre todo evitar manipulaciones que alteren la representación de la realidad en favor de intereses personales, organizativos o ideológicos. Asignaturas de diferentes áreas contribuyen al desarrollo de las competencias del analista en el ámbito del lenguaje, como portugués (gramática y redacción y corrección), lingüística (análisis del discurso, análisis de contenido y lingüística textual), comunicación (expresión escrita y narración de historias), psicología (percepción, cognición, modelos mentales, heurística y sesgos cognitivos), estadística y análisis de datos. Estos conocimientos dan a los profesionales de la inteligencia más confianza a la hora de tratar con el lenguaje y garantizan que los conocimientos producidos sean más fiables.

Tras describir la organización y el funcionamiento del elemento de análisis, es hora de precisar la otra forma en que se lleva a cabo la actividad de inteligencia, el elemento operativo.



6

**Elemento
Operativo**

6. Elemento Operativo

La actividad de inteligencia se caracteriza por el ejercicio permanente de acciones especializadas para cumplir dos funciones: informar y ejecutar. El elemento de operaciones es, por excelencia, el principal responsable del cumplimiento de la función de ejecutar.

Las operaciones de inteligencia constituyen la forma singular de actuación de la actividad de inteligencia en el mundo. Esta actuación se orienta principalmente a la obtención de insumos para la producción de conocimiento de inteligencia y la producción de acontecimientos. Los datos, la información y el conocimiento de libre acceso pueden recopilarse mediante técnicas de prospección en fuentes abiertas, sin necesidad de una acción operativa por parte de los profesionales de inteligencia. Sin embargo, existen insumos que no están disponibles, es decir, que son difíciles de obtener, ya sea porque se encuentran en entornos de acceso restringido o porque están protegidos por quienes los poseen. La obtención de este tipo de información requiere el uso de acciones operativas especializadas, que por su naturaleza son secretas.

Las operaciones de inteligencia también pueden ser utilizadas para producir eventos destinados a implementar medidas para contrarrestar acciones adversas llevadas a cabo dentro de la rama de contrainteligencia. Esta condición viene impuesta por el hecho de que la inteligencia adversa, cuando opera, hace uso de acciones especializadas que no pueden ser evitadas por un individuo no entrenado en ellas.

Tanto en la función informativa como en la ejecutiva, la utilización de operaciones de inteligencia es una forma de sortear obstáculos para alcanzar determinados objetivos en un contexto de adversidad.

El uso de acciones encubiertas por parte del Estado brasileño está previsto en los artículos 3º y 4º de la Ley 9883/1999 y en la Política Nacional de Inteligencia, establecida por el Decreto 8763/2016. Su principal objetivo es reunir y luego difundir datos, información y conocimiento de manera oportuna con el fin de apoyar la producción de análisis de inteligencia y el proceso de toma de decisiones, ayu-

dando a lograr los intereses de la sociedad brasileña y del Estado. Las operaciones de inteligencia se llevan a cabo después de que la planificación operativa haya sido expresamente aprobada por la máxima autoridad del organismo, o por la autoridad en la que se haya delegado la prerrogativa. Esta aprobación requiere el ejercicio de juicios sobre la legitimidad de las operaciones de inteligencia. Para ello, deben tenerse en cuenta criterios que garanticen el cumplimiento de la ley, la relevancia temática de los objetos vigilados y la razonabilidad y adecuación de los medios a utilizar. Las operaciones, como todas las actividades de inteligencia de ABIN, están sujetas a los mismos procedimientos establecidos por la ley para el control interno y externo de cumplimiento, calidad e impacto.

6.1. Aspectos teóricos

La utilización del elemento operaciones se caracteriza por la actuación en campo, con la utilización secreta de recursos humanos y tecnológicos, en ambientes físicos o virtuales, de forma planificada y coordinada. Por lo tanto, el trabajo de los profesionales de inteligencia en este elemento es siempre potencialmente riesgoso. Por esta razón, sus acciones requieren personal entrenado, planificación detallada y ejecución cuidadosa, así como el estricto cumplimiento de los preceptos legales que rigen el Estado brasileño, su patrocinador.

Componentes

El agente es la persona encargada de actuar para alcanzar los objetivos de la acción operativa. Puede pertenecer a la organización de inteligencia, lo que lo convierte en un agente orgánico, o puede ser una persona empleada para realizar o facilitar la ejecución de una determinada acción, sin vínculos formales con la organización. En este caso, se clasifican como agentes no orgánicos.

Los agentes orgánicos están debidamente cualificados en el uso de técnicas operativas especializadas, con la misión de obtener datos, información y conocimientos no disponibles o llevar a cabo acciones para detectar, identificar, obstruir y neutralizar acciones adversas. Los

agentes no orgánicos son señalados, abordados y entrenados para llevar a cabo sus acciones. Están sometidos permanentemente a medidas de control específicas destinadas a reducir los riesgos de seguridad a los que están sometidos y a evaluar la calidad de su trabajo.

La acción operativa es la aplicación de estas técnicas especializadas. En este sentido, la técnica es el procedimiento y método a utilizar y la acción, el acto de utilizarla.

El blanco es el objeto sobre el que actúa la acción encubierta para cumplir su objetivo. Es a partir del objetivo, de sus características y del contexto en el que se inserta, que se establecen las acciones necesarias para alcanzar el resultado esperado de la operación. Por lo general, se trata de la persona que posee los datos, la información o los conocimientos deseados. En el caso de las contra-acciones, el blanco será la persona que lleva a cabo la acción adversa o los medios utilizados para conseguir dicha acción. Pueden estar situados en entornos físicos o virtuales, en el país o en el extranjero. Los blancos pueden caracterizarse como objetos simples, cuando son fácilmente delimitables y calificables, o como objetos complejos, cuando son difusos y difíciles de determinar. La acción operativa sobre objetos complejos requiere un enfoque sistémico y polifacético y suele exigir la ejecución de múltiples acciones encubiertas.

El entorno operativo es el espacio físico o virtual donde tiene lugar la acción operativa. Es el ámbito en el que actuará el elemento de operaciones, y puede estar situado en el país, en el extranjero, en la intersección entre ambos o en espacios virtuales. El entorno operativo suele determinarse al planificar una acción encubierta. El alcance de la acción determinará si el entorno se limitará a zonas bien delimitadas, como una propiedad o una red social, o si implicará espacios más amplios, como regiones, países o entornos virtuales genéricos. La correcta delimitación y caracterización del entorno operativo y su contexto son fundamentales para la mitigación de riesgos y el éxito de la acción.

Si una operación de inteligencia consta de más de una acción, puede tener más de un entorno operativo. Además, en función de la dinámica de la operación, puede ser necesario incorporar nuevos entornos a la planificación inicial. Por lo tanto, es importante que

haya margen para los ajustes y adaptaciones que puedan ser necesarios en el transcurso de las acciones.

Las técnicas operativas son procedimientos y métodos especializados para utilizar personal y material en acciones encubiertas. Los profesionales de inteligencia que trabajan en el elemento de operaciones deben recibir formación continua en el uso de estas técnicas especializadas.

Acción, operación y casos operativos

Las acciones operativas son el uso encubierto de técnicas operativas especializadas para alcanzar un objetivo previamente determinado en función de la demanda recibida del cliente. Las operaciones de inteligencia son el uso planificado y coordinado de acciones operativas, cada una con un objetivo. Idealmente, la consecución de los objetivos de las acciones empleadas conduce al cumplimiento de la misión de la operación, es decir, a la satisfacción de la demanda que la generó.

Existen situaciones en las que la fracción operativa trabaja sobre demandas que exigen el empleo de más de una operación de inteligencia, ya sea debido a la complejidad de la cuestión abordada, a la condición difusa de sus blancos o a la multiplicidad de factores que influyen en el contexto de la operación y en el entorno operativo. Esta situación conduce al establecimiento de casos operativos.

Los casos operativos son la utilización planificada y coordinada de operaciones de inteligencia en torno a un tema específico con múltiples misiones y blancos. En otras palabras, un caso operativo se trabaja en un contexto definido, generalmente complejo, con múltiples blancos, a veces también difusos, que requieren el empleo de diferentes esfuerzos operativos.

Funciones

La búsqueda es la aplicación combinada de técnicas operativas para obtener datos, información y conocimientos no disponibles. Es

necesaria en la fase de recopilación del ciclo de Análisis y se diferencia de la recopilación, que es la obtención de datos, información y conocimientos sin la aplicación de técnicas operativas.

La búsqueda suele utilizarse cuando los datos, la información o los conocimientos deseados no pueden obtenerse por medios manifiestos. Esta situación puede darse porque sea necesario ocultar el interés de la organización de inteligencia en obtener dichos datos, información o conocimiento; porque no se encuentren en lugares de acceso público; o porque estén efectivamente bajo las medidas de protección de sus titulares, en cuyo caso se habla de datos denegados.

La producción de eventos es el conjunto de acciones llevadas a cabo de forma secreta con el fin de producir eventos para cumplir los objetivos de la actividad de inteligencia. El principal uso de este tipo de acción es detectar, identificar, obstruir y neutralizar inteligencia adversa, lo que ocurre en el contexto de la contrainteligencia.

Por último, la acción operativa también puede utilizarse con fines de protección. Ocasionalmente, según lo exija la planificación o incluso la realidad cambiante del entorno operativo, también será necesario que el elemento de operaciones desempeñe la función de Protección. Se trata de utilizar medidas complementarias para proteger la integridad y la identidad de los agentes empleados, el sigilo y los objetivos de la acción operativa y la propia agencia de inteligencia.

Cliente y usuario

El cliente es la persona que convoca al elemento de operaciones, aportando la demanda que definirá el objetivo de las acciones operativas a emplear. El cliente puede ser el elemento de análisis de la organización o el propio responsable del elemento de operaciones, según relaciones y procedimientos de trabajo claramente establecidos y justificados administrativamente.

Es habitual que la demanda recibida del cliente necesite ser aclarada o redimensionada durante la planificación de la acción operativa. Del mismo modo, las necesidades de la actividad de inteligencia son dinámicas y puede ser necesario modificar los objetivos inicia-

les en el transcurso de las acciones operativas. Por lo tanto, el diálogo entre el elemento de operaciones y el cliente debe ser sistemático a lo largo de todo el trabajo realizado, de modo que puedan efectuarse los ajustes pertinentes para obtener los mejores resultados. Cualquier ajuste del plan de operaciones deberá quedar debidamente registrado y justificado administrativamente, y estará sujeto a los mismos controles internos y externos que el conjunto de las actividades de inteligencia.

El usuario es el consumidor final del resultado de la acción operativa, de acuerdo con una cadena jerárquica y unos procedimientos administrativos bien establecidos y auditables. Son las personas a las que se destina el conocimiento que se producirá a partir de los datos, informaciones o conocimientos obtenidos por la búsqueda. Los usuarios de la inteligencia nacional brasileña son las autoridades gubernamentales en sus respectivos niveles y en sus áreas de responsabilidad legalmente definidas.

6.2. Tipos de acción

Las acciones de inteligencia se clasifican de acuerdo con su finalidad, naturaleza y alcance. La finalidad indica el objetivo de la operación. La naturaleza se refiere a los medios y métodos operativos prioritarios. El alcance expresa el ámbito y la duración de la operación.

Por finalidad

Por su finalidad, las acciones de inteligencia se clasifican en acciones de búsqueda, que incluyen la ejecución de acciones operativas destinadas a obtener datos, información o conocimientos no disponibles; acciones de producción de eventos, que incluyen la ejecución de acciones operativas destinadas a crear eventos, principalmente en el contexto de la rama de contrainteligencia; y acciones de protección, que incluyen la ejecución de acciones operativas destinadas a proteger al agente y la operación.

Por naturaleza

En términos de naturaleza, las acciones son de los siguientes tipos: acción basada en recursos humanos, cuando prioriza el uso especializado de recursos humanos; acción basada en recursos técnicos, cuando prioriza el uso especializado de recursos técnicos; y acción cibernética, cuando tiene lugar en el ciberespacio y puede combinar el uso de recursos humanos y técnicos especializados en la misma acción.

Por ámbito

Por su alcance, las acciones se clasifican en exploratorias, que consisten en la realización de acciones puntuales, que proporcionan resultados concretos en un momento determinado, con un inicio y un final preestablecidos, o sistemáticas, que consisten en la realización de acciones continuas, que dan lugar a un flujo constante de datos, con un inicio preestablecido y un final indeterminado.

El tipo de acción a realizar depende de la idoneidad de los requisitos del objetivo a alcanzar, de las características del blanco, de la seguridad de los agentes implicados y de los recursos disponibles. Independientemente del tipo de acción a emplear, cabe destacar que su planificación debe buscar la integración en la aplicación de los recursos humanos y tecnológicos de que dispone el elemento de operaciones, con vistas a maximizar el cumplimiento del principio de oportunidad, con riesgos mínimos y una cuidadosa evaluación de los costes.

6.3. Ciclo de las operaciones

Las operaciones de inteligencia comienzan con una demanda expresada por el cliente, justificada por la necesidad de producir conocimiento oportuno y relevante para los usuarios. Una vez recibida la demanda, se designa a un profesional de inteligencia para planificar la operación y mantener la comunicación con el cliente. Este profesional suele realizar un estudio de situación para apoyar la planificación de la



Figura 6: Ciclo operativo

acción. También dirige a los demás profesionales de su segmento que participan en la operación. Este profesional será el principal interlocutor del elemento de operaciones con el cliente, con el que debe mantener una comunicación constante para evaluar los resultados, comprender y reevaluar las demandas. Es el profesional del elemento de operaciones que trabaja más cerca del elemento de análisis.

Los resultados obtenidos de las acciones operativas deben difundirse oportunamente. Esto permite al elemento de análisis contextualizar e interpretar más rápidamente los datos, la información y los conocimientos obtenidos, lo que facilita el asesoramiento oportuno para el proceso de toma de decisiones. También permite ampliar la comprensión de la realidad, lo que puede dar lugar a la definición de nuevas demandas por parte del cliente o incluso del usuario.

Cada operación de inteligencia sigue un ciclo compuesto por cuatro fases: planificación, ejecución, difusión y cierre. Estas fases tienen límites flexibles, permitiendo cambios cuando sea necesario como resultado del desarrollo de acciones secretas.

Planificación

Es la fase del ciclo operativo en la que el profesional responsable evalúa la demanda recibida y sistematiza el trabajo a realizar, estableciendo la composición de los recursos necesarios y la forma de conducir las acciones operativas para alcanzar sus objetivos con el mínimo de gastos y riesgos.

La planificación operativa debe realizarse por etapas con el mayor detalle posible, buscando establecer acciones realistas y adecuadas para alcanzar el resultado deseado. En este sentido, con cada solicitud debe analizarse cuidadosamente la petición, siempre que sea posible en comunicación con el cliente. A continuación, deben planificarse meticulosamente las acciones de acuerdo con la realidad operativa, evaluando la viabilidad de la realización de cada una y priorizándolas de acuerdo con la lógica que permita optimizar y agilizar las entregas. Por último, los recursos operativos definidos deben prepararse para el despliegue que tendrá lugar en la fase siguiente.

Al final de la fase de planificación, se espera que el elemento de operaciones comprenda los objetivos y misiones que deben alcanzarse, disponga de un plan preliminar aprobado sobre cómo llevarlos a cabo y esté preparado para empezar a ejecutarlos.

Ejecución

Es la fase en la que se llevan a cabo las acciones establecidas en el planeamiento operativo, con el objetivo de cumplir la misión. El profesional responsable de la operación coordina las acciones secretas, verificando su desarrollo, evaluando los resultados obtenidos y valorando la necesidad de alterar las acciones previstas.

La gestión de la actividad operativa debe garantizar la correcta asignación y gestión de los recursos disponibles, con vistas a la máxima seguridad y excelencia en el desempeño operativo. Para ello, es esencial que las tareas se distribuyan correctamente entre los agentes implicados.

La utilización del elemento operaciones en contextos con un alto nivel de complejidad, que incluye operaciones relacionadas con sistemas adaptativos complejos, requiere que los agentes implicados actúen con resiliencia y capacidad de adaptación rápida a patrones de comportamiento cambiantes. En otras palabras, el equipo sobre el terreno también debe ser capaz de actuar como un sistema adaptativo complejo. Esto requiere una gran sensibilidad a los cambios en sus blancos y entornos operativos y una reprogramación constante de la planificación, así como un buen diálogo interno dentro del ele-

mento de operaciones. Por ello, entre las principales características de una operación de inteligencia en contextos complejos se encuentran la flexibilidad, la adaptabilidad, la posibilidad de personalización y la mejora incremental de sus acciones.

Tras la realización de la acción, se prevé una reunión de evaluación, en la que se presentan y examinan los procedimientos llevados a cabo, los resultados obtenidos y las dificultades encontradas, así como el nivel de exposición de los agentes, equipos e instalaciones de apoyo. Al final de esta fase, se espera que se hayan llevado a cabo las acciones previstas y que el profesional responsable de la acción pueda presentar los resultados obtenidos de la acción operativa.

Difusión de los resultados obtenidos

Esta es la fase en la que se difunden los resultados de la operación a los clientes, normalmente por parte del profesional responsable de la acción.

En el transcurso de la misión, el equipo de la acción operativa procesa los resultados obtenidos y difunde al cliente los datos, la información o el conocimiento que ha encontrado o la inteligencia que ha producido, utilizando técnicas analíticas. Dependiendo de la complejidad de la operación, los datos, la información o los conocimientos obtenidos o producidos pueden desglosarse en entregas graduales, según la periodicidad establecida en la planificación inicial y la priorización de los objetivos de la acción y los requisitos de la misión.

La evaluación por parte de los clientes y usuarios después de cada entrega, así como la interacción constante entre el profesional responsable de la operación y el cliente, son esenciales para la replanificación de las acciones operativas posteriores. Los resultados obtenidos pueden comunicarse al cliente mediante documentos de texto formales, canales de mensajería seguros, informes orales y otros medios que sean necesarios y adecuados. Al final de esta fase, se espera que el cliente haya recibido los resultados de las acciones operativas y haya evaluado su pertinencia, integridad y utilidad.

Cierre

Es la fase en la que se determina el final del caso o de la operación. Puede cerrarse por las siguientes razones: cumplimiento de la misión; expiración del plazo estipulado; decisión de una autoridad superior; o reducción de los niveles de seguridad aceptables.

El cierre de una operación o caso operativo requiere una evaluación general de las acciones realizadas, sus consecuencias, éxitos y fracasos, lo que se conoce como "*debriefing* de cierre". Cuando sea necesario, deberán definirse procedimientos para mitigar, con la máxima discreción, cualquier impacto negativo sobre el usuario, la organización o los agentes implicados.

El elemento de operaciones debe prestar especial atención a la gestión del conocimiento en la conducción de las acciones especializadas, lo que incluye el intercambio de información sobre el desarrollo de las acciones entre el equipo, el correcto tratamiento de los datos, informaciones y conocimientos obtenidos, instancias de control de calidad y la preservación de la memoria institucional. Las reuniones periódicas celebradas a lo largo del esfuerzo operativo son herramientas importantes para el aprendizaje del elemento operativo, en la búsqueda de la mejora continua y la adaptabilidad, que deben guiar el trabajo de sus profesionales.

Cuando proceda, los agentes orgánicos de estos segmentos deben utilizar herramientas de gestión colaborativa o de gestión de proyectos para ayudar a planificar, conducir y controlar las acciones operativas. Además, el uso sistemático de este tipo de herramientas facilita la construcción de la memoria institucional y de una base de experiencia para el elemento operativo. En este sentido, los documentos utilizados en la actividad operativa deben ser objetivos, completos, claros y sencillos, tanto al describir los resultados de las acciones como al expresar la planificación realizada y los mecanismos de gestión y control utilizados.

Al final de esta fase, se espera que las acciones operativas se hayan completado y que el profesional responsable de las mismas haya realizado una evaluación coherente de los resultados globales obtenidos, enumerando las dificultades técnicas, humanas y de ges-

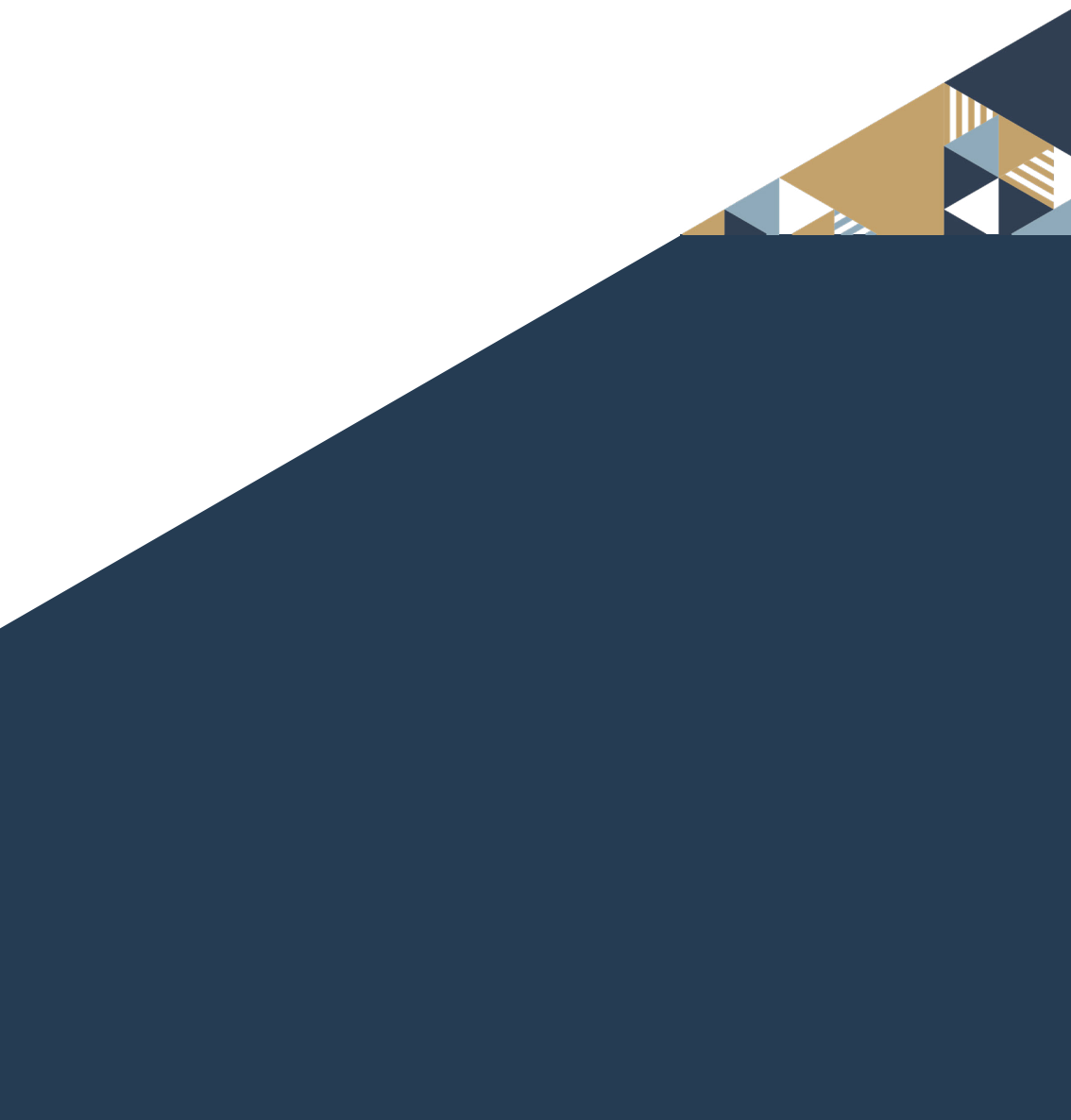
tión afrontadas, el compromiso y la relación entre los diversos actores y fracciones implicados y cualquier otro aspecto que considere relevante. La evaluación de la ejecución de la operación, en la que se destacarán las oportunidades de aprendizaje y los aciertos, deberá ser considerada en la planificación posterior de las acciones operativas, con vistas a un proceso de aprendizaje y perfeccionamiento constantes de los profesionales de inteligencia actuantes.

6.4. Técnicas operativas

Las técnicas operativas son métodos y procedimientos especializados utilizados en la ejecución de acciones secretas típicas de la actividad de inteligencia. Cada técnica tiene una finalidad específica, para lo cual utiliza los recursos operativos disponibles de forma característica.

Su utilización es una herramienta necesaria para superar obstáculos en la obtención de datos no disponibles o para contrarrestar acciones adversas. Debido a sus peculiaridades y objetivos, su ejercicio requiere una planificación detallada y una ejecución cuidadosa.

Las técnicas operativas rara vez se utilizan de forma aislada. Por el contrario, suelen aplicarse simultánea o consecutivamente. Su utilización debe llevarse a cabo respetando estrictamente las garantías y prerrogativas constitucionales y la legislación vigente, con sujeción a controles internos y externos.





7

Consideraciones Finales

7. Consideraciones Finales

La inteligencia se ha convertido en una institución estatal esencial para que los Estados operen en el entorno internacional desde la segunda mitad del siglo XX. La aparición de actores no estatales, como organizaciones criminales y grupos extremistas y terroristas, ha ampliado el ámbito tradicional de las agencias de inteligencia, añadiendo temas a su trabajo interno que van más allá de la protección contra la inteligencia adversa.

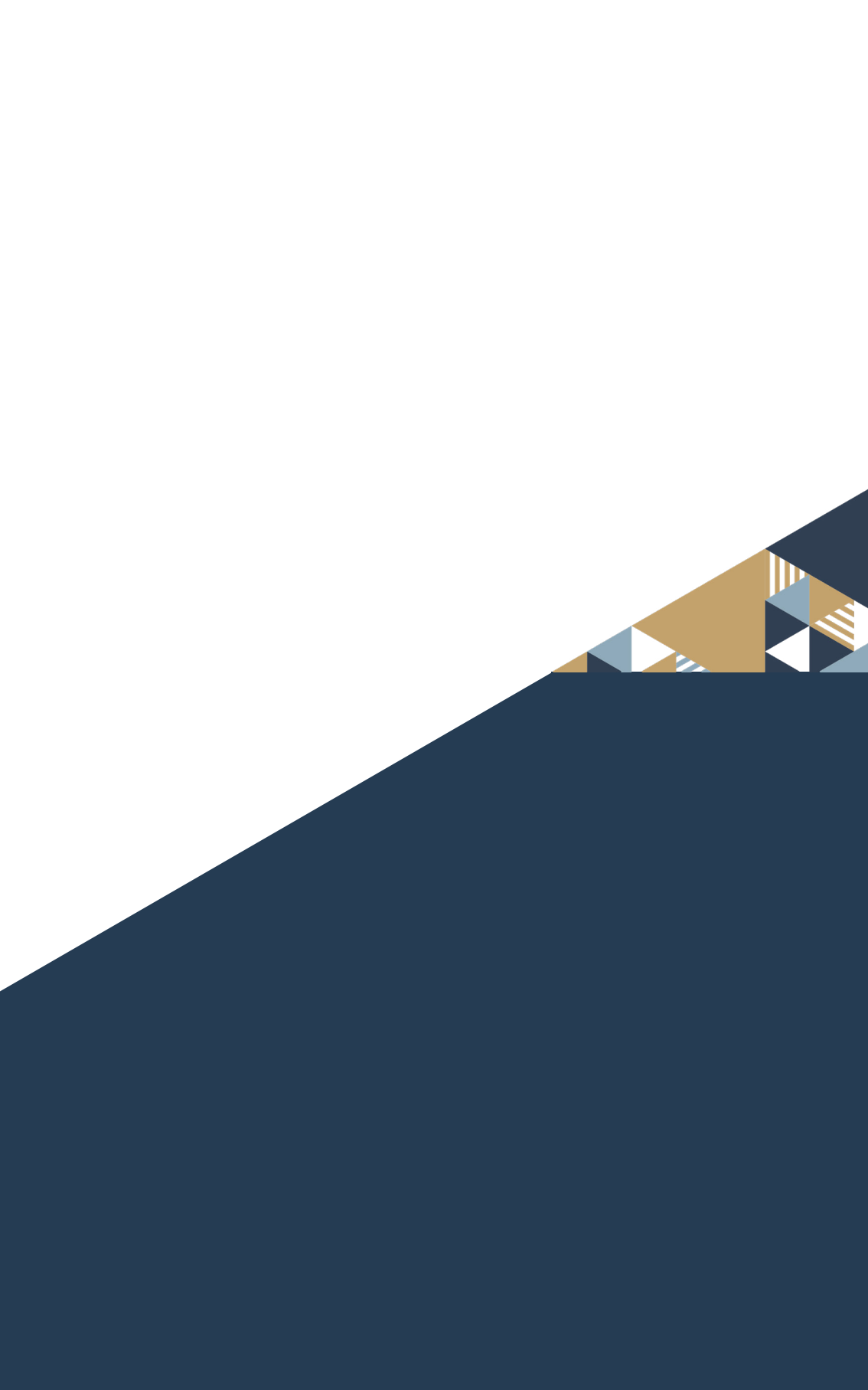
Hoy en día, las organizaciones de inteligencia trabajan en una amplia gama de temas, como los cambios tecnológicos, las cuestiones medioambientales, los grandes flujos de personas y los mercados económicos. El propósito de analizar temas tan diversos es el mismo: transmitir conocimientos fiables y oportunos a las autoridades gubernamentales. A partir de este conocimiento, dichas autoridades podrán tomar decisiones más informadas sobre la conducción de las políticas públicas, aprovechando las oportunidades y mitigando las amenazas para el cumplimiento de los intereses nacionales.

Ningún país que quiera ser relevante en la escena internacional puede prescindir de organizaciones de inteligencia fuertes y activas, orientadas a promover los objetivos fundamentales del Estado. La fuerza de cualquier institución está anclada en su legitimidad de acción, que, en los Estados democráticos de derecho, es conferida por el respeto al orden jurídico vigente en el país y a los mecanismos de control político, administrativo y social a los que toda institución debe estar sujeta.

El servicio de inteligencia brasileño se rige por preceptos éticos y por la impersonalidad de sus acciones. Sus profesionales son continuamente capacitados para realizar sus trabajos, análisis y operaciones, buscando siempre el bien común como fin último de su trabajo.

La actividad de inteligencia de un país democrático está al servicio de su pueblo. Opera a partir de las demandas generadas por los gobernantes elegidos por la población, instruida por lo que considera que son los intereses del Estado, y actúa bajo el control de sus representantes parlamentarios. Por lo tanto, es un reflejo de la sociedad en

la que opera, de las formas en que se ejerce el poder en esa sociedad y de las prioridades de sus dirigentes.





8

Glosario

8. Glosario

Este glosario define la interpretación que hace la ABIN de los términos clave de la actividad de inteligencia. Pretende, por tanto, facilitar la consulta y promover la consolidación de un vocabulario común y una comprensión compartida entre los profesionales de inteligencia, sin perjuicio de otras definiciones y conceptos que existan en ámbitos afines y contextos sociales e institucionales diferentes.

A

Abogado del diablo: técnica destinada a desafiar líneas de análisis, modelos mentales o consensos analíticos establecidos, consistente en designar a una persona o equipo para que desarrolle argumentos consistentes en contra de una determinada proposición o conclusión.

Acceso: posibilidad u oportunidad de obtener datos, información o conocimientos clasificados como consecuencia de la autorización oficial de una autoridad competente o de la superación de medidas de salvaguardia.

Acción adversa: acción intencional, patrocinada o no, que se opone a la consecución de intereses nacionales, busca el acceso a conocimientos, informaciones y datos sensibles, o amenaza la seguridad de la sociedad brasileña y del Estado.

Acción operativa: utilización sigilosa de técnicas operativas especializadas para alcanzar un objetivo previamente determinado en función de la demanda recibida del cliente.

Acción operativa basada en los recursos humanos: acción operativa que prioriza el uso especializado de los recursos humanos.

Acción operativa basada en recursos técnicos: acción operativa que prioriza el uso especializado de recursos técnicos.

Acción operativa de búsqueda: comprende la ejecución de acciones operativas destinadas a obtener datos, información o conocimientos no disponibles.

Acción operativa cibernética: acción operativa que ocurre en el espacio cibernético y que puede combinar el empleo de recursos humanos y técnicos especializados en una misma acción.

Acción operativa exploratoria: consiste en la realización de acciones operativas puntuales, que proporcionan resultados concretos, con un inicio y un final preestablecidos.

Acción operativa de producción de eventos: comprende la ejecución de acciones operativas destinadas a crear eventos.

Acción operativa de protección: comprende la ejecución de acciones operativas destinadas a proteger al agente y la operación.

Acción operativa sistemática: consiste en el desarrollo de acciones continuas, que dan lugar a un flujo constante de datos, información y conocimientos, con un inicio preestablecido y un final indeterminado.

Acciones especializadas: todas las acciones que utilizan técnicas específicas de las actividades de inteligencia, como: recolección estructurada de datos de libre acceso; aplicación de medidas de protección; utilización confidencial de técnicas operativas; tratamiento de datos, información y conocimientos mediante la Metodología de Producción de Conocimientos de Inteligencia.

Acreditación: autorización oficial, concedida por una autoridad competente, que faculta a una determinada persona para acceder a datos, a informaciones o a conocimientos en diferentes niveles de sigilo.

Adaptabilidad: principio del elemento operativo que preconiza que la planificación y la ejecución de las acciones operativas deben permitir la aplicación rápida y eficaz de los ajustes y reorientaciones que puedan resultar necesarios.

Adecuación: regla del elemento de operaciones que determina qué medios y técnicas elegidos conducirán al cumplimiento del objetivo de la acción encubierta.

Agente: persona encargada de actuar para alcanzar los objetivos de la acción operativa, que puede pertenecer a la agencia de

inteligencia (agente orgánico) o ser una persona empleada para llevar a cabo o facilitar la ejecución de una acción concreta, sin vínculos formales con la agencia (agente no orgánico).

Actuar: fase de los ciclos de las ramas de inteligencia y contrainteligencia en la que el Estado pone en práctica la decisión tomada en la fase de decidir.

Alerta: aviso emitido por la actividad de inteligencia con el fin de anticipar acontecimientos que podrían tener un impacto en la consecución de los objetivos constitucionales, el orden nacional o la seguridad de la sociedad y del Estado, que contiene los indicios que llevaron a emitir la alerta, así como una descripción de la amenaza prevista y la tendencia a que se produzca. (Véase también: alerta de inteligencia).

Amenaza: condición o factor desfavorable para la consecución de los intereses nacionales y la salvaguarda de conocimientos y datos sensibles.

Amplitud: principio del elemento de análisis que determina el alcance necesario de los objetos de análisis para la elucidación más completa posible del tema propuesto.

Análisis: operación mental que consiste en descomponer un todo en sus elementos constitutivos para comprender la función de cada elemento en el conjunto.

Análisis de hipótesis contrapuestas (AHC): técnica destinada a desarrollar y cuestionar hipótesis, adecuada para analizar situaciones complejas en las que existen múltiples factores y pruebas que pueden respaldar argumentos diferentes, explicaciones alternativas y conclusiones contradictorias.

Análisis de inteligencia: conjunto de acciones llevadas a cabo por el elemento de análisis de una organización de inteligencia, encargado de producir y difundir conocimientos para asesorar el proceso de toma de decisiones y la acción gubernamental. (Véase también: elemento de análisis y producción de conocimientos).

Análisis de redes: técnica de visualización utilizada principalmente para supervisar las actividades de los individuos, cartografiando

redes, interacciones y conexiones entre personas, grupos y otras entidades de interés.

Análisis visual: herramienta utilizada por los profesionales de inteligencia para organizar los insumos y generar presentaciones visuales sucintas y atractivas de los conocimientos de inteligencia para los usuarios en determinadas situaciones, como el seguimiento continuo de acontecimientos dinámicos, en los que los nuevos insumos obtenidos o generados alimentan una base de datos y cambian la situación todo el tiempo.

Analista: puesto ocupado por un profesional de inteligencia que lleva a cabo actividades de producción bajo la supervisión de un jefe de producción.

Analista de apoyo: puesto ocupado por un profesional de inteligencia responsable de apoyar los esfuerzos de análisis del analista responsable, colaborando en las tareas y recibiendo las acciones de análisis delegadas.

Analista responsable: puesto ocupado por un profesional de inteligencia encargado de la gestión de la producción y principal responsable del producto final.

Antagonismos: amenazas que se oponen intencionadamente a la consecución de los intereses nacionales.

Apoyo a la manipulación legal: la manipulación legal (*Lawfare*) es el uso de maniobras legales para tratar de impedir o dificultar la consecución de los intereses de un adversario que entran en conflicto con los del patrocinador.

Actividad de inteligencia: actividad permanente del Estado, ejercida mediante el empleo de técnicas y acciones especializadas dirigidas a la producción de conocimiento, que constituye un instrumento de asesoramiento a los sucesivos gobiernos, con vistas a la seguridad del Estado y al bienestar de la sociedad.

Actores adversos: Estados, organizaciones, grupos o personas con interés y capacidad para actuar en el contexto de cada una de las vertientes de la contrainteligencia.

Autenticidad: condición que permite identificar quién ha producido, enviado, modificado o destruido un determinado conocimiento, información o dato sensible.

B

Blanco: objeto sobre el que actúa la acción encubierta para cumplir su objetivo. Posee datos, información y conocimientos esenciales para la actividad de inteligencia o se utiliza para llevar a cabo acciones adversas.

Búsqueda: aplicación combinada de técnicas operativas para obtener datos, información y conocimientos no disponibles.

C

Canal: emisor a través del cual los datos, la información y el conocimiento llegan a la organización de inteligencia.

Casos operativos: despliegue planificado y coordinado de operaciones de inteligencia en torno a un tema específico con múltiples misiones y blancos.

Ciclo de análisis: proceso cíclico compuesto por una secuencia de pasos procedimentales interrelacionados cuyo objetivo es generar productos que respondan a una formulación de interés para el Estado o la sociedad, mediante la transformación de datos, informaciones y conocimientos en conocimientos de inteligencia. (Véase también: Metodología para la producción de conocimientos de inteligencia).

Ciclo de contrainteligencia: compuesto por seis fases caracterizadas por acciones: seguir, orientar, detectar, evaluar, decidir y actuar.

Ciclo de operaciones: ciclo compuesto por las fases de planificación, ejecución, difusión y cierre, con límites flexibles entre ellas.

Ciclo de la rama de Inteligencia: compuesto por cinco fases, caracterizadas por acciones: objetivar, seguir, informar, decidir y actuar.

Cliente operativo: responsable de desencadenar el elemento de operaciones, presentando la demanda que definirá el objetivo de las acciones operativas a emplear.

Compartimentación: restricción de acceso en función de la necesidad de conocer.

Comprometimiento: pérdida de seguridad resultante de un acceso no autorizado.

Comunidad de inteligencia: conjunto del que forman parte organismos de inteligencia que establecen relaciones de cooperación. (Véase también: Comunidad internacional de inteligencia, Sistema de inteligencia y Sistema Brasileño de Inteligencia).

Comunidad internacional de inteligencia: grupo formado por todos los servicios de inteligencia activos en el mundo. Se divide en subcomunidades. (Véase también: Comunidad de Inteligencia).

Conocimiento: representación registrada o no de un aspecto de la realidad con un significado contextualizado que se asume como verdadero y validado.

Conocimiento de inteligencia: representación registrada o no de un aspecto de la realidad, contextualizada y asumida como verdadera según los procedimientos metódicos de la actividad de inteligencia, útil para el proceso nacional de toma de decisiones.

Conocimiento de Inteligencia interpretativo: conocimiento resultante de juicios y razonamientos sobre hechos, acontecimientos, situaciones o fenómenos pasados o presentes, que permiten proyectar los objetos de análisis hacia el futuro inmediato, expresando tendencias o evoluciones, pero sin carácter prospectivo.

Conocimiento de inteligencia narrativo-descriptivo: conocimiento resultante de juicios sobre hechos, sucesos, situaciones o fenómenos pasados o presentes, que se limita a narrar o describir objetos de análisis, bien porque la demanda recibida orienta la producción, bien porque las evidencias reunidas no permiten elaborar razonamientos.

Conocimiento de inteligencia prospectivo: conocimiento resultante de juicios y razonamientos sobre la evolución futura de hechos, acontecimientos, situaciones o fenómenos, con un enfoque en el futuro lejano, que requiere el uso de técnicas auxiliares a la Metodología de Producción de Conocimiento (MPC) debido a su naturaleza.

Consulta a especialistas: recurso utilizado por los profesionales de inteligencia para tratar cuestiones específicas que, por su complejidad o particularidad, superan sus conocimientos o capacidad profesional.

Contrainsurgencia: rama de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones adversas de individuos y grupos insurgentes.

Contrainteligencia (CI): rama de la actividad de inteligencia que tiene por objeto prevenir, detectar, identificar, obstruir y neutralizar la inteligencia y las acciones adversas que supongan una amenaza para la salvaguarda de datos, conocimientos, personas, zonas e instalaciones de interés para la seguridad de la sociedad y del Estado.

Contraterrorismo: rama de la contrainteligencia activa que propugna la adopción de medidas y procedimientos destinados a detectar, identificar, evaluar, obstruir y neutralizar las acciones adversas de individuos y grupos extremistas violentos.

Control: principio general de la actividad de inteligencia que determina la supervisión sobre todas las acciones de la actividad de inteligencia, a fin de garantizar la conformidad de sus medios y la correcta finalidad de su aplicación.

Control externo específico: control y fiscalización de las actividades de inteligencia ejercido por el Poder Legislativo, a través de la Comisión Mixta de Control de las Actividades de Inteligencia (CCAI) del Congreso Nacional, de acuerdo a su propio reglamento.

Control interno específico: control y supervisión de las actividades de inteligencia por la Cámara de Relaciones Exteriores y Defensa Nacional (Creden) del Consejo de Gobierno, encargada de supervisar la aplicación de la Política Nacional de Inteligencia (PNI).

Control externo ordinario: control y fiscalización de los órganos de inteligencia, al que están sujetos todos los organismos públicos, ejercido por el Congreso Nacional, con el auxilio del Tribunal de Cuentas de la Unión (TCU). Consiste en el control contable, financiero, presupuestario, operativo y patrimonial, y exige la rendición permanente de cuentas.

Control interno ordinario: control y fiscalización de los órganos de inteligencia, al que están sujetos todos los organismos públicos, ejercido por la Contraloría General de la Unión (CGU). En el caso específico de la ABIN, ese control también es ejercido por la Secretaría de Control Interno de la Presidencia de la República (Ciset/PR), que realiza el control interno sobre la aplicación de los recursos presupuestarios de la Agencia. También forman parte de esa área de control el Sistema de Integridad Pública del Poder Ejecutivo Federal (Sipef) y la Comisión de Ética de la Presidencia y Vicepresidencia de la República (CEPR).

Cooperación: principio general de la actividad de inteligencia que establece la colaboración en todas las labores de inteligencia.

Credencial de seguridad: certificado que concede una autorización oficial, por parte de una autoridad competente, para que una determinada persona tenga acceso a datos, información y conocimientos de diversos grados de confidencialidad.

Cronologías y líneas del tiempo: técnicas de descomposición y visualización, especialmente indicadas para analizar temas que se siguen sistemáticamente a lo largo del tiempo.

Cultura de seguridad: proceso de educación que pretende crear, desarrollar y mantener una mentalidad de seguridad eficaz en los procedimientos que implican datos, información o conocimientos sensibles.

D

Dato: representación registrada o no de un aspecto de la realidad con un significado descontextualizado.

Dato denegado: elemento informativo que está bajo la protección de su detentor cuyo acceso por el organismo de inteligencia exige el empleo de técnicas operativas.

Datos, información y conocimientos de acceso abierto: información no protegida a la que pueden acceder libremente quienes deseen obtenerla.

Datos no disponibles: información a la que el organismo de inteligencia no puede acceder libremente.

Datos, información y conocimientos sensibles: información que, por ser esencial para la seguridad personal de los ciudadanos, la sociedad o el Estado, tiene difusión controlada y acceso restringido a personas acreditadas.

Debriefing: reunión de evaluación de las actividades de inteligencia, celebrada tras su finalización, en la que se debaten las mejores prácticas y los fallos observados, con vistas al aprendizaje de los profesionales implicados y a la mejora de la institución.

Decidir: fase de los ciclos de inteligencia y contrainteligencia en la que el usuario define el curso de acción a seguir a la luz de los conocimientos que se le han proporcionado.

Desclasificación: anulación, por la autoridad competente o por caducidad, de la clasificación, haciendo ostensibles datos, informaciones o conocimientos.

Desinformación: conjunto de acciones que difunden deliberadamente información falsa, con la intención de engañar o confundir a un público objetivo específico para causar daño, inducir a error o manipular una situación o acontecimiento a favor de los intereses del patrocinador.

Desradicalización: reversión del proceso de radicalización de grupos o individuos extremistas o insurgentes.

Detectar: 1) descubrir una acción adversa planificada o realizada, ya sea finalizada o en curso, y comprender sus características. 2) fase del ciclo de contrainteligencia en la que se detecta una posible acción adversa, ya sea finalizada o en curso.

Difusión y resultados: fase del MPC en la que se llevan a cabo los procedimientos de difusión de los conocimientos de inteligencia, así como la evaluación de los resultados para mejorar los ciclos de producción posteriores.

Disponibilidad: 1) la condición atribuida a los datos, la información o el conocimiento de que estén disponibles y puedan ser utilizados a petición de una persona, organización, sistema o entidad determinada. 2) el principio del elemento operativo, que establece que debe estructurarse de tal modo que permita su activación inmediata siempre que sea necesario, con el máximo alcance posible, teniendo en cuenta las amenazas enumeradas en los instrumentos que rigen la actividad de inteligencia.

Disimulación: manipulación intencionada de las características de un objeto determinado o de datos, informaciones, conocimientos, reales o no, con el fin de disimular la capacidad o la intención de la acción o de desorientar a un adversario.

Documento: unidad de registro de datos, información y conocimientos, cualquiera que sea el soporte o formato.

Doctrina: conjunto de conceptos, métodos, procesos, normas, principios y valores que orientan y disciplinan el ejercicio de la actividad de inteligencia, normalizando y regulando los procedimientos.

E

Elemento de análisis: sector constitutivo de la actividad de inteligencia responsable de la producción de conocimientos de inteligencia, cuyo trabajo profesional consiste en recoger y reunir los insumos, analizarlos, procesarlos y difundir el resultado a las autoridades competentes.

Elementos de operaciones: sector constitutivo de la actividad de inteligencia encargado de llevar a cabo acciones especializadas y secretas destinadas a obtener insumos no disponibles, contrarrestar acciones adversas y crear situaciones favorables a los intereses nacionales, con el fin de cumplir objetivos previamente establecidos.

Entorno operativo: espacio físico o virtual donde ocurre la acción operativa

Escenarios: conjunto de acontecimientos que configuran una imagen futura, junto con su evolución.

Espionaje: cualquier actividad dirigida a la obtención no autorizada de datos, información o conocimientos sensibles, confidenciales o clasificados en beneficio de Estados, grupos de países, organizaciones, facciones, grupos de interés, empresas o particulares.

Estado de certeza: estado mental en el que el individuo considera que su interpretación mental de la realidad se corresponde plenamente con el objeto real considerado, es decir, el individuo cree que ha alcanzado plenamente la verdad.

Estado de ignorancia: estado mental caracterizado por la ausencia total de cualquier imagen de la realidad.

Estado de posibilidad: estado mental en el que no hay pruebas suficientes que respalden ninguna imagen mental y existen razones tanto para aceptar como para negar las distintas posibilidades de representación de la realidad.

Estado de probabilidad: estado mental en el que el individuo considera que su interpretación de la realidad se corresponde con el objeto real, pero con alguna posibilidad de equivocarse.

Evaluación: fase del CPM en la que se evalúan las aportaciones reunidas en la fase de reunión, lo que da lugar a una calificación de credibilidad para cada aportación evaluada.

Evaluador: función desempeñada por un profesional de inteligencia responsable de aplicar los procedimientos de la fase de

evaluación a los insumos que aún no han sido evaluados por un profesional de inteligencia, así como de registrar los resultados de las evaluaciones.

Evaluar: 1) acción que consiste en analizar, integrar y contextualizar una amenaza y sus daños reales y potenciales para Brasil. 2) fase del ciclo de contrainteligencia en la que se considera el blanco de la acción adversa, su modo de realización, sus probables patrocinadores y las consecuencias de su posible realización para el país objetivo.

Eventos: acontecimientos situados en el tiempo y en el espacio, que pueden delimitarse geográfica y cronológicamente por hitos específicos. (CDI)

Extremismo violento: se refiere a la planificación, preparación, promoción, financiación y ejecución de actos violentos motivados por ideologías extremistas que desprecian preceptos constitucionales fundamentales.

F

Fenómenos: procesos que modifican situaciones. Un fenómeno está formado por la evolución de hechos, acontecimientos y situaciones, la dinámica entre ellos y la forma en que esta dinámica se refleja en la experiencia humana.

Filtración: divulgación no autorizada de datos, información y conocimientos sensibles.

Finalidad: principio del elemento de operaciones que propugna que la acción encubierta debe llevarse a cabo en apoyo de la realización de los intereses de la sociedad y del Estado, con el bien común como lema.

Fomento encubierto de grupos y organizaciones: acción que pretende, de forma velada, crear, estructurar, financiar, cooptar o mantener grupos u organizaciones que promuevan los intereses del patrocinador.

Fuente: origen de datos, informaciones o conocimientos.

Fuente humana: persona que es fuente de datos, informaciones o conocimientos. (Véase también: Canal; Fuente; e Inteligencia humana)

Fuentes abiertas: véase inteligencia de fuentes abiertas.

Formalización y validación: es la fase del MPC en la que, teniendo en cuenta los formatos de difusión propuestos en la planificación, se lleva a cabo el formateo final de los conocimientos de inteligencia y su validación analítica y técnica.

Fracción de inteligencia: organización dedicada a llevar a cabo actividades de inteligencia en organismos con otros fines. (Véase también: organismo/organización de inteligencia y servicio de inteligencia).

Función de ejecución de la actividad de inteligencia: la función de ejecutar las decisiones previamente adoptadas en el marco de la política exterior del Estado. En el contexto de la contrainteligencia, busca obstruir y neutralizar las acciones llevadas a cabo por la inteligencia adversa.

Función informativa de la actividad de inteligencia: la función de informar al Estado sobre asuntos de su interés.

G

Geoint: acrónimo en inglés de *Geospatial Intelligence*. Véase: inteligencia geoespacial.

Gerente de producción: puesto ocupado por un profesional de la inteligencia responsable de supervisar al equipo, prestar apoyo, aprobar acciones y controlar plazos y entregas.

Grado de sigilo: gradación atribuida a los datos, informaciones, conocimientos, materiales, sistemas, áreas e instalaciones considerados confidenciales por su naturaleza o contenido.

H

Hechos: sucesos verificables, susceptibles de descripción o predicción, que cualquiera puede valorar utilizando referencias o metodologías adecuadas.

Humint: acrónimo en inglés de *Human Intelligence*. Véase: Inteligencia humana.

I

Idea: generalización de un objeto determinado que refleja únicamente sus aspectos esenciales.

Identificar: atribuir a un agente (persona o entidad) la autoría o coautoría de la acción adversa, incluso como mentor o patrocinador intelectual.

Imint: acrónimo en inglés de *Imagery Intelligence*. Véase: Inteligencia de imágenes.

Imparcialidad: principio del elemento de análisis que determina una aproximación imparcial a los objetos de análisis, para evitar que juicios de valor derivados de intereses, convicciones personales o ideas preconcebidas distorsionen los resultados de la producción.

Indispensabilidad: regla que deben observar la planificación y la ejecución operativas en relación con los medios y técnicas operativas elegidos como alternativas necesarias para el cumplimiento del objetivo de la acción encubierta.

Indicadores: técnica diseñada para alertar sobre acontecimientos futuros, identificar tendencias emergentes o cambios no deseados en los escenarios bajo vigilancia, entre otras cosas.

Inferencia bayesiana: método basado en la fórmula de Bayes, utilizado en el campo de la estadística para apoyar la toma de decisiones basadas en datos ante la incertidumbre, cuyo objetivo

es estimar la probabilidad de que ocurra un suceso a partir de un suceso inicial

Información: representación registrada o no de un aspecto de la realidad con significado contextualizado según un tratamiento metódico, racional y objetivo.

Informar: fase del ciclo de la rama de inteligencia que tiene lugar siempre que el equipo responsable de la vigilancia de un área determinada se da cuenta de que se ha producido un hecho, suceso o situación que debe ser comunicado a las autoridades competentes, bien porque ayuda al diagnóstico de la situación, bien porque requiere que el Estado tome posición.

Infraestructuras críticas: instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción total o parcial tendría un grave impacto social, medioambiental, económico, político, internacional o de seguridad para el Estado y la sociedad.

Insurgencia: rebelión contra un poder establecido llevada a cabo o planeada por un grupo formado o apoyado por una parte de la población.

Integración: 1) en contrainteligencia, incluye las medidas que tienen en cuenta el contexto del objeto de interés adverso, tratando de abarcar no sólo a la institución, grupo o persona que puede verse afectada negativamente, sino también a quienes facilitan el acceso al objeto y pueden favorecer al agente. 2) principio del elemento operativo, que propugna que sus acciones sean integradas, de forma ordenada, sistemática y continua.

Integración e interpretación: fase del MPC en la que se aclara el tema, es decir, se da respuesta a la pregunta definida en la planificación. Para ello, se analizan, integran e interpretan las fracciones en estado de certeza o probabilidad, generando una elaboración textual coherente que permita aclarar el tema.

Integridad: condición atribuida a los datos, la información o el conocimiento de que no han sido alterados o destruidos de forma no autorizada.

Inteligencia actual: clasificación temporal de la producción de inteligencia destinada a mantener continuamente informados a los responsables de la toma de decisiones sobre los acontecimientos y situaciones en curso y su evolución.

Inteligencia adversa: actividad llevada a cabo por un agente estatal o no estatal, utilizando acciones especializadas, para promover los intereses de su patrocinador, mediante el acceso indebido o no autorizado a datos, conocimientos, personas, zonas o instalaciones, o utilizando técnicas destinadas a modificar las percepciones y el comportamiento del Estado y de la sociedad en detrimento de los intereses nacionales.

Inteligencia de alerta: clasificación temporal de la producción de inteligencia destinada a anticipar acontecimientos que puedan tener un impacto en el cumplimiento de los objetivos constitucionales, el orden nacional o la seguridad de la sociedad y del Estado.

Inteligencia de base: clasificación por finalidad de la producción de inteligencia destinada a construir un conjunto de bases y referencias para comprender y contextualizar los temas tratados, como subsidio de otros análisis con un enfoque más definido.

Inteligencia cibernética: área de inteligencia centrada en cuestiones relacionadas con el ciberespacio, cuya producción busca apoyar las acciones de Brasil frente a las vulnerabilidades y amenazas cibernéticas, informando las políticas públicas y los planes estatales en esta área, así como monitoreando y evaluando las capacidades, intenciones y actividades de actores externos en el ciberespacio.

Inteligencia de Estado: actividad realizada por organizaciones de inteligencia que forman parte de la estructura del Estado brasileño.

Inteligencia de fuente abierta: clasificación, según el origen de los datos, de la inteligencia realizada a partir de datos, información y conocimientos disponibles, es decir, de libre acceso. (Véase también: Osint).

Inteligencia de imágenes: clasificación según el origen de los datos de inteligencia basada en datos e información obtenidos a partir de la producción de imágenes fotográficas y multiespectrales. (Véase también: Imint)

Inteligencia de medición: clasificación según el origen de los datos de inteligencia basada en datos e información obtenidos mediante la medición de determinados tipos de emanaciones, como sísmicas y térmicas, generalmente resultantes de firmas de eventos, como explosiones atómicas. (Véase también: Masint)

Inteligencia de medios sociales: clasificación según el origen de los datos de inteligencia realizada a partir de los datos y la información obtenidos de los medios sociales y los metadatos asociados a ellos, lo que permite realizar análisis de sentimientos, patrones de publicación y evaluación de la relevancia de los temas de masas. (Véase también: Socmint)

Inteligencia de seguridad: actividad de inteligencia destinada a detectar y evaluar actores dentro del Estado que podrían poner en peligro la consecución de sus objetivos y amenazar el bienestar de la sociedad.

Inteligencia de señales: clasificación según el origen de los datos de inteligencia basada en datos e información obtenidos mediante la interpretación y decodificación de comunicaciones y señales electromagnéticas. (Véase también: Sigint).

Inteligencia diplomática: actividad de inteligencia destinada a anticipar las posiciones que adoptarán otros países y que podrían repercutir en la consecución de los intereses nacionales.

Inteligencia estratégica: clasificación por finalidad de la producción de inteligencia destinada a analizar e interpretar fenómenos con potencial para incidir en los objetivos e intereses fundamentales del Estado.

Inteligencia explicativa: clasificación temporal de la producción de inteligencia destinada a asesorar continuamente al proceso nacional de toma de decisiones sobre hechos, acontecimientos, situaciones y fenómenos que puedan representar amenazas u

oportunidades para la consecución de los objetivos fundamentales del Estado.

Inteligencia exterior: área de inteligencia centrada en asuntos en los que el Estado tiene poco o ningún poder de decisión o intervención unilateral y que requieren estrategias de posicionamiento internacional para negociar y lograr los intereses nacionales.

Inteligencia geoespacial: clasificación según el origen de los datos de inteligencia basados en imágenes y datos de geolocalización obtenidos para describir, evaluar y representar visualmente características físicas o actividades referenciadas geográficamente. (Véase también: Geoint)

Inteligencia humana: clasificación según el origen de los datos de inteligencia basada en datos, información y percepciones procedentes de informes elaborados por individuos o aportados por ellos mismos. (Véase también: Humint)

Inteligencia interna: área de actividad de inteligencia centrada en cuestiones que son competencia exclusiva de la intervención del Estado, respetando la situación política y jurídica del país.

Inteligencia Militar: actividad de inteligencia cuyo escopo es evaluar potenciales adversarios bélicos por medio de la obtención de datos, informaciones y conocimientos sobre la disposición espacial del enemigo, su movimentación, el ánimo de sus tropas, el campo de batalla y las condiciones climáticas del conflicto.

Inteligencia operativa: clasificación por finalidad de la producción de inteligencia destinada a contextualizar una acción concreta del Estado, en apoyo a la ejecución de acciones ya definidas en el ámbito de una determinada política pública.

Inteligencia prospectiva: clasificación por marco temporal de la producción de inteligencia destinada a proporcionar escenarios sobre el futuro para ayudar a dirigir la acción gubernamental.

Inteligencia táctica: clasificación según la finalidad de la producción de inteligencia destinada a recopilar datos, información y conocimientos para apoyar el desarrollo de políticas gubernamentales previamente definidas.

Inteligencia técnica: clasificación según el origen de los datos de inteligencia realizada a partir de datos e información obtenidos por medios técnicos. (Véase también: Techint)

Inteligencia transnacional: área de actividad de inteligencia centrada en cuestiones transfronterizas, parcialmente dentro de la capacidad de intervención del Estado, pero que requieren negociaciones y asociaciones internacionales para adoptar políticas eficaces que permitan alcanzar los objetivos del Estado.

Intereses nacionales: deseos y aspiraciones de la sociedad que contribuyen al progreso de Brasil y a la consecución del bienestar, la seguridad y la defensa de todos los ciudadanos, preservándolos para el disfrute de las generaciones futuras.

Interferencia externa: acción deliberada de gobiernos, grupos de interés, individuos o empresas que pueden influir en la dirección política del país con el fin de favorecer intereses extranjeros en detrimento de los nacionales.

Intrusión: introducción de agentes en un entorno adverso, en un soporte físico o digital, con el fin de detectar acciones, identificar agentes adversos e influir en su comportamiento.

Investigación social: proceso de investigación de los antecedentes de cada candidato, elaborado desde el punto de vista de la contrainteligencia, con el objetivo de dificultar la infiltración y evitar la contratación de personal con potencial para comprometer conocimientos y datos confidenciales.

J

Juicio: Relación entre ideas, que compone una proposición o afirmación sobre un objeto.

L

Lluvia de ideas (*brainstorming*): técnica creada para uso en grupos con finalidad de generar nuevas ideas y estimular el pensamiento creativo según reglas y pasos específicos.

M

Masint: acrónimo de *Measurement Intelligence*. Véase: Inteligencia de medición.

Material: sustancia, modelo, prototipo, molde, máquina, equipo o similar que representa datos, información y conocimientos.

Matriz de impactos cruzados: técnica de generación de ideas, adecuada para las primeras fases de un proyecto de análisis, cuando el analista o el equipo de análisis aún están intentando comprender una situación compleja.

Medios técnicos: recursos materiales y tecnológicos utilizados en una operación de inteligencia, dentro de los límites de las posibilidades legales de la agencia.

Metadatos: elemento contextualizador vinculado a un registro, ya sean datos, información, conocimiento o inteligencia.

Método Delphi: método que permite la comunicación colectiva y, eventualmente, la construcción gradual de consensos entre expertos separados geográficamente, y que consiste en la elaboración de un conjunto de cuestionarios que se responden secuencial e individualmente por los participantes.

Metodología para la Producción de Conocimientos de Inteligencia (MPC): metodología que abarca todo el ciclo de análisis, compuesto por seis fases: planificación; recopilación; evaluación; integración e interpretación; formalización y validación; difusión y resultados. (Véase también: Ciclo de análisis).

N

Necesidad de conocer: 1) la disponibilidad de fracciones significativas extraídas de datos, informaciones y conocimientos, en la medida necesaria para que los profesionales de inteligencia puedan llevar a cabo sus actividades con la debida precisión y exhaustividad. 2) condición inherente al ejercicio efectivo de un cargo, función, empleo o actividad, indispensable para que el titular de una credencial de seguridad tenga acceso a datos, informaciones o conocimientos confidenciales.

Neutralización: reducción de los efectos de la acción adversa, tratando de revertir o mitigar sus resultados. Para ello se pueden utilizar acciones especializadas como la contrapropaganda, la desinformación, el comprometimiento del agente adverso y las filtraciones controladas de información a los medios de comunicación.

Neutralizar: anular o mitigar los efectos de una acción adversa realizada o en curso.

O

Óbices: amenazas que se interponen en el curso de los intereses nacionales, pero que no pretenden causar daño.

Objetivar: fase del ciclo de la rama de inteligencia en la que se determinan los temas, apartados y enfoques de las áreas sobre las que se va a trabajar.

Objetivos nacionales: identificación de las necesidades, intereses y aspiraciones que la nación pretende satisfacer.

Objetos de interés adverso: personas, datos, información, conocimientos, zonas, instalaciones, bienes, servicios, materiales o equipos, sistemas de información y comunicaciones que son objeto de agentes adversos.

Obstrucción: obstaculización de la realización de la acción adversa, iniciada en la fase de orientación, cuando se aplican las medidas

preventivas de protección de contrainteligencia, así como otras necesarias para la situación objeto de seguimiento.

Obstruir: impedir el inicio de una acción adversa cuya planificación se ha detectado o interrumpir su desarrollo una vez iniciada.

Operación: estructura funcional básica del elemento de operaciones responsable de gestionar y ejecutar las propias acciones especializadas.

Operaciones de inteligencia: conjunto de acciones operativas destinadas a obtener datos, información y conocimientos no disponibles, así como a aplicar medidas para contrarrestar acciones adversas, como forma de sortear obstáculos y alcanzar objetivos en un contexto de adversidad.

Oportunidad: principio general de la actividad de inteligencia que determina que el trabajo realizado por los profesionales de la inteligencia debe presentarse en un plazo adecuado para que pueda utilizarse eficazmente.

Oportunidades: condiciones o factores favorables a la consecución de los intereses nacionales.

Orientar: fase del ciclo de contrainteligencia en la que se dan instrucciones a los responsables de potenciales blancos de interés adverso, tratando de concienciarlos de la necesidad de protección para evitar o minimizar daños al Estado y a la sociedad brasileña.

Órgano/Organismo de Inteligencia: estructura continua de trabajo responsable del ejercicio profesional de la actividad de inteligencia. (Véase también: Servicio de Inteligencia y Fracción de Inteligencia)

Osint: acrónimo en inglés de *Open Source Intelligence*. Véase: Inteligencia de fuentes abiertas.

P

Pensamiento crítico: capacidad de analizar el objeto de forma clara y racional, utilizando planteamientos razonados para interpretarlo de forma imparcial, reflexiva y ética, a partir de la construcción de argumentos basados en datos, información y conocimientos fiables y en pruebas objetivas.

Planificación: fase de los MPC en la que se planifica el trabajo a realizar, a partir de una demanda de producción de conocimientos.

Plan de Inteligencia: documento que orienta las acciones dirigidas al cumplimiento de la Política Nacional de Inteligencia y sirve de parámetro para que las organizaciones que realizan actividades de inteligencia elaboren sus planes específicos.

Política Nacional de Inteligencia (PNI): documento de más alto nivel que orienta la actividad de inteligencia en el país, concebido a la luz de los valores y principios fundamentales consagrados en la Constitución Federal, de las obligaciones derivadas de los tratados, acuerdos y demás instrumentos internacionales de los que Brasil es parte, de las condiciones de inserción internacional del país y de su organización social, política y económica.

Preparador de insumos: función desempeñada por un profesional de la inteligencia que se encarga del tratamiento inicial de los insumos recopilados, si es necesario, así como de su limpieza, corrección, comprobación de lagunas e imprecisiones, resumen, corrección de formatos, traducción y organización para facilitar su evaluación y análisis.

Prevenir: anticiparse a las amenazas en abstracto, con el fin de evitar que se materialicen o mitigar sus efectos.

Proceso nacional de toma de decisiones: conjunto de actos realizados en el seno del poder ejecutivo que culminan en la elección de los objetivos gubernamentales, la formulación de políticas y la definición de estrategias para alcanzarlos o mantenerlos.

Producción de conocimiento: proceso intelectual en el que la capacidad humana, ayudada por su propia metodología, permite producir conocimiento especializado y estructurado a partir de datos, debidamente valorados y analizados, para satisfacer las demandas del proceso de toma de decisiones en cualquiera de sus niveles.

Producción de eventos: acciones llevadas a cabo de forma secreta destinadas a producir eventos para cumplir los objetivos de la actividad de inteligencia.

Propaganda adversa: conjunto de acciones llevadas a cabo mediante técnicas y métodos de comunicación social para persuadir de algún modo a los destinatarios e influir en su actitud, opinión, emoción y comportamiento.

Proporcionalidad: norma del elemento operativo que determina que los medios y técnicas elegidos se llevarán a cabo en la medida estrictamente necesaria para cumplir el objetivo de la acción encubierta.

Protección: utilización de medidas complementarias para proteger la integridad y la identidad de los agentes empleados, el sigilo y los objetivos de la acción operativa y la propia agencia de inteligencia.

R

Razonamiento: elaboración mental a partir de la cual los juicios previos permiten generar lógicamente un nuevo juicio.

Rama de contrainteligencia: rama de la actividad de inteligencia que lleva a cabo acciones especializadas destinadas a prevenir, detectar, identificar, evaluar, obstruir y neutralizar actividades adversas de inteligencia, incluyendo acciones que constituyan una amenaza para los intereses de la sociedad y del Estado, para el proceso de toma de decisiones, para la salvaguarda de conocimientos, informaciones y datos sensibles, los medios que

los poseen o transitan por ellos, sus poseedores y sus áreas e instalaciones.

Rama de inteligencia: rama de la actividad de inteligencia que tiene por objeto producir y difundir conocimientos a las autoridades competentes, relativos a hechos, acontecimientos, situaciones o fenómenos ocurridos dentro o fuera del territorio nacional, de influencia inmediata o potencial en el proceso de toma de decisiones y en la acción gubernamental, que constituyan o indiquen oportunidades o amenazas para los objetivos fundamentales del Estado.

Reclasificación: modificación del grado de sigilo asignado.

Reclutamiento: acción destinada a convencer a una persona para que trabaje, consciente o inconscientemente, en beneficio de una organización de inteligencia.

Reclutamiento de agentes de influencia: acción dirigida a seducir y controlar a entidades extranjeras para que utilicen a personas como instrumentos para enviar mensajes e interferir en la política, el mercado y la sociedad de forma que favorezcan los intereses del patrocinador. Funcionarios gubernamentales, políticos, académicos y personas influyentes, entre otros, pueden ser reclutados de esta forma.

Recolección: acción especializada destinada a obtener datos e información de libre acceso.

Recolector: función desempeñada por un profesional de la inteligencia responsable de recoger y registrar los insumos y sus metadatos.

Recursos financieros: capital disponible para llevar a cabo una acción secreta.

Recursos operativos: aplicación combinada de las capacidades humanas, técnicas, financieras y logísticas de que dispone el elemento de operaciones.

Reflexión crítica: principio del elemento de análisis que propugna que el analista mantenga un alto nivel de criticidad sobre su propia comprensión de la realidad.

Resiliencia: principio del elemento operativo que establece que debe ser resistente a las dificultades y frustraciones para poder percibir, evaluar y reaccionar rápidamente ante situaciones adversas y controlar sus acciones para no poner en peligro las acciones operativas que se están llevando a cabo.

Reunión: fase del MPC en la que se llevan a cabo acciones para obtener y preparar insumos con el fin de responder a los aspectos esenciales que deben conocerse, es decir, las preguntas enumeradas en la planificación que tienen por objeto dilucidar el problema formulado a partir del tema.

Revisor: función desempeñada por un profesional de la inteligencia responsable de garantizar la detección de los problemas más simples y superficiales antes de enviar el producto al validador, incluidas cuestiones como la adecuación al usuario, la corrección gramatical, la adecuación a los principios del lenguaje de la inteligencia y los problemas de argumentación y lógica.

S

Sabotaje: acción dirigida a destruir, dañar, comprometer o inutilizar, total o parcialmente, datos, información, conocimientos, materiales, equipos, instalaciones, sistemas logísticos, cadenas de producción e infraestructuras críticas del país, y afectar así a la capacidad de satisfacer las necesidades esenciales de la población y los intereses del Estado.

Seguir: fase de los ciclos de inteligencia y contrainteligencia que se refiere al proceso constante de planificación, reunión y procesamiento de datos, información y conocimientos sobre los temas tratados.

Seguridad: principio general de la actividad de inteligencia que exige la adopción de medidas de salvaguardia adecuadas a cada

situación, con el fin de garantizar la debida protección de los conocimientos producidos y de las acciones emprendidas.

Seguridad institucional: actividad encargada de aplicar medidas de seguridad, medidas de prevención y, en su caso, contramedidas.

Servicios de inteligencia: organizaciones cuyo único objetivo es llevar a cabo actividades de inteligencia. (Véase también: órgano/organización de inteligencia y fracción de inteligencia)

Sigilo: condición atribuida a los datos, informaciones o conocimientos para que sólo sean revelados a la persona, organización, sistema o entidad autorizada y acreditada para ello.

Sigilo de las fuentes: confidencialidad de las fuentes de datos, informaciones y conocimientos utilizados para elaborar el producto de inteligencia.

Sigint: acrónimo en inglés de *Signals Intelligence*. Véase Inteligencia de señales.

Simplicidad: principio general de la actividad de inteligencia que establece las acciones planificadas y llevadas a cabo por la actividad de inteligencia con el fin de evitar la complejidad, los costes innecesarios y los riesgos.

Síntesis: operación mental en la que se concibe la composición o recomposición de un todo a partir de elementos constitutivos ya analizados, proporcionando así un conjunto coherente y comprensible.

Sistema Brasileño de Inteligencia (Sisbin): sistema establecido por la Ley 9.883/1999, compuesto por órganos y entidades en los términos del Decreto 11.693/2023, que directa o indirectamente pueden producir conocimientos de interés para la actividad de inteligencia. (Véase también: Comunidad de inteligencia y Sistema de inteligencia)

Sistema de inteligencia: conjunto de organizaciones de inteligencia de un Estado sujetas, total o parcialmente, a una normativa que regula su interacción. (Véase también: Comunidad de Inteligencia y Sistema de Inteligencia de Brasil).

Situaciones: sucesos contextualizados de la experiencia humana, constitutivos de la realidad de los acontecimientos, que designan el contexto en el que deben evaluarse uno o varios acontecimientos en curso.

Socmint: acrónimo en inglés de *Social Media Intelligence*. Véase: Inteligencia de las redes sociales.

Sombrero rojo: técnica diseñada para ayudar a comprender cómo tienden a actuar o comportarse otros actores o agentes adversos en determinadas situaciones.

T

Techint: acrónimo en inglés de *Technical Intelligence*. Véase Inteligencia técnica.

Técnica de Evaluación de Datos, Información y Conocimientos (TAD): técnica destinada a atribuir un grado de credibilidad a los insumos para la producción de conocimientos de inteligencia mediante la evaluación de todo tipo de insumos por parte de un profesional de inteligencia, ya sean datos, información u otros conocimientos.

Técnicas accesorias: técnicas utilizadas para complementar la producción de conocimientos de inteligencia, respetando los procedimientos recomendados por el MPC.

Técnicas analíticas estructuradas (TAE): técnicas adicionales a los métodos tradicionales de producción de inteligencia, que proporcionan medios sistemáticos para exteriorizar los procesos mentales individuales.

Técnicas operativas: procedimientos y métodos especializados para utilizar personal y material en acciones encubiertas.

Terrorismo: consiste en que uno o más individuos cometan los actos enunciados en el § 2º del artículo 2º de la Ley N° 13.260/2016, por motivos de xenofobia, discriminación o prejuicio de raza, color, etnia y religión, cuando se cometan con el propósito de

provocar terror social o generalizado, exponiendo al peligro a las personas, los bienes, la paz pública o la seguridad pública.

Trazabilidad: principio general de la actividad de inteligencia que estipula el registro de las acciones llevadas a cabo en la actividad de inteligencia con el fin de garantizar que puedan ser auditadas.

U

Usuario: autoridad u organización gubernamental que recibe los conocimientos producidos.

Utilidad: principio general de la actividad de inteligencia que prevé la orientación de los resultados de las acciones de inteligencia en función de las necesidades de quienes la utilizarán, proporcionando así un producto potencialmente útil.

V

Validador: función desempeñada por un profesional de inteligencia responsable de evaluar y validar técnicamente la calidad analítica de los conocimientos de inteligencia.



9

**Fuentes
y Lecturas
Adicionales**

9. Fuentes y Lecturas Adicionales

Libros y artículos

AGRELL, Wilhelm; TREVERTON, Gregory F. **National Intelligence and Science: Beyond the Great Divide in Analysis and Policy**. New York: Oxford University Press, 2015.

AGRELL, Wilhelm; TREVERTON, Gregory. **National Intelligence Systems: current research and future prospects**. Cambridge University Press, 2009.

ANDREW, Christopher; ALDRICH, Richard J.; WARK, Wesley K. (eds) **Secret intelligence: a reader**. Routledge, 2019.

CEPIK, Marco (org.). **Inteligência Governamental: contextos nacionais e desafios contemporâneos**. Impetus, 2011.

CEPIK, Marco. **Espionagem e democracia: agilidade e transparência como dilemas na institucionalização dos serviços de inteligência**. Editora Parabellum, 2023.

COULTHART, Stephen. *An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques*. In: **International Journal of Intelligence and CounterIntelligence**, v.30, n.2, 2017, pp. 368-391.

GEORGE, Roger Z.; BRUCE, James B. (ed.) **Analyzing Intelligence: Origins, Obstacles, and Innovations**. Georgetown University Press, 2008.

GILL, Peter; MARRIN, Stephen; PHYTHIAN, Mark (eds.). **Intelligence Theory: key questions and debates**. Routledge, 2008.

GONÇALVES, Joannisval. **Políticos e espiões**. Impetus, 2018.

HERMAN, Michael. **Intelligence power in peace and war**. Royal Institute of International Affairs/Cambridge University Press, 1996.

JOHNSON, Loch (ed.). **Strategic Intelligence (5 volumes)**. Praeger, 2007.

- LANDON-MURRAY, Michael. *Putting a Little More “Time” into Strategic Intelligence Analysis*. In: **International Journal of Intelligence and CounterIntelligence**, v. 30, n. 4, 2017, pp. 785-809.
- MCDOWELL, Don. **Strategic Intelligence: a handbook for practitioners, managers, and users**. Scarecrow Press, 2009.
- MCGLYNN, Patrick; GARNER, Godfrey. **Intelligence Analysis Fundamentals**. Boca Raton: CRC Press, 2019. 334 p.
- PERSON, Randolph; HEUER Jr., Richards. **Structured Analytic Techniques for Intelligence Analysis**. CQ Press, 2021.
- PHYTHIAN, Mark. *Intelligence analysis and social science methods: exploring the potential for and possible limits of mutual learning*. In: **Intelligence and National Security**, v. 32, n. 5, 2017, pp 600-612.
- REVISTA BRASILEIRA DE INTELIGÊNCIA. n° 17 (dez. 2022). Brasília, DF: Agência Brasileira de Inteligência. 162p.
- SHULSKY, Abram e SCHMITT, Gary. **Silent warfare: understanding the world of Intelligence**. Potomac books, 2002.
- SIMS, Jennifer E. **Decision Advantage: intelligence in international politics from the Spanish armada to cyberwar**. Oxford University Press, 2022.

Legislación

- BRASIL. Decreto de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência. **Diário Oficial da União**, n. 241, Brasília, DF: 18 dez. 2017. Seção 1, pp. 36-40.
- BRASIL. Decreto nº 10.777, de 24 de agosto de 2021. Institui a Política Nacional de Inteligência de Segurança Pública. **Diário Oficial da União**, n. 161, Brasília, DF: 25 ago. 2021. Seção 1, p.2.
- BRASIL. Decreto nº 10.778, de 24 de agosto de 2021 Aprova a Estratégia Nacional de Inteligência de Segurança Pública. Disponível em: **http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/d**. Acesso em: 20 abr. 2022

BRASIL. Decreto nº 11.693, de 6 de setembro de 2023. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. **Diário Oficial da União**, n. 171-A, Brasília, DF: 25 ago. 2021. Seção 1 – Extra A, p.1.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. **Diário Oficial da União**, n. 124, Brasília, DF: 30 jun. 2016. Seção 1, p.5.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Disponível em: **http://www.planalto.gov.br/ccivil_03/leis/19883.htm**. Acesso em: 16 nov. 2023.

BRASIL. Portaria GAB/DG/ABIN/CC/PR Nº 925, de 6 de setembro de 2023. Fixa os critérios e procedimentos de ingresso de órgãos e entidades no Sistema Brasileiro de Inteligência como órgãos dedicados, associados e federados, e dá outras providências. **Diário Oficial da União**, n. 175, Brasília, DF: 13 set. 2023. Seção 1, p.4.

BRASIL. Portaria GAB/DG/ABIN/CC/PR Nº 926, de 6 de setembro de 2023. Estabelece o rol de órgãos e de entidades que integram o Sistema Brasileiro de Inteligência - Sisbin como órgãos dedicados e associados, e dá outras providências. **Diário Oficial da União**, n. 175, Brasília, DF: 13 set. 2023. Seção 1, p.5.

Doctrinas y Manuales

BRASIL. Presidência da República. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública – DNISP. – 4. ed. rev. e atual.** – Brasília: Secretaria Nacional de Segurança Pública, 2014.

BRASIL. Exército. Comando de Operações Terrestres. **Manual de Campanha – Contrainteligência** EB70-MC-10.220. Brasília, DF: Estado Maior do Exército, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Manual Técnico – Produção do Conhecimento de Inteligência** EB70-MT-10.401. Brasília, DF: Centro de Doutrina do Exército, 2019.



CASA CIVIL





CASA CIVIL

